ECONOMICS OF DEVELOPMENT
Journal homepage: https://ecdev.com.ua/
ISSN: 1683-1942
E-ISSN: 2304-6155
Vol. 25, No. 2, 2026
UDC 338.24:336.02:004.738.5(4)
DOI: 10.63341/econ/2.2026.53

Maryna Berest
PhD in Economics, Associate Professor
Simon Kuznets Kharkiv National University of Economics
61165, 9A Nauky Ave., Kharkiv, Ukraine
https://orcid.org/0000-0002-2410-3210
Nataliia Sablina*
PhD in Economics, Associate Professor
Simon Kuznets Kharkiv National University of Economics
61165, 9A Nauky Ave., Kharkiv, Ukraine
https://orcid.org/0000-0002-1931-2851

The transformation of the financial and economic security of economic systems: European experience and the challenges of the digital economy

Abstract. The relevance of this study stems from the need to rethink approaches to ensuring the financial security of economic systems in the context of digital transformation, increasing geopolitical instability and growing systemic risks. The aim of this article was to examine the transformation of the financial security of economic systems in the context of the digital economy, based on the integration of institutional, risk-oriented and digital approaches, as well as to summarise European experience in countering financial risks and threats to financial security, and to identify opportunities for its adaptation to the Ukrainian context. To achieve this aim, methods of theoretical generalisation, content analysis of academic and analytical sources, and systematic and comparative analysis were employed. The application of these methods made it possible to examine the evolution of academic approaches to the interpretation of financial security, to identify the characteristics of its transformation under the influence of digitalisation, and to carry out a comparative analysis of threats to financial security in the countries of the European Union and Ukraine. As a result of the research, an original interpretation of financial security as an integrated property of the economic system is proposed; a mechanism for the interaction between the macro- and micro-levels of financial security has been developed; and an integrated conceptual model of its transformation in the context of the digital economy has been formulated. It has been established that the digitalisation of the financial sector is significantly altering the structure of threats to financial security due to the intensification of cyber risks, technological dependence and the impact of digital infrastructure on the resilience of economic systems. Differences have been identified in the structure of threats to financial security in the EU and Ukraine. It has been determined that the modern European model for ensuring financial security is based on the principles of digital resilience, institutional coordination and proactive risk management. The practical significance of the findings lies in the potential to utilise the proposed approaches when formulating state policy in the field of financial security, developing strategies for the digital transformation of the financial sector, enhancing digital resilience, and adapting European experience to the conditions of Ukraine's post-war economic recovery

Keywords: diagnosis; resilience; financial stability; financial engineering; credit burden; digital technologies; European integration

INTRODUCTION

In the current climate of digital transformation, geopolitical instability and rising systemic risks, the financial security of economic systems is becoming particularly relevant. The traditional understanding of this concept

Article's History: Received: 24.11.2025; Revised: 06.04.2026; Accepted: 19.05.2026; Published: 29.06.2026

Suggested Citation:
Berest, M., & Sablina, N. (2026). The transformation of the financial and economic security of economic systems: European experience and the challenges of the digital economy. *Economics of Development*, 25(2), 53-65. doi: 10.63341/econ/2.2026.53.

*Corresponding author (*ns04111974@gmail.com*)

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

through the prism of macro-financial stability no longer fully addresses contemporary challenges, as the digitalisation of the financial sector amplifies the role of cyber risks, technological dependence, data protection and the resilience of digital infrastructure. In these circumstances, financial security should be viewed not merely as the financial system's ability to maintain equilibrium, but as a multi-level characteristic of the economic system, reflecting its capacity to adapt to financial, digital, institutional and geopolitical threats. This issue is of particular significance for the countries of the European Union and Ukraine. The European model for ensuring financial security is gradually shifting towards a combination of macroprudential regulation, digital operational resilience and proactive risk management. For Ukraine, the relevance of this research is heightened by the impact of the war, macroeconomic instability, the destruction of critical infrastructure and the need to adapt European experience to the conditions of post-war recovery. This necessitates the development of an integrated approach to studying the financial security of economic systems in the context of the digital economy.

The study by G. Gorton & G. Ordoñez (2020) focuses on the mechanisms underlying the formation of financial cycles and systemic crises. The authors concluded that periods of financial growth can have both positive and negative effects on the economy, depending on the nature of the accumulation of credit imbalances and the quality of information in financial markets. Particular attention is paid to the mechanisms by which systemic risks spread among financial institutions. The study's findings confirm the need to take systemic risks into account as a key component of modern financial security. B. Walker (2020) examined the nature of resilience as a property of complex systems. As a result of the study, the author concluded that resilience lies not only in a system's ability to withstand shocks, but also in the preservation of its key functions and its adaptation to changes in the external environment. This approach allows for a broader interpretation of financial security beyond the traditional understanding of financial stability.

N. Nosan & S. Nazarenko (2022) investigated methodological issues in the management of financial security within economic security systems at various levels of governance. The authors justified the need to consider financial security as a component of a broader economic security system and concluded that it is important to coordinate financial security management mechanisms across different levels of the economic system. These findings confirm the validity of a systematic approach to the study of financial security in economic systems. J. Haldon *et al.* (2021) analysed the historical experience of societies functioning under conditions of crisis and prolonged stress. Based on the results of their study, the authors found that the resilience of systems is determined not only by their ability to adapt to change, but also by their capacity to undergo structural transformation in response to new challenges. The findings indicate the need to view financial security not only as a mechanism for protection against risks, but also as the economic system's capacity for adaptation and transformation in the face of long-term crisis impacts.

The relationship between resilience and sustainable development in a war economy was investigated by O. Semenenko *et al*. (2025). The authors concluded that modern resilience should be viewed as the ability of economic systems not only to recover from crisis events, but also to develop new mechanisms for growth in conditions of prolonged uncertainty and military risks. The findings of the study confirm the need to take security and military factors into account when assessing the financial stability of economic systems. Alongside the development of concepts of systemic risk and resilience, a separate strand of contemporary research focuses on the impact of digital transformation on financial security. The BIS (2023) report analyses the consequences of the proliferation of financial technologies, digital platforms and the activities of large technology companies in the financial sector. The report concludes that digitalisation creates new opportunities to improve the efficiency of financial services, but at the same time gives rise to additional risks related to cybersecurity, data concentration and the technological dependence of financial infrastructure. These findings highlight the need to incorporate a digital component into contemporary approaches to ensuring financial security.

Thus, the results of recent research demonstrate the evolution of approaches to interpreting financial security from ensuring macro-financial stability to understanding it as a multi-level characteristic of the economic system, combining risk-based, resilience-based and digital approaches. At the same time, the digital transformation of the financial sector is creating new challenges that require the further development of the theoretical and methodological foundations for ensuring financial security. Despite the significant contribution of the studies cited to the development of financial security theory, a number of aspects remain insufficiently explored. In particular, most studies focus on issues of financial stability and systemic risks, as well as on the resilience of economic systems, whilst the interrelationship between institutional, digital, geopolitical and financial factors in the transformation of financial security has been studied only in a fragmented manner. However, aspects relating to the integration of risk-based, institutional and digital approaches to ensuring financial security, as well as the adaptation of European experience in ensuring financial stability to the conditions of Ukraine's economy during a period of digital transformation and military challenges, remain under-researched. The aim of this article was to examine the transformation of financial security in economic systems within the context of the digital economy, based on the integration of institutional, risk-oriented and digital approaches, as well as to summarise European experience in countering financial risks and threats to financial security, and to identify opportunities for its adaptation to the Ukrainian context.

