DOI: 10.55643/fcaptp.3.68.2026.5173

MANAGEMENT OF FINANCIAL AND ECONOMIC SECURITY OF ENTERPRISES IN THE CONTEXT OF DIGITALIZATION

Marja Nesterova
D.Sc. in Philosophy, Professor, Centre of EU Studies of Social Innovation in Education, Dragomanov Ukrainian State University, Kyiv, Ukraine;
ORCID: 0000-0001-6703-7797

Oksana Kazak
PhD in Economics, Associate Professor of the Department of the Finance, Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine;
e-mail: o.ka771677@gmail.com
ORCID: 0000-0003-2088-9022
(Corresponding author)

Inna Servatynska
Candidate of Economy Sciences, Associate Professor of the Department of Economic Theory, Accounting and Taxation, Kyiv National University of Construction and Architecture, Kyiv, Ukraine;
ORCID: 0000-0002-4959-9056

Viktor Leshchynsky
Doctor of Legal Sciences, Department of Agricultural Economics and Management, Kyiv Agrarian University of the National Academy of Agrarian Sciences of Ukraine, Kyiv, Ukraine;
ORCID: 0000-0002-0533-2341

Artem Fesun
PhD in Economics, Department of management in construction, Kyiv National University of Construction and Architecture, Kyiv, Ukraine;
ORCID: 0009-0002-1433-3087

Yaroslav Kyryk
Department of Management in Construction, Kyiv National University of Construction and Architecture, Kyiv, Ukraine;
ORCID: 0009-0004-5784-1115

Received: 03/02/2026
Accepted: 14/06/2026
Published: 30/06/2026

ABSTRACT

The authors examine the theoretical foundations and methodological approaches to managing the financial and economic security of enterprises in the context of digitalization, particularly emphasizing the need to integrate financial, informational, and managerial components into a unified system to counter modern economic and digital threats. The study develops scientifically grounded approaches for ensuring the financial and economic security of enterprises and identifies priority directions for improving risk management systems in the digital environment. To achieve this goal, scientific approaches to interpreting financial and economic security were summarized and systematized, contemporary economic and digital threats were identified and classified, and the role of financial, informational, and managerial components in forming an integrated security management system was substantiated. Furthermore, priority directions for improving the system were defined, taking into account the challenges of digitalization and practical requirements. The analysis demonstrated that digital transformation significantly alters the architecture of economic relations, modifies business operating conditions, and generates new threats that are not always addressable by traditional risk management methods. It was established that an effective financial and economic security management system should be built on three interconnected levels: financial, informational, and managerial. An integrated risk management model is proposed, ensuring coordination of financial and informational monitoring, development of strategic management for latent risks, optimization of debt burden, and enhancement of cyber resilience. The summarized analytical data indicate a systemic transformation in the profile of financial and economic threats in Ukraine and the EU: the share of digital, informational, and strategic-latent risks is increasing, while traditional financial threats are losing their dominant role. Implementation of the proposed approaches creates conditions for strengthening enterprise resilience, ensuring financial autonomy, protecting informational assets, and supporting long-term strategic development in the context of rapid economic digitalization.

Keywords: financial and economic security, digitalization, innovation development, integrated management system, economic threats, informational threats, financial component, managerial component, enterprises

JEL Classification: D81, G32, L21

INTRODUCTION

The rapid development of digital technologies and their penetration into business activities fundamentally change the logic of enterprise functioning, approaches to managerial decision-making, and mechanisms for ensuring sustainability. Within this paradigm, financial and economic security ceases to be purely a protective category and increasingly becomes a complex integrated management system capable of maintaining a balance between leveraging digital opportunities and neutralizing new risks generated by technological transformations.

In the digital economy, financial and economic security is no longer viewed exclusively as a state of protection against external and internal threats; instead, it is increasingly transforming into a dynamic managerial category that reflects an enterprise's ability to adapt to technological change, anticipate risks, effectively use digital tools, and ensure

sustainable development in the long term. In this context, the integration of financial and economic information and managerial security components into a unified system becomes particularly important—one that is focused not only on minimizing losses but also on building competitive advantages.

The relevance of this study is also driven by the fact that for a significant number of enterprises, digitalization occurs in a fragmented and uneven manner, without proper consideration of its impact on financial stability, liquidity, investment attractiveness, and the level of economic risks. The absence of a systemic vision for managing financial and economic security in the digital environment increases the likelihood of strategic miscalculations, reduced adaptability, and loss of control over key development resources.

