УДК 336.717:004.738.5:005.334
https://doi.org/10.32342/3041-2153-2025-2-39-8

V.V. ZIANKO,
Doctor Sciences (Economic), Professor,
Head of the Department of Finance and Innovation Management,
Vinnytsia National Technical University, Vinnytsia (Ukraine)
https://orcid.org/0000-0003-0095-5248

T.D. NECHYPORENKO,
PhD (Economics), Associate Professor of the Department
of Entrepreneurship, Logistics and Management,
Vinnytsia National Technical University, Vinnytsia (Ukraine)
https://orcid.org/0000-0002-0690-1534

FINANCIAL SECURITY OF BANKS IN THE DIGITAL SPACE: CURRENT CHALLENGES AND ADAPTATION OF FINANCIAL INSTRUMENTS

The issue of ensuring the financial security of banks in the digital space is investigated, in the context of modern challenges and the need to transform financial instruments. The key threats to the banking sector, including cyber risks, technological vulnerabilities, regulatory fragmentation and risks associated with the integration of financial and digital technologies, are identified and systematized. It is substantiated that the proliferation of innovations, such as artificial intelligence, distributed ledger technologies and cloud computing, is shaping a new risk architecture that requires adaptive management and proactive regulation. It is determined that the threats are complex and multifactorial, covering technical and systemic aspects, including IT infrastructure failures, phishing attacks, ransomware, and regulatory delays. The author analyses modern approaches to the adaptation of financial instruments, including the integration of RegTech and SupTech, as a means of enhancing cyber resilience and ensuring financial stability. A conceptual model of adaptation of financial instruments to increase the resilience of banks and counteract threats is proposed. It is noted that financial security in the digital economy is a complex problem that requires a systematic approach, continuous updating of tools and strategic vision, opening up opportunities for sustainable development and increasing the competitiveness of banks.

Keywords: digitalization, financial innovations, banking technologies, financial stability

JEL classification*: G21, G28, O33*

Досліджено проблематику забезпечення фінансової безпеки банків у цифровому просторі, в контексті сучасних викликів та необхідності трансформації фінансових інструментів. Ідентифіковано та систематизовано ключові загрози для банківського сектору, зокрема кіберризики, технологічні уразливості, регуляторну фрагментацію та ризики, пов'язані з інтеграцією фінансових і цифрових технологій. Обґрунтовано, що поширення інновацій, таких як штучний інтелект, технології розподіленого реєстру та хмарні обчислення, формує нову архітектоніку ризиків, яка потребує адаптивного управління та проактивного регулювання. Визначено, що загрози мають складний

багатофакторний характеру, охоплюючи технічні та системні аспекти, зокрема відмови в IT-інфраструктурі, фішингові атаки, програми-вимагачі, а також регуляторні затримки. Проаналізовано сучасні підходи до адаптації фінансових інструментів, зокрема інтеграцію RegTech і SupTech, як засобів підвищення кіберстійкості та забезпечення фінансової стабільності. Запропоновано концептуальну модель адаптації фінансових інструментів для підвищення резильєнтності банків та протидії загрозам. Наголошено, що фінансова безпека в цифровій економіці є комплексною проблемою, яка вимагає системного підходу, безперервного оновлення інструментарію і стратегічного бачення, відкриваючи можливості для сталого розвитку та підвищення конкурентоспроможності банків.

Ключові слова: цифровізація, фінансові інновації, банківські технології, фінансова стабільність

JEL classification*: G21, G28, O33*

Statement of the problem and its connection with important scientific or practical problems. Ensuring the financial security of banks in the digital environment is a key factor in maintaining the stability of the banking sector and overall macrofinancial balance in the context of intensive digitalization. The rapid growth of electronic transactions, the introduction of innovative financial technologies (FinTech) and the expansion of virtual ecosystems are transforming traditional approaches to managing banking processes, assets and information infrastructure. This is leading to a rethinking of the paradigms of asset protection, data protection, and operational processes, with financial security being viewed not only as a key indicator of the sustainability of individual banking institutions, but also as a systemic task that determines macrofinancial stability.

The transition to the dominant role of the digital space in the banking sector is accompanied by an escalation of multi-vector threats, both technical and regulatory. On the one hand, the increased use of cloud computing, artificial intelligence and distributed ledger technologies increases vulnerability to cyber risks, including sophisticated phishing attacks, ransomware and targeted cyber-attacks on critical infrastructure. On the other hand, the integration of financial and digital technologies (DeFi, Open Banking) is creating new forms of interaction between market participants that do not always fit within the existing regulatory framework. Regulatory lags, the lack of unified cybersecurity standards, and fragmented supervision create preconditions for the accumulation of systemic risks.

Thus, there is an urgent need for a scientific rethinking of approaches to financial security in the digital space. This involves developing integrated strategies that combine technological solutions, adaptive financial instruments, effective risk management, and regulatory innovations (RegTech, SupTech). The systematic construction of a cyber defence architecture, development of analytical platforms based on big data, and strengthening of cryptographic information security mechanisms are key vectors that will help consolidate financial security and ensure sustainable development of banks in a dynamic digital landscape.