MATERIALS AND METHODS

The methodological basis of the study was an interdisciplinary approach to the analysis of the financial security of economic systems, which combined institutional, systemic, comparative and risk-oriented approaches. The application of this approach was dictated by the multi-level nature of financial security, which is shaped by macroeconomic, institutional, geopolitical and digital factors and is undergoing transformation in the context of the digitalisation of the economy. The study utilised the methods

of theoretical generalisation, scientific abstraction and content analysis of academic and analytical sources – to systematise approaches to interpreting the categories of "economic system" and "financial security", as well as to identify the evolution of scholarly approaches to understanding financial security within the Anglo-American and European traditions. The institutional approach was applied to examine the role of the regulatory environment, the architecture of the financial system and the mechanisms for coordinating economic policy in shaping the financial security of economic systems, particularly in the context of European practice in ensuring macro-financial and digital stability. The systems approach was used to justify financial security as an integrative characteristic of the economic system, shaped through the interaction of macro- and micro-levels, and to construct a conceptual model of the transformation of financial security in the context of the digital economy. Attention was paid to the mechanisms linking a state's financial stability, the functioning of the financial system and the financial security of economic entities against a backdrop of growing digital, geopolitical and macroeconomic risks.

A comparative analysis was used to contrast Anglo-American and European academic traditions in the interpretation of financial security, as well as to identify differences in the structure of threats to financial security in the European Union and Ukraine, and the potential for adapting European experience to Ukrainian conditions (Adrian & Brunnermeier, 2016; Gorton & Ordoñez, 2020; European Central Bank, 2024). To conduct a comparative analysis of threats to financial security, a targeted selection of academic publications and analytical reports from international organisations and specialist institutions was carried out (International Monetary Fund, 2024; European Union Agency for Cybersecurity, 2024a; European Central Bank, 2024), published predominantly between 2022 and 2025. The criteria for including sources were: relevance to the issue of financial security in the context of digital transformation; the presence of an analysis of contemporary financial, cyber, geopolitical and institutional risks; and the possibility of using the results to compare the operating conditions of the economic systems of the EU and Ukraine.

Methods of analysis and synthesis were used to summarise the findings of contemporary scientific and analytical studies on digital, financial, geopolitical and institutional risks, as well as to develop an integrated approach to ensuring the financial security of economic systems in the context of digital transformation. The analysis includes human resources and social factors, as contemporary research on financial security and digital resilience considers the shortage of skilled personnel, migration processes and the level of digital competences to be important factors in the formation of financial and cyber risks. To summarise European experience in ensuring economic and financial security, the "Promote – Protect – Partner" analytical framework, proposed by the European Commission as part of the EU Economic Security Strategy initiative package (European Commission, 2024a), was used; this enabled the systematisation of instruments for enhancing resilience, protection and international partnership in the field of economic security.

RESULTS AND DISCUSSION

Against a backdrop of high uncertainty, digital transformation and geopolitical challenges, the issue of financial security becomes rather complex. It is difficult to consider it in isolation, without taking into account the broader environment in which the economy operates. Thus, to gain a thorough understanding of financial security, it is advisable to analyse it through the prism of the economic system, which is the primary subject of study. In international economics, the economic system is viewed as an organised structure comprising rules – both formal and informal – and mechanisms for regulating economic activity. The quality of resource allocation, the development of the banking sector and the economy's capacity for stable growth depend on the quality of its institutional framework (Rodrik, 2021). In this context, the financial subsystem, as an integral part of this structure, plays a vital role in the reallocation of resources, risk management and ensuring overall macroeconomic stability.

In the works of Ukrainian researchers, the economic system is defined as a complex, unified and multifaceted socio-economic structure capable of adapting to external changes (Kanova, 2023). A study of Ukraine's banking sector during times of war and crisis has shown that the resilience of the economic system is largely determined by the ability of the financial subsystem to function effectively, the flexibility of its regulatory framework, and the ability of financial institutions to maintain the continuity of financial flows (Tymoshyk *et al.*, 2022; Arzhevityn *et al.*, 2023). This is corroborated by data from the Financial Stability Report (National Bank of Ukraine, 2024), according to which the high liquidity and operational resilience of the banking infrastructure have served as key buffers against systemic shocks. In this sense, the economic system emerges as an integrated complex of production, financial and regulatory mechanisms operating within a single institutional architecture. As noted in the World Bank (2026) report, it is the quality of institutional design that determines the ability of national economies to recover in the face of global fragmentation. Its stability is based on the financial subsystem's capacity to offset internal and external disruptions, thereby ensuring a high level of confidence in financial institutions.

Thus, the economic system constitutes a coherent structure that integrates production, financial and regulatory instruments. It operates within a defined institutional framework and ensures the continuity of economic processes. Its stability depends on the financial subsystem's ability to adapt to changes in the risk environment, to maintain confidence in the institutions of the financial system, and to preserve the balance and continuity of financial flows. Based on an analysis of international and Ukrainian academic sources, the author proposes the following definition: an economic system is a multi-level, institutionally organised model of economic activity that integrates mechanisms for the production, distribution and redistribution of resources and ensures the coordination of interaction between economic agents and risk management. The stability of such a system depends on the quality of its institutional structure, its ability to regulate processes, and the adaptability of the financial subsystem to changes in the internal and external risk environment.

From this perspective, financial security is an integral component of the economic system, as it ensures the continuity of financial flows, the efficient reallocation of resources and the support of economic agents' operations in conditions of risk. A high level of financial security helps to preserve macroeconomic stability, enhance investment attractiveness, maintain the financial resilience of businesses and households, and strengthen confidence in financial institutions. In this context, financial security is one of the key factors in ensuring the resilience and adaptability of the economic system in the face of digital transformation and growing uncertainty. Thus, the institutional organisation of the economic system plays a key role in developing mechanisms to ensure financial security and adapting them to the conditions of the digital economy. Within this framework, financial security is regarded as a comprehensive characteristic of the economic system, reflecting the financial subsystem's ability to ensure the uninterrupted flow of financial resources, their optimal reallocation and resilience to exogenous and endogenous risks.

Financial systems are being transformed by digital technologies, which are changing the ways in which financial resources are moved, risks are assessed and financial flows are managed. They use algorithms and artificial intelligence to assess risks and manage the assets of their clients and other financial institutions, creating a new way in which the financial sector is interconnected and interdependent (BIS, 2023). The BIS (2023) report notes that digitalisation accelerates the processing of financial information, improves access to financial services and reduces transaction costs, but at the same time increases financial institutions' technological dependence. Institutions must be able to resolve issues and protect themselves against cyber-attacks, as they rely on services and algorithms that can change rapidly and affect their funds (BIS, 2023).

In its latest Financial Stability Review, the European Central Bank examined how digital assets, artificial intelligence and cyber-attacks could cause major problems, as they can rapidly propagate shocks in the digital environment (European Central Bank, 2024). Digital financial services enhance the speed, accessibility and efficiency of financial transactions for individuals and businesses, whilst also making them more accessible and equitable; however, they also create new challenges and risks for the financial and technological systems that utilise them. A report by the International Monetary Fund (2024) notes that AI can help banks and other financial institutions to better coordinate their plans and strategies, but it will also make them more vulnerable to sudden and unpredictable market changes, which could cause problems for the entire system. Digitalisation is changing thinking about financial security, making risk management more complex and dependent on factors unrelated to the economy or the monetary system. Financial security is taking on a more comprehensive scope, encompassing digital infrastructure, data protection, and operational and financial systems that operate with a high degree of technological dependence. Consequently, the concept of financial security has undergone a significant transformation: from a predominantly macro-financial focus on stability and equilibrium to a more comprehensive understanding that encompasses systemic risks, adaptive capacity and digital challenges. Financial security is increasingly viewed as a multi-level category combining institutional, risk-oriented and technological aspects. At the same time, these dimensions are often analysed in isolation, without sufficient conceptual alignment. This is precisely why an integrated framework is needed – one that would combine institutional analysis of the economic system with the digital and risk-driven transformation of the financial environment.

