DOI: 10.55643/fcaptp.5.70.2026.5321

STATE POLICY ON BANKING REGULATION AMID THE DEVELOPMENT OF FINTECH TECHNOLOGIES AND GROWING DIGITAL RISKS TO NATIONAL SECURITY

Mariia Blikhar
Doctor of Legal Sciences, Professor, Head of the Department of Administrative and Informational Law, Lviv Polytechnic National University, Lviv, Ukraine;
e-mail: blikharm@ukr.net
ORCID: 0000-0003-2974-0419
(Corresponding author)

Olha Dilai
Doctor of Legal Sciences, Associate Professor of the Department of Civil Law Disciplines, Lviv State University of Internal Affairs, Lviv, Ukraine;
ORCID: 0000-0003-2872-5567

Zoryana Dobosh
Doctor of Legal Sciences, Associate Professor of the Department of Civil Law and Procedure, Lviv Polytechnic National University, Lviv, Ukraine;
ORCID: 0000-0002-3680-7207

Mariia Vinichuk
Candidate of Economic Sciences, Associate Professor of the Department of National Resistance and Physical Education, Ukrainian National Forestry University, Lviv, Ukraine;
ORCID: 0000-0002-6588-1254

Mariya Havryltsiv
Candidate of Legal Sciences, Associate Professor of the Department of Administrative and Informational Law, Educational and Research Institute of Law, Psychology and Innovative Education, Lviv Polytechnic National University, Lviv, Ukraine;
ORCID: 0000-0002-6735-7181

Received: 20/08/2026
Accepted: 13/10/2026
Published: 31/10/2026

© Copyright
2026 by the author(s)

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

ABSTRACT

The purpose of the study is to examine the transformation of state regulation of banking activities in Ukraine in the context of the development of FinTech technologies and the intensification of digital risks, as well as to substantiate directions for improving the regulatory framework and banking supervision mechanisms, taking into account the requirements of financial stability and national security. The article substantiates that the digital transformation of the financial sector causes the modernization of banking services, contributes to increasing the efficiency of financial intermediation, expands financial inclusion, and ensures the development of innovative business models; however, it generates new challenges for the system of state regulation of banking activities, ensuring financial stability and cybersecurity. The principal trends in the digitalization of banking activities are identified, and the impact of FinTech technologies on the transformation of state regulatory mechanisms in the financial sector is characterized. The performance of Ukraine's major banks — PrivatBank, Oschadbank, and Raiffeisen Bank — during 2022–2025 is analyzed, revealing growing trends toward the digitalization of banking operations, the expansion of remote service channels, an increase in the number of users of digital services, and a strengthening role of financial technologies in ensuring the competitiveness of banking institutions. It is established that, alongside the positive effects of digital transformation, cyber risks, digital fraud, data leakage, technological dependence on external platforms, and other threats affecting national security are increasing. The need to improve state banking regulation is substantiated through the development of RegTech and SupTech technologies, the introduction of risk-based digital supervision, stronger cyber resilience of banking infrastructure, improved digital-risk management mechanisms, and the harmonization of national legislation with European standards of digital financial regulation. It is demonstrated that an effective combination of innovative development in the financial sector and modern mechanisms of state oversight is a necessary prerequisite for ensuring financial stability and protecting national interests in the digital economy.

Keywords: banking activities, state policy, national security, state regulation, FinTech technologies, banking system, digitalization, digital banking, risks, cybersecurity, financial innovation

JEL Classification: G21, G28, O33, K23, E58

INTRODUCTION

In the context of the global digital transformation of the economy, the banking sector is undergoing substantial structural and functional changes associated with the rapid development of FinTech technologies, digital platforms, artificial intelligence, blockchain solutions, Big Data, and innovative payment services. Contemporary financial technologies are reshaping the architecture of financial markets, transforming traditional banking-service mechanisms, and changing the nature of interaction among banks, customers, and public regulators. As a result, banking institutions are compelled to adapt their business models, enhance digital infrastructure, and implement innovative tools for managing financial risks, cybersecurity, and data protection. At the current stage, the

development of the FinTech sector creates new opportunities to improve banking efficiency, financial inclusion, and access to financial services, while simultaneously generating major challenges for state regulation and the institutional framework of the banking sector. The growing role of non-bank financial platforms, digital currencies, virtual assets, and decentralized financial services underscores the need for a modern model of regulatory intervention capable of balancing the promotion of financial innovation with the maintenance of banking-system stability. In this context, particular importance attaches to improving the regulatory and legal framework, developing digital supervisory mechanisms (SupTech), and ensuring the cyber resilience and information security of banking institutions.

Under conditions of military threats, macroeconomic instability, and Ukraine's pursuit of integration into the European financial area, the challenge of establishing effective institutional foundations for banking regulation becomes even more acute and strategically significant. The increasing technological dependence of banking institutions creates a new risk environment in which technical failures, cyberattacks, fraud, information leakage, breaches of confidentiality, and dependence on external technology providers pose threats not only to individual financial institutions but also to the stability of the financial system and the national security of the state. It is evident that the digitalization of the financial sector requires central-bank functions to be adapted, banking supervision to be modernized, and new approaches to financial-risk management in the digital environment to be introduced. At the same time, insufficient regulatory certainty regarding certain FinTech instruments, asymmetry in regulatory requirements applicable to traditional banks and technology companies, and the growth of cyber threats increase risks to the state's financial security and generate significant threats to national security.

The relevance of the research topic is determined by the need to improve the institutional foundations of state regulation of banking activities amid the development of FinTech technologies, to ensure financial stability, to increase the competitiveness of the banking system, and to establish an effective mechanism for adapting the financial sector to the challenges of a digital economy operating under wartime conditions. Accordingly, there is a need for a comprehensive study of current trends in the digitalization of banking and for the identification of directions for improving state policy on banking regulation amid FinTech development and the growth of digital threats to national security.

LITERATURE REVIEW

In the current environment of digital transformation in the financial sector, the formation of effective state policy for regulating banking activities amid the development of FinTech technologies and intensifying digital risks to national security has become particularly relevant. The active introduction of digital financial services, artificial intelligence, blockchain technologies, Big Data, cloud platforms, and digital payment systems is substantially transforming the banking system, creating both new opportunities for financial-market development and additional threats to financial stability, cybersecurity, and national security. Moreover, the rapid spread of FinTech technologies is transforming the traditional model of banking-system operation by changing mechanisms for delivering financial services, approaches to risk-management regulation, and methods of ensuring financial stability. This makes it necessary to consider FinTech both as a technological instrument for enhancing banking efficiency and as a systemic factor in financial-market transformation. Consequently, state regulation of digital banking is increasingly becoming the subject of research in financial law, public administration, banking, and national-security studies.

A foundational contribution to the contemporary understanding of these issues is the study by V. Murinde, E. Rizopoulos, and M. Zachariadis (Murinde et al., 2022), which provides a comprehensive analysis of the impact of FinTech technologies on the future of banking. The authors emphasize the dual nature of FinTech: on the one hand, technological innovation promotes the development of financial services, improves bank efficiency, and broadens access to finance; on the other, it creates new risks that require regulatory policy to adapt. In this context, it is particularly important that the future configuration of the banking sector will be determined not only by technological progress but also by regulatory mechanisms, global financial infrastructure, and geopolitical factors.

The relationship between FinTech development and banks' financial stability remains an important research issue. In this regard, the findings of M. Safiullah and S. R. Paramati (Safiullah and Paramati, 2022) are particularly relevant. They establish that the development of FinTech firms may contribute to stronger bank financial stability because broader technological capabilities, greater efficiency, and improved financial processes can partially mitigate the risks arising from digitalization, while the effect of technological transformation depends to a considerable extent on the institutional and regulatory environment.

DOI: 10.55643/fcaptp.5.70.2026.5321

A significant contribution to the study of the impact of FinTech technologies on the transformation of the financial sector and mechanisms of state regulation was made by D. Arner, J. Barberis, and R. Buckley (Arner et al., 2016), who substantiate that the development of digital financial technologies is giving rise to a new model of financial regulation based on the use of RegTech and SupTech tools, automated monitoring of financial transactions, and digital supervision. The authors emphasize that traditional mechanisms of state control are gradually losing effectiveness as financial markets become digitalized, which requires a reconsideration of the concept of financial regulation and a stronger role for digital technologies in the activities of regulatory authorities. Generally speaking, the risks associated with the digital concentration of financial data also amplify the influence of large technology corporations on the financial sector, underscoring the need to improve mechanisms for government oversight of digital financial platforms.

Further development of this research direction is provided by Q. Ni, L. Zhang, and C. Wu (Ni et al., 2023), who, using data from Chinese commercial banks, demonstrate the nonlinear nature of the impact of FinTech technologies on banking risks. They establish that at the early stages of digital transformation, FinTech development may increase risks, whereas at higher levels of technological development, its effect becomes risk-reducing. Financial regulation performs a moderating role by mitigating the adverse effects of the initial phase of technological adoption. This implies that technological modernization of the banking sector does not by itself guarantee greater stability; an appropriate regulatory infrastructure is also required. A similar view is held by S. Cevik (Cevik, 2024), who examines the impact of FinTech technologies on financial stability and emphasizes that this impact is ambiguous. According to the author, the positive effect depends on the specific type of FinTech instrument and the level of economic development. Digital lending, for example, may create additional stability risks, while digital capital raising may, under certain institutional conditions, exert a stabilizing effect. These findings indicate that FinTech regulation cannot be universal but should take account of the type of technology, the level of risk, and the institutional context in which it is applied.