Analysis of recent studies and publications, which laid the foundation for solving the problem under study, and highlighting previously unresolved parts of the general problem, which are the subject of the article. The issue of financial security of banks in the digital environment has been the subject of numerous studies by both domestic and foreign scholars. The current scientific

literature actively analyses the impact of digitalization on the transformation of banking models, the growth of cyber risks, the adaptation of financial instruments, and the effectiveness of risk management mechanisms.

In particular, Ozarslan S. and Rubina A. [17] study the massive spread of cyber threats and their destructive impact on the operational resilience of banking institutions in the context of digital transformation. Current trends in the adaptation of financial instruments to digital challenges are highlighted by Banerjee S., Craig L. and Greis J. [2], focusing on innovative approaches to risk management and data protection. Hao G., Banerjee S., and Boer M. [8] focus on systemic cyber resilience and adaptation of financial instruments at the interinstitutional level.

Practical aspects of cyber risk management in the banking sector are considered in the works of Craig L., Hao G. and Idler M. [4], which summarize international experience in building global strategies for strengthening financial security. Ozarslan S. [16] examines the effectiveness of digital protocols for protecting financial institutions, in particular in the context of growing cyber risks, which allows assessing the technological readiness of banks to modern threats. Pattni P. [18] focuses on the aspects of digital banking as a driver of transformation of traditional financial instruments, while Garcia T., Grodzicki M. and Radulova P. [7] cover the transformation of banking business models in the digital economy.

Ukrainian scientists also make a significant contribution to the study of the issue. For example, Kopylyuk O., Zhyhar N. and Petrynyak A. [11] analyze structural threats to the financial stability of Ukrainian banks in the context of digitalization. Khomyshyn I. and Havts O. [9] compare the experience of cyber defence of the banking sector of Ukraine with the practices of foreign countries. Yehorycheva S., Hlushko A. and Khudolii Y. [22] describe in detail the impact of the digital environment on the organization of information security of banking systems. The research of Kulalaiev V. [13] traces the connection between digital transformation and financial indicators of Ukrainian banking institutions, which allows assessing the effectiveness of digital strategies. Bondarenko S. and Hubanov O. [3] focus on the issues of national financial security, outlining strategic priorities for strengthening state control. Krysovatyy A., Desyatnyuk O. and Ptashchenko O. [12] explore the challenges of digital innovations in the context of state security, outlining institutional threats and adaptation scenarios.

Among the foreign works, Diener F. and Spacek M. [5] explain the phenomenon of regulatory lag, which hinders the timely implementation of FinTech solutions, identifying structural barriers at the level of European financial regulators. Vives X. [21] emphasizes the relationship between the digital transformation of banking and financial stability at the systemic level. Atkins L., Boer M., Greis J., and Idler M. [1] in their international study demonstrate the key global trends in cybersecurity in the financial sector. Pramanik H., Kirtania M. and Pani A. [19] reveal comparative aspects of cyber defence of banks in different regions, focusing on global challenges to digital trust. For their part, Feher P. and Varga K. [6] analyze new risks associated with the formation of digital trust in the financial environment, proposing a model for assessing its stability at the interregional level.

Thus, current research confirms that ensuring the financial security of banks in the digital space is not only a response to growing risks, but also one of the key

factors in the strategic renewal of the financial system as a whole. The researchers emphasize that the adaptation of financial instruments and the introduction of innovative digital technologies not only increase the effectiveness of protective mechanisms, but also act as a catalyst for reengineering banks' business models, helping to counter dynamic threats and create new competitive advantages. A synthesis of these approaches confirms that financial security in the digital space is a multidimensional category that requires an integrated, adaptive approach, taking into account the specifics of each financial institution and market environment.

Highlighting previously unresolved parts of the general problem to which the specified article is devoted. Despite the existing scientific achievements, a number of key aspects of financial security of banks in the digital environment remain insufficiently studied. In particular, there is a lack of comprehensive approaches to assessing the effectiveness of adapting financial instruments in response to the latest hybrid threats. The absence of a holistic view of the relationship between financial resilience, digital technologies, and risk management makes it difficult to develop effective protection mechanisms.

Digital transformation is radically changing the role of the banking sector, driving the need for adaptive financial instruments and enhanced cybersecurity. Along with new opportunities, digitalization brings with it specific risks, such as growing cyber threats, volatility of digital assets, and regulatory uncertainty. In this context, the article is aimed at addressing the current research gaps: development of methodological approaches to the adaptation of financial instruments, integration of cyber resilience into risk management, and conceptualization of the strategic architecture of financial security of banks in the digital space.

Statement of the objectives of the article. The purpose of the study is a comprehensive analysis of the mechanisms for ensuring financial security of banks in the digital space, taking into account current challenges and the need to adapt financial instruments in the context of global digital transformation. Particular attention is paid to the impact of the latest digital technologies, such as artificial intelligence, distributed ledger technologies (DLT), cloud computing, and open APIs, on the operational resilience, data protection, and competitiveness of banks in the face of growing cyber threats, technological risks, and regulatory inertia. Identification of the current vectors of adaptation of financial instruments allows us to outline the prospects for modernizing banking security systems in line with the dynamics of the digital economy.