The evolution of approaches to financial security shows that its meaning varies across different academic schools. The element that is emphasised – whether it be the stability of financial markets, institutional resilience, regulatory policy or socio-economic stability – depends significantly on the methodology and analytical context. Thus, in contemporary literature, it is useful to distinguish between two main conceptual traditions – the Anglo-American and the European – which differ both in terms of analytical tools and research priorities. The Anglo-American school views financial security primarily through the concepts of "financial stability" and "systemic risk" (Adrian & Brunnermeier, 2016; Gorton & Ordoñez, 2020). Within this approach, the main focus is on the emergence and spread of financial crises, the role of interbank linkages, contagion effects and the cyclical nature of financial markets (Gorton & Ordoñez, 2020). Research has continued along these lines within the macro-financial paradigm, analysing the relationship between financial cycles, the capitalisation of financial intermediaries and the build-up of systemic risk (He & Krishnamurthy, 2013; Bianchi & Mendoza, 2018). Within this framework, financial stability is understood primarily as the financial system's ability to reduce the likelihood of a systemic crisis or to limit its macroeconomic consequences through the use of macroprudential policy instruments and market discipline.

Against the backdrop of digitalisation, the Anglo-American school is increasingly integrating issues of operational resilience, cyber resilience and algorithmic risks into the broader context of financial stability (BIS, 2023). At the same time, even in the digital sphere, the focus remains on ensuring the functional continuity of market mechanisms and minimising systemic disruptions. The European tradition favours a more institutionally integrated and regulatory-oriented approach. Financial security is viewed as a multi-layered system combining macroprudential regulation, fiscal policy coordination, the activities of supranational supervisory bodies and digital mechanisms for protecting financial infrastructure. Particular attention is paid to financial resilience – the ability of institutions to adapt to external shocks and changes in the risk environment (European Central Bank, 2024).

In European research, the integration of the digital dimension of financial security is becoming increasingly important – taking into account cyber risks, the platformisation of financial services and regulatory mechanisms to ensure digital operational resilience (BIS, 2023). In this context, financial security goes beyond a narrow understanding of market stability and emerges as the institutionally underpinned capacity of the financial system to sustain economic development amidst growing uncertainty and technological change. The main difference between the schools lies in which aspect is primarily studied: the Anglo-American school examines the behaviour of financial markets and the mechanisms by which systemic

risks arise, whilst the European school focuses on the institutional structure and the multi-level regulatory system designed to ensure financial stability. However, this does not mean that there are markedly different views; rather, they simply highlight different aspects of a single overarching issue. A synthesis of the approaches from the Anglo-American and European traditions has shown that financial security should be viewed not only as an indicator of the stability of the financial system or the reduction of systemic risks, but also as a property of the economic system that is shaped by structural and digital changes, and which is multi-level and dynamic in nature.

The financial security of an economic system is the ongoing state and functioning of the financial sector, which demonstrates its capacity to ensure the stability of cash flows, to allocate and utilise financial resources effectively, and to withstand various risks – whether systemic, geopolitical or digital – with a view to sustaining stable socio-economic development. Financial security is a fundamental characteristic of the economic system, shaped by the institutional framework, the structure of financial relations and the level of development of digital technologies. It operates at two levels: the macro- and micro-levels. Financial security at the macro-level is determined by the soundness of the state's financial position, the stability of the banking system and the effective management of systemic risks. It reflects the state's ability to ensure debt sustainability, maintain macroeconomic equilibrium and preserve confidence in financial institutions. Macro-financial security is shaped by fiscal and monetary policy, macro-prudential regulation and the quality of the financial system's institutional architecture.

At the micro level, financial security is linked to the financial stability of businesses and households. It reflects their ability to maintain liquidity, solvency and investment activity in a changing environment. Key factors include capital structure, access to financial resources, the effectiveness of financial management and risk mitigation. The interdependence of these levels is crucial for ensuring the overall financial stability of the economy. The accumulation of imbalances at the micro level can turn into systemic risks, whilst macroeconomic instability leads to a rise in the cost of capital and an increase in financial risks for businesses. Consequently, the macro and micro levels form a single system of financial security (Table 1).

Table 1. Comparative characteristics of the macro- and micro-levels of financial security

Criterion	Macro-level of financial security	Micro-level of financial security
Object	The State, the financial system	Businesses, households
Objective	Ensuring macro-financial stability	Ensuring solvency and financial stability
Indicators	Public debt, budget deficit, inflation, systemic risk, stability of the banking system	Liquidity, profitability, capital structure, debt burden
Risks	Financial crises, currency shocks, debt instability, systemic risk	Insolvency, default, decline in profitability, financial distress
Supporting tools	Fiscal and monetary policy, macro-prudential regulation	Diversification of funding, risk mitigation
Outcome	Financial system stability and investor confidence	Business resilience and investment activity

Source: summarised by the authors

Table 1 illustrates the differences between the macro- and micro-levels of financial security in terms of the subject matter, indicators, risks and support instruments. At the same time, these levels do not operate in isolation, but form part of a single system of financial stability within the economic system. The macro- and micro-levels constantly interact, creating a unified system of financial stability (Fig. 1). When the financial condition of enterprises deteriorates, tax revenues fall and the debt burden increases. On the other hand, macroeconomic instability increases the cost of borrowing and the risks to business. In the digital economy, this interdependence becomes even greater due to the faster spread of financial crises and the emergence of new cyber risks.

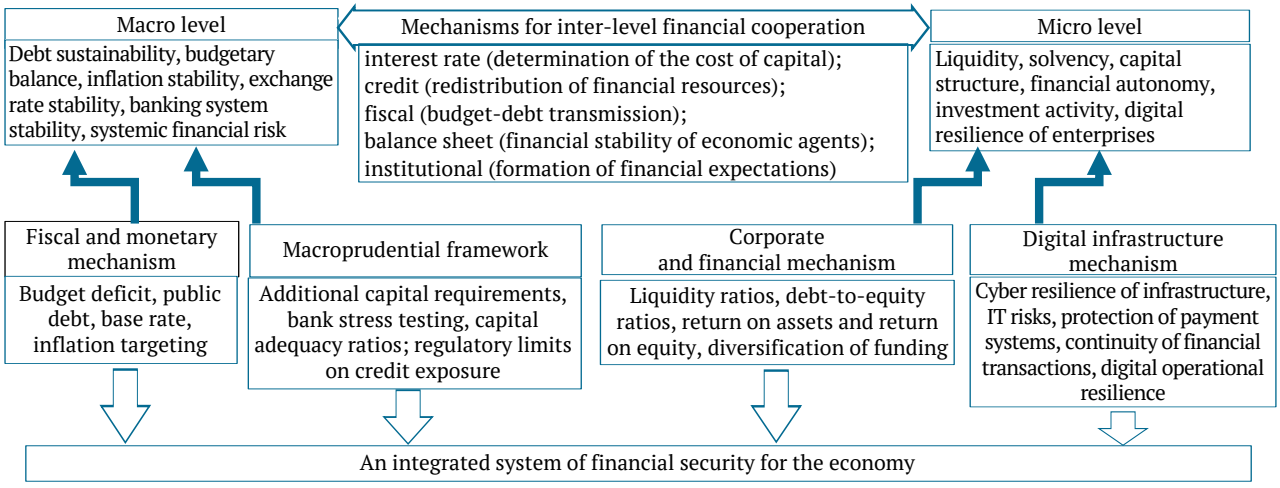


Figure 1. The mechanism of interaction between the macro- and micro-levels of financial security in the economic system
Source: compiled by the authors

The European Union demonstrates an integrated model for ensuring financial security, combining macro- and micro-level regulatory mechanisms. At the macro level, financial security is ensured through the coordination of fiscal policy within the framework of the Stability and Growth Pact, the development of macroprudential regulation, and the activities of supranational financial supervisory institutions. The functioning of the European Banking Union, uniform capital adequacy rules and the monitoring of systemic risks form the basis of system-wide financial stability. At the micro level, financial security is underpinned by corporate standards, transparency requirements for financial reporting, regulatory mechanisms to mitigate risks, and the protection of the rights of investors and consumers of financial services. In the current environment, the digital component of financial security is of particular importance: regulatory acts in the field of digital operational resilience (in particular the Digital Operational Resilience Act (DORA)) are aimed at enhancing the cyber resilience of financial institutions and minimising digital risks. Thus, the European model of financial security is characterised by the institutional integration of the macro- and micro-levels and the combination of traditional regulatory mechanisms with digital tools for ensuring resilience. Consequently, the financial security of the economic system is shaped through the interaction of the macro- and micro-levels, and European practice demonstrates their institutional integration. This approach allows financial security to be viewed not merely as a characteristic of public finances or corporate resilience, but as a systemic property of the economy, ensured through coordinated regulatory, market and digital mechanisms.