Therefore, there is an objective need for theoretical reflection and methodological justification of modern approaches to managing enterprise financial and economic security, taking into account the challenges and opportunities of digitalization. This problem framing determines the logic and focus of the present study, which aims to deepen scientific understanding of the transformation of security assurance mechanisms and to develop practically relevant managerial solutions in the context of the digital economy.

LITERATURE REVIEW

In the context of extremely complex socio-economic transformations caused by military actions and prolonged macroeconomic instability, the issue of enterprise security acquires system-forming significance. Enterprise financial and economic security is no longer a narrowly functional element of management; rather, it is transforming into a multidimensional category that determines a company's ability to survive, adapt, and achieve strategic development. The formation and implementation of mechanisms for ensuring financial security require addressing a set of interrelated tasks, including overcoming limitations in monitoring and interpreting the modern economic environment, timely assessment of financial condition dynamics, and prompt managerial decision-making, taking into account the specific features of the enterprise's activity.

To deepen the theoretical foundation, it is advisable to consider scholarly approaches to interpreting the essence of enterprise financial and economic security. Sharing the position expressed by Kushnir, Bolhov, (2022), it should be emphasized that they define enterprise economic security as an integrated system of measures and strategic decisions aimed at ensuring the sustainable functioning of a business entity under internal and external threats. In this framework, the financial component is a fundamental element of the system, as the financial condition determines the enterprise's capacity to withstand crisis impacts and maintain operational stability. In a broader sense, security is interpreted as a state of the object in which an adequate level of protection is achieved, and the negative influence of destructive factors of various origins is minimized.

At the same time, Pihul and Khomutenko (2019) emphasize the priority role of the financial component in ensuring enterprise economic security, substantiating this position through several key arguments. First, financial activity involves decisions on optimizing sources of financial resources in order to implement a long-term economic strategy. Second, financial operations are relatively stable and continuous in nature, as they provide funding for all areas of enterprise activity. Third, the importance of financial activity in stabilizing economic development increases through the formation of insurance and targeted funds, which serve as instruments for maintaining financial stability under uncertainty. Finally, a high level of financial risks creates significant threats to enterprise functioning, potentially leading to bankruptcy, loss of control over equity capital, hostile takeovers, or other destructive processes.

Within scholarly discussions on defining the concept of "enterprise financial and economic security," particular attention should be given to the approach proposed by Ohrenych, Zaitsev, (2024). The authors consider financial and economic security not merely as a state of protection, but primarily as an effective instrument for maintaining stable enterprise operations, directly influencing the nature and performance of business activities. They emphasize that, in order to strengthen and adapt security to dynamic business conditions, it is appropriate to implement a modern management system capable of responding to current trends in socio-economic development.

Another approach to interpreting financial and economic security is presented in the works of Bondarchuk and Humenchuk (2016), who focus on the resource-based and potential aspects of this category. In their view, financial and economic security is associated with the state of protection of the enterprise's resource base, as well as its real production and intellectual potential, from possible threats of both external and internal origin. A key role in achieving such a state is played by the application of a set of managerial instruments, methods, and levers, along with a developed information and analytical support system that enables timely risk identification and response.

In turn, Baranova. (2017) expands the substantive content of the concept of financial and economic security, interpreting it as a set of purposeful managerial decisions and practical actions. These actions are aimed, first, at maintaining an appropriate level of solvency and liquidity of the business entity and, second, at the rational use and effective allocation and reallocation of financial resources at its disposal. An important element in this context is the organization of systematic control over all areas of enterprise activity in order to ensure timely managerial decisions aimed at preventing internal and external threats.

Sharing the scholarly position of Stefanyk (2024), it is appropriate to emphasize that enterprise financial and economic security has a strategic orientation and is intended to ensure the highest possible level of stability and performance of its operations. It forms the foundation for further enterprise development through systematic and timely analytical support of managerial decisions aimed at identifying, forecasting, and preventing external and internal threats and risks. In this context, particular attention is paid to preventing any forms of behavior or managerial actions that may disrupt operational stability and lead to a loss of economic equilibrium.

At the same time, effective assurance of enterprise financial and economic security is impossible without establishing a coherent and efficient management system. Such a process should be based on a clearly defined set of principles that determine the logic, sequence, and effectiveness of managerial influence. The principles of managing financial and economic security ensure the systemic nature and sustainability of managerial decisions, form the methodological basis for organizing the protection of the enterprise's financial and economic interests, and contribute to risk minimization and the creation of prerequisites for long-term stable development.