Methodology. To achieve the goal, a systematic interdisciplinary approach was applied, combining: empirical methods (observation, comparison, description) – for analyzing financial security practices in leading financial systems, as well as for identifying global and national trends in the banking sector; theoretical and cognitive approach – to conceptualize financial security in the digital environment, formalize key concepts and test hypotheses about the impact of technological innovations on risk management strategies; logical methods (analysis, synthesis, induction, deduction, generalization, scientific abstraction) – to identify methodological problems, risks and opportunities for optimizing financial security in national and global contexts.

Presentation of the main research material with full justification of the scientific results obtained. The financial security of banks in the digital space is a

complex process of integrating advanced digital technologies into the functioning of financial institutions, where its provision is one of the key factors of stability and competitiveness. In the context of growing global competition and escalating customer expectations, banks are forced to transform their business models to adapt them to digital realities, which directly affects the architecture of security systems. This process is not limited to the automation of routine operations, but involves a radical transformation of all aspects of banking, from the development of secure products to customer interaction in the face of cyber threats.

In the current scientific literature, the concept of «financial security of banks in the digital space» is interpreted as a comprehensive system of measures aimed at protecting financial institutions from internal and external threats arising from the use of digital technologies and operation in the cyber-physical environment [9; 11]. In addition to classical economic risks, this system should take into account the exponential growth of cybercrime; technological vulnerabilities of infrastructures; and fragmentation of the regulatory space.

Since the 2010s, a period of rapid development of mobile applications, cloud services and open APIs, financial security issues have become increasingly acute. According to analytical data [2; 17], the number of cyber incidents in the banking sector is showing an exponential growth trend, which requires immediate proactive response and revision of security approaches.

In response to these challenges, banks are increasingly adopting digital technologies, including:

- artificial intelligence (AI) and machine learning (ML) – for analyzing Big Data, detecting anomalies and fraudulent transactions [5];
- distributed ledger technology (blockchain) – to ensure the immutability and cryptographic protection of financial transactions;
- cloud computing – to create scalable, adaptive and secure IT systems;
- 5G networks as the basis for fast and secure real-time data exchange.

As noted by leading experts [1; 8], the concept of financial security in the digital era is not limited to technical protection, but is integrated into a customer-centric ecosystem focused on ensuring consumer confidence. The key tools in this context are multi-factor authentication, biometric technologies, user behavior monitoring systems, and chatbots for quick response to security queries. These tools not only reduce risks, but also increase customer loyalty to the banking institution, which is an important condition for maintaining a competitive position in the digital environment.

Therefore, ensuring financial security in the digital space is a complex process of restructuring banking activities due to the rapid evolution of the cyber landscape and information and communication technologies. It involves the systematic implementation of innovative solutions to increase resilience to cyber threats, create new, secure products and services, and continuously adapt to changing regulatory requirements. This process can be viewed as an evolution of organizational structures aimed at building sustainable competitive advantages through increased security and customer focus.

Thus, the financial security of banks in the digital space is a multifactorial category that covers a set of organizational, technological, economic and legal measures aimed at ensuring the continuity of operations and protection of banking institutions assets in the digital risk environment.

As the analysis of Table 1 shows, the interpretation of the concept of «financial security of banks in the digital space» is systemic and interdisciplinary. It is seen as an institutional response to the transformational challenges of the digital economy. The content of each aspect demonstrates that security is not only a technology, but also a new logic of bank development that requires organizational flexibility, customer focus and strategic ability to change.

Table 1

Interpretation of the concept "Financial security of banks in the digital space" [5; 9; 11]

Aspect	Feature
Evolution of business models	Driving a radical paradigm shift in the way banking is done, refocusing institutions on data protection, cyber resilience and efficiency through the use of digital security tools.
The technological imperative	It is considered an integral part of modern development due to the exponential growth of digital threats and the penetration of cyber risks into all areas of banking.
Social and economic transformation	Driving profound transformations that are leading to new forms of customer interaction and risk management that affect the confidence and stability of the financial system.
Integrating the physical and digital worlds	Creates a new reality in which traditional banking operations are increasingly integrated with digital systems, opening up new opportunities for optimising and automating security processes.
A new paradigm for development	Creates a new development paradigm in which digital technologies become the basis for creating innovative, secure products, services and business models.

Ensuring the financial security of banks in the digital space is a cyclical and iterative process that includes a number of interrelated strategic stages. This approach allows financial institutions to adapt to the dynamic conditions of the cyber landscape and effectively counter evolving threats. These stages include: assessing risks and vulnerabilities of the bank's digital infrastructure, formulating security policies, implementing protective technological solutions, continuous monitoring, responding to incidents, and reviewing and optimising security systems. The structure of this process is illustrated in Fig. 1, which demonstrates a conceptual model of building a financial security system for banks that involves continuous improvement based on the principles of Security Lifecycle Management. Each stage is logically linked to the previous and subsequent ones, forming a closed cycle of response, adaptation and development of digital cyber defence strategies.