A generalisation of the multi-level structure of financial security and European practice regarding its institutional integration enables to move towards the formation of an integrated conceptual model for the transformation of financial security in economic systems within the context of the digital economy. In the digital economy, financial security ceases to be solely a function of macro-financial stability. It is transforming into a multi-level system for countering risks, integrating regulatory, market and digital mechanisms. In order to systematise these interrelationships, it is advisable to develop an integrated conceptual model of the transformation of the financial security of economic systems, which reflects the logic of interaction between the characteristics of the economic system, the risk environment, the instruments for ensuring security and the expected outcomes (Fig. 2).

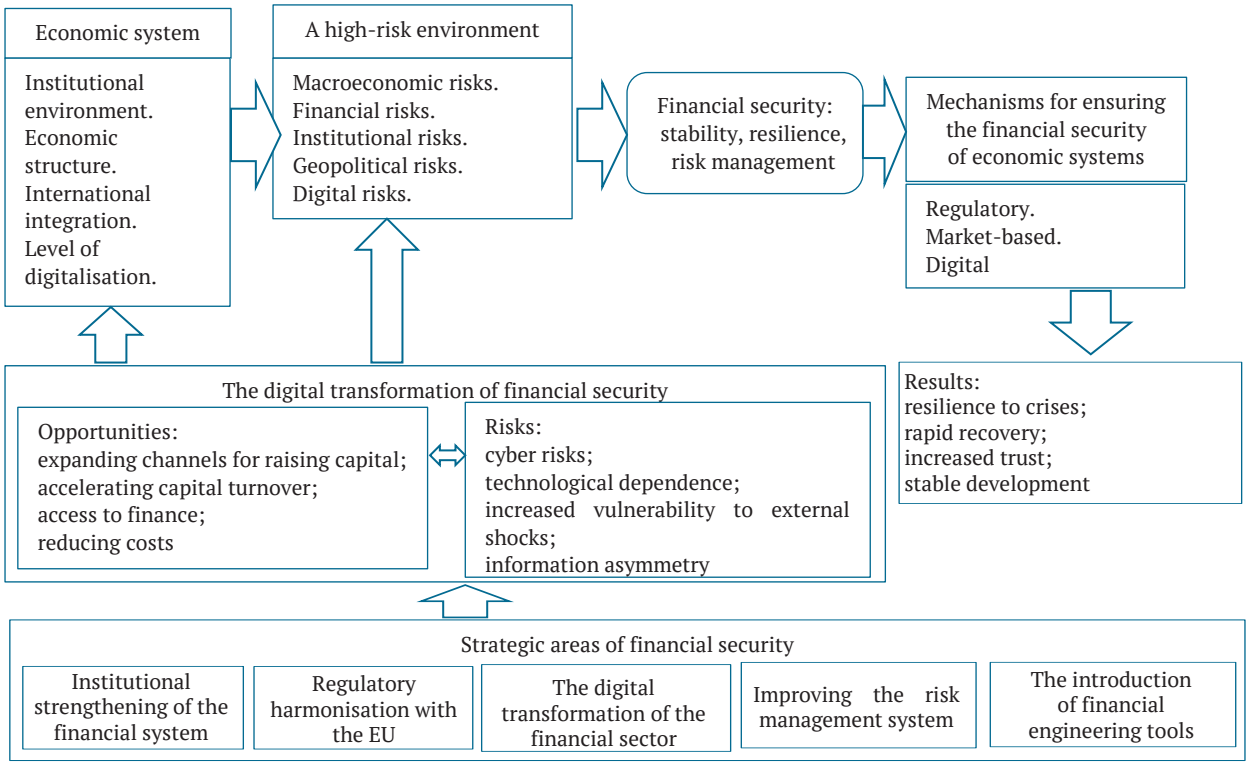


Figure 2. A conceptual model of the transformation of the financial security of economic systems
Source: compiled by the authors

The proposed integrated conceptual model reflects the systemic nature of financial security as a property of the economic system. It combines an institutional approach to the analysis of economic systems with risk-oriented and digital approaches to the interpretation of financial security. The model demonstrates that financial security is shaped by two interrelated components: the structural characteristics of the economic system (institutional architecture, level of openness, digital maturity) and changes in the risk environment (macroeconomic, financial, geopolitical and digital risks). Financial security takes centre stage as an integrative category, combining the stability of financial flows, resilience to shocks and risk manageability at all levels of the economic system. The European institutional

framework in the model serves as an example of a coordinated regulatory approach to ensuring financial security in the digital economy. It is precisely the integration of macroprudential policy, market mechanisms and digital risk mitigation tools that shapes the new architecture of financial security for economic systems. Thus, the proposed model has made it possible to conceptualise the transformation of financial security not as an isolated financial phenomenon, but as a systemic change in the mechanisms governing the functioning of the economic system in the context of digitalisation and growing uncertainty. Implementing the developed model requires taking into account the system of threats arising in the surrounding environment, which have a decisive impact on the financial security of economic systems at both the macro- and micro-levels.

This paper analyses academic and analytical publications concerning the nature, list and characteristics of threats to financial security in Europe and Ukraine. A study by S. Nermin (2025) analyses the current threat environment for European financial institutions against the backdrop of the digitalisation of the economy and growing geopolitical instability. The main focus is on cyber threats as one of the key factors destabilising the financial security of enterprises and financial institutions. It is emphasised that the digitalisation of financial processes, the proliferation of cloud services and automated payment systems, and reliance on third-party IT providers are giving rise to new threats to financial security that go beyond traditional economic risks. The most critical threats include DDoS attacks, ransomware, data breaches, phishing campaigns, social engineering attacks and the compromise of digital service providers. Such threats can result in financial losses, operational disruptions, breaches of business continuity and reputational damage. Attention is drawn to the impact of geopolitical processes on financial security: cyber incidents in the financial sector are increasingly linked to international conflicts, and financial institutions are becoming targets of attacks by both criminal groups and state actors. At the same time, the report emphasises the growing role of threats associated with the use of artificial intelligence, particularly for personalised phishing, automated fraud and the manipulation of digital financial data.

The study by S. Piserà *et al*. (2024) examines the impact of the Russia-Ukraine war on the systemic risk of European non-financial companies during the period 2021-2022. The authors analysed changes in the beta coefficient as an indicator of companies' sensitivity to market and geopolitical shocks, which allows for an assessment of the transformation of financial risks in crisis conditions. The results of the study showed that, following the outbreak of the military conflict, systemic risk for firms in Europe increased in a statistically significant manner, indicating a heightened vulnerability of the corporate sector to external shocks, in particular geopolitical instability, supply chain disruptions, energy crises and financial market volatility. At the same time, it was found that companies with a higher proportion of international sales exhibited a relatively lower level of risk, which can be explained by the diversification of their sales markets and reduced dependence on individual regions. This highlighted the role of globalisation as a factor in partially mitigating financial threats during periods of crisis. In the context of financial security, the study's findings demonstrated that geopolitical events can act as a systemic risk factor that directly affects the financial stability of businesses through changes in market expectations, the cost of capital and investment attractiveness. Thus, the financial security of enterprises in the current environment depends to a large extent on their ability to adapt to external shocks and to ensure geographical and operational diversification of their activities.