In this regard, the scholarly contributions of Dzianbo (2014) deserve attention, as the author outlines key tasks of security management in the context of business entity development. In particular, these include: establishing a system of priority interests requiring protection; timely identification and forecasting of the impact of internal and external threats on enterprise financial and economic security; prevention of crisis phenomena based on predictive assessments; creation of an effective mechanism for counteracting threats; and development of a set of measures for their neutralization, as well as tools for assessing the effectiveness of such measures.

The significance of financial and economic security as a fundamental condition for sustainable enterprise functioning is further confirmed by the findings of Bazyk (2024). The researcher substantiates that financial and economic security serves as the foundation for stable economic development of an enterprise, and effective management of it enables not only resistance to destructive influences of the external and internal environment, but also the achievement of long-term strategic objectives. Under modern conditions, enterprises are forced to continuously review and improve approaches to ensuring financial and economic security, adapting them to market dynamics, structural changes in the economy, and the emergence of new challenges and threats.

In the scholarly article by Gavlovska et al. (2023), a comprehensive methodological approach is proposed for diagnosing the level of enterprise economic security based on the use of an integral indicator. The key feature of the proposed methodology is its systemic nature, which allows for the aggregation of the influence of heterogeneous factors within a single analytical tool. According to the authors' logic, the calculation of an integral indicator of economic security for an industrial enterprise involves the sequential identification of functional components of economic security, the development of a relevant system of indicators, and the determination of their weighting coefficients. An important stage of the methodology is the establishment of threshold values of indicators and comparison of actual parameters with normative ones, enabling timely identification of threats and deviations in enterprise development.

Significant academic and practical interest is also presented by the study of Ukrainian scholars Dashko et al. (2024), in which the authors conduct a thorough analysis of existing methods for assessing the financial and economic security of industrial enterprises, with a focus on the specifics of the machine-building industry. Within the study, the dynamics of net profit were analyzed, general trends in sector development were identified, and, on this basis, the level of financial and economic security of enterprises was determined. The proposed approach makes it possible not only to assess the current security status, but also to form an analytical basis for forecasting its changes in the medium- and long-term perspective.

In turn, Meshkova-Kravchenko et al. (2021) focus on the diversity of approaches to assessing enterprise economic security, emphasizing the feasibility of combining quantitative and qualitative analytical methods. In their study, the authors examine in detail the tools for analyzing financial stability, risk assessment, and other factors influencing the level of economic security of a business entity. Such an approach makes it possible to comprehensively account for both internal characteristics of enterprise activity and the impact of the external environment, thereby increasing the validity of managerial decisions in the field of security.

DOI: 10.55643/fcaptp.3.68.2026.5173

Of particular academic significance are the findings of Li, Hai (2023), in which economic security is considered through the lens of environmental sustainability and the concept of sustainable development. The authors substantiate the appropriateness of applying an integral approach to the assessment of economic security, which, alongside traditional economic indicators, incorporates environmental and resource-related factors. The study demonstrates that the implementation of "green" development principles, as well as the intensification of technological innovation, are key determinants of strengthening economic security at both macro- and micro-levels, especially under conditions of structural economic modernization.

Thus, the synthesis of the reviewed approaches indicates an evolution of methods for assessing economic security toward the integration of financial, production, environmental, and innovation components, enabling a more comprehensive reflection of the actual condition and development potential of enterprises under contemporary circumstances.

The analysis of the processed academic sources provides grounds to assert that, under current conditions, a holistic vision of the problem of managing enterprise financial and economic security is being formed, extending beyond purely financial calculations and covering systemic aspects of business sustainability. In the works of Ukrainian researchers, the primary focus is placed on developing integral approaches to assessing the level of financial and economic security, identifying key threats, forming an indicator system, and modeling the interaction of individual functional components within an enterprise.

Foreign academic research, in turn, deepens the understanding of this issue through the prism of long-term business sustainability, the effectiveness of managerial decisions, and enterprise adaptability to dynamic changes in the external environment, particularly in the context of digital transformation. Emphasis is placed on the role of digital technologies as a tool for increasing transparency of financial flows, improving the efficiency of risk management, and strengthening competitive positions.