In addition to the technical dimension, the process of ensuring financial security has a significant impact on both customers and banks: on the part of customers, it means increased trust, access to an expanded list of secure digital services, faster and better service quality with guaranteed protection of personal data; on the part of banks, it means a constant need to invest in technology, improve cyber resilience, adapt business processes to the new requirements of the digital age and strengthen interaction with regulators in the context of compliance with security standards.

Thus, the financial security of banks in the digital environment is not static, but a dynamic system that develops in sync with innovative changes, user needs, and global challenges of the cyber environment.

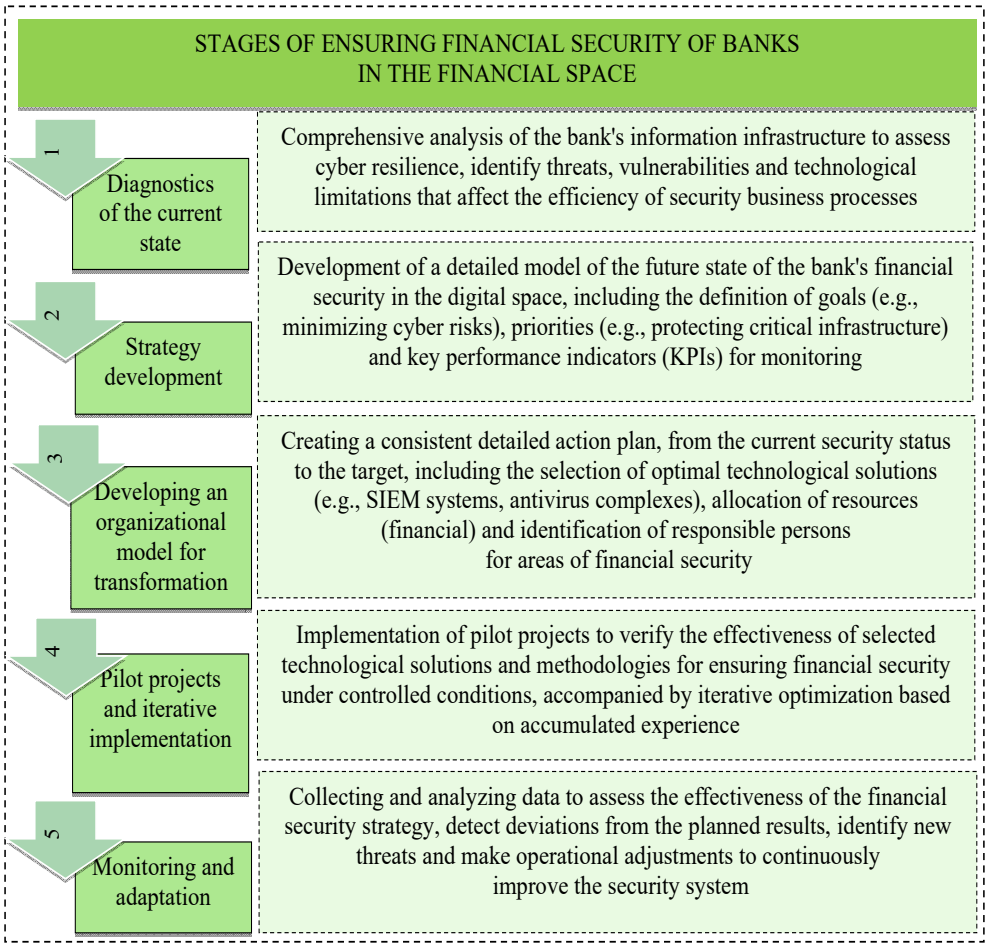

Fig.1. Stages of ensuring financial security of banks in the digital space [8; 9; 16]

Further empirical analysis of the relationship between digital investments, operational efficiency, and customer loyalty will help identify ways to neutralize financial imbalances and formulate strategies for sustainable development of the banking sector. In this context, Fig. 2 shows the multi-vector dynamics of the Ukrainian banking sector in 2022-2024, which reflects the process of adaptation to digital transformation and geopolitical challenges.

Fig. 2 shows that during this period, Ukraine's banking sector actively responded to the changes brought about by the digitalization of financial services. The significant growth in online payments, the widespread use of mobile applications, and the increase in the number of internet banking users indicate a fundamental shift in the paradigm of financial interaction. In such circumstances, the architecture of financial security is undergoing significant changes, and the adaptation of security tools is becoming a strategic priority.