A different perspective is offered by Y. Zhao and F. Ma (Zhao and Ma, 2025), who focus primarily on the transformation of the financial-regulation system itself. Their empirical analysis of the impact of FinTech development on financial regulation shows that technological progress can increase both the intensity and the effectiveness of regulatory intervention. At the same time, the authors note a potential contradiction between technological innovation and the resilience of the regulatory system: FinTech technologies reduce information asymmetry and expand supervisory capabilities, yet they also generate new types of risk that traditional regulatory mechanisms are not always able to address in a timely manner.

A promising direction for the development of regulatory architecture is the integration of digital technologies with information-protection mechanisms. This approach is actively developed by Y.-S. Ren, C. Ma, and Y. Wang (Ren et al., 2024), who propose a digital-finance regulatory model combining blockchain technology with homomorphic encryption. Their findings demonstrate the potential of technologies that enable regulatory oversight without disclosing confidential

information of financial institutions. This is of fundamental importance for modern state policy because it makes it possible to combine regulatory transparency, protection of banking data, and the technological efficiency of supervision.

The protection of banking data is examined in greater detail by S. Wang, M. Asif, M. F. Shahzad, and M. Ashfaq (Wang et al., 2024), who analyze cybersecurity and privacy challenges arising from the digital transformation of the banking sector. Among the main problems, the authors identify the integration of legacy information systems, evolving compliance requirements, third-party risks, the need for continuous monitoring of cyber threats, and the preservation of customer trust. They also identify information-protection mechanisms that include access control, continuous threat monitoring, data encryption, staff training, and the integration of cybersecurity into the overall corporate-governance framework. Thus, cybersecurity is gradually evolving from a purely technological issue into an element of bank governance and regulatory responsibility.

A distinct strand of recent research addresses the transition from general FinTech risks to specific cyber risks and data-protection risks. This strand is actively developed by D. Javaheri, M. Fahmideh, H. Chizari, P. Lalbakhsh, and J. Hur (Javaheri et al., 2024). The authors develop a taxonomy of cyber threats in FinTech, identify their principal categories, and propose protective measures, thereby demonstrating the complexity and multidimensional nature of digital threats to the financial sector. An important conclusion of their study is that traditional cybersecurity tools do not always correspond to the nature of emerging threats associated with artificial intelligence, automation, the interconnectedness of digital platforms, and dependence on data.

The macro-level relationship between cybersecurity and digital finance is examined by S. Cheng, J. Li, L. Luo, and Y. Zhu (Cheng et al., 2024), who establish that digital finance generates not only economic opportunities but also threats in the form of data leakage, network attacks, and financial fraud. In this context, cybersecurity is treated not merely as a characteristic of an individual financial institution but also as an element of public governance of the financial system and socio-

economic stability. The authors emphasize the particular importance of international coordination because digital financial threats are not confined to the jurisdictional boundaries of a single state.

Other scholars also devote considerable attention to state regulation of digital finance. In particular, S. Naumenkova, V. Mishchenko, and D. Dorofieiev (Naumenkova et al., 2020) examine institutional mechanisms for regulating innovation processes in the banking sector and substantiate the need to improve state policy supporting financial innovation. The authors stress the importance of building a modern regulatory infrastructure, developing digital banking supervision, and adapting national regulatory mechanisms to international standards governing digital financial markets, which is justified and appropriate under contemporary conditions. Research on the development of digital money and the transformation of modern payment systems is likewise important for understanding the digital transformation of the financial sector.

Among Ukrainian scholars, D. Kretov (Kretov, 2024) has also examined state regulation of banking activities, financial-sector digitalization, and national-security issues, focusing on the development of digital banking, modernization of Ukraine's banking system, improvement of financial-monitoring mechanisms, adaptation of national legislation to European standards of digital financial regulation, and ensuring the resilience of the banking system under crisis conditions. N. Davydenko, V. Shepylenko, and M. Davydenko (Davydenko et al., 2025) analyze the current state of the digital transformation of Ukraine's banking system, including the implementation of financial technologies, digital platforms, remote banking, and innovative customer-service models. On this basis, they emphasize that FinTech development requires modernization of state banking-regulation policy, improvement of financial-monitoring mechanisms, and stronger cyber protection of banking institutions. In addition, they examine the digital transformation of the banking system through the lens of financial-security risks and argue that the introduction of digital technologies, blockchain solutions, artificial intelligence, and digital platforms substantially increases banking efficiency while simultaneously generating new threats to the state's information and national security. I. Borshchuk and O. Myshchyshyn (Borshchuk et al., 2023) also pay considerable attention to digital risks, examining the digitalization of business processes in Ukraine's banking sector and substantiating the proposition that the digitalization of banking operations is accompanied by increasing risks of cybercrime, unauthorized access to financial data, and digital fraud, which requires stronger state oversight of the cybersecurity of financial institutions.

A separate research direction concerns the impact of digital technologies on the financial security of the banking system and the national security of the state. L. Kliusko and N. Moskalenko (Kliusko and Moskalenko, 2021) analyze new risks and threats to banks' financial resilience associated with the digitalization of the financial sector and emphasize that the development of digital financial services requires a comprehensive state policy for protecting the information infrastructure of the banking system as a component of the state's economic and national security.

At the same time, the analysis of scholarly publications indicates that the formation of a comprehensive state policy for regulating banking activities amid the development of FinTech technologies and intensifying digital risks to national security remains insufficiently studied. Further scholarly substantiation is also required for mechanisms integrating RegTech and SupTech technologies into the system of state banking supervision, improving the institutional framework for financial-sector cybersecurity, establishing a digital-risk management system, and harmonizing national financial legislation with European Union requirements concerning digital financial services and banking-system cyber resilience. Although some work in this area already exists, it remains relatively limited. In particular, the study by S. Chao, Q. Ran, J. Chen, T. Li, Q. Qian, and D. Ergu (Chao et al., 2022) develops the concept of technology-based financial-sector regulation and examines the potential of RegTech for maintaining financial stability, systematizing the use of artificial intelligence, machine learning, complex-network analysis, knowledge graphs, and other technologies for risk identification and early warning of financial instability. In this context, a fundamentally important direction for contemporary state policy is the transition from traditional reactive supervision to intelligent, preventive, and risk-based regulation capable of identifying potential threats to the financial system in near real time. However, the analysis also revealed a research gap: in most studies, FinTech regulation, banking stability, cybersecurity, and digital risks are treated as separate areas.

At the current stage, there remains a shortage of comprehensive research in which state policy, economic and legal mechanisms of banking regulation, FinTech innovation, digital risks, and national security are considered as an interconnected system. This gap determines the relevance of further research into the economic and legal foundations of state regulation of banking activities under conditions of digital transformation and growing threats to national security. Accordingly, the reviewed literature demonstrates the high relevance of state policy on banking regulation amid FinTech development and intensifying digital risks to national security, as well as the need for further research aimed at improving digital banking-supervision mechanisms, developing the institutional infrastructure of the digital financial market, and ensuring the resilience of Ukraine's banking system in the context of the digitalization of the global economy and the imperative of strengthening national security.

DOI: 10.55643/fcaptp.5.70.2026.5321

AIMS AND OBJECTIVES

The purpose of this article is to examine the transformation of government regulation of banking activities in Ukraine amid the development of FinTech technologies and the rise of digital risks, as well as to propose ways to improve the regulatory framework and banking supervision mechanisms, taking into account the requirements of financial stability and national security. To achieve this purpose, the following main objectives were defined:

1. To examine the theoretical, methodological, economic, and legal foundations of state regulation of banking activities amid the development of FinTech technologies by systematizing contemporary scholarly approaches to the regulation of digital financial services, Open Banking, and RegTech in the banking sector.
2. To analyze the current state of public regulation of banking activities and identify the principal digital risks arising from FinTech development, assessing their impact on financial stability, cyber resilience, and national security.
3. To substantiate priority directions for improving state policy, the economic and legal mechanisms of banking regulation aimed at maintaining a balance between promoting FinTech innovation, protecting financial data, managing digital and cyber risks, and strengthening national security.

METHODS

The methodological framework of the study is based on systems, institutional, risk-based, and process approaches to state regulation of banking activities in the context of the digital transformation of the financial sector. The systems approach made it possible to consider banking activities, FinTech technologies, digital infrastructure, state-regulatory mechanisms, financial stability, and national security as interrelated elements of a single system. The institutional approach was used to examine the roles of the National Bank of Ukraine, public authorities, banking institutions, and FinTech companies in shaping the contemporary regulatory environment. A combination of general scientific and specialized research methods was employed to achieve the research purpose and objectives.