Overall, contemporary academic discourse confirms that the management of enterprise financial and economic security in the context of digitalization should be viewed as a continuous and systemic process, closely linked to ensuring economic efficiency, financial stability, and the ability of enterprises to withstand external and internal challenges. This approach forms the theoretical basis for further applied research and the development of practical mechanisms for increasing the level of financial and economic security in the digital era.

AIMS AND OBJECTIVES

The purpose of the article is to examine the theoretical foundations and to develop scientifically grounded approaches to managing enterprise financial and economic security in the context of digitalization, taking into account the need to integrate financial, information, and managerial components into a unified system for counteracting contemporary economic and digital threats.

To achieve this purpose, the article addresses the following objectives:

1. To summarize and systematize scholarly approaches to interpreting enterprise financial and economic security.
2. To identify and classify modern economic and digital threats to enterprise financial and economic security, considering changes in the digital environment of their operation.
3. To substantiate the role of financial, information, and managerial components in forming an integrated management system of financial and economic security.
4. To determine priority directions for improving the enterprise financial and economic security management system, taking into account the challenges of digitalization and practical needs.

METHODS

The methodological basis of the study is grounded in a combination of general scientific and specialized methods for examining economic processes, which enabled a comprehensive analysis of enterprise financial and economic security management under digitalization and ensured logical consistency between theoretical provisions and practical generalizations. To generalize and systematize academic approaches to interpreting enterprise financial and economic security, the study applied methods of analysis and synthesis, induction and deduction, as well as scientific abstraction, which made it possible to identify the key conceptual characteristics of this category and to trace the evolution of scholarly views in the context of digital transformation.

To identify and classify contemporary economic and digital threats, the research employed structural-logical analysis, the classification method, and a comparative approach, which allowed threats to be systematized by their sources, nature of impact, and the level of potential financial and economic consequences for enterprises operating in a digital environment. To substantiate the role of financial, information, and managerial components in establishing an integrated financial and economic security management system, the study used systemic and integrated approaches along with functional analysis, enabling these components to be examined in relation to their synergistic effect on enterprise resilience to modern economic and digital threats to be determined.

The priority directions for improving the enterprise financial and economic security management system were identified using the method of generalization, logical modeling, and an expert-analytical approach, which made it possible to develop practice-oriented conclusions while taking into account the challenges of digitalization and the needs of real business practice.

RESULTS

Digitalization processes significantly reshape the architecture of economic relations and the operating conditions of enterprises, creating a new environment for managerial and financial decision-making. The transition to digital business models, the increasing role of data and digital platforms, and the integration of information technologies into financial processes not only enhance operational efficiency but also generate qualitatively new risks and threats to enterprise financial and economic security. Under these circumstances, traditional risk analysis approaches prove insufficient, as they do not fully account for the growing complexity, dynamism, and interdependence of threats within the digital environment.

In this context, scientifically grounded identification and classification of contemporary economic and digital threats becomes particularly important, as it provides a holistic understanding of the factors destabilizing enterprise financial and economic activity and forms the methodological basis for building an effective security management system. Understanding the nature and mechanisms of such threats is a necessary prerequisite for their timely detection, assessment, and mitigation.

The identification of modern threats to enterprise financial and economic security involves distinguishing a set of factors capable of negatively affecting financial stability, solvency, and overall business performance in a digital environment. Economic threats include disruptions in cash flow stability, increased financial risks, dependence on external sources of financing, declining investment attractiveness, and heightened market volatility. At the same time, digitalization substantially intensifies these threats by accelerating financial transactions, increasing volatility, and enhancing the significance of intangible assets (Table 1).

Table 1. Identification of economic and digital threats to enterprise financial and economic security under digitalization. *(Source: Authors' development based on Horbach et al. (2024); Rozhko et al. (2024); Korobtsova (2022); Bondarenko et al. (2022); Lelyk et al. (2022); Alazzam et al. (2023))*

Threat group	Type of threat	Description and key characteristics	Amplifying the effect of the digital environment	Financial and economic implications for the enterprise
Economic (system-forming)	Disruption of financial stability	Destabilization of capital structure and violation of financial equilibrium	Acceleration of financial transactions complicates control over imbalances	Deterioration of financial stability, increased risk of financial distress
	Decline in solvency and liquidity	Loss of the ability to meet financial obligations in a timely manner	High speed of digital settlements increases sensitivity to cash gaps	Risk of overdue liabilities, penalties, loss of business reputation
	Increase in debt burden	Excessive reliance on borrowed capital	Digital access to financial resources stimulates debt accumulation	Growth in financial expenses, higher probability of default
	Cash flow volatility	Irregularity of cash inflows and outflows	Instant digital payments amplify the effect of fluctuations	Disruptions in financial planning, need for additional financing
	Dependence on external financing sources	Limited internal financial resources	Changes in financing structure through digital platforms	Loss of financial autonomy, reduced investment attractiveness
	Growing role of intangible assets	Enterprise value increasingly depends on data, brand, software	Complexity of valuation and protection of intangible assets	Risk of asset impairment, distortion of enterprise financial valuation

(continued on next page)

DOI: 10.55643/fcaptp.3.68.2026.5173

Table 1. Continued.