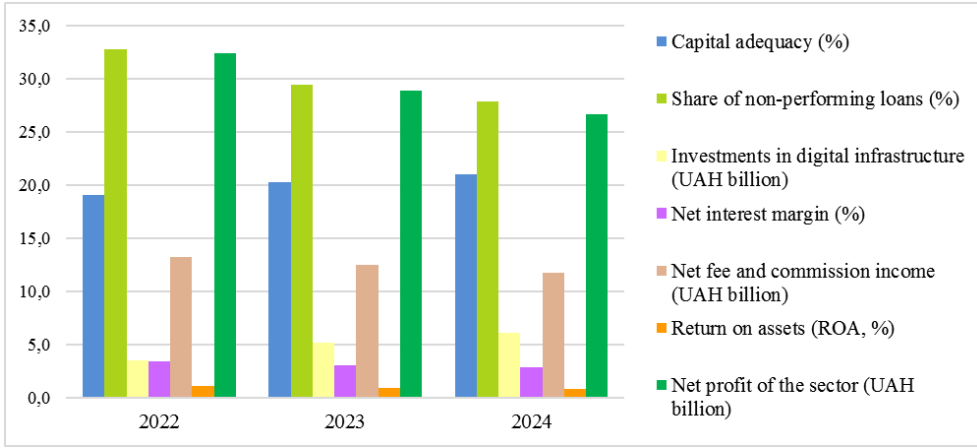

Fig.2. Dynamics of development of the Ukrainian banking sector in the context of transformation and geopolitical challenges in 2022-2024 [10; 15; 20]

Key positive trends that enhance financial security in the digital environment include:

- an increase in capital adequacy from 19.1% in 2022 to 21.0% in 2024, which indicates an increase in bank's resilience to external shocks, in particular due to the NBU's enhanced supervision;
- reduction in the share of non-performing loans from 32.8% to 27.9%, which demonstrates the improvement in the quality of loan portfolios and the introduction of digital risk assessment systems;
- doubling investments in digital infrastructure from UAH 3.5 billion to UAH 6.1 billion, which underscores the strategic importance of cybersecurity for the banking system.

At the same time, digitalization is putting additional pressure on banks' operational efficiency:

- net interest margin decreased from 3.4% to 2.9%, which may be the result of both adaptation to the new monetary policy environment and increased competition from fintech platforms;
- net fee and commission income decreased from UAH 13.2 billion to UAH 11.8 billion, reflecting the impact of economic instability and reduced customer purchasing power;
- return on assets (ROA) decreased from 1.1% to 0.8%, and the banking sector's net profit decreased from UAH 32.4 billion to UAH 26.7 billion.

These figures reflect the growing financial pressure caused by the high costs of implementing and maintaining digital security tools, as well as the overall macroeconomic instability caused by the war.

Thus, ensuring financial security in the digital space today is not just a technical task, but a complex management process that combines targeted investments in security technologies, development of effective business models to maintain profitability, and optimization of operational processes in line with the new challenges of the digital economy.

Investments in digital infrastructure, while necessary to counter new threats, may temporarily reduce bank's profitability. Combined with macroeconomic risks, including martial law, this necessitates balancing cyber defence spending with maintaining financial efficiency.

The intensive digitalization of the banking sector, despite its obvious benefits, inevitably generates qualitatively new and constantly evolving threats to its financial security. These challenges are becoming hybrid in nature, integrating cyber, operational, systemic and regulatory determinants, which makes them difficult to identify and effectively neutralize in advance. Let's look at the key threats that require in-depth research:

1. Escalation of cyber risks. The exponential growth of digital channels of interaction and the integration of the latest technologies are leading to an unprecedented increase in the number and sophistication of cyber threats. The most significant manifestations are:

– unauthorized access: attempts to unlawfully access critical banking systems, confidential customer data or financial transactions by exploiting software vulnerabilities, compromising credentials or using insider information;

– phishing attacks: the use of social engineering techniques to manipulate staff or customers to compromise sensitive financial data by imitating legitimate communications from the bank or other trusted sources;

– ransomware: malicious software that blocks or encrypts critical data and systems, paralyzing the bank's operations and causing significant financial and reputational losses;

– DDoS attacks (Distributed Denial of Service): coordinated distributed attacks aimed at overloading online banking services with abnormal traffic, leading to denial of service and undermining confidence in the banking system.

2. Operational dysfunctions in highly complex IT infrastructures. The rapid integration of heterogeneous technology components – including legacy systems, the latest cloud solutions and microservices architecture – is creating unprecedented complexity in banking IT systems. This increases the likelihood of operational disruptions caused by:

– software defects and incompatibilities: the presence of logical errors or hidden vulnerabilities in the code, as well as compatibility problems between integrated systems, which can lead to failures in transaction processing, generation of incorrect data or leaks of confidential information;

– hardware failures: dysfunctions of key infrastructure elements (servers, network equipment, data storage), which can lead to complete or partial paralysis of critical banking services;

– human factor: errors, negligence or intentional actions (insider fraud) on the part of personnel, which remain a significant source of operational risks in the face of increasing complexity of managing IT infrastructures.