Analysis and synthesis were used to systematize scholarly approaches to defining the nature of FinTech, the digital transformation of banking, Open Banking, RegTech, and SupTech, and to summarize approaches to managing digital and cyber risks. Scientific abstraction was applied to identify the key characteristics of the contemporary mechanism of state regulation of banking activities and to determine the relationship among digital innovation, financial stability, and national security. The comparative method was used to compare approaches to regulating digital financial services, including the development of Open Banking, protection of financial data, cyber resilience, regulation of technology providers, and the use of digital instruments in banking supervision. This made it possible to identify directions for implementing modern regulatory practices while taking into account the specific features of Ukraine's financial sector under military and digital risks. The statistical method was used to analyze the dynamics of the principal indicators of banking-sector development and the digitalization of banking services, including the volume and number of cashless transactions, the degree of digital use of payment instruments, banks' assets, and financial results. On this basis, absolute and relative changes in the indicators under study were determined, allowing the scale of the digital transformation of banking activities to be assessed. Graphical and tabular methods were employed to visualize indicator dynamics, systematize regulatory and legal provisions, and structure the main digital risks of banking activities. Their application enhanced the clarity of the findings and enabled a comprehensive comparison of individual characteristics of the banking sector's digital transformation. The legal-regulatory method was used to examine the economic and legal foundations of state regulation of banking activities, requirements concerning payment services, information and personal data protection, cybersecurity, digital identification, and the functioning of Open Banking, as well as to identify regulatory gaps and determine directions for further improvement in the context of FinTech development. The method of expert generalization was used to systematize contemporary scholarly positions regarding the impact of FinTech technologies on financial stability and banking risks and to formulate substantiated proposals for improving state policy. In developing the recommendations, the study took into account the findings of recent academic research, international regulatory practices, and official materials of central public authorities and financial-sector regulators.

The information base of the study comprised scholarly publications on FinTech, the digital transformation of banking activities, financial stability, cybersecurity, and state regulation; official statistical and analytical materials of the National Bank of Ukraine and other competent public institutions; and materials of commercial banks and regulatory bodies. To ensure the reliability of the results, preference was given to official statistical data, regulatory documents, and peer-reviewed academic sources. The integrated application of the methods described above ensured methodological consistency and made it possible to move from analyzing the current state of banking regulation to substantiating priority

directions for improving the economic and legal regulatory mechanism, oriented toward the simultaneous promotion of FinTech innovation, protection of financial data, enhancement of the banking system's cyber resilience, and strengthening of national security.

RESULTS

The ongoing transformation of banking activities driven by FinTech technologies is accompanied by both the expansion of banks' digital capabilities and increasing requirements for their financial, technological, and cyber resilience. Under these conditions, state regulation assumes particular importance, as it must ensure not only the stability of banking activities but also an adequate level of protection of digital infrastructure, customer data, and the continuity of financial services.

The regulatory and legal framework governing banking activities in Ukraine is primarily based on the Law of Ukraine "On the National Bank of Ukraine" (On the National Bank of Ukraine, 1999), the Law of Ukraine "On Banks and Banking Activity" (On Banks and Banking Activity, 2000), the Law of Ukraine "On Payment Services" (On Payment Services, 2021), legislation in the fields of financial monitoring and cybersecurity, as well as regulatory acts adopted by the National Bank of Ukraine. In the context of digitalisation, regulatory requirements concerning risk management, information security, cybersecurity, remote customer identification, payment services, and the operational continuity of banks' information systems are becoming increasingly important.

Particular significance under current conditions is attached to the activities of the National Bank of Ukraine, which combines the functions of banking regulation and supervision, macroprudential policy, payment market regulation, oversight of risk management, and the establishment of requirements for information security and cybersecurity. As a result of the digital transformation of banking activities, traditional regulatory instruments are being supplemented by requirements relating to information protection, cyber resilience, the security of remote banking operations, technology risk management, the use of third-party technology service providers, and the operation of Open Banking.

For the purposes of this study, state policy on banking regulation is understood as a system of interrelated legal, institutional, prudential, supervisory, organisational, and technological measures implemented by the state with the aim of ensuring the stability of the banking sector, protecting the rights of financial services consumers, maintaining the continuity of banking activities, mitigating systemic risks, and safeguarding national financial interests.

It is therefore evident that contemporary state policy on banking regulation is being shaped at the intersection of four interrelated areas:

1. Financial regulation – ensuring adequate capital, liquidity, solvency, and the overall financial resilience of banks.
2. Prudential and risk-based supervision – identifying, assessing, and mitigating financial, operational, and systemic risks.
3. Digital and technological regulation – establishing requirements for payment services, Open Banking, authentication, information security, and digital infrastructure.
4. Regulation of digital resilience and security – ensuring cybersecurity, the continuity of critical banking services, data protection, and resilience to technological disruptions.

The integration of these areas constitutes the contemporary model of state policy on banking regulation in the context of FinTech-driven transformation. Accordingly, the principal regulatory instruments of state policy governing digital banking activities in Ukraine may be summarised in Table 1.

The regulatory instruments outlined above demonstrate that state policy on banking regulation is gradually shifting from predominantly financial control towards comprehensive risk-based regulation encompassing financial, technological, information, and operational dimensions. Importantly, each of these instruments performs a distinct function within the overall framework of state policy. Legislation governing payment services establishes the legal environment for digital payments; risk management requirements ensure the institutional integration of relevant risks into banks' risk management systems; cybersecurity regulation sets requirements for the protection of information systems; authentication regulation enhances the security of remote transactions; while the implementation of Open Banking establishes a new model of interaction among banks, payment institutions, and financial services users.

DOI: 10.55643/fcaptp.5.70.2026.5321

Table 1. Key regulatory instruments of state policy for digital banking regulation in Ukraine. *(Source: On Payment Services, 2021; On Approval of the Regulation on the Organization of the Risk Management System in Ukrainian Banks and Banking Groups, 2018; On Approval of the Regulation on Information Protection and Cybersecurity by Payment Market Participants, 2021; On Approval of the Regulation on Authentication and the Use of Strong Authentication in the Payment Market, 2023; On Approval of the Regulation on Open Banking in Ukraine 2025; On Amendments to Certain Regulatory and Legal Acts of the National Bank of Ukraine, 2025)*

No.	Regulatory Instrument	Area of State Regulation	Key Provisions	Impact on Banking Activities
1	Law of Ukraine No. 1591-IX "On Payment Services"	Payment services and digital financial infrastructure	Establishes the modern legal framework for the functioning of the payment market and the provision of digital payment services	Requires banks to adapt their payment infrastructure, internal procedures, and digital products
2	NBU Resolution No. 64 of 11 June 2018	Risk management	Establishes requirements for the organisation of risk management systems in banks and banking groups	Ensures that operational, technological, and other risks are integrated into banks' risk management systems
3	NBU Resolution No. 43 of 19 May 2021	Information security and cybersecurity	Establishes requirements for information security and cybersecurity applicable to payment market participants	Strengthens organisational and technological requirements governing digital operations
4	NBU Resolution No. 58 of 3 May 2023	Authentication	Regulates authentication and strong customer authentication requirements	Enhances the security of remote payment transactions and the protection of customer data
5	NBU Resolution No. 80 of 25 July 2025	Open Banking	Establishes the organisational and technological framework for Open Banking, including API-based interaction and user consent management	Introduces new requirements for secure data exchange and the integration of banking systems
6	NBU Resolution No. 52 of 6 May 2025	Recovery planning	Enhances the requirements for recovery plans applicable to systemically important and other banks	Strengthens banks' capacity to maintain business continuity and restore critical functions

Furthermore, state regulation of banking activities in the context of FinTech development is implemented through a combination of legal, prudential, supervisory, organisational, and technological instruments aimed not only at maintaining banks' financial resilience, but also at mitigating digital and cyber risks, ensuring information security, and maintaining the continuity of critical banking services. The principal instruments of such regulation include:

- legal and regulatory governance of banking activities and digital financial services;
- prudential regulation, including capital, liquidity, and risk management requirements;
- banking supervision and risk-based supervision;
- regulation of information security and cybersecurity;
- requirements concerning internal control systems and risk management;
- regulation of payment services and remote customer service;
- customer identification and verification requirements;
- monitoring of cyber incidents and ensuring interaction between banks and the regulator in the field of cybersecurity.

A distinctive feature of the current stage of development is the gradual integration of traditional banking supervision with technological instruments such as SupTech and RegTech. This enables the regulator to identify risks more promptly, while allowing banks to automate compliance with regulatory requirements and enhance the effectiveness of control over digital operations.

It therefore becomes evident that state regulation of banking activities in the context of FinTech development should be understood as a comprehensive process in which regulatory requirements are combined with prudential, supervisory, and technological instruments designed to ensure the financial and digital resilience of banks.

In recent years, the development of FinTech technologies in Ukraine's banking sector has been accompanied by the active digital transformation of financial institutions, the introduction of innovative banking services, remote service channels, digital payment instruments, and automated financial-risk management systems. At the same time, during 2022–2025, the Ukrainian banking system operated under the special legal regime of martial law, conditions of high macroeconomic uncertainty, cyber threats, and structural transformation of the financial market. Under these circumstances, institutional

mechanisms of state regulation of banking activities aimed at ensuring financial stability, supporting the digitalization of banking services, and facilitating banks' adaptation to new technological challenges acquired particular importance.

The analysis of Ukraine's banking sector demonstrates a substantial structural transformation during 2022–2025, as evidenced by empirical research conducted at three interrelated levels: the banking sector as a whole, groups of banks classified by ownership structure, and individual banks selected for in-depth analysis with due regard to their ownership structure and systemic importance.

