Банки сучасного та майбутнього

Banks of the present and the future

DOI: 10.26565/2786-4995-2025-1-01
UDC 336.71:[351.746:007]

Azarenkov Serhii
Ph.D. Student of the Department of Banking
Odesa National Economics University, Odesa, Ukraine
e-mail: serdgzhio@gmail.com
ORCID ID: 0000-0002-1159-8699

Cybersecurity and Security of the Banking Business Under Martial Law

Abstract. The relevance of the research topic lies in the need to find solutions for the cybersecurity of the banking business, thereby enhancing the overall security of banking operations. The purpose of this study is to establish the importance of cybersecurity in ensuring the security of the banking business and the development of banks in the modern digital space. To achieve this goal, a structural-logical and systemic approach was used to construct a model for ensuring banking cybersecurity. Additionally, systematization and grouping methods were applied to characterize cyberattacks and their consequences, as well as to systematize regulatory and legal acts on banking security and cybersecurity. The object of the study is the process of ensuring banking cybersecurity and its integration into the overall banking security system. The main focus of the study is to identify emerging threats to banking security and cybersecurity, as well as to determine the challenges banks face when forming cybersecurity systems, including the use of artificial intelligence, security issues related to cloud technologies, digitalization of banking business processes, and third-party security risk management. The obtained results can be used to improve the cybersecurity system of the banking business and its integration into the general system of corporate banking governance. The study's conclusions emphasize the necessity of incorporating international cybersecurity standards into national regulatory frameworks. Moreover, the findings can contribute to the development of a tailored approach to building a cybersecurity model for banks, which should include principles, implementation measures, quality assessment approaches, and a cooperative cybersecurity strategy.

Keywords: *banking business, security, cybersecurity, cyber defense, cyberattacks, threats.*
Formulas: 0; fig.: 2, tabl.: 4, bibl.: 19;

For citation: Azarenkov S. Cybersecurity and Security of the Banking Business Under Martial Law. Financial and Credit Systems: Prospects for Development. №1(16) 2024. P. 9-19. DOI: https://doi.org/10.26565/2786-4995-2025-1-01

Introduction. The security of banking business in modern realities reflects a key role in protecting the interests of consumers of banking services, investors and creditors. The prolonged period of martial law in Ukraine is bringing new adjustments to the activities of banks, which are increasingly using innovative digital technologies. On the one hand, this is a positive development for banking business, but on the other hand, new security threats are emerging. These threats are particularly evident in systematic cyberattacks that lead to the loss of accumulated information, growing losses from the inability to conduct banking activities, and the emergence of new fraud schemes. In this context, we should also consider the use of artificial intelligence (AI), which opens up meta-opportunities for the banking business, namely, big data analysis, market research, economic forecasting, payments, etc. However, the use of artificial intelligence creates new risks related to data security and confidentiality; risks inherent in artificial intelligence models (e.g., hallucinations) and reputational risks. It should be noted that cybercriminals use artificial intelligence to implement their own fraudulent schemes. Gartner Inc. predicts that by 2027, 17% of all cyberattacks will involve generative AI. The company also predicts that global end-user spending on information security in 2025 will amount to 212 billion USD. This is 15.1% more than in 2024 [1]. Therefore, the issues raised today actualize the process of finding solutions for cyber security of the banking business and thus increasing the level of security of banking activities.

Literature Review. Based on the issues raised, the review of scientific achievements will be conducted according to the criteria of "security" and "cybersecurity".

Scholars such as O. Kolodiziev [2], A. Tesliuk and co-authors [3], N. Blaschuk-Devyatkina, and I. Batsman [4], and V. Kovalenko [5], G. Azarenkova [6] reveal the essence of banking business security in the context of digitalization and its peculiarities in martial law.

Cybersecurity issues specific to the banking industry are explored in the works of Y. Semenenko [7], N. Trusova and I. Chkan [8], K. Hrytsenko [9], O. Kryklii [10], and L. Shostak [11] and many others.

Despite a significant amount of scientific research, further improvement of the mechanism of cybersecurity of the banking business is needed, especially during martial law and the expansion of the range of threats with the accelerated use of digitalized banking technologies, which in turn increases the priority of cybersecurity among the goals and objectives of ensuring the security of banking institutions.

Purpose, objectives and methods of the study. The purpose of the study is to establish the importance of cybersecurity for ensuring the security of banking business and the development of banks in the modern digital space. One of the main objectives of this research is to study approaches and tools for building an effective cybersecurity system. To achieve these goals, a detailed analysis of the threats that affect the effectiveness of the cyber defense and security system of the banking business was conducted. A structural, logical and systematic approach was also used to build a model for ensuring the cyber defense of banks. The methods of analysis and synthesis were also used to characterize cyber-attacks and their consequences, and to systematize the regulatory legal acts on security and cybersecurity of banking business.