An analysis of reports by ENISA (European Union Agency for Cybersecurity, 2024a; 2024b; 2025) has shown that the financial security of enterprises in the EU is shaped by a hybrid cyber-economic threat, suggesting that cyber risks constitute a distinct systemic factor in business financial stability. The most critical of these remain ransomware attacks, phishing and other forms of social engineering, leaks of financial and personal data, as well as DDoS attacks that disrupt the availability of financial services. These threats lead to direct financial losses, the disruption of business processes, the disruption of payment transactions and a decline in confidence in financial institutions. A negative trend is the increasing structural complexity of cyber risks, particularly due to attacks on supply chains, growing reliance on cloud technologies and digital platforms, and the active use of artificial intelligence to automate cyberattacks and financial fraud. As a result, cyber threats extend beyond the purely technical sphere and are becoming a factor in macroeconomic and financial instability. It can be summarised that ENISA's reports view the modern cyberspace as an environment of hybrid threats, in which technological, economic and geopolitical factors interact and reinforce one another. The reports also highlight staff shortages as one of the threats to business security.

The study by Z. Varnalii & A. Mekhed (2022) examines the theoretical and practical aspects of ensuring the financial security of enterprises in the context of the digital transformation of the economy. The authors emphasised that the development of the digital economy is significantly altering the nature of threats to financial security, shifting them from traditional financial and economic factors to complex digital and cyber risks. The study emphasises that the digitalisation of business processes, the active implementation of fintech solutions, automated management systems and electronic financial services enhance the efficiency of enterprises' operations, but at the same time create new vulnerabilities. Key threats to financial security include cybercrime, leaks of confidential financial information, fraud in electronic payment systems, as well as risks associated with dependence on external digital platforms and IT service providers. The authors drew particular attention to the growing importance of systems for mitigating financial risks in the digital economy. They emphasised that businesses must implement modern cyber-security tools, improve staff digital literacy and ensure the diversification of their digital infrastructure to reduce dependence on individual technological solutions.

The authors, L. Dokiienko *et al*. (2024), investigated the system of determinants that shape the level of financial security of enterprises, with a focus on the impact of financial indicators and the risks associated with financing business operations. The publication emphasises that financial security is shaped by a combination of internal and external factors, among which the risks associated with financing a company's operations and the overall level of financial

stability are of particular significance. Accordingly, an increase in the risk of unbalanced financing or a decline in liquidity was considered a direct source of threats to financial security. The article by researchers V. Marchenko & O. Usyk (2025) emphasises that the financial security of enterprises is shaped by a complex of external and internal threats, amongst which macroeconomic instability, fluctuations in financial markets, rising inflation and limited access to investment resources play a particularly significant role. The article highlights the growing role of geopolitical factors, which are increasingly acting as systemic determinants of financial losses and the destabilisation of the business environment. Particular attention is paid to the impact of the digitalisation of the economy, which, on the one hand, helps to improve the efficiency of financial flow management, whilst on the other, creates new threats in the form of cyber risks, dependence on digital platforms, data breaches and increased vulnerability of companies' information systems. The article notes that digital transformation is changing the nature of financial threats, shifting them into the realm of technological and cyber risks.

An analytical report by Sayenko Kharenko (2025) examined the current state of the security environment for enterprises in Ukraine based on a survey of companies across various sectors of the economy. According to the survey results, a key trend identified is the maintenance of high business resilience despite the risks posed by the war: the overwhelming majority of companies do not plan to relocate, which indicates that businesses have adapted to crisis conditions. At the same time, the report highlights a significant increase in security expenditure, particularly on cyber defence, physical security and the development of digital infrastructure. In the context of threats to enterprises' financial security, the document highlights the growing role of cyber risks, which are becoming one of the key factors in financial losses. These include cyberattacks on corporate systems, disruptions to digital processes, attacks on remote infrastructure and the risk of data breaches. These threats directly impact financial stability through operational disruptions, loss of revenue and increased costs of system recovery. Particular emphasis is placed on the importance of investing in the digital resilience of businesses, including the development of cybersecurity and the protection of information systems as a key element of modern financial security. Thus, financial security was considered not only in terms of economic indicators but also in terms of the level of protection afforded to businesses' digital infrastructure.

The KPMG (2025) report examines the business environment in Ukraine during the period of a war economy, as well as the key factors influencing the investment attractiveness and financial resilience of enterprises. The report emphasises that the main systemic threat remains military risk, which directly affects the stability of cash flows, supply chains and infrastructure. The destruction of transport and energy systems during the war results in additional financial losses for businesses and increases the cost of operations. Macroeconomic instability, in particular inflationary pressures, currency restrictions and fluctuations in economic growth, has been identified as a significant group of threats. Such factors affect the availability of capital, investment decisions and the overall solvency of enterprises. At the same time, the report highlights the role of financial restrictions and regulatory changes introduced under martial law to stabilise the economy. Particular attention is paid to infrastructure and operational threats, which are exacerbated by the destruction of logistics routes, restrictions on transport accessibility and the risk of supply disruptions. This creates additional financial costs for enterprises and reduces the efficiency of their resource utilisation. At the same time, the report emphasises that, despite the high level of risks, the Ukrainian economy has demonstrated adaptability and resilience, in particular through the advancement of digitalisation, government business support programmes and international investment mechanisms for capital protection. This has partially offset the impact of these threats and contributed to the formation of a more resilient model of corporate financial security. Thus, a synthesis of the research findings has enabled the compilation of a list of threats to financial security in the context of a comparison between Europe and Ukraine (Table 2).

Table 2. Comparative analysis of threats to the financial security of the EU and Ukraine

Threat category	EU	Ukraine
Geopolitical threats	Geoeconomic competition (US-China-EU)	War as a systemic factor, destruction of assets, loss of markets, high war risks
Digital/cyber threats	Cyberattacks on banks and corporations (ransomware, DDoS), data breaches, dependence on Big Tech and cloud services	Massive cyber-attacks (including cyber-warfare), attacks on state registers, banks and the energy sector, financial fraud
Macroeconomic threats	Inflation, interest rate rises, financial market volatility, energy price fluctuations	Inflation, devaluation, GDP volatility, a sharp decline in investment and consumer demand
Infrastructure threats	Disruptions to global supply chains, dependence on critical technologies and logistics	Destruction of the power grid, disruptions to electricity and internet supply, disruption to logistics
Financial and market threats	Fintech risks, algorithmic errors, capital market instability	Limited access to credit, high cost of capital, dependence on international aid
Regulatory and institutional threats	Tighter digital regulation (GDPR, DORA), compliance costs, investment controls	Instability of the regulatory environment, weak institutional safeguards, corruption risks
Data and AI threats	Artificial intelligence risks (algorithmic errors), data manipulation, Big Data leaks	Limited digital security, low adoption of secure AI, poor cyber literacy
Human resources and social threats	Shortage of digital skills, need for reskilling	Brain drain (particularly in IT), population migration, labour force contraction
Operational digital threats	Dependence on SaaS and cloud platforms, third-party supplier risks	Low digital maturity of businesses, critical dependence on foreign software

Source: compiled by the authors

The data in Table 2 provide a systematic comparison of threats to the financial security of enterprises in the EU and Ukraine, organised by key risk categories. Both contexts are characterised by the multidimensional nature of the threats, which encompass geopolitical, digital, macroeconomic and institutional factors. At the same time, in the EU these threats are more manageable, as they arise in an environment where digitalisation and globalisation create predominantly structural challenges (cyber threats, dependence on technology platforms, fintech risks), which are mitigated by well-developed institutional mechanisms (GDPR, DORA, investment controls). For Ukraine, however, threats to financial security are cumulative and existential in nature. The war acts as a systemic factor, exacerbating other groups of threats – ranging from the destruction of infrastructure and disruption to logistics to restricted access to capital and high volatility in the macroeconomic environment. Digital threats in the Ukrainian context are also more intense due to cyber warfare, weaker infrastructure resilience and limited cyber defence resources.