Current practice of the National Bank of Ukraine applies a specific classification of banks (Table 2), according to which banks are divided into state-owned banks, banks belonging to foreign banking groups, and privately owned banks, while the status of PrivatBank as a systemically important bank constitutes a separate characteristic. Accordingly, PrivatBank should be considered separately, since its scale and role within the state-owned banking sector differ substantially from those of other state-owned banks.

Table 2. Classification of banks in Ukraine.

No.	Bank Group	Banks Included in the Group
1	State-owned banks	PrivatBank, Oschadbank, Ukreximbank, Ukrgasbank, Sense Bank
2	Foreign-owned banks	Raiffeisen Bank, Ukrsibbank, OTP Bank, Crédit Agricole Bank
3	Privately owned banks	FUIB, TASCOMBANK, Universal Bank, Bank Pivdenny

In its 2025 Banking Sector Review, the National Bank of Ukraine reports a substantial increase in the assets of all three banking groups. In particular, during 2022–2025, the assets of state-owned banks excluding PrivatBank increased from UAH 638 billion to UAH 1,178 billion, while PrivatBank's assets rose from UAH 550 billion to UAH 904 billion. The assets of banks belonging to foreign banking groups increased from UAH 694 billion to UAH 1,000 billion, whereas those of privately owned banks grew from UAH 470 billion to UAH 919 billion. The total assets of the banking sector increased from UAH 2,352 billion to UAH 4,001 billion (Table 3).

In view of these developments, there is a need to examine the structural changes in Ukraine's banking sector during 2022–2025. Such an approach makes it possible to avoid equating the performance of individual banks with the characteristics of the banking system as a whole and ensures that differences among banks in terms of ownership structure, scale of operations, and systemic importance are properly taken into account.

Table 3. Dynamics of net assets of Ukrainian banks by ownership group in 2022–2025, UAH billion. *(Source: Overview of Ukraine's Banking Sector, 2022–2025; Financial Stability Report, 2022–2025; Banking Sector Statistics, 2022–2025)*

No.	Bank Group	2022	2023	2024	2025	Change, 2022–2025
1	State-owned banks, excluding JSC CB PrivatBank	638	892	1,046	1,178	+84.6%
2	JSC CB PrivatBank	550	687	772	904	+64.4%
3	Banks belonging to foreign banking groups	694	764	885	1,000	+44.1%
4	Privately owned banks	470	603	712	919	+95.5%
5	Total banking sector	2,352	2,945	3,415	4,001	+70.1%

According to the National Bank of Ukraine, the total assets of the banking sector increased from UAH 2,352 billion in 2022 to UAH 4,001 billion in 2025, representing growth of 70.1%. At the same time, the dynamics varied considerably across individual groups of banks. The assets of state-owned banks excluding PrivatBank increased from UAH 638 billion to UAH 1,178 billion, or by 84.6%. PrivatBank's assets rose from UAH 550 billion to UAH 904 billion, or by 64.4%. The assets of banks belonging to foreign banking groups increased from UAH 694 billion to UAH 1,000 billion, or by 44.1%, whereas the assets of privately owned banks grew from UAH 470 billion to UAH 919 billion, or by 95.5%. Thus, the largest absolute increase in assets over the period under review was recorded in the state-owned banking segment and PrivatBank, while the highest relative growth rate was observed among privately owned banks. This confirms the structural heterogeneity of the banking sector and highlights the need for a differentiated regulatory approach.

According to the National Bank of Ukraine, the net assets of the banking sector increased from UAH 2,352 billion in 2022 to UAH 4,001 billion in 2025, representing an increase of 70.1%. The data presented indicate that privately owned banks demonstrated the highest relative increase in net assets during 2022–2025, at 95.5%. Meanwhile, the net assets of state-

DOI: 10.55643/fcaptp.5.70.2026.5321

owned banks excluding JSC CB PrivatBank increased by 84.6%, those of JSC CB PrivatBank by 64.4%, and those of banks belonging to foreign banking groups by 44.1%. These developments indicate changes in the structure of the banking sector: the share of privately owned banks increased from approximately 20.0% in 2022 to 23.0% in 2025, while the share of state-owned banks excluding JSC CB PrivatBank rose from 27.1% to 29.4%. By contrast, the share of banks belonging to foreign banking groups declined from 29.5% to 25.0%, while the share of JSC CB PrivatBank changed from 23.4% to 22.6%.

It should also be noted that the NBU applies a special supervisory regime to systemically important banks, which entails enhanced requirements for risk management, capital, liquidity, and recovery planning. Systemic importance therefore constitutes an additional significant criterion of state regulatory policy. As of 1 January 2025, the NBU had designated 15 banks as systemically important. This category includes institutions with different ownership structures, demonstrating the need to distinguish between the concepts of "ownership structure" and "systemic importance."

This distinction is particularly important for state policy on the regulation of digital risks. A disruption in the operations of a systemically important bank or its critical digital infrastructure may potentially have broader consequences for financial sector stability than a comparable disruption affecting an institution of lower systemic importance. Consequently, state regulation of digital resilience should take into account not only a bank's legal status or ownership structure, but also the scale of its operations, transaction volumes, number of customers, criticality of its digital infrastructure, technological dependencies, and the potential systemic effects of operational disruptions.

In this context, regulatory impact should be considered on the basis of two interrelated criteria: a bank's affiliation with a particular structural group and its systemic importance. This approach makes it possible to develop a differentiated model of state regulation. For systemically important banks, priority should be given to requirements relating to capital, liquidity, recovery planning, operational continuity, and the management of systemic digital risks. For large banks that make extensive use of digital platforms, particular emphasis should be placed on cybersecurity requirements and the management of IT and other technology-related risks. For smaller banks, regulatory proportionality is particularly important in order to ensure that higher levels of digital security do not impose a disproportionate administrative and financial burden.

The findings have significant regulatory implications, as the growth of assets across all groups of banks indicates that the Ukrainian banking sector maintained its functional capacity under martial law. At the same time, differences in the pace of structural change confirm the need to take into account the scale and nature of banks' activities when establishing regulatory requirements. Moreover, the increase in assets cannot in itself be regarded as direct evidence of the positive impact of FinTech technologies, since asset dynamics are simultaneously influenced by macroeconomic, monetary, credit, fiscal, and war-related factors.

The study demonstrates that the current system of state regulation of banking activities in Ukraine already incorporates a range of specific instruments directly related to the digitalisation of financial services. These include the Law of Ukraine "On Payment Services", which establishes the legal framework for the functioning of the modern payment market; NBU Board Resolution No. 64 of 11 June 2018 "On Approval of the Regulation on the Organisation of the Risk Management System in Ukrainian Banks and Banking Groups"; NBU Board Resolution No. 43 of 19 May 2021, which regulates information security and cybersecurity requirements for payment market participants; NBU Board Resolution No. 58 of 3 May 2023, which establishes requirements for authentication and strong customer authentication; NBU Board Resolution No. 80 of 25 July 2025 "On Approval of the Regulation on Open Banking in Ukraine"; as well as regulatory amendments introduced by the NBU concerning bank recovery plans and the enhancement of banks' operational resilience.

Accordingly, regulatory influence on digital banking activities is exercised not through a single universal instrument, but through a set of interconnected requirements relating to risk management, information security, authentication, payment services, Open Banking, and business continuity.

It is therefore evident that the financial performance of the banking sector should not be analysed in isolation from the regulatory environment, but rather in the broader context of changes in capital, liquidity, credit risk, and asset quality. One significant development has been the substantial decline in the share of non-performing loans (NPLs), which, according to NBU data, amounted to 13.9% of the banking sector's loan portfolio at the end of 2025, the lowest level recorded in more than 15 years. This indicator also declined significantly among state-owned banks, although it remained higher than in some other groups of banks. This development indicates an improvement in loan portfolio quality; however, it should not be directly attributed to digitalisation. Rather, it should be viewed as the result of the combined effects of loan restructuring, write-offs of distressed debt, changes in the structure of lending, economic conditions, and regulatory requirements.

To ensure the representativeness of the study of state regulation of banking activities, the sample is not limited to the three largest banks. Nevertheless, PrivatBank, Oschadbank, and Raiffeisen Bank provide an appropriate basis for a more detailed analysis of financial performance, digital transformation, and banks' responses to regulatory requirements. Such an analysis makes it possible to examine the specific features of individual banks' adaptation to the development of FinTech technologies and the intensification of digital risks.

Accordingly, findings relating to individual banks are not equated with the characteristics of the banking system as a whole. Recommendations for improving state regulation are therefore formulated with due regard to differences among groups of banks in terms of their scale of operations, level of digitalisation, resource capacity, and the nature of the digital risks they face.

To assess current trends in banking development amid the spread of FinTech technologies, it is appropriate to analyze the performance of Ukraine's leading banks, which demonstrate a high level of digital transformation and the implementation of innovative financial services: PrivatBank, Oschadbank, and Raiffeisen Bank. During 2022–2025, these banks actively expanded digital channels of customer interaction, introduced mobile-banking platforms, electronic-identification systems, digital payment services, and remote-banking technologies. Mobile applications, Big Data, automated transaction-monitoring systems, and elements of artificial intelligence used in financial analysis and risk management played a particularly important role in the development of digital banking at the institutions analyzed. Table 1 summarizes the principal financial results of PrivatBank, Oschadbank, and Raiffeisen Bank for 2022–2025.