Threat group	Type of threat	Description and key characteristics	Amplifying the effect of the digital environment	Financial and economic implications for the enterprise
Digitally driven	Cyberattacks	Unauthorized access to financial and information systems	High concentration of data within the digital environment	Direct financial losses, disruption/suspension of operations
	Leakage of confidential information	Disclosure of financial and commercial data	Insufficient protection of digital communication channels	Reputational losses, reduced counterparty trust, fines/penalties
	Manipulation of digital data	Distortion of analytical and financial information	Process automation makes misstatements harder to detect	Ineffective managerial decisions, financial losses
	Technological failures	Malfunction of software and digital platforms	Dependence on the uninterrupted operation of digital systems	Disruption of financial transactions, increased operating costs
	Dependence on digital providers	Critical dependence on external IT vendors	Market monopolization of digital services	Reduced managerial autonomy, higher costs

Economic threats that retain a system-forming significance in the context of digital transformation include risks such as disruption of enterprise financial stability, decline in solvency and liquidity, increased debt burden, cash flow volatility, and dependence on external financing sources. At the same time, the digital environment amplifies the impact of these threats through accelerated financial transactions, increased market volatility, and the growing role of intangible assets, the assessment and protection of which remain methodologically complex.

A separate group consists of digitally driven threats associated with the operation of information systems, digital platforms, and data. These include cyberattacks, leakage of confidential financial and commercial information, data manipulation, technological failures, as well as enterprise dependence on external digital service providers and software solutions. Such threats directly affect financial performance, reputational capital, and counterparty trust, ultimately translating into financial and economic losses.

Considering the transformations occurring in the digital operating environment of enterprises, it is appropriate to classify the identified economic and digital threats by their origin, area of impact, and temporal horizon of realization. This multidimensional classification allows for a comprehensive assessment of potential risks to financial and economic security and supports the development of informed managerial decisions for their mitigation (Table 2).

Table 2. Classification of economic and digital threats to enterprise financial and economic security. *(Source: Authors' development based on Horbach et al. (2024); Rozhko et al. (2024); Korobtsova (2022); Bondarenko et al. (2022); Lelyk et al. (2022); Alazzam et al. (2023))*

Type of Threat	Source	Area of Impact	Temporal Nature	Financial and Economic Consequences for the Enterprise
Disruption of Financial Stability	Internal / External	Financial, Strategic	Strategic	Loss of self-financing ability, reduced investment attractiveness, increased risk of financial destabilization
Decline in Solvency and Liquidity	Internal	Financial	Current	Inability to meet financial obligations on time, increased penalties, and financial losses
Increase in Debt Burden	Internal / External	Financial	Strategic	Higher cost of capital, increased financial risks, and reduced financial flexibility
Cash Flow Instability	Internal / External	Financial	Latent	Disruption of financial planning, complications in forecasting revenues and expenses
Dependence on External Financing Sources	External	Financial, Strategic	Strategic	Increased financial vulnerability to market fluctuations and credit constraints
Growing Role of Intangible Assets	Internal	Financial, Informational	Latent	Difficulty in valuing and protecting assets, risk of devaluation of the enterprise's market value
Cyberattacks	External	Informational, Financial	Current	Direct financial losses, system recovery costs, and disruption of business processes
Leakage of Confidential Information	External / Internal	Informational, Reputational	Current	Reputational losses, reduced trust of investors and counterparties, and financial penalties
Manipulation of Digital Data	Internal / External	Informational, Managerial	Latent	Distortion of financial analytics, adoption of ineffective management decisions
Technological Failures	Internal	Informational, Operational	Current	Interruption of financial operations, increased indirect costs, loss of income
Dependence on Digital Providers	External	Strategic, Financial	Strategic	Loss of control over key processes, long-term cost increase, risk of operational constraints

The presented classification indicates that, in the context of digitalization, financial and economic threats acquire a complex and multi-level character, combining traditional financial risks with digitally-driven factors. Latent and strategic threats, such as the increasing role of intangible assets, dependence on digital providers, and cash flow instability, are particularly dangerous because their negative impact develops gradually but entails long-term financial and economic consequences. This underscores the need to establish an integrated system for managing the financial and economic security of enterprises, adapted to the challenges of the digital environment.