Results. The study of the scientific work on the definition of the concept of banking business security shows that the scientific community treats it to a greater extent from the standpoint of ensuring financial security. This is understandable, since the adequacy of financial resources determines the viability of the adopted banking business policies, including the overall security system by its various types. As O. Kolodiziev notes, "...the issue of ensuring the protection of financial resources, cyber security of information, property and personnel of the bank, and the creation of effective mechanisms for financial protection of the entire banking system is becoming increasingly acute" [2, p. 337].

The authors of the scientific article, S. Tesliuk and co-authors, identified indicators for ensuring the financial security of banks in the context of the use of digitalized banking technologies, namely: the presence of a unit in the bank that is designed to manage network risks; availability of a

network of ATMs and POS terminals; Internet banking and mobile banking services; online customer access to banking services; availability of a cyber defense system; means of centralized detection of illegal attempts to penetrate the resource base; means of network interaction for the protection of the bank's resources. use of AI technologies; availability of databases based on the client-server model [3].

V. Kovalenko identified the main threats to the security of the banking business since the introduction of martial law in Ukraine, "...domestic banks have lost a significant part of their customer base, banking operations are aimed more at servicing cash flows. Banks are forced to apply prolongation of credit debt repayment, sources of formation of their own resources have significantly decreased" [5, p.142].

The presented developments indicate that today the main threats to the security of the banking business are the socio-economic consequences of martial law, negative factors of the use of digitalized banking technologies and the growing volume of cyber-attacks. Therefore, ensuring the continuity of the banking business is a key basis for the successful operation of banks. At the same time, cybersecurity plays an important role in ensuring the sustainability and continuity of banking business operations in the face of dynamically growing and persistent cyber threats.

Today, there are types of cyber threats in cyberspace, which are described in Table 1.

Таблиця 1. Характеристика кібератак та їх наслідки
Table 1. Characteristics of Cyberattacks and Their Consequences

Species lineup of cyber attacks	Characteristics	Наслідки
Phishing	Attacks aimed at obtaining confidential information (logins, passwords, card details) by disguising them as legitimate messages The main goal of phishing is to force users to provide personal data or install malware. It is usually carried out through emails, messages, or websites that mimic legitimate groups.	Compromise of customer accounts, financial losses, reputational risks.
Smishing	The use of text messages instead of email to gain access to confidential information stored on mobile devices or to install PUPs.	Spreading of PKI in the corporate network, theft of confidential information, and breach of the network security.
PUPS	Trojans, spyware, viruses, and worms. Trojans disguise themselves as legitimate programs and provide attackers with access to business systems. Spyware monitors user actions and collects confidential information without their knowledge. Worms, unlike viruses, do not require user interaction to spread and can multiply rapidly through networks.	Direct financial losses, restoration costs, fines and compensation, data theft, system disruption, reputational losses, compromise of banking business security.
Ransomware	Blocking access to the system or encrypting user files until a ransom is paid.	Financial, reputational and operational losses.
DDoS attacks (Denial of service attacks)	They are aimed at overloading bank servers by means of excessive traffic (botnets are networks of infected devices that attacker's control to send a large number of requests to the target system simultaneously).	Temporary suspension of online banking, loss of customers, additional costs for system recovery.
Zero-day attacks	Exploit previously unknown vulnerabilities in software.	Loss of significant amounts of money due to data theft, ransom demands, or loss of business.
Social engineering.	Manipulation of bank employees or customers to obtain confidential information.	Access to critical data, the ability to submit.

Джерело: систематизовано автором за матеріалами [7, с. 988-999; 11, с. 124]
Source: compiled by the author based on matters [7, p. 988-999; 11, p. 124]

According to the data officially published by the State Service for Special Communications and Information Protection of Ukraine, since the beginning of russian full-scale invasion of Ukraine, 796 russian cyberattacks were carried out against Ukraine, which is three times more than in the same period the year before [2]. In 2022, almost all cyberattacks on the banking sector of the national economy were carried out by hacker groups backed by the authorities of the aggressor country (hacker groups Armageddon, Fancy Bears and others (01.2022 - Whispergate, DDoS, State-sponsored hacking group; 02.2022 - Ranic Attack, BGP Hijack, Meris, HermeticWiper, DDoS, State-sponsored hacking group; 03.2022 - Deface, CaddyWiper, DDoS, State-sponsored hacking group; 04-05.2022 - DDoS - Hacktivist, fraud - motivated by finance) [8, p. 154; 12].
Today, cyberattacks by the aggressor country are manifested in two ways: DDoS attacks of various kinds and phishing attacks of various types.
In general, since the beginning of the 21st century, most politically motivated cyberattacks have been carried out from China (almost 12% of all attacks). It is followed by Russia (11.6 %), Iran (5.3 %), North Korea (4.7 %) and Ukraine (2.6 %) (Fig. 1) [13].