3. Systemic risks driven by the convergence of the financial and technology sectors. The intense integration of traditional banks with innovative fintech companies, the growth of the use of new digital assets, and the expansion of decentralized finance (DeFi) are creating new vectors of systemic risks:

– critical infrastructure interdependence: problems in one technology company that provides key services to several banks can trigger cascading failures throughout the financial sector;

– uncontrolled volatility of new digital assets: the widespread use of cryptocurrencies and other tokenized assets, characterized by high volatility and low transparency, can have a destabilizing effect on financial stability in the absence of adequate mechanisms for managing their risks;

– specific risks of DeFi ecosystems: lack of centralized regulatory oversight, anonymity of participants, potential vulnerabilities in smart contract architecture, and complexity of dispute resolution in decentralized protocols create significant risks for investors and can destabilize the broader financial market.

4. Regulatory lags and their consequences. The speed and dynamics of digital innovations in the financial sector significantly outpace the pace of development and implementation of an adequate regulatory framework. This leads to:

– legal uncertainty: the lack of clear legislation and regulations regarding new technologies (blockchain, DeFi, AI algorithms) creates legal loopholes that can be used for fraud or money laundering;

– limitations of proactive response: regulatory authorities often react to existing problems rather than preventing them from occurring, which limits the ability to effectively counter dynamic innovation threats;

– international divergence of regulatory approaches: significant differences in the regulatory frameworks of digital finance between different jurisdictions can create "regulatory arbitrage" and complicate the fight against cross-border cybercrime.

To comprehensively reflect the mechanisms for adapting and improving financial security in the face of identified threats, key tools, conceptual approaches, and the role of technologies in the regulatory and supervisory environment are comprehensively systematized in Table 2.

Table 2

Adaptation of financial instruments and approaches to ensure the financial security of banks in the digital space [6; 9; 19]

Category	Instrument	Purpose
Adaptation of financial instruments	Artificial intelligence (AI) and machine learning (ML)	Predictive transaction analysis, anomaly and fraud detection, automated risk assessment.
	Distributed ledger technologies (DLT, blockchain)	Ensuring the integrity and immutability of transactional data, increasing cryptographic security.
	Biometric authentication systems	Increase security of access to services and data due to unique biological characteristics of users.
	Cyber insurance tools	Coverage of financial losses from cyberattacks and digital incidents, increasing resilience.
	Platforms for secure data exchange (APIs)	Secure interaction with fintech companies, integration of new services while maintaining information security.

End of table 2

Category	Instrument	Purpose
Conceptual approaches	Security by Design	Integrate security at all stages of the life cycle of tools and services.
	Risk-based approach	Continuous assessment and monitoring of risks, adaptation of tools' functionality to threats.
	The concept of Zero Trust	Verify all access requests, regardless of user/ device location, for enhanced security.
	Integrating cyber resilience and financial stability	Consideration of financial security as a component of overall stability, ensuring business continuity.
The role of technology in regulation and supervision	RegTech (Regulatory Technology)	Compliance automation, AML/CFT monitoring, risk management, regulatory reporting.
	SupTech (Supervisory Technology)	Improved monitoring, analysis and risk management functions by regulators, proactive identification of systemic vulnerabilities.

As can be seen from table 2, ensuring financial security in the digital space requires a comprehensive approach that takes into account both investments in technology and optimization of business processes to maintain profitability.

Thus, effective financial security of banks in the digital space goes beyond purely technical adaptation and improvement. It requires a profound rethinking of risk management strategies, enhanced cooperation with regulators and international partners, and the development of flexible and adaptive mechanisms to respond to the ever-changing landscape of digital threats.

Conclusions from this study and prospects for further research in this area. Based on the analysis of the financial security of banks in the digital space, which is determined by modern challenges and the need to adapt financial instruments, the following key conclusions can be drawn:

1. Digital transformation is changing the banking environment, creating a new, hybrid functional field. The active implementation of innovative technologies – artificial intelligence, distributed ledger technologies (DLT), cloud solutions – is radically transforming the financial security architecture, which requires not only automation but also a fundamental restructuring of approaches in all aspects of banking activities.

2. Modern threats to financial security are multi-vector and hybrid in nature. Cyber risks (unauthorized access, phishing, ransomware, DDoS attacks), operational dysfunctions (software and hardware failures, human factors), systemic risks associated with the convergence of the financial and technology sectors (infrastructure interdependence, volatility of digital assets, DeFi risks), and regulatory lags – all these factors interact and increase the overall level of threats.

3. Effective financial security requires a comprehensive and systemic approach. The use of advanced technologies (AI/ML for data analysis, blockchain for integrity, biometric systems for authentication) combined with the concepts

of Security by Design, Zero Trust and a risk-based approach allows for increased protection of banking systems and processes.

4. Integrating cyber resilience and financial stability is key. Financial security should be an organic part of a customer-centric ecosystem, where ensuring trust through data confidentiality, integrity and availability is a primary goal. In this context, regulatory technology (RegTech) and supervisory technology (SupTech) play a significant role, automating compliance and improving risk monitoring.

5. The experience of the Ukrainian banking sector in 2022–2024 illustrates the dual impact of digitalization and geopolitical challenges. Capital growth, reduction of non-performing loans, and investments in digital infrastructure contribute to increasing bank resilience. At the same time, the reduction in net interest margins and profits against the backdrop of war requires balancing cyber defense and profitability, which poses the task of developing new effective business models.