Table 1. Financial performance of PrivatBank, Oschadbank, and Raiffeisen Bank in Ukraine, 2022–2025. *(Source: Overview of Ukraine's Banking Sector, 2022–2025; Financial Stability Report, 2022–2025; Banking sector statistics, 2022–2025; Annual Report of JSC CB "PrivatBank" for 2022; Annual Report of JSC CB "PrivatBank" for 2023; Financial statements and corporate information, 2022–2025; Oschadbank Annual Report for 2022; Annual financial statements and activity reports, 2022–2025; Raiffeisen Bank JSC Annual Report for 2022; Raiffeisen Bank JSC Annual Report for 2023; JSC Raiffeisen Bank. Annual financial statements and corporate information, 2022–2025)*

No.	Indicator	Years			
		2022	2023	2024	2025
PrivatBank					
1.	Net profit, UAH billion	30,25	37,8	40,1	29,1
2.	Share of digital transactions, %	78	84	89	92
3.	Number of mobile-banking users, million persons	13,5	15,1	16,3	17,4
Oschadbank					
1.	Net profit, UAH billion	0,69	4,8	8,6	10,2
2.	Share of digital transactions, %	52	61	69	75
3.	Number of online-banking users, million persons	3,8	4,5	5,2	5,9
Raiffeisen Bank					
1.	Net profit, UAH billion	1,5	5,4	7,2	8,1
2.	Share of digital transactions, %	67	74	81	86
3.	Number of active digital customers, million persons	2,9	3,4	3,9	4,3

The analysis indicates that PrivatBank recorded the highest level of digitalization among the banks examined and effectively serves as a leader in digital banking in Ukraine. Despite the difficult operating environment under martial law, the bank maintained consistently strong financial results, remained profitable, and continued the large-scale implementation of digital financial services. The increase in the share of digital transactions to 92% in 2025 indicates a high level of customer adaptation to digital banking services and the effectiveness of the bank's institutional model of digital management.

An important trend has been the active implementation of FinTech solutions in state-owned banks. In particular, during the period analyzed, Oschadbank significantly strengthened remote banking, digital payment services, and electronic customer identification. This enabled the bank to substantially increase the share of digital transactions and to achieve a gradual rise in profitability even under heightened wartime risks.

Raiffeisen Bank likewise demonstrates a high degree of adaptability to digital change by actively introducing innovative payment technologies, electronic document management, digital credit products, and automated systems for analyzing customer transactions. The growing number of digital customers and improved financial indicators demonstrate the effectiveness of integrating FinTech technologies into the bank's operations.

DOI: 10.55643/fcaptp.5.70.2026.5321

An important element of state regulation of digital risks is the Regulation on the Organisation of Cybersecurity in the Banking System of Ukraine, approved by Resolution No. 178 of the Board of the National Bank of Ukraine dated 12 August 2022. This regulatory act establishes the organisational framework for cybersecurity in banks, mechanisms of interaction with the NBU Cybersecurity Centre and CSIRT-NBU, as well as requirements aimed at countering cyber threats.

Another significant regulatory instrument is the Regulation on the Organisation of the Risk Management System in Ukrainian Banks and Banking Groups, approved by Resolution No. 64 of the Board of the National Bank of Ukraine dated 11 June 2018. Its provisions establish the organisational framework for the identification, assessment, monitoring, control, and mitigation of material risks arising from banking activities.

Thus, the regulatory influence of the NBU on banks extends beyond the establishment of financial prudential requirements and also encompasses mandatory requirements relating to risk management, information security, and cybersecurity. This directly affects banks' organisational costs, the structure of their internal control systems, technological infrastructure, and their capacity to ensure the continuity of financial services.

A significant influence on the transformation of banking activities has been exerted by the strengthening regulatory role of the National Bank of Ukraine in the digitalization of the financial sector. The regulator introduced a number of digital-supervision mechanisms and tightened requirements concerning cybersecurity, digital customer identification, personal-data protection, and the monitoring of financial transactions. At the same time, the development of FinTech technologies has increased the need to improve the regulatory and legal framework governing digital banking and non-bank financial platforms. Table 2 systematizes the results of assessing the impact of FinTech technologies on the activities of Ukrainian banks during 2022–2025.

Table 2. The impact of fintech technologies on the activities of Ukrainian banks in 2022–2025. *(Source: Overview of Ukraine's Banking Sector, 2022–2025; Financial Stability Report, 2022–2025; Banking sector statistics, 2022–2025; Annual Report of JSC CB "PrivatBank" for 2022; Annual Report of JSC CB "PrivatBank" for 2023; Financial statements and corporate information, 2022–2025; Oschadbank Annual Report for 2022; Annual financial statements and activity reports, 2022–2025; Raiffeisen Bank JSC Annual Report for 2022; Raiffeisen Bank JSC Annual Report for 2023; JSC Raiffeisen Bank. Annual financial statements and corporate information, 2022–2025)*

No.	Area of impact	PrivatBank	Oschadbank	Raiffeisen Bank
1.	Development of mobile banking	High	Medium	High
2.	Use of AI and Big Data	High	Low	Medium
3.	Automation of financial operations	High	Medium	High
4.	Level of digitalization of customer services	High	Medium	High
5.	Development of contactless payments	High	High	High
6.	Cyber resilience and digital protection	High	Medium	High
7.	Integration of FinTech services	High	Medium	High

The findings indicate that the development of FinTech technologies has contributed to the substantial modernisation of Ukrainian banks' activities, enhanced financial inclusion, optimised banking operations, and expanded public access to digital financial services. At the same time, the increasing digitalisation of the banks analysed has been accompanied by growing cyber risks, highlighting the need to improve digital supervision mechanisms and adapt the institutional framework of state regulation to the emerging challenges of the digital economy.

To ensure the validity and comparability of the assessment, the study applies an author-developed scale for evaluating the level of digital and regulatory impact. The assessment is based on a set of criteria reflecting the intensity of digitalisation of banking activities, the scale of FinTech adoption, the degree of dependence on digital infrastructure, and the significance of requirements related to the management of digital and cyber risks. Each criterion is assigned a score ranging from 0 to 3, where 0 indicates the absence or minimal manifestation of the respective characteristic; 1 represents a low level; 2 corresponds to a medium level; and 3 indicates a high level. The composite indicator is calculated as the arithmetic mean of the scores assigned across all criteria.

The following ranges are used to interpret the results: 0.00–1.00 – low level; 1.01–2.00 – medium level; and 2.01–3.00 – high level. The thresholds of the scale were developed by the author and are used exclusively to ensure internal comparability among the banks included in the study. The resulting scores do not constitute regulatory assessments by the National Bank of Ukraine and should not be equated with the findings of official banking supervision. Rather, they represent the results of the author's analytical assessment based on publicly available information disclosed by banks, NBU regulatory documents, and available indicators of digital banking activity.

An analysis of the regulatory framework and the current structure of banking activities makes it possible to identify five principal categories of digital risks: (1) cyber risks – unauthorised access, cyberattacks, and disruptions to information systems; (2) data protection risks – leakage, misuse, or compromise of financial and personal information; (3) technology risks – failures of software, infrastructure, networks, and critical information systems; (4) third-party risks – banks' dependence on cloud services, technology providers, external platforms, and other IT service providers; and (5) business continuity risks – the inability to restore critical banking services in a timely manner following technical, cyber, or physical disruptions.

Importantly, these risks cannot be regarded solely as technological problems affecting individual banks. Their systemic nature emerges when disruptions to digital infrastructure have the potential to simultaneously affect a significant number of customers, banks, payment services, or critical financial operations. Accordingly, state regulation should be aimed not only at protecting individual banking institutions, but also at ensuring the continuity and resilience of critical financial services.

In view of the above, it is appropriate to implement strategic directions for improving state policy in the field of banking regulation, which, within the framework of this study, is understood as a set of legal, regulatory, supervisory, and organisational measures undertaken by the state to ensure financial stability, protect the rights of financial services users, strengthen cybersecurity, and enhance the resilience of the banking system.

The National Bank of Ukraine is the central authority responsible for implementing the regulatory and supervisory components of this policy. The Verkhovna Rada of Ukraine establishes the legislative framework for banking regulation, while other public authorities participate in the implementation of specific policy areas in accordance with the powers assigned to them by law.

The recommendations of international organisations, including the International Monetary Fund (IMF), are considered in this study not as instruments of Ukraine's state policy, but as external factors and reference points for its further improvement.

The principal directions of such policy may be summarised as follows in Figure 1.