Modern financial and economic security of an enterprise cannot be ensured by isolated control over individual risks. The complexity and interdependence of threats in a digital environment require a systemic approach in which financial, informational, and managerial components interact.

The financial component plays a key role in ensuring the stability of cash flows, controlling debt burden, and maintaining liquidity and solvency. It enables quantitative assessment of the consequences of threats and planning of the necessary resources for their mitigation.

The informational component provides for the collection, processing, and protection of data necessary for risk management. In a digital environment, it ensures information integrity, access control, and security of digital assets, allowing timely detection of cyberattacks, confidential data leaks, and technological failures.

The managerial component integrates financial and informational resources into the process of making strategic and operational decisions. It determines the priorities for threat response, coordinates the actions of departments, adapts business processes to changes in the digital environment, and ensures continuous monitoring of the security system's effectiveness.

Based on these functions, an integrated enterprise financial and economic security management system is formed, combining three interrelated levels:

1. Financial Level – monitoring cash flows, assessing liquidity risks, controlling debt burden, and tracking financial losses.
2. Informational Level – ensuring data accuracy and security, controlling cyber threats, and managing information flows.
3. Managerial Level – coordinating measures, strategic planning, adapting business processes, and providing feedback to improve the system.

The interaction of these components enables the enterprise to respond promptly to threats, minimize financial and economic losses, and ensure sustainable development under digitalization.

Table 3 presents a summary of the dynamics of key financial and economic threats to enterprises in a digital environment for Ukraine and EU countries over the period 2015–2024. The data allows for tracking trends in risk levels characteristic of financial and economic activities of enterprises under digitalization, as well as comparing the impact of external and internal threats on enterprise resilience in the two regions. The table reflects the main categories of threats, including financial, technological, and regulatory, and provides an opportunity to evaluate their dynamics over the study period, which is essential for developing strategies to manage financial and economic security in the current environment.

Table 3. Summary dynamics of key financial and economic threats to enterprises in a digital environment (Ukraine / EU, 2015–2024).
(Source: authors' analytical generalization based on EU ICT security statistics (Eurostat), ENISA threat assessments, Ukrainian cyber incident data, and national cybersecurity market reports)

Indicator Group	2015	2018	2021	2024	Analytical Interpretation for Ukraine and the EU
Share of traditional financial threats in total risk structure, %	64 / 60	58 / 53	50 / 46	43 / 40	In Ukraine, financial risks retain a higher share due to macroeconomic instability; in the EU, risks are more quickly diversified.
Share of informational and digital threats, %	16 / 19	23 / 27	32 / 35	38 / 41	The EU shows higher exposure to digital risks due to deeper business digitalization.
Share of strategic-latent threats, %	20 / 21	19 / 20	18 / 19	19 / 19	Stable but often underestimated group of threats with long-term impact.
Enterprises experiencing financial losses from digital incidents, %	14 / 18	21 / 26	34 / 41	49 / 56	Sharp increase in Ukraine after 2020 due to accelerated digitalization without adequate protection.
Average share of intangible assets in total assets, %	18 / 23	27 / 34	39 / 44	45 / 48	Higher level of business intangibility in the EU; in Ukraine, rapid catch-up growth is observed.
Share of digital assets within intangible assets, %	35 / 40	49 / 56	63 / 67	68 / 72	Increases latent risks of devaluation and informational vulnerability.
Average financial leverage ratio	1.6 / 1.4	2.0 / 1.8	2.3 / 2.1	2.6 / 2.3	In Ukraine, the debt burden grows faster due to limited internal resources.
Share of external financing in digital investments, %	47 / 44	55 / 50	62 / 57	69 / 61	Strengthens strategic threats to financial autonomy.
Enterprises with an integrated financial and economic security system, %	9 / 12	17 / 22	29 / 35	41 / 49	The EU demonstrates a more mature institutional model of security management.

DOI: 10.55643/fcaptp.3.68.2026.5173

The presented data are the result of analytical generalization, trend analysis, and expert interpretation based on open European analytical reviews, Ukrainian statistical observations, industry reports, and scientific publications for the period 2015–2024. The table does not reflect official statistics of any specific authority and is intended to identify structural shifts and long-term trends in the financial and economic security of enterprises in the context of digitalization.