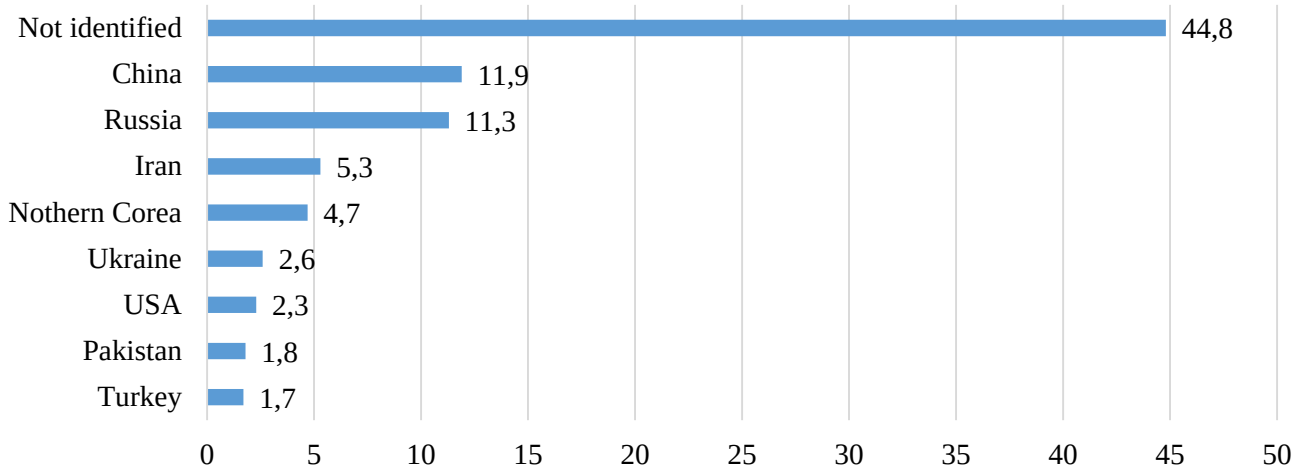

Рис.1 – Країни, які відповідальні за найбільшу частку кіберінцидентів з політичним підтекстом з 2000 по 2023 рік.
Figure 1 – Countries Responsible for the Largest Share of Politically Motivated Cyber Incidents from 2000 to 2023.
Джерело: складено *автором за матеріалами [13]*
Source: compiled by the author based on matters [13]

In 2024, the number of cyberattacks reached a record high, doubling financial losses compared to the previous year. The use of AI has made these attacks more precise and sophisticated. According to the government's Cyber Operations Response Center CERT-UA, in 2024, Ukraine was subjected to 4,315 cyberattacks, which is 70% more than in 2023. The largest cyberattack took place on December 19, 2024, when hackers disabled the registers of the Ministry of Justice of Ukraine [14].

The introduction of AI and generative AI (GenAI) continues to increase investments in security software markets, starting with application security, data and privacy security, and infrastructure protection. By 2025. GenAI will lead to a sharp increase in the cybersecurity resources required to protect it, resulting in an expected 15% increase in security software spending (Table 2).

Given that businesses continue to move to the cloud, Gartner analysts expect an increase in cloud security solutions, and the market share of cloud solutions will grow. The combined market for cloud access security brokers (CASBs) and cloud workload protection platforms (CWPPs) is estimated at USD 8.7 billion in 2025, up from a projected USD 6.7 billion in 2024.

Таблиця 2. Витрати кінцевих користувачів на інформаційну безпеку за сегментами, у всьому світі, 2023-2025, млн дол США.
Table 2. End-User Spending on Information Security by Segment, Worldwide, 2023-2025, million USD.

Market segment	2023		2024		2025	
	Expenses (USD million)	Share (%)	Expenses (USD million)	Share (%)	Expenses (USD million)	Share (%)
Security software	76,574	13,6	87,481	14,2	100,692	15,1
Security service	65,556	13,6	74,478	13,6	86,073	15,6
Network security	19,985	6.2	21,912	9.6	24,787	13.1
Total	162,115	12.7	183,872	13.4	211,552	15.1

Джерело: складено автором за матеріалами [1]
Source: compiled by the author based on matters [1]

Proceeding from the fact that for the security of the domestic banking services market it is expedient to formulate the conceptual framework for cyber defense of banking business, the author of this article has identified the key regulatory legal acts relating to security and the key determinant - cybersecurity (Table 3).

Таблиця 3. Характеристика нормативно-правових актів, що регламентують забезпечення безпеки банківського бізнесу та його кіберзахисту.
Table 3. Characteristics of Regulatory and Legal Acts Governing the Security and Cybersecurity of the Banking Business.