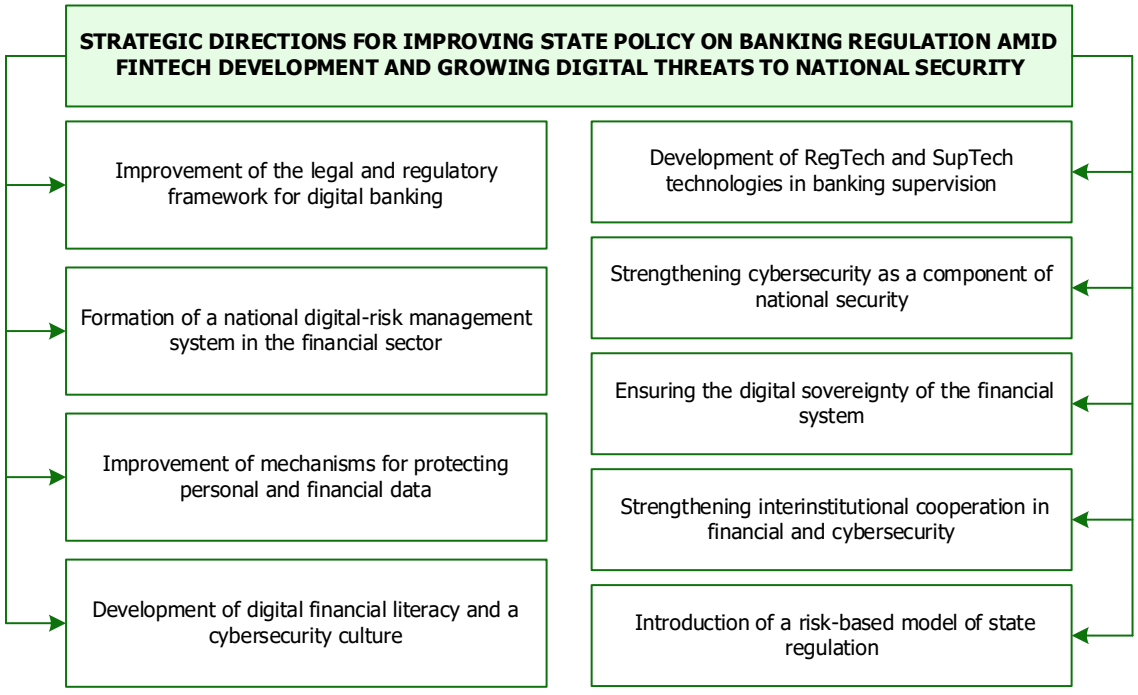


Figure 1. Main directions of state policy for regulating banking activities.

It is evident that a primary task in improving state policy for regulating banking activities amid FinTech development and growing digital threats to national security is the harmonization of national legislation with European Union legislation in the areas of digital financial services, Open Banking, digital operational resilience, and cybersecurity. The European dimension of improving state regulation of banking activities should be pursued not through general declarations of "legislative harmonisation", but through the gradual alignment of specific regulatory requirements in the areas of digital financial services, cybersecurity, operational resilience, and financial data exchange.

DOI: 10.55643/fcaptp.5.70.2026.5321

In particular, one of the key directions is the approximation of the regulatory framework for digital financial services and Open Banking to European requirements. This involves defining the legal conditions governing third-party access to payment information, user authentication mechanisms, the liability of participants in digital interactions, and the protection of consumer rights.

Another important direction is the strengthening of requirements for banks' digital operational resilience. In this regard, it is appropriate to take into account the provisions of the Digital Operational Resilience Act (DORA), particularly those concerning ICT risk management, resilience testing of information systems, reporting of major ICT-related incidents, and the management of risks associated with critical technology service providers.

A third direction involves aligning cybersecurity requirements with European approaches, particularly with regard to cyber risk management, incident response, business continuity, and cooperation between financial institutions and the relevant cybersecurity authorities.

Another area of improvement concerns the alignment of regulatory approaches to digital assets and the risks associated with them. At the same time, the provisions of MiCA should be regarded not as a regulatory act directly governing the activities of Ukrainian banks, but as a European reference framework for shaping the national regulatory environment in the field of digital assets.

Thus, harmonisation should involve the specification and gradual alignment of national requirements relating to ICT risk management, cybersecurity, digital payment services, data access, and operational resilience, rather than being limited to a general reference to the need to adapt national legislation to European Union standards.

Considerable attention should also be paid to increasing the effectiveness of state regulation, which requires the active introduction of digital technologies into the activities of regulatory authorities. In this context, it is advisable to establish an integrated digital platform for banking-sector supervision using artificial intelligence, machine learning, and Big Data technologies to automate risk monitoring, identify suspicious financial transactions, and forecast crisis developments in the banking system. Another important direction is the creation of a comprehensive system for identifying, assessing, and monitoring digital risks in banking. Such a system should cover cyber threats, data leakage, digital fraud, technological failures, dependence on cloud services, and risks associated with the use of artificial intelligence and digital platforms. Accordingly, common standards for assessing the digital resilience of banking institutions should be introduced.

As the number of cyberattacks on the financial sector increases, requirements concerning the cyber resilience of banking infrastructure need to be strengthened. This entails establishing a system of continuous cybersecurity audits, mandatory cyber stress testing of banks, improving mechanisms for responding to cyber incidents, and expanding cooperation among banks, the National Bank of Ukraine, the State Service of Special Communications and Information Protection of Ukraine, and security and defense-sector entities. The growing volume of digital financial transactions also heightens the need to strengthen protection of bank customers' personal data. State policy should provide for modern digital-identification mechanisms, multi-layered information protection, cryptographic technologies, and greater liability for breaches of information-security requirements. In view of intensifying geopolitical challenges and military threats, another important direction of state policy is to reduce the banking sector's dependence on foreign digital platforms, software, and cloud infrastructure. It is therefore advisable to promote the development of national digital solutions, data centers, and critical financial infrastructure, thereby strengthening the state's digital sovereignty.

At the same time, effective digital-risk management requires systematic interaction among the National Bank of Ukraine, the Ministry of Digital Transformation of Ukraine, the National Securities and Stock Market Commission, law-enforcement agencies, cybersecurity entities, and FinTech companies. Such cooperation should focus on exchanging information about cyber threats, coordinating response measures, and developing a unified digital-security policy for the financial sector.

An important element of state policy should be improving the digital financial literacy of the population and banking-sector employees. Educational programs on the safe use of digital financial services can reduce the risks of digital fraud and increase trust in financial innovation. Further development of the banking system requires a transition from a predominantly control-oriented model to a proactive, risk-based model of state regulation involving continuous monitoring of digital threats, risk forecasting, the use of AI-based analytical platforms, and timely adjustment of regulatory mechanisms in response to changes in the digital environment.

Thus, improving state policy for regulating banking activities amid the development of FinTech technologies should focus on building an integrated digital-risk management system, ensuring the cyber resilience of the financial sector, fostering an innovative environment, and strengthening national security. Implementation of the proposed directions will enhance

the competitiveness of the banking system, financial stability, and the adaptability of state regulation to the challenges of the digital economy.

DISCUSSION

The findings confirm the general trend identified in contemporary research regarding the dual impact of FinTech technologies on the banking system. On the one hand, digitalization increases the accessibility and speed of financial services, improves banks' operational efficiency, and supports new business models; on the other hand, it creates additional sources of operational, cyber, information, and systemic risks. This conclusion is consistent with Murinde et al. (2022), who regard FinTech technologies as a factor in the structural transformation of banking that simultaneously creates new opportunities for financial-sector development and new regulatory challenges. The findings of the present study, however, allow this approach to be extended. Whereas Murinde et al. (2022) focus primarily on the transformation of bank business models and the future of banking, the analysis of Ukraine's financial sector indicates that FinTech technologies should be considered not only as a factor of competitive and technological transformation but also as a factor in state resilience and national security. For Ukraine, this perspective is particularly important because military, macroeconomic, and cyber threats operate simultaneously.

The observed increase in cashless transactions and the spread of contactless and tokenized payment instruments support the conclusions of Safiullah and Paramati (2022) concerning the potentially positive impact of FinTech technologies on banks' financial stability. However, the Ukrainian context demonstrates that the positive effects of digitalization cannot be assessed solely through efficiency or bank-stability indicators. As the population, enterprises, and public institutions become increasingly dependent on digital channels for financial services, the potential damage resulting from disruption of the relevant digital infrastructure also increases. Thus, higher levels of digitalization simultaneously increase the economic value of the banking system and its cyber vulnerability. This conclusion is partly consistent with Ni et al. (2023), who identify a nonlinear relationship between FinTech technologies and banking risks. They show that at the initial stages of digital transformation, technological innovation may increase bank risk, whereas at more advanced stages its impact can become risk-reducing provided that appropriate financial regulation is in place. The findings for Ukraine confirm the fundamental importance of the regulatory environment while also suggesting that its scope should be broadened. Effective FinTech regulation should encompass not only financial risk but also cyber risk, concentration of technological resources, third-party risk, risks to the continuity of critical financial services, and risks associated with the use of artificial intelligence.

It is also important to compare the findings with Cevik (2024), who shows that the impact of FinTech on financial stability is not unambiguous and depends on the type of technological innovation and the institutional environment. The findings for Ukraine support this proposition because the accelerated digitalization of payments is occurring in parallel with the growing importance of cyber threats. Ukraine is additionally characterized by a military-cyber transmission channel, under which banks' digital infrastructure should be viewed not only as an element of the financial system but also as part of the state's critical infrastructure. Comparison with cybersecurity research is especially important. Javaheri et al. (2024), in systematizing contemporary FinTech cyber threats, emphasize their multidimensional nature and the need to move from traditional protective measures to comprehensive models of digital-risk management. Wang et al. (2024) similarly demonstrate that the digital transformation of the banking sector increases the importance of data protection, third-party risk management, access control, and continuous threat monitoring. The findings of the present study extend these propositions by directly linking banks' cyber resilience with the financial and national security of the state.