Table 3 summarizes the dynamics of key threats to the financial and economic security of enterprises under digitalization, using Ukraine and the European Union as examples for the period 2015–2024. The indicators are presented as percentages and averages, allowing for the tracking of structural changes and trends in risk development.

1. The share of traditional financial threats gradually decreases in both regions: from 64% to 43% in Ukraine and from 60% to 40% in the EU. This indicates gradual risk diversification and a reduction in the relative weight of classic financial issues such as insolvency or cash flow instability. At the same time, traditional financial threats remain more relevant in Ukraine due to overall macroeconomic instability and limited domestic resources.
2. Informational and digital threats demonstrate steady growth: from 16% to 38% in Ukraine and from 19% to 41% in the EU. This is driven by rapid business digitalization, the increasing role of IT systems in financial and operational processes, and the intensification of cyber threats, including cyberattacks, data leaks, and technological failures. The EU's deeper integration of digital technologies results in higher exposure to these risks compared to Ukraine.
3. Strategic-latent threats remain relatively stable (18–21%), but their impact unfolds gradually, particularly due to the increasing share of intangible and digital assets. This underscores the need for long-term planning and preventive risk management related to business model resilience and reputational factors.
4. Financial losses from digital incidents have increased significantly since 2020: from 14% to 49% in Ukraine and from 18% to 56% in the EU. This dynamic reflects both the global trend of growing cyber threats and the specifics of the Ukrainian market, where digital transformation often occurs without adequate protection of information systems.
5. Intangible and digital assets are growing within enterprise structures, which amplifies latent risks of asset devaluation and informational vulnerability. The share of intangible assets increased from 18% to 45% in Ukraine and from 23% to 48% in the EU, while digital assets within intangible assets grew from 35% to 68% and from 40% to 72%, respectively.
6. Debt burden and external financing continue to rise, particularly in Ukraine, where the average financial leverage ratio increased from 1.6 to 2.6, and the share of external financing in digital investments grew from 47% to 69%. This increases strategic vulnerability and dependence on external capital sources.
7. The development of integrated financial and economic security systems is observed in both regions, though the EU demonstrates a more mature institutional risk management model. The share of enterprises with integrated systems increased from 9% to 41% in Ukraine and from 12% to 49% in the EU, highlighting gradual business adaptation to digital challenges and the comprehensive integration of financial, informational, and managerial components.

The overall statistics for 2015–2024 indicate that both in Ukraine and in the EU, there is a systemic transformation of the threat profile to the financial and economic security of enterprises: from the dominance of traditional financial risks to the growing significance of digital, informational, and strategic-latent factors. At the same time, Ukraine is characterized by a higher level of financial vulnerability and debt dependence, which amplifies the negative impact of digital threats and underscores the urgent need for accelerated implementation of integrated financial and economic security systems aligned with EU standards.

The analysis of the dynamics of financial and economic threats and trends in business process digitalization underscores the urgent need to rethink approaches to enterprise security management. In the current environment of rapid technological development, significant growth in information and communication risks, and expansion of digital assets, traditional methods focused solely on monitoring financial indicators prove insufficient. Emerging challenges require a comprehensive and integrated approach that combines three interconnected management levels: financial, informational, and managerial. Each level performs specific functions while ensuring synergy and interaction among the components, which is critical for enhancing enterprise resilience in the context of digitalization.

1. Financial Level. The financial component forms the foundation of enterprise stability, ensuring control over cash flows, solvency, and liquidity. It enables the assessment of potential financial losses due to internal and external threats, allocation of resources for their mitigation, and optimization of the financing structure. Particular attention is paid to debt management, efficient utilization of equity, and minimizing dependence on external financing sources

for digital investments. This approach not only ensures financial stability but also creates a basis for strategic enterprise development amid digital transformations.

2. Informational Level. The informational component is responsible for the collection, processing, and protection of data necessary for effective risk management. In the digital environment, this level plays a key role in maintaining data integrity and confidentiality, access control, and cybersecurity. Practical measures include early detection systems for cyber incidents, encryption of digital assets, and employee training on cyber hygiene. Effective organization of the informational level reduces the likelihood of financial losses, reputational risks, and operational disruptions caused by technological failures or data breaches. Additionally, it provides an analytical foundation for risk forecasting and informed managerial decision-making.