1.	*Regulatory and legal acts governing the security of the banking business*
1.1.	The Law of Ukraine "On Banks and Banking Activities", approved by the Verkhovna Rada of Ukraine on December 7, 2000, No. 2121-III (as amended on January 10, 2025, the basis - 4174-IX). [https://surl.li/yvdhlr].
1.2.	The Law of Ukraine "On the National Bank of Ukraine", approved by the Verkhovna Rada of Ukraine of 20.05.1999, No. 679-XIV (as amended on 19.12.2024, the basis - 4042-IX). [https://surl.li/yudgou].
1.3.	The Law of Ukraine "On National Security of Ukraine", approved by the Verkhovna Rada of Ukraine on June 21, 2018, No. 2469-VIII (as amended on August 09, 2024, the basis - 3858-IX). [https://surl.li/moigut]
1.4	Economic Security Strategy of Ukraine for the period up to 2025: Decree of the President of Ukraine No. 347 of 11.08.2021. [https://www.president.gov.ua/ documents/3472021-39613].
1.5.	Strategy for Ensuring State Security. Decree of the President of Ukraine No. 56 of February 16, 2022. [https://surl.li/dafyoi].
1.6	Strategy "Financial Fortress of Ukraine". National Bank of Ukraine. [https://surl.li/wuqtao].
1.7.	Strategy for the Development of Fintech in Ukraine until 2025. [https://surl.li/xlsyvx].
2.	*Regulatory and legal acts on cybersecurity*
2.1.	The Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", approved by the Verkhovna Rada of Ukraine on October 5, 2017, No. 2163-VIII (as amended on June 28, 2024, the basis - 3783-IX). [https://surl.li/ouwlzd].
2.2.	The Law of Ukraine "On Cloud Services", approved by the Verkhovna Rada of Ukraine on February 17, 2022, No. 2075-IX (as amended on June 28, 2024, the basis - 3783-IX). [https://surl.li/txjiuf].
2.3.	Regulation on the Organization of Measures to Ensure Information Security in the Banking System of Ukraine, adopted by the Board of the National Bank of Ukraine on 28.09.2017 No. 95. [https://surl.li/tghkbq].
2.4.	On the Implementation Plan of the Cybersecurity Strategy of Ukraine. Decree of the President of Ukraine of February 1, 2022, No. 37/2022. [https://surl.li/fngbgb].
2.5.	Regulation on the Organization of Cybersecurity in the Banking System of Ukraine and Amendments to the Regulation on the Definition of Critical Infrastructure Objects in the Banking System of Ukraine, adopted by the Board of the National Bank of Ukraine on August 12, 2022, No. 178. [https://surl.li/rolupc].

Джерело: систематизовано автором.
Source: systematized by the author.

The presented legal acts make it possible to identify strategic vectors for strengthening the cyber defense of the banking business.

According to a study by 15.PwC, the main cybersecurity threats to the national economy and banking business in particular include: hybrid aggression of russia, namely destabilization of information systems and access to the Internet, provoking a situation of chaos in the work of state

institutions, financial and banking and business centers in order to harm the security and sovereignty of Ukraine; cyberattacks organized and financed by the governments of other states, which involve the theft of confidential information; cybercrime that harms information resources, social processes, and citizens personally, reduces public confidence in information technology and leads to significant material losses; high technological dependence of our country on foreign manufacturers of IT products; high vulnerability of the IT infrastructure due to the dispersion of employees and the remote format of their work; partial lack of proper control over the implementation of cybersecurity and information security measures in financial institutions; imperfection of the current regulatory framework in the field of cybersecurity and slow implementation of relevant EU regulations [15].

To overcome cybersecurity threats to the banking business, it is necessary to develop a cybersecurity model for each banking institution and the banking system as a whole (Fig. 2). To form the model we propose, we used the scientific developments of K. Hrytsenko [9] and O. Kryklii [10], who proposed to assess the level of cybersecurity by qualitative and quantitative characteristics.