It can therefore be argued that financial security threats to Ukraine are characterised by a higher level of intensity and mutual reinforcement, and a lower level of manageability. In the EU, digitalisation primarily gives rise to new regulatory and technological challenges within a stable environment; in Ukraine, however, it overlaps with military and macroeconomic shocks, creating a high concentration of risks of financial destabilisation for enterprises. The European experience in countering these complex threats is examined. On 24 January 2024, the European Commission presented a package of initiatives to strengthen the EU's economic security (the EU Economic Security Package), which covers foreign investment screening, export controls, monitoring of outbound investment, research security and support for dual-use technologies, aimed at strengthening the Union's economic security against a backdrop of growing geopolitical tensions and technological transformations. Supporting security is viewed as the EU's ability to minimise risks whilst maintaining the openness of the economy and the competitiveness of the internal market (European Commission, 2024a; 2024b). Four groups of strategic risks have been identified, namely: supply chain vulnerabilities; threats to critical infrastructure, including cyber infrastructure; risks to technological security and the leakage of critical technologies; and risks of economic coercion and the "weaponisation of dependencies" – the use of economic dependence as a tool of pressure. It is precisely these risks that should be regarded as key sources of potential destabilisation of the EU's financial and economic system.

To counter these threats, the European Commission (2024a) has proposed a comprehensive approach based on three strategic pillars: "promote – protect – partner". The first involves enhancing the competitiveness and resilience of the internal market through the development of the industrial, scientific and technological base. The second focuses on creating protective measures, in particular strengthening controls on foreign direct investment, improving export controls, monitoring outbound investment and enhancing the security of critical technologies. The third pillar involves expanding international partnerships with countries that share the EU's approach to economic security. Thus, the EU has proposed a model of proactive economic security, in which the key lies not only in responding to threats but also in pre-emptively countering them through regulatory, investment and technological instruments. In the context of corporate financial security, this entails a transition to a system where the stability of the business environment is ensured through the management of strategic risks, the strengthening of cyber and technological resilience, and the reduction of the EU economy's critical external dependencies. In the authors' view, this approach to ensuring and maintaining financial and economic security under contemporary conditions could be adapted for Ukraine, provided that due consideration is given to the country-specific risks and threats discussed above, particularly those associated with wartime conditions and infrastructures (Table 3).

Table 3. Adapting European experience in countering threats to financial security

Area of support	Ways of adapting to threats to financial security
"Promote" (development and strengthening of resilience)	Accelerating economic recovery and modernisation through the development of critical infrastructure, supporting the relocation of businesses, stimulating investment and expanding the digital transformation of business. Strengthening the financial resilience of businesses through access to capital, state loan guarantees and the development of financial recovery instruments. Developing mechanisms for insuring against war risks. Supporting the restoration of damaged production facilities. Diversifying logistics routes.
"Protect" (protection of strategic assets)	Strengthening cyber security in the financial sector, the energy sector and public registers, as well as developing a system to counter risks to critical infrastructure. Integrating the EU's expertise on investment controls, data protection and the regulation of digital platforms, whilst placing an emphasis on countering cyber warfare and hybrid threats. Protecting critical energy and transport infrastructure. Establishing contingency financial and logistical mechanisms to ensure the economy can continue to function in times of crisis
"Partner" (international cooperation)	Ensuring access to financial resources, technologies and security support mechanisms through integration into European cybersecurity and economic initiatives, participation in joint threat monitoring systems, and the expansion of cooperation with the EU in the field of critical technologies and economic recovery.

Source: compiled by the authors

It should be recognised that European mechanisms for ensuring financial security have been developed largely in the absence of large-scale military conflict on the territory of EU Member States. Consequently, their adaptation

to Ukrainian conditions does not provide a direct solution to the problems of physical destruction of assets or infrastructure, but is aimed at enhancing the economic system's resilience to the consequences of military shocks. In particular, the development of digital infrastructure, cyber-security mechanisms, financial support for businesses, credit guarantee instruments and the enhancement of the state's institutional capacity helps to minimise economic losses, accelerate the recovery of economic activity and strengthen the financial resilience of economic actors in wartime. Thus, in the authors' view, what is most relevant for Ukraine is not the direct replication of the model, but its adaptation as a system for countering cumulative crisis threats, where economic security is directly linked to the financial and cyber resilience of businesses. In wartime, the function of "economic survival" and stabilisation of the business environment can be ensured through the implementation of the first "promote" pillar. Measures within the "protect" pillar can be implemented by integrating the EU's experience in investment controls, data protection and the regulation of digital platforms, which, in financial terms, should lead to a reduction in the risks of payment system failures, data loss and market destabilisation. The "partner" strand (international cooperation) is of strategic importance to Ukraine, as it provides access to the necessary financial resources, technologies and security support mechanisms, through expanded cooperation with the EU in the field of critical technologies and economic recovery.

Thus, adapting the European model for Ukraine entails a transition to an integrated system of economic and financial security, where risk mitigation combines military challenges, digital threats and financial instability, and where the key principle is not only defence but also active resilience and the recovery of the state's economic system. The study's findings confirmed that the financial security of modern economic systems is shaped not only by traditional macro-financial factors, but also by digital, geopolitical and cyber risks. These findings are consistent with the approaches of the European Central Bank (2024), according to which financial stability increasingly depends on the operational resilience of financial infrastructure, the level of cyber security and the ability of financial institutions to adapt to digital transformations. A review by the European Central Bank (2024) emphasises that cyber risks and the digital concentration of financial services can be a source of systemic instability and the rapid spread of financial shocks.

The approach proposed in this article to interpreting financial security as an integrated property of the economic system also correlates with the conclusions of the BIS (2024) regarding the transformation of the global financial architecture under the influence of digitalisation and artificial intelligence. The BIS (2024) report emphasises that the adoption of AI, the platformisation of financial services and reliance on digital technologies enhance the efficiency of the financial sector, but at the same time give rise to new systemic risks associated with cyber threats, algorithmic errors and the concentration of technological infrastructure. Particular attention is paid to risks associated with the use of generative artificial intelligence, the high concentration of cloud services and the dependence of financial institutions on Big Tech companies, which may increase the vulnerability of the global financial system to operational and systemic failures. The findings also corroborate the conclusions of recent studies regarding the growing role of cyber risks in the structure of financial security. In particular, J.C. Crisanto *et al*. (2021) demonstrated that the digitalisation of financial services contributes to the emergence of new channels for the propagation of systemic risks through cyber dependency and the concentration of digital infrastructure. The authors emphasise that cyber risks are not only technological but also systemic in nature, as their spread depends on the scale of digitalisation, the interconnectedness of financial institutions and the concentration of critical digital services. This has confirmed the need to integrate cyber resilience and digital operational resilience into the modern system for ensuring the financial security of economic systems.

A key finding of the study is the justification for the need to adopt a resilient approach to ensuring financial security. This is in line with contemporary academic concepts of "financial resilience" and "operational resilience", according to which the resilience of an economic system is determined not only by its ability to avoid crises, but also by its capacity to adapt, recover swiftly and undergo structural transformation following shocks. Recent research emphasises that, in the context of digitalisation and the growing interdependence of financial institutions, it is the operational resilience of the financial system that takes on key importance; this encompasses the ability to maintain critical functions, the continuity of financial services and confidence in financial institutions, even during large-scale disruptions or cyber-attacks. For instance, in the study by R. Adeney *et al*. (2024), operational resilience is defined as the ability of financial institutions and the financial system as a whole to prevent, adapt to, respond to and recover from operational disruptions that may pose systemic risks to financial stability. Furthermore, recent research on financial resilience has shown that the stability of the financial system increasingly depends on the ability to ensure not only financial liquidity but also digital and institutional continuity. In particular, Y.C. Lou *et al.* (2025) demonstrated that the use of financial technologies has a positive impact on companies' operational resilience by increasing the flexibility of business processes, the resilience of supply chains and the level of adaptability to the external environment.