The article proposes a risk-based approach to state regulation of banking activities in the context of FinTech development, which involves the consistent integration of four key elements: the identification of digital risks, assessment of their potential impact on banks' activities, application of differentiated regulatory instruments, and continuous monitoring of the effectiveness of regulatory measures.

Unlike approaches in which FinTech innovations and cyber risks are treated as separate areas of regulation, the proposed framework provides for their integrated assessment within a unified framework aimed at ensuring both the digital and financial resilience of banks.

The findings are also consistent with Chao et al. (2022), who substantiate the potential of RegTech to improve the effectiveness of financial supervision. The use of artificial intelligence, machine learning, large-scale data analytics, and automated monitoring enables the regulator to move from reacting to risks after they materialize toward their early detection. However, amid rapid FinTech development, the regulator's technological capabilities must advance at least as quickly as those of banks and FinTech companies. This creates the problem of a regulatory technology gap, in which the traditional regulatory framework and institutional supervisory mechanisms fail to keep pace with the emergence of new financial

DOI: 10.55643/fcaptp.5.70.2026.5321

technologies. In this context, the findings of Zhao and Ma (2025) concerning FinTech's capacity to enhance the effectiveness of financial regulation are particularly relevant. On the one hand, technologies enable regulators to obtain more data, automate inspections, and identify atypical behavior; on the other hand, their use creates new risks associated with data quality, algorithmic bias, the opacity of artificial-intelligence models, and the cybersecurity of regulatory infrastructure. Therefore, the digitalization of public financial supervision must be accompanied by the digitalization of regulatory risk management itself.

A distinctive feature of the proposed risk-based approach is the differentiation of regulatory measures depending on a bank's level of digital maturity, the scale of its operations, and the nature of the digital risks it faces. For banks with a high degree of technological dependence, priority should be given to requirements concerning ICT risk management, cybersecurity, business continuity, and oversight of third-party technology providers.

For banks with a lower level of digital maturity, greater emphasis should be placed on developing essential digital infrastructure, strengthening internal control systems and data protection mechanisms, and ensuring a gradual transition towards automated risk monitoring.

Another distinction of the proposed approach from some previous studies is the shift in emphasis from "FinTech as a source of innovation" to "FinTech as an object of risk-based state regulatory policy." This change of focus is fundamentally important for Ukraine because the state simultaneously seeks to accelerate the digitalization of the financial sector, ensure the competitiveness of Ukrainian banks, integrate with the European financial area, and prevent technological dependence from creating additional threats to economic and national security. In this regard, the balancing function of state policy should be emphasized. Excessive regulation may constrain FinTech innovation, increase compliance costs, and reduce bank competitiveness, whereas insufficient regulation may encourage the accumulation of cyber risks, data-protection problems, technological concentration, and systemic vulnerability. The preferable model is therefore proportional, risk-based, and technology-neutral regulation in which the intensity of regulatory intervention depends less on the legal status of the entity than on the nature of the service, the scale of operations, and the potential systemic risk.

Accordingly, the findings advance existing scholarly approaches in three principal directions:

1. They demonstrate the need to assess the economic effects of FinTech technologies and the associated digital risks simultaneously.
2. They substantiate the transition from traditional banking supervision to integrated digital supervision based on RegTech/SupTech, artificial intelligence, and data analytics.
3. They propose treating the cyber resilience of the banking system as a component of national security, which is particularly relevant for a state operating under military and hybrid threats.

The study has several limitations that should be taken into account when interpreting the findings. In particular, some indicators relating to digitalisation, cyber risks, and banks' expenditures on digital infrastructure are not disclosed in publicly available reports, which limits the possibility of direct quantitative comparison.

In addition, some of the results concerning digital and regulatory impact were obtained using an author-developed assessment methodology. Therefore, they reflect the authors' analytical judgement and should not be interpreted as official assessments of the National Bank of Ukraine.

The period from 2022 to 2025 was characterised by substantial structural changes in Ukraine's financial sector associated with the full-scale war, shifts in customer behaviour, the transformation of payment infrastructure, and the intensification of cyber threats. Consequently, the findings should not be mechanically extrapolated to the long term without taking into account changes in the regulatory and macroeconomic environment.

At the same time, the results of the in-depth analysis of individual banks cannot be automatically generalised to the banking system as a whole. Therefore, conclusions at the systemic level were formulated on the basis of aggregated banking sector data, while data on individual banks were used to identify specific patterns of adaptation to digital and regulatory changes.

CONCLUSIONS

The findings provide grounds for concluding that the development of FinTech technologies is one of the dominant drivers of banking-system transformation, substantially influencing the mechanisms through which the financial sector operates, the nature of interaction between banking institutions and customers, and the institutional foundations of state regulation

of banking activities. The digitalization of financial services and the spread of mobile banking, digital payment systems, artificial intelligence, Big Data, and blockchain solutions improve the efficiency of banking operations, expand financial inclusion, and promote the development of an innovative financial ecosystem.

The analysis of PrivatBank, Oschadbank, and Raiffeisen Bank during 2022–2025 established that the introduction of FinTech technologies contributed to the expansion of digital service channels, growth in the number of mobile-banking users, increased automation of banking processes, and improved financial performance of banking institutions. PrivatBank demonstrated the highest level of digital transformation, effectively creating a digital banking ecosystem and becoming one of Ukraine's leaders in the implementation of innovative financial services. State-owned banks also intensified their digitalization processes, indicating a general trend toward modernization of the banking sector.

It was established that, alongside the positive effects of digitalization, digital risks are increasing, acquiring a systemic character and creating potential threats to national security. The most significant risks include cyberattacks on financial infrastructure, leakage of personal and financial data, digital fraud, the use of artificial intelligence to commit cybercrime, dependence of banking systems on external digital platforms and cloud services, and risks associated with virtual assets and digital financial instruments. The analysis of NBU regulatory documents, publicly available bank reports, and trends in digital activity indicators for 2022–2025 demonstrates an expansion in the range of digital risks that need to be taken into account in banking regulation. The most significant of these include cyber risks, risks related to data confidentiality breaches, digital fraud, dependence on external IT infrastructure and cloud services, as well as risks associated with the use of emerging digital technologies. At the same time, the available public data do not allow for a comprehensive quantitative assessment of all categories of cyber risk at the level of individual banks. Therefore, the findings presented primarily reflect broader regulatory and analytical trends rather than the full scale of the respective risks. It is substantiated that improving the effectiveness of state policy on banking regulation amid FinTech development requires a more advanced institutional mechanism for digital-risk management. Priority directions of state policy should include the development of RegTech and SupTech technologies in banking supervision, the establishment of a unified system for monitoring digital risks in the financial sector, stronger requirements for the cyber resilience of banking infrastructure, improved mechanisms for protecting personal data and financial information, and expanded cooperation among public authorities, banking institutions, and FinTech companies in the field of cybersecurity. A transition to data-driven supervision would enable the National Bank of Ukraine to identify atypical transactions, risk concentrations, signs of fraud, and potential threats to financial-system stability more promptly. In addition, a comprehensive framework for regulating digital and cyber risks requires common minimum cyber-resilience requirements for banks and FinTech providers, regular testing of digital infrastructure, third-party risk management, redundancy of critical information resources, cyber-incident response, and restoration of continuity in financial services. Cyber risk should therefore be regarded not only as an operational risk of an individual bank but also as a potential systemic risk to the financial and national security of the state.

It is demonstrated that, in the context of Ukraine's European integration, harmonization of national legislation with European Union legislation in the areas of digital financial services, cyber resilience, and digital banking is of particular importance. Such harmonization will facilitate the formation of a modern regulatory model for the banking system capable of balancing the promotion of financial innovation, the maintenance of financial stability, and the protection of national interests amid the digital transformation of the economy.

The scientific novelty of the findings lies in substantiating a comprehensive approach to state regulation of banking activities in which FinTech innovation, financial-data protection, and digital and cyber risks are treated not as isolated regulatory objects but as interrelated components of a unified economic and legal mechanism for ensuring the resilience of the financial system and national security.

The scientific novelty of the study lies in the further development of the theoretical and methodological foundations of state regulation of banking activities under conditions of digital transformation through the substantiation of a risk-based approach that integrates the assessment of FinTech innovations, digital risks, and cyber risks with the selection of appropriate regulatory instruments.

Unlike approaches in which the digitalisation of banking activities and cyber risks are considered predominantly as separate areas of regulation, the proposed approach provides for their consistent integration within a unified regulatory cycle comprising the following stages: identification of digital risks, assessment of their level, determination of the required regulatory response, selection of appropriate NBU instruments, monitoring of regulatory effectiveness, and adjustment of regulatory measures.