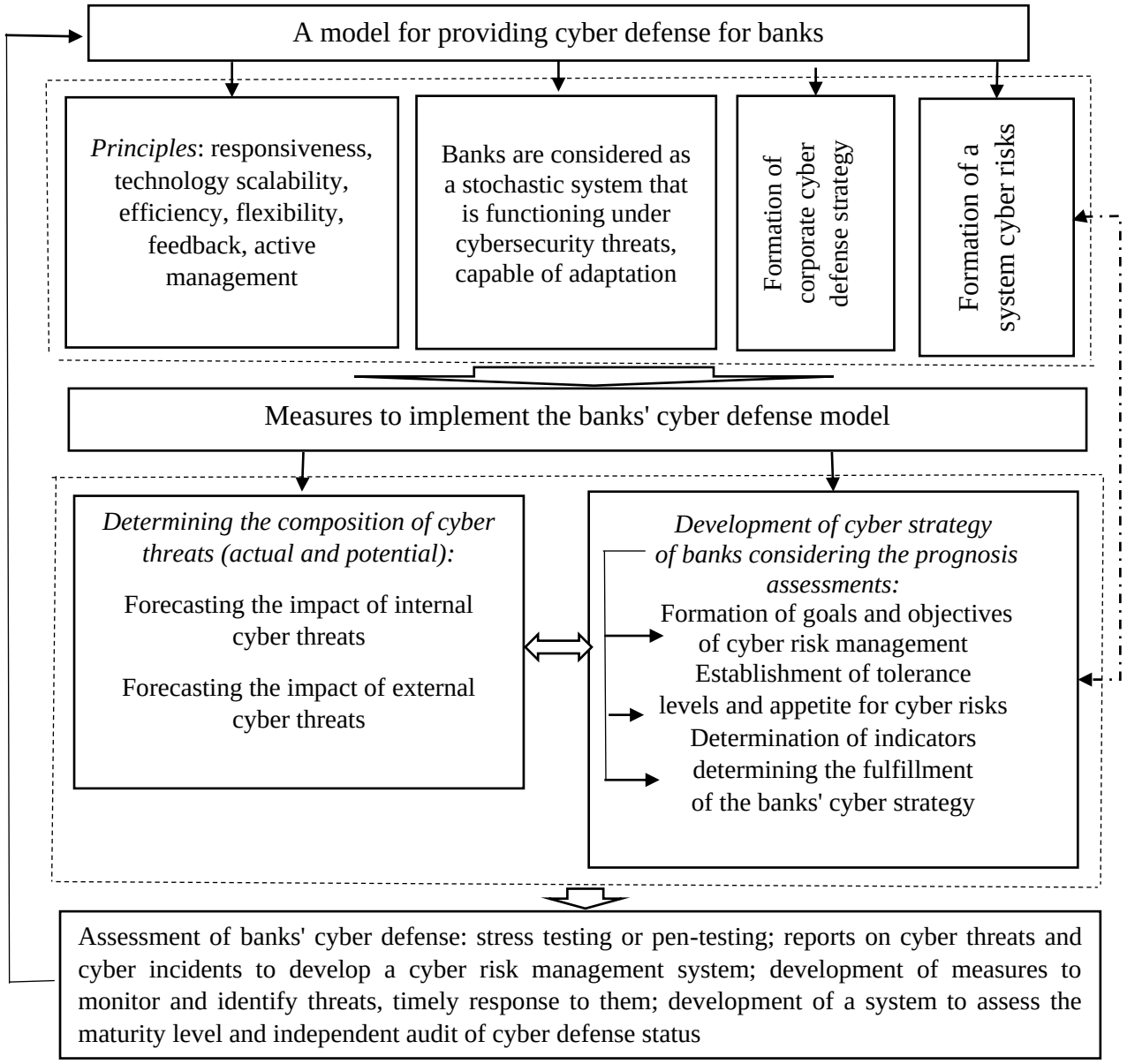

Рис.2 – Модель забезпечення кіберзахисту банків.
Figure 2 – Model for Ensuring Banking Cybersecurity.
Джерело: складено автором за матеріалами [9, с. 277; 10]
Source: compiled by the author based on matters [9, p. 277; 10]

Discussion. Based on the study, we conclude that cyber defense in the modern realities of banking business acquires a strategic mission to ensure the security of banking activities, in particular, financial security.

Based on the research of G. Azarenkova [6], we can state the fact that the world community has recently been paying a lot of attention to the cyber activities of economic entities. If we consider a bank as a subject of economic activity, we can confidently refer to the analysis of publication activity on security mentioned in the above article, namely: the growth in the number of publications and interest in the topic of security; the determining role of the United States as a provider in financial security research; bibliometric analysis of the relationship between the concepts of security; the impact of war on the security of domestic economic entities; implementation of international experience and determination of prospects for Ukraine [6, p. 39-40].

Most of scientific works in this area emphasizes the implementation of international experience in the formation of cybersecurity of business structures. For example, E. Kurii and I. Opirsky analyzed the differences between versions 4.0 and 3.2.1 of the PCI DSS standard. The authors emphasize that the new requirements and security controls meet current trends and threats in the field of cybersecurity, which helps to ensure a higher level of data protection of payment card holders [16, p. 148-151].

S. Lincke proved that PCI DSS 4.0 contains several changes aimed at achieving four key goals: continuing to meet the needs of the payment industry; promoting security as a continuous process; adding flexibility and additional methods to support payment security; improving payment confirmation methods and procedures [17].

It worth to emphasize the use of the European Union's experience. In this vector, attention should be paid to the adopted EU Directive "NIS2: New rules for the cybersecurity of network and information systems", which establishes a unified legal framework for supporting cybersecurity in 18 critical sectors across the EU. It also calls on Member States to define national cybersecurity strategies and cooperate with the EU for cross-border response and enforcement [18]. The NIS2 classifies institutions as "important legal entity" and "major legal entity" based on two criteria: size (number of employees, annual global revenue, balance sheet) and criticality of the business sector in which the institution operates (Table 4). The inclusion of the sectors presented in Table 4 emphasizes their importance in supporting public functions and the EU economy.