Promising areas for further exploration are: developing integrated financial strategies that will allow banks to invest in digital infrastructure and cybersecurity as efficiently as possible, optimizing the cost-to-income ratio; modeling the impact of investments in digital technologies on the formation of stable sources of income in a competitive environment, in particular, in the face of FinTech companies; analysis of regulatory instruments and policies that can stimulate capitalization growth, increase the financial resilience of banks, as well as support innovation and ensure the adaptability of the regulatory environment to dynamic digital threats; developing and implementing flexible cooperation mechanisms between banks, regulators and international partners to respond promptly to the transformation of cyber risks and global challenges.

Thus, future research should contribute to the formation of scientifically sound, practically applicable solutions to ensure sustainable, adaptive, and secure digital transformation of the banking sector.

References

1. Atkins, L., Boer, M., Greis, J., & Idler, M. (2023). Cybersecurity in Financial Services: Global Survey. *McKinsey & Company*. https://www.mckinsey.com/ capabilities/risk-and-resilience/our-insights/the-cyber-clock-is-ticking-derisking-emerging-technologies-in-financial-services

2. Banerjee, S., Craig, L., & Greis, J. (2023). The Cyber Clock is Ticking: Derisking Emerging Technologies in Financial Services. *McKinsey & Company*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cyber-clock-is-ticking-derisking-emerging-technologies-in-financial-services

3. Bondarenko, S., & Hubanov, O. (2022). Improving the state system of strategic planning of national security in the context of informatization of society. *Journal of Information Technology Management, 14*, 1–24. https://doi.org/10.22059/jitm.2022. 88861

4. Craig, L., Hao, G., & Idler, M. (2023). Cybersecurity in Financial Services: Survey Insights. *McKinsey & Company*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cyber-clock-is-ticking-derisking-emerging-technologies-in-financial-services

5. Diener, F., & Spacek, M. (2023). Regulatory Lag and the Adoption of FinTech in Europe. *European Journal of Regulation*, *12*(2), 107–120. https://doi.org/10.2139/ssrn.4122067

6. Feher, P., & Varga, K. (2024). Emerging Challenges of Digital Trust in the Financial Sector. *Journal of Financial Services Technology*, *8*(2), 95–112. https://doi.org/10.1177/0972150924120418

7. Garcia, T., Grodzicki, M., & Radulova, P. (2025). Digital Banking: How New Bank Business Models Are Disrupting Traditional Banks. *European Central Bank*. https://www.ecb.europa.eu/press/financial-stability-publications/fsr/focus/2025/html/ ecb.fsrbox202505_04~17b39a3c1a.en.html

8. Hao, G., Banerjee, S., & Boer, M. (2023). Cybersecurity and Financial System Resilience. *McKinsey & Company*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cyber-clock-is-ticking-derisking-emerging-technologies-in-financial-services

9. Khomyshyn, I., & Havts, O. (2023). Cyber Security of the Banking Sector of Ukraine: Concepts, Problems and Experience of Foreign Countries. *Bulletin of Lviv Polytechnic National U-ty. 10*(4), 170–178. https://doi.org/10.23939/law2023.40.170

10. KPMG Ukraine. (2023). Banking Sector Overview. https://home.kpmg/ua/en/home/industries/banking.html

11. Kopylyuk, O., Zhyhar, N., & Petrynyak, A. (2024). Threats to the Financial Security of Ukrainian Banking Institutions under the Conditions of Digitalization. *Economic Journal of Lesya Ukrainka Volyn National University*, *2*(38), 61–68. https://doi.org/10.29038/2786-4618-2024-02-61-68

12. Krysovatyy, A., Desyatnyuk, O., & Ptashchenko, O. (2024). Digital innovations and their ramifications for financial and state security. *African Journal of Applied Research,* 10(1). https://doi.org/10.26437/ajar.v10i1.713

13. Kulalaiev, V. (2022). The Effect of Digital Transformation on Ukrainian Banks' Performance. https://kse.ua/wp-content/uploads/2023/07.pdf

14. Ministry of Finance of Ukraine. (2024). Financial Sector Statistics. https://mof.gov.ua/en

15. National Bank of Ukraine. (2024). Annual Report 2023. https://bank.gov.ua/en/publications

16. Ozarslan, S. (2024). Financial Services Cybersecurity: 2024 Performance in Banking. *Picus Security*. https://www.picussecurity.com/resource/blog/financial-services-cybersecurity-performance-2024

17. Ozarslan, S., & Rubina, A. (2022). Key Threats and Cyber Risks Facing Financial Services and Banking Firms. *Picus Security.* https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

18. Pattni, P. (2024). Digital Banking Transformation: Accelerating into 2024. *FinTech Magazine*. https://fintechmagazine.com/articles/digital-banking-trans formation-accelerating-into-2024