Further research should focus on developing methodological approaches to assessing digital risks in the banking sector, establishing a system of indicators of banking institutions' digital resilience, and improving mechanisms of state regulation

DOI: 10.55643/fcaptp.5.70.2026.5321

governing the use of artificial intelligence and digital financial platforms in the context of ensuring Ukraine's national security.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

FUNDING

The Authors received no funding for this research.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Arner, D. W., Barberis, J. N., & Buckley, R. P. (2016). *FinTech, RegTech and the reconceptualization of financial regulation* (University of Hong Kong Faculty of Law Research Paper No. 2016/035). SSRN. https://ssrn.com/abstract=2847806
2. Borshchuk, I., & Myshchyshyn, O. (2023). Key aspects of the digitalization of business processes in Ukraine's banking sector. *Financial Space*, *4*(52), 73–79. https://doi.org/10.30970/fp.4(52).2023.738081
3. Cevik, S. (2024). The dark side of the moon? Fintech and financial stability. *International Review of Economics, 71*, 421–433. https://doi.org/10.1007/s12232-024-00449-8
4. Chao, X., Ran, Q., Chen, J., Li, T., Qian, Q., & Ergu, D. (2022). Regulatory technology (Reg-Tech) in financial stability supervision: Taxonomy, key methods, applications and future directions. *International Review of Financial Analysis, 80*, Article 102023. https://doi.org/10.1016/j.irfa.2022.102023
5. Cheng, S., Li, J., Luo, L., & Zhu, Y. (2024). Cybersecurity governance and digital finance: Evidence from sovereign states. *Finance Research Letters, 65*, Article 105533. https://doi.org/10.1016/j.frl.2024.105533
6. Davydenko, N. M., Shepylenko, V. Yu., & Davydenko, M. A. (2025). Digital transformation of Ukraine's banking system: Innovative models, technologies, and economic efficiency. *Scientific Papers of the Interregional Academy of Personnel Management*, (3)(79), 132–137. https://doi.org/10.32689/2523-4536/79-15
7. Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications, 241*, Article 122697. https://doi.org/10.1016/j.eswa.2023.122697
8. Joint Stock Company Commercial Bank "PrivatBank." (2022). *Annual report for 2022*. https://privatbank.ua/about/finansovaja-otchetnost
9. Joint Stock Company Commercial Bank "PrivatBank." (2023). *Annual report for 2023*. https://static.privatbank.ua/files/Richnyy_zvit_za_2023.pdf
10. Joint Stock Company "Oschadbank." (2022). *Annual report for 2022*. https://www.oschadbank.ua/finansova-zvitnist
11. Joint Stock Company "Raiffeisen Bank." (2022). *Annual report for 2022*. https://raiffeisen.ua/storage/files/34-196-p.pdf
12. Joint Stock Company "Raiffeisen Bank." (2023). *Annual report for 2023*. https://raiffeisen.ua/storage/files/rbi-report-2023.pdf
13. Kliusko, L., & Moskalenko, N. (2021). Banking activities in the information economy. *Collection of Scientific Papers of the State Tax University*, (1), 126–140. https://doi.org/10.33244/2617-5940.1.2021.126-140
14. Kretov, D. (2024). Current state of digitalization in corporate banking in Ukraine. *Kyiv Economic Scientific Journal*, *6,* 78–85. https://doi.org/10.32782/2786-765X/2024-6-11
15. Law of Ukraine No. 679-XIV "On the National Bank of Ukraine." (1999, May 20). https://zakon.rada.gov.ua/laws/show/679-14#Text
16. Law of Ukraine No. 2121-III "On Banks and Banking Activity." (2000, December 7). https://zakon.rada.gov.ua/laws/show/2121-14#Text
17. Law of Ukraine No. 1591-IX "On Payment Services." (2021, June 30). https://zakon.rada.gov.ua/laws/show/1591-20#Text
18. Murinde, V., Rizopoulos, E., & Zachariadis, M. (2022). The impact of the FinTech revolution on the future of banking: Opportunities and risks. *International Review of Financial Analysis, 81*, Article 102103. https://doi.org/10.1016/j.irfa.2022.102103
19. National Bank of Ukraine. (n.d.-a). *Banking sector statistics and supervisory data*. https://bank.gov.ua/ua/statistic/supervision-statist
20. National Bank of Ukraine. (n.d.-b). *Financial stability reports*. https://bank.gov.ua/ua/stability/report

21. National Bank of Ukraine. (n.d.-c). *Overview of Ukraine's banking sector*. https://bank.gov.ua/ua/news/all?tag=banking-sector-review

22. National Bank of Ukraine. (2021, May 19). *Resolution No. 43 on approval of the regulation on information protection and cybersecurity by payment market participants*. https://zakon.rada.gov.ua/laws/show/v0043500-21#Text

23. National Bank of Ukraine. (2018, June 11). *Resolution No. 64 on approval of the regulation on the organization of the risk management system in Ukrainian banks and banking groups*. https://zakon.rada.gov.ua/laws/show/v0064500-18#Text

24. National Bank of Ukraine. (2023, May 3). *Resolution No. 58 on approval of the regulation on authentication and the use of strong authentication in the payment market*. https://zakon.rada.gov.ua/laws/show/v0058500-23#Text

25. National Bank of Ukraine. (2025, May 6). *Resolution No. 52 on amendments to certain regulatory and legal acts of the National Bank of Ukraine*. https://zakon.rada.gov.ua/laws/show/v0052500-25#Text

26. National Bank of Ukraine. (2025, July 25). *Resolution No. 80 on approval of the regulation on open banking in Ukraine*. https://zakon.rada.gov.ua/laws/show/v0080500-25#Text

27. Naumenkova, S. V., Mishchenko, S. V., & Dorofieiev, D. A. (2020). Global experience in the institutionalization of innovation process management in the banking system. *Economic Space*, *163*, 126–132. https://doi.org/10.32782/2224-6282/163-22

28. Ni, Q., Zhang, L., & Wu, C. (2023). Fintech and commercial bank risks: The moderating effect of financial regulation. *Finance Research Letters, 58*, Article 104536. https://doi.org/10.1016/j.frl.2023.104536

29. Ren, Y.-S., Ma, C., & Wang, Y. (2024). A new financial regulatory framework for digital finance: Inspired by CBDC. *Global Finance Journal, 62*, Article 101025. https://doi.org/10.1016/j.gfj.2024.101025

30. Safiullah, M., & Paramati, S. R. (2024). The impact of FinTech firms on bank financial stability. *Electronic Commerce Research, 24*, 453–475. https://doi.org/10.1007/s10660-022-09595-z

31. Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security, 147*, Article 104051. https://doi.org/10.1016/j.cose.2024.104051

32. Zhao, Y., & Ma, F. (2025). Will fintech enhance financial regulation? *Research in International Business and Finance, 78*, Article 103005. https://doi.org/10.1016/j.ribaf.2025.103005

Бліхар М., Ділай О., Добош З., Вінічук М., Гаврильців М.

ДЕРЖАВНА ПОЛІТИКА РЕГУЛЮВАННЯ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ В УМОВАХ РОЗВИТКУ FINTECH–ТЕХНОЛОГІЙ ТА ПОСИЛЕННЯ ЦИФРОВИХ РИЗИКІВ ДЛЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

Метою статті є дослідження трансформації державного регулювання банківської діяльності в Україні в умовах розвитку FinTech-технологій та посилення цифрових ризиків, а також обґрунтування напрямів удосконалення нормативно-регуляторної бази й механізмів банківського нагляду з урахуванням вимог фінансової стабільності та національної безпеки. У статті аргументовано, що цифрова трансформація фінансового сектору обумовлює модернізацію банківських послуг, сприяє підвищенню ефективності фінансового посередництва, розширює фінансову інклюзію та забезпечує розвиток інноваційних бізнес-моделей, однак, генерує нові виклики для системи державного регулювання банківської діяльності, забезпечення фінансової стабільності та кібербезпеки. Визначено основні тенденції цифровізації банківської діяльності та охарактеризовано вплив FinTech–технологій на трансформацію механізмів державного регулювання фінансового сектору. Здійснено аналіз роботи основних банків України: ПриватБанку, Ощадбанку та Райффайзен Банку за період з 2022 р. по 2025 р., що дозволило виявити зростаючі тенденції щодо посилення цифровізації банківських операцій, поширення дистанційних каналів обслуговування, збільшення кількості користувачів цифрових сервісів та посилення ролі фінансових технологій у забезпеченні конкурентоспроможності банківських установ. З'ясовано, що поряд із позитивним ефектом цифрової трансформації констатується зростання кіберризиків, ризиків цифрового шахрайства, витоку інформації, технологічної залежності від зовнішніх платформ та інших загроз, які впливають на національну безпеку держави. Обґрунтовано необхідність удосконалення державної політики регулювання банківської діяльності шляхом розвитку RegTech- і SupTech-технологій, упровадження ризик-орієнтованого цифрового нагляду, посилення кіберстійкості банківської інфраструктури, удосконалення механізмів управління цифровими ризиками та гармонізації національного законодавства з європейськими стандартами цифрового фінансового регулювання. Доведено, що ефективне поєднання інноваційного розвитку фінансового сектору та сучасних механізмів державного контролю виявляється необхідною передумовою забезпечення фінансової стабільності та захисту національних інтересів держави в умовах цифрової економіки.

DOI: 10.55643/fcaptp.5.70.2026.5321

Ключові слова: банківська діяльність, державна політика, національна безпека, державне регулювання, FinTech технології, банківська система, цифровізація, цифровий банкінг, ризики, кібербезпека, фінансові інновації

JEL Класифікація: G21, G28, O33, K23, E58