Таблиця 4. Класифікація суб'єктів економічної діяльності NIS2 за розміром, доходом і балансом.
Table 4. Classification of NIS2 Economic Entities by Size, Revenue, and Balance Sheet.

Size of business	Number of employees	Revenue (MEUR)	Balance sheet (MEUR)	Highly critical sectors	Other critical sectors
Large	X>=250	y>=50	z>=43	Essential	Important
Medium	50>=X>250	10>=y>50	10>=z>43	Important	Important
Small	X<50	Y<10	Z<10	Out of scope	Out of scope
Sectors that fall under the category of "essential entities (EE)" :			Sectors falling under the category of "important entities (IE)" :		
Energy	Water	Space	Manufacturing	Food	Research
Healthcare	Public administration	***Financial sector***	Postal services	Chemicals	Waste management
Transport	Digital infrastructure		Digitalization support sector		

Джерело: складено автором за матеріалами [18; 19]
Source: compiled by the author based on matters [18; 19]

Today, we can identify the main threats to the banking business in terms of cybersecurity.

First. Accelerated use of digital technologies in banking. Banks are promoting new technologies to improve customer-focused interaction. However, with the growing number of

digital tools, there is a need for reliable security measures to prevent hackers from exploiting weaknesses in online banking platforms and mobile applications.

Secondly. AI and process automation in cybersecurity. AI-enabled banking security tools are becoming increasingly necessary to detect and neutralize cyber threats in real time. Automated detection systems, behavioral analytics, and machine learning help banks respond quickly to potential breaches. However, cybercriminals are also using AI to launch smarter attacks, which means that banks must continue to improve their security strategies.

Third. Growing security issues with the use of cloud technologies. As more and more banks move to the cloud, the security of these systems must become a top priority. Misconfiguration, unauthorized access, and data leakage are the main risks. In order to counter these threats, banks are investing in encryption, multi-factor authentication, and continuous monitoring to protect sensitive information.

Fourth. The need to comply with regulatory requirements in the field of cybersecurity. Governments and regulators are introducing stricter cybersecurity rules for banks. Compliance with new data privacy laws and security standards is key to maintaining customer confidence and avoiding fines. Therefore, banks should focus on regular risk assessments, transparent reporting, and alignment with international security frameworks.

Fifth. Third-party security risk management. Today, banks are increasingly relying on third-party providers of services such as payment processing and cloud hosting. At the same time, such partnerships also create additional security risks. Therefore, banks should conduct thorough security due diligence, implement strict access control and monitoring to mitigate potential threats from third-party relationships.

The outlined problems in the organization of cyber defense of the banking business are the basis for further research and determining the trajectory of the formation of the bank security system.

Conclusions. The problem of ensuring the security of the banking business is actualized based on the emergence of new threats such as the socio-economic consequences of martial law, negative factors of the use of digitalized banking technologies and the growing volume of cyber-attacks.

Cyber threats have become more complex in recent years, and banks face challenges related to AI-driven cybercrime, geopolitical risks, supply chain vulnerabilities, and fragmented legislation.

Banks should utilize AI-powered security, strengthen cloud-based protection, and adopt a proactive approach to risk management. By focusing on security awareness, following regulations, and establishing robust defenses, banks can protect their systems from emerging threats. Staying ahead of cybercriminals is not only about security, but also about ensuring trust and stability in the banking industry.

Therefore, regulators and banks should take a holistic approach to cybersecurity, integrating risk management with technological innovation and the development of professional competencies of employees. Further research is needed to improve the regulatory framework for cybersecurity and bring it in line with international best practices.

References

1. STAMFORD. (2024, August 28). *Gartner Forecasts Global Information Security Spending to Grow 15% in 2025*. Retrieved from https://surl.li/ryvody
2. Kolodiziev, O. M., & Berehovyi, V. O. (2024). Financial security of banks under martial law: The impact of digital instruments and innovations. *Business-Inform, 9*, 335-341. Retrieved from https://doi.org/10.32983/2222-4459-2024-9-335-341 [in Ukrainian].
3. Tesliuk, S., Matviichuk, N., & Levchuk, A. (2024). Financial security of banking institutions in the conditions of digitalization. *Economics and Society, (60).* Retrieved from https://doi.org/10.32782/2524-0072/2024-60-117 [in Ukrainian].
4. Blaschuk-Devyatkina, N. V., & Batsman, I. (2023). Financial security of the banking system of Ukraine. *Galician Economic Journal, 85*(6), 104-112. Retrieved from https://doi.org/10.33108/galicianvisnyk_tntu2023.06.104 [in Ukrainian].