A comparative analysis of threats to the financial security of the EU and Ukraine has shown that, in the Ukrainian context, digital risks overlap with military and macroeconomic shocks, creating a cumulative nature of threats. Similar conclusions are presented in recent international studies on the impact of geopolitical instability on financial markets and corporate resilience. In particular, W. Boungou & A. Yatié (2022) demonstrated that the outbreak of a full-scale Russian-Ukrainian war led to a significant decline in the returns of global stock markets and an increase in financial volatility, particularly in European countries, due to rising uncertainty, energy risks and disruptions to global economic linkages. A similar view was supported by S. Boubaker *et al.* (2022), who noted that geopolitical conflicts and military risks have a significant impact on financial stability through increased market volatility, heightened inflationary pressures, energy shocks

and rising levels of global uncertainty. This confirmed that geopolitical risks in the modern economy act as an independent factor in financial instability and the transformation of the financial security system.

The study also demonstrated that the European model of financial security is based on the integration of macroprudential regulation, digital operational resilience and mechanisms for protecting critical infrastructure. Of particular significance in this context is Regulation (EU) of the European Parliament and of the Council No. 2022/2554 (2022), which establishes uniform requirements for the identification of ICT risks, incident reporting, digital resilience testing and the management of risks associated with third-party ICT service providers in the EU financial sector. Similar conclusions are presented in the work by C.P. Buttigieg & B.B. Zimmermann (2024), where DORA is considered a key element in strengthening the digital operational resilience of the EU financial sector, although the author also highlighted challenges regarding supervisory convergence, coordination and the fragmentation of the control system. This confirmed that the current European model of financial security combines traditional financial stability regulation with digital mechanisms to ensure cyber resilience and the continuity of financial services. Thus, the study's findings confirmed the need to transition to an integrated model of financial security, within which financial stability is viewed as a comprehensive characteristic of the economic system, shaped by institutional, digital, financial and geopolitical factors. Unlike traditional approaches, the proposed model emphasises the interconnection between digital, geopolitical and institutional risks in the context of the transformation of economic systems and military instability. This broadens current academic understanding of financial security and provides a theoretical foundation for the development of new mechanisms to counter risks in the digital economy.

CONCLUSIONS

As a result of the study, the authors propose an original interpretation of financial security as an integrated property of the economic system, reflecting the financial subsystem's ability to ensure the continuity of financial flows, the efficient allocation of resources, and resilience to exogenous and endogenous risks and threats. A mechanism for the interaction between the macro- and micro-levels of financial security has been developed, and an integrated conceptual model of its transformation in the context of the digital economy has been formulated. It has been established that the current transformation of financial security is taking place under the influence of the digitalisation of financial services, the development of financial technologies, the spread of platformisation and growing dependence on digital infrastructure, which gives rise to new types of systemic risks and cyber threats.

The article summarises the distinctive features of the Anglo-American and European academic traditions in the interpretation of financial security. It has been established that the Anglo-American approach focuses primarily on the study of systemic risk and financial stability, whilst the European model is based on the institutional integration of macroprudential regulation, digital operational resilience and risk mitigation mechanisms. Based on a systemic approach, an integrated conceptual model of the transformation of financial security in economic systems has been developed, combining institutional, risk-oriented and digital approaches. The proposed model allows financial security to be viewed as a dynamic system of interaction between the macro- and micro-levels of the economy in the context of digital transformation and growing uncertainty. A comparative analysis of threats to the financial security of the EU and Ukraine was carried out; the results showed that, for European Union countries, the dominant challenges are digital, cyber and regulatory in nature, linked to the high level of digitalisation in the financial sector. In Ukraine, by contrast, digital risks compound military, macroeconomic and infrastructural threats, creating a cumulative nature of financial instability and increasing the economic system's vulnerability to systemic shocks.

An examination of European experience in ensuring financial security has revealed that the current EU model is based on the principles of proactive risk management, digital resilience and institutional coordination. Particular importance is attached to mechanisms for digital operational resilience, cybersecurity, and the protection of critical infrastructure, as established within the current EU regulatory framework, particularly through the DORA and the European Union's economic security policy. It is argued that the most promising approach for Ukraine is an adaptive one to utilising European experience, focused on establishing an integrated financial security system that combines mechanisms for macro-financial stabilisation, digital resilience, cyber resilience and countering military risks. The key areas of such adaptation are identified as strengthening cyber defence in the financial and military sectors, developing digital infrastructure, supporting the financial resilience of businesses, and integrating Ukraine into European security and financial mechanisms. The proposed approach has made it possible to integrate an institutional understanding of the economic system with a multi-level model of financial security and to incorporate the digital risk dimension as an independent factor in its transformation. Further research should focus on improving the system for countering financial risks at the meso- and micro-levels, taking into account the identified digital, macroeconomic and cyber threats, through the development of modern risk mitigation methods and the implementation of digital protection tools. Another promising area of research is the development of measures to enhance the financial stability and resilience of Ukrainian businesses in the context of post-war recovery.

ACKNOWLEDGEMENTS

None.

FUNDING

Co-funded by the European Union as part of the Erasmus+ Jean Monnet module project "Financial system institutional transformations in era of digital economics: EU experience for Ukraine" (Grant Agreement No. 101127532).

CONFLICT OF INTEREST

None.

REFERENCES

[1] Adeney, R., Hitchins, A., Lane, C., Mehta, H., & Quashie, A. (2024). Operational resilience in a macroprudential framework. *Financial Stability Paper*, 50.

[2] Adrian, T., & Brunnermeier, M.K. (2016). CoVaR. *American Economic Review*, 106(7), 1705-1741. doi: 10.1257/aer.20120555.

[3] Arzhevityn, S., Bortnikov, H., Bublyk, Y., & Liubych, O. (2023). The impact of martial law on the performance of Ukraine's banking sector. *Financial and Credit Activity: Problems of Theory and Practice*, 1(48), 23-41. doi: 10.55643/fcaptp.1.48.2023.3966.

[4] Bianchi, J., & Mendoza, E.G. (2018). Optimal time-consistent macroprudential policy. *Journal of Political Economy*, 126(2), 588-634.

[5] BIS. (2023). *Annual economic report*. Basel: Bank for International Settlements.

[6] BIS. (2024). *Annual economic report*. Basel: Bank for International Settlements.

[7] Boubaker, S., Goodell, J.W., Pandey, D.K., & Kumari, V. (2022). Heterogeneous impacts of wars on global equity markets: Evidence from the invasion of Ukraine. *Finance Research Letters*, 48, article number 102934. doi: 10.1016/j.frl.2022.102934.

[8] Boungou, W., & Yatié, A. (2022). The impact of the Ukraine-Russia war on world stock market returns. *Economics Letters*, 215, article number 110516. doi: 10.1016/j.econlet.2022.110516.

[9] Buttigieg, C.P., & Zimmermann, B.B. (2024). The digital operational resilience act: Challenges and some possible solutions. *ERA Forum*, 25, 11-28. doi: 10.1007/s12027-024-00793-w.

[10] Crisanto, J.C., Ehrentraud, J., & Fabian, M. (2021). Big techs in finance: Regulatory approaches and policy options. *FSI Briefs*, 12.

[11] Dokiienko, L., Hrynyuk, N., Britchenko, I., Trynchuk, V., & Levchenko, V. (2024). Determinants of enterprise's financial security. *Quantitative Finance and Economics*, 8(1), 52-74. doi: 10.3934/QFE.2024003.

[12] European Central Bank. (2024). *Financial stability review*. Frankfurt am Main: European Central Bank.