19. Pramanik, H., Kirtania, M., & Pani, A. (2024). Cybersecurity in Banking: A Comparative Study Across Regions. *International Journal of Banking Technology*, *9*(3), 212–230. https://doi.org/10.1016/ijbt.2024.212

20. PwC (2023). Ukrainian Banking Sector: Annual Review. https://www.pwc.com/ua/en/industries/banking.html

21. Vives, X. (2023). Digital Banking and Financial Stability. *Journal of Financial Regulation and Compliance, 31*(1), 48–59. https://doi.org/10.1108/JFRC-11-2022-0092

22. Yehorycheva, S., Hlushko, A., & Khudolii, Y. (2023). Issue of Ukrainian Financial Sector Information Security. *Development Management, 21*(4), 45–52. https://doi.org/10.57111/devt/4.2023.45

FINANCIAL SECURITY OF BANKS IN THE DIGITAL SPACE: CURRENT CHALLENGES AND ADAPTATION OF FINANCIAL INSTRUMENTS

Vitalii V. Zianko, Vinnytsia National Technical University, Vinnytsia (Ukraine).

E-mail: k.zank@gmail.com

Tetiana D. Nechyporenko, Vinnytsia National Technical University, Vinnytsia (Ukraine).

E-mail: sittanya33@gmail.com

https://doi.org/10.32342/3041-2153-2025-2-39-8

Keywords: digitalization, financial innovations, banking technologies, financial stability

JEL classification*: G21, G28, O33*

Introduction. Ensuring the financial security of banks in the digital environment is a key factor in maintaining the stability of the banking sector and overall macro-financial balance in the context of intensive digitalization. The rapid growth of electronic transaction volumes, the introduction of innovative financial technologies (FinTech), and the expansion of virtual ecosystems are transforming traditional approaches to managing banking processes, assets, and information infrastructure. This necessitates a rethinking of the paradigms of asset, data, and operational process protection, as a result of which financial security is viewed not only as a key indicator of the stability of individual banking institutions, but also as a systemic task that determines macrofinancial stability. There is an urgent need for a scientific rethinking of approaches to financial security in the digital space. This involves developing integrated strategies that combine technological solutions, adaptive financial instruments, effective risk management, and regulatory innovations (RegTech, SupTech). Systematic construction of cyber defense architecture, development of analytical platforms based on big data, and strengthening cryptographic information protection mechanisms are key vectors that will contribute to the consolidation of financial security and ensure the sustainable development of banks in a dynamic digital landscape.

Problem Statement. The transition to a dominant role of the digital space in the banking sector is accompanied by an escalation of multi-vector threats – both technical and regulatory. On the one hand, the intensification of the use of cloud computing, artificial intelligence and distributed ledger technologies increases vulnerability to cyber risks, including sophisticated phishing attacks, ransomware and targeted cyberattacks on critical infrastructure. On the other hand, the integration of financial and digital technologies (DeFi, Open Banking) generates new forms of interaction between market entities that do not always fit into the existing regulatory framework. Regulatory lags, the lack of unified cybersecurity standards, and fragmented supervision create the prerequisites for the accumulation of systemic risks.

Purpose. The purpose of the study is a comprehensive analysis of mechanisms for ensuring the financial security of banks in the digital space, taking into account modern challenges and the need to adapt financial instruments in the context of global digital transformation.

Materials and Methods. To achieve the goal, a systematic interdisciplinary approach was applied, combining: empirical methods (observation, comparison, description) – to analyze financial security practices in leading financial systems, as well as to identify global and national trends in the banking sector; theoretical and cognitive approach – to conceptualize financial security in the digital environment, formalize key concepts and test hypotheses regarding the impact of technological innovations on risk management strategies; logical methods (analysis, synthesis, induction, deduction, generalization, scientific abstraction) – to identify methodological problems, risks and opportunities for optimizing financial security in national and global contexts.

Results. The issue of ensuring the financial security of banks in the digital space is investigated, in the context of modern challenges and the need to transform financial instruments. Key threats to the banking sector have been identified and systematized, including cyber risks, technological vulnerabilities, regulatory fragmentation, and risks associated with the integration of financial and digital technologies. It is argued that the spread of innovations such as artificial intelligence, distributed ledger technologies, and cloud computing is shaping a new risk architecture that requires adaptive management and proactive regulation. Threats are identified as being complex and multifactorial, encompassing technical and systemic aspects, including IT infrastructure failures, phishing attacks, ransomware, and regulatory delays. Modern approaches to adapting financial instruments, in particular the integration of RegTech and SupTech, as a means of increasing cyber resilience and ensuring financial stability, are analyzed.

Conclusions. A conceptual model of adapting financial instruments to increase the resilience of banks and counter threats has been proposed. It was emphasized that financial security in the digital economy is a complex problem that requires a systemic approach, continuous updating of tools and strategic vision, opening up opportunities for sustainable development and increasing the competitiveness of banks.

Дата надходження до редакції / Submitted: 19.03.2025
Дата прийняття до публікації / Accepted: 21.08.2025
Дата публікації / Published: 03.11.2025