5. Kovalenko, V. V. (2022). Financial security of banks: Realities and prospects of provision. *Economic Forum, 2,* 141-151. Retrieved from https://doi.org/10.36910/6775-2308-8559-2022-2-18 [in Ukrainian].
6. Azarenkova, G., & Vepretska, S. (2024). System for ensuring the financial security of the enterprise. *Financial and Credit Systems: Development Prospects*, *4*(15), 32-42. Retrieved from https://doi.org/10.26565/2786-4995-2024-4-03 [in Ukrainian].
7. Semenenko, Yu. S. (2024). Cybersecurity and its importance for economic stability. *Scientific Perspectives*, *5*(47), 983-996. Retrieved from https://doi.org/10.52058/2708-7530-2024-5(47)-983-996 [in Ukrainian].
8. Trusova, N. V., & Chkan, I. O. (2023). Cybersecurity of the banking system of Ukraine in the context of digital transformations. *Collected Scientific Works of the State Technical University of Ukraine Named After Dmytro Motornyi (Economic Sciences), 1*(47), 151-163. Retrieved from https://doi.org/10.31388/2519-884X-2023-47-151-163 [in Ukrainian].
9. Hrytsenko, K. G. (2020). Ways to improve the efficiency of bank cybersecurity. *Market Infrastructure*, *45*, 274-279. Retrieved from https://doi.org/10.32843/infrastruct45-44 [in Ukrainian].
10. Kryklii, O. A. (2020). Theory and practice of ensuring cyber resilience of banks. *Effective Economy, 10.* Retrieved from http://www.economy.nayka.com.ua/?op=1&z=8248 DOI: 10.32702/2307-2105-2020.10.50 [in Ukrainian].
11. Shostak, L., Fedonyuk, A., & Pomazun, O. (2024). Peculiarities of business cybersecurity in wartime. *Digital Economy and Economic Security*, *3*(12), 121-125. Retrieved from https://doi.org/10.32782/dees.12-22 [in Ukrainian].
12. PwC Ukraine. (2022). Business cybersecurity in an unstable environment. Retrieved from https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html [in Ukrainian].
13. Prysyazhnyuk, N. (2024). Which countries carry out the most politicized cyberattacks in the world: Ukraine is in the top five. *Liga.net*. Retrieved from https://surl.li/axbnxj [in Ukrainian].
14. IT Ukrainian Association. (2025). Ukraine is among the leaders in the number of cyberattacks in the world. Retrieved from https://surl.gd/eyfaqe [in Ukrainian].
15. PwC Ukraine. (2022). Business cybersecurity in times of instability. Retrieved from https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html [in Ukrainian].
16. Kurii, E. O., & Opirsky, I. R. (2024). Security of payment transactions: Review and characteristics of key changes in the new edition of the PCI DSS standard. *Cybersecurity: Education, Science, Technology*, *3*(23), 144-154. Retrieved from https://doi.org/10.28925/2663-4023.2024.23.144154 [in Ukrainian].
17. Lincke, S. (2024). Complying with the PCI DSS Standard. In *Information Security Planning* (pp. 45-63). Springer, Cham. Retrieved from https://doi.org/10.1007/978-3-031-43118-0_3
18. ASEE. (2024). Understanding the NIS2 Directive and Its Implications on Your Organization. Retrieved from https://cybersecurity.asee.io/blog/understanding-the-nis2-directive/
19. European Commission. (2025). *NIS2 Directive:* New rules on cybersecurity of network and information systems. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

The article was received by the editors 14.11.2024
The article is recommended for printing 23.01.2025

Азаренков Сергій
аспірант кафедри банківської справи
Одеський національний економічний університет
Преображенська 8, Одеса, 65028, Україна
e-mail: serdgzhio@gmail.com
ORCID ID: 0000-0002-1159-8699

Кіберзахист та безпека банківського бізнесу в умовах воєнного стану

Анотація. Актуальність теми дослідження полягає у необхідності пошуку рішень щодо кіберзахисту банківського бізнесу, а тим самим і підвищення рівня безпеки банківської діяльності. Метою даного дослідження є встановлення важливості кіберзахисту для забезпечення безпеки банківського бізнесу та розвитку банків у сучасному цифровому просторі. Для досягнення поставленої цілі використано структурно-логічний та системний підхід для побудови моделі забезпечення кіберзахисту банків. Також використані методи систематизації та групування при характеристиці кібератак та їх наслідків, систематизаціїї нормативно-правових актів з безпеки та кібербезпеки банківського бізнесу. Об'єктом дослідження є процес забезпечння кіберзахисту банківського бізнесу та його інтеграція у загальну систему безпеки банків. Основний акцент дослідження спрямований на виявлення новітніх загроз для безпеки та кіберзахисту банківського бізнесу, визначенню проблем при формуванні банками системи кіберзахисту, а саме: використання штучного інтелекту, проблеми безпеки з використанням хмарних технологій, цифровізація банківських бізнес-процесів, управління ризиками безпеки третіх сторін. Отримані результати можуть бути використані для вдосконалення системи кіберзахисту банківського бізнесу та її інтеграції в загальну систему корпоративного управління банків. Висновки дослідження акцентують увагу на необхідності врахування міжнародних стандартів забезпечення кіберзахисту у національному нормативно-правовому полі. Крім того, результати можуть сприяти формуванню власної траєкторії при побудові моделі забезпечення кіберзахисту банків, що міститить принципи, заходи реалізації моделі; підходи до оцінювання якості моделі та формування кооперативної стратегії кіберзахисту.