[13] European Commission. (2024a). *Communication from the Commission to the European Parliament and the Council: Advancing European economic security: An introduction to five new initiatives*. Retrieved from https://commission.europa.eu/system/files/2024-01/Communication%20on%20European%20economic%20security.pdf.

[14] European Commission. (2024b). *New tools to reinforce the EU's economic security*. Retrieved from https://commission.europa.eu/news-and-media/news/new-tools-reinforce-eus-economic-security-2024-01-24_en.

[15] European Union Agency for Cybersecurity. (2024a). *ENISA threat landscape 2024*. Athens: ENISA.

[16] European Union Agency for Cybersecurity. (2024b). *2024 report on the state of cybersecurity in the Union*. Athens: ENISA.

[17] European Union Agency for Cybersecurity. (2025). *The EU cybersecurity index 2024: EU-level insights and next steps*. Athens: ENISA.

[18] Gorton, G., & Ordoñez, G. (2020). Good booms, bad booms. *Journal of the European Economic Association*, 18(2), 618-665. doi: 10.1093/jeea/jvy058.

[19] Haldon, J., Eisenberg, M., Izdebski, A., Mordechai, L., Newfield, T.P., Sarris, P., & White, S. (2021). Between resilience and adaptation: A historical framework for understanding stability and transformation of societies under shock and stress. In I. Linkov, J.M. Keenan & B.D. Trump (Eds.), *COVID-19: Systemic risk and resilience* (pp. 235-268). Cham: Springer. doi: 10.1007/978-3-030-71587-8_14.

[20] He, Z., & Krishnamurthy, A. (2013). Intermediary asset pricing. *American Economic Review*, 103(2), 732-770. doi: 10.1257/aer.103.2.732.

[21] International Monetary Fund. (2024). *Global financial stability report*. Washington: International Monetary Fund.

[22] Kanova, O. (2023). Approaches to interpreting the concept of an economic system and its research. *Economy and Society*, 50. doi: 10.32782/2524-0072/2023-50-13.

[23] KPMG. (2025). *Your business in Ukraine*. Kyiv: KPMG.

[24] Lou, Y.C., Zhu, Q.Y., & Liang, C.J. (2025). Financial technology and firm operational resilience: The roles of supply chain resilience and marketing capability. *International Review of Economics & Finance*, 104, article number 104744. doi: 10.1016/j.iref.2025.104744.

[25] Marchenko, V., & Usyk, O. (2025). External and internal threats to the financial and economic security of enterprises. *Herald of Khmelnytskyi National University. Economic Sciences*, 338(1), 329-333. doi: 10.31891/2307-5740-2025-338-49.

[26] National Bank of Ukraine. (2024). *Financial stability report*. Retrieved from https://surl.li/vnqmzy.

[27] Nermin, S. (2025). *Threat landscape briefing: Financial institutions in Europe*. Retrieved from https://www.linkedin.com/pulse/threat-landscape-briefing-financial-institutions-europe-nermin-smajić-1dthf/.

[28] Nosan, N., & Nazarenko, S. (2022). Financial security management in economic security systems at different management levels: Methodological issues. *Financial and Credit Activity: Problems of Theory and Practice*, 6(41), 138-146. doi: 10.18371/fcaptp.v6i41.251418.

[29] Pisera, S., Chiaramonte, L., Paltrinieri, A., & Pichler, F. (2024). Firm systematic risk after the Russia-Ukraine invasion. *Finance Research Letters*, 64, article number 105489. doi: 10.1016/j.frl.2024.105191.

[30] Regulation (EU) of the European Parliament and of the Council No. 2022/2554 "On Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011". (2022, December). Retrieved from https://surl.lt/iqikhm.

[31] Rodrik, D. (2021). Why does globalization fuel populism? Economics, culture, and the rise of right-wing populism. *Annual Review of Economics*, 13, 133-170. doi: 10.1146/annurev-economics-070220-032416.
[32] Sayenko Kharenko. (2025). *Assessment of business security in Ukraine*. Retrieved from https://sk.ua/wp-content/uploads/2025/12/opituvannja-bezpeki_2025_ukr-2-2.pdf.
[33] Semenenko, O., Abramova, M., Tarasov, O., Mytchenko, S., Dziubchuk, R., & Fomkin, D. (2025). Resilience and sustainable development: Key theoretical and practical narratives and lessons of the military economy. *Social Development and Security*, 15(2), 314-326. doi: 10.33445/sds.2025.15.2.24.
[34] Tymoshyk, N., Krylova, O., Miroshnychenko, Y., Kyrychenko, K., & Myronchuk, V. (2022). Dilemmas and solutions in the functioning of Ukraine's banking system under martial law. *Financial and Credit Activity: Problems of Theory and Practice*, 5(46), 40-53. doi: 10.55643/fcaptp.5.46.2022.3905.
[35] Varnalii, Z., & Mekhed, A. (2022). Business entities' financial security under digital economy. *Financial and Credit Activity: Problems of Theory and Practice*, 4(45), 267-275. doi: 10.55643/fcaptp.4.45.2022.3813.
[36] Walker, B. (2020). Resilience: What it is and is not. *Ecology and Society*, 25(2), article number 11. doi: 10.5751/ES-11647-250211.
[37] World Bank. (2026). *Global economic prospects*. Washington: World Bank.

Марина Берест
Кандидат економічних наук, доцент
Харківський національний економічний університет імені Семена Кузнеця
61165, просп. Науки, 9А, м. Харків, Україна
https://orcid.org/0000-0002-2410-3210

Наталія Сабліна
Кандидат економічних наук, доцент
Харківський національний економічний університет імені Семена Кузнеця
61165, просп. Науки, 9А, м. Харків, Україна
https://orcid.org/0000-0002-1931-2851

Трансформація фінансово-економічної безпеки економічних систем: європейський досвід та виклики цифрової економіки

Анотація. Актуальність дослідження зумовлена необхідністю переосмислення підходів до забезпечення фінансової безпеки економічних систем в умовах цифрової трансформації, посилення геополітичної нестабільності та зростання системних ризиків. Метою статті було дослідження трансформації фінансової безпеки економічних систем в умовах цифрової економіки на основі інтеграції інституційного, ризик-орієнтованого та цифрового підходів, а також узагальнення європейського досвіду протидії фінансовим ризикам та загрозам фінансовій безпеці, і визначення можливостей його адаптації для України. Для досягнення поставленої мети використано методи теоретичного узагальнення, контент-аналізу наукових і аналітичних джерел, системного та порівняльного аналізу. Їх застосування дозволило дослідити еволюцію наукових підходів до трактування фінансової безпеки, визначити особливості її трансформації під впливом цифровізації та здійснити порівняльний аналіз загроз фінансовій безпеці в країнах Європейського Союзу та Україні. У результаті дослідження запропоновано авторське трактування фінансової безпеки як інтегрованої властивості економічної системи, розроблено механізм взаємодії макро- та мікрорівнів фінансової безпеки та сформовано інтегровану концептуальну модель її трансформації в умовах цифрової економіки. Встановлено, що цифровізація фінансового сектору суттєво змінює структуру загроз фінансовій безпеці через посилення кіберризиків, технологічної залежності та впливу цифрової інфраструктури на стійкість економічних систем. Виявлено відмінності у структурі загроз фінансовій безпеці ЄС та України. Визначено, що сучасна європейська модель забезпечення фінансової безпеки базується на принципах цифрової резильєнтності, інституційної координації та проактивної протидії ризикам. Практичне значення отриманих результатів полягає у можливості використання запропонованих підходів під час формування державної політики у сфері фінансової безпеки, розроблення стратегій цифрової трансформації фінансового сектору, підвищення цифрової резильєнтності та адаптації європейського досвіду до умов повоєнного відновлення економіки України

Ключові слова: діагностика; резильєнтність; фінансова стійкість; фінансовий інжиніринг; кредитне навантаження; цифрові технології; євроінтеграція