***Ключові слова**: банківський бізнес, безпека, кібербезпека, кіберзахист, кібератаки, загрози.*
JEL Classification: G21; K24; M15
Формули: 0; рис.: 2; табл.: 4; бібл.: 19.

Для цитування: Azarenkov S. Cybersecurity and Security of the Banking Business Under Martial Law. Фінансово-кредитні системи: перспективи розвитку. №1(16) 2025. С. 9-19. DOI: https://doi.org/10.26565/2786-4995-2025-1-01

Список літератури

1. Gartner Forecasts Global Information Security Spending to Grow 15% in 2025. STAMFORD, Conn., August 28, 2024. URL: https://surl.li/ryvody.
2. Колодізєв О. М., Береговий В. О. Фінансова безпека банків в умовах воєнного стану: вплив диджитал-інструментів та інновацій *Бізнес-Інформ*. 2024. № 9. С. 335–341. DOI: 10.32983/2222-4459-2024-9-335-341.
3. Теслюк С. А., Матвійчук Н. М., Левчук А. О. Фінансова безпека банківських установ в умовах цифровізації *Економіка та суспільство*. 2024. Вип. 60. DOI: 10.32782/2524-0072/2024-60-117.
4. Блащук-Дев'яткіна Н., Бацман І. Фінансова безпека банківської системи України *Галицький економічний вісник*. 2023. № 6 (85). С. 104–112. DOI: 10.33108/galicianvisnyk_tntu2023.06.104.
5. Коваленко В. В. Фінансова безпека банків: реалії та перспективи забезпечення *Економічний форум*. 2022. № 2. С. 141–151. DOI: 10.36910/6775-2308-8559-2022-2-18.
6. Азаренкова Г., Вепрецька С. Система забезпечення фінансової безпеки підприємства *Фінансово-кредитні системи: перспективи розвитку*. 2024. № 4(15). С. 32–42. DOI: 10.26565/2786-4995-2024-4-03.
7. Семененко Ю. С. Кібербезпека та її значення для економічної стабільності *Наукові перспективи*. 2024. № 5(47). С. 983–996. DOI: 10.52058/2708-7530-2024-5(47)-983-996.
8. Трусова Н. В., Чкан І. О. Кіберзахист банківської системи України в умовах цифрових трансформацій *Збірник наукових праць ТДАТУ імені Дмитра Моторного (економічні науки).* 2023. № 1(47). С. 151–163. DOI: 10.31388/2519-884X-2023-47-151-163.
9. Гриценко К. Г. Шляхи підвищення ефективності забезпечення кібербезпеки банку *Інфраструктура ринку*. 2020. Вип. 45. С. 274–279. DOI: 10.32843/infrastruct45-44.
10. Криклій О. А. Теорія та практика забезпечення кіберстійкості банків *Ефективна економіка.* 2020. № 10. DOI: 10.32702/2307-2105-2020.10.50.
11. Шостак Л., Федонюк А., Помазун О. Особливості кібербезпеки бізнесу в умовах воєнного часу *Цифрова економіка та економічна безпека*. 2024. № 3(12). С. 121–125. DOI: 10.32782/dees.12-22.
12. Кібербезпека бізнесу в умовах нестабільності. URL: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html.
13. Присяжнюк Н. Які країни проводять найбільше політизованих кібератак у світі: Україна увійшла до п'ятірки *Liga.net.* 2024. URL: https://surl.li/axbnxj.
14. Україна – серед лідерів за кількістю кібератак у світі *IT Ukrainian Association*. 2025. URL: https://surl.gd/eyfaqe.

15. PwC. Кібербезпека бізнесу в умовах нестабільності. 2022. URL: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.
16. Курій Є. О., Опірський І. Р. Безпека платіжних операцій: огляд і характеристика ключових змін у новій редакції стандарту PCI DSS *Кібербезпека: освіта, наука, техніка*. 2024. № 3(23). С. 144–154. DOI: 10.28925/2663-4023.2024.23.144154.
17. Lincke S. Complying with the PCI DSS Standard *Information Security Planning. Springer, Cham*. 2024. P. 45–63. DOI: 10.1007/978-3-031-43118-0_3.
18. ASEE. Understanding the NIS2 Directive and Its Implications on Your Organization. 2024. URL: https://cybersecurity.asee.io/blog/understanding-the-nis2-directive/.
19. NIS2 Directive: new rules on cybersecurity of network and information systems *European Commission*. 2025. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

Стаття надійшла до редакції 14.11.2024
Статтю рекомендовано до друку 23.01.2025