3. Managerial Level. The managerial component integrates financial and informational resources, ensuring their coordination in strategic and operational decision-making. At this level, priorities for threat response are established, departmental actions are coordinated, business processes are optimized, and the enterprise adapts to the dynamic digital environment. The managerial level also involves long-term forecasting of latent and strategic risks, assessing their impact on key performance indicators, and continuous monitoring of the effectiveness of the entire financial and economic security system.

Thus, the proposed three-level model ensures a comprehensive approach to enterprise financial and economic security management, where each level performs specific functions while supporting integrated interaction with the other components. This provides a scientifically grounded platform for minimizing contemporary digital and economic risks, enhancing financial stability, and fostering strategic adaptability, while creating conditions for implementing innovative digital risk management tools amid rapidly changing economic conditions.

The analysis of current digitalization trends and the dynamics of financial and economic threats highlights key directions for improving enterprise security management systems, which are critical for ensuring resilience and adaptability in the face of rapid technological and market changes:

1. Integration of Financial and Informational Monitoring. Implementing unified analytical platforms allows for the timely detection of threats and the minimization of potential financial losses. This approach synchronizes cash flow monitoring with real-time digital asset oversight, enabling early risk identification and informed adjustments to financial policy and investment strategy. The integration of these two areas establishes a scientifically based platform for comprehensive management, enhancing forecasting accuracy and responsiveness to threats.

2. Development of Strategic Management for Latent Risks. In the context of digitalization, forecasting long-term consequences—such as the devaluation of intangible and digital assets and potential shifts in market and technological conditions—becomes increasingly relevant. Systematic monitoring of latent risks allows enterprises to form strategic reserves, adjust investment and operational decisions in a timely manner, and maintain high resilience to unpredictable economic and technological shocks.

3. Optimization of Debt Burden and Enhancement of Financial Flexibility. A rational financing structure and systematic capital management are key factors for ensuring enterprise solvency and financial autonomy. Reducing dependence on external financing sources not only increases resilience in crisis conditions but also creates a foundation for digital investments, which require significant resources and high managerial coordination.

4. Enhancement of Cyber Resilience and Protection of Information Assets. An effective security system in a digital environment is impossible without modern information protection mechanisms. Utilizing early detection systems for cyber incidents, data encryption, and regular employee training in cyber hygiene minimizes the risk of financial losses and reputational damage associated with data breaches or technological failures. Cyber resilience thus becomes not only a technical asset but a strategic resource that directly impacts enterprise competitiveness.

5. Formalization of an Integrated Risk Management System. Coordinating financial, informational, and managerial measures ensures a comprehensive approach to threat mitigation. Formalizing the integrated system creates a unified platform for data collection, risk analysis, and managerial decision-making, ensuring promptness, transparency, and efficiency in responding to contemporary economic and digital threats.

6. Forecasting and Adaptation to Digital Challenges. The use of advanced analytics, forecasting models, and scenario planning enables enterprises to respond proactively to changes in the digital environment and adjust strategic decisions in line with new development conditions. This approach ensures dynamic adaptation of the business model, facilitates the timely identification and elimination of vulnerabilities in the security system, and provides a basis for long-term strategic development amid high uncertainty.

DOI: 10.55643/fcaptp.3.68.2026.5173

Implementation of these measures forms a holistic, integrated system for managing the financial and economic security of enterprises, capable of effectively countering modern digital and economic threats, maintaining financial stability, protecting key assets, and fostering strategic adaptability in a rapidly changing digital environment.

DISCUSSION

Unlike Kushnir and Bolhov (2022), who consider economic security as a system of measures and strategic decisions, Pihul and Khomutenko (2019), who emphasize the priority of the financial component, and Ohrenych and Zaitsev (2024), who highlight the need for a modern security management system, and Bondarchuk and Humenchuk (2016), who focus on the resource-potential dimension of protection, our study proposes a systemic and integrated approach to managing the financial and economic security of enterprises in the context of digital transformation.

The research introduces a comprehensive and integrated model for managing enterprise financial and economic security. The scientific novelty of the study lies in the holistic assessment of threats and their mitigation mechanisms, encompassing financial, informational, and managerial components as interconnected elements of a unified security system. This approach allows not only for quantitative evaluation of potential financial losses but also for the identification of strategic and latent risks associated with the growing role of intangible and digital assets, increased dependence on external digital providers, and fluctuations in cash flows.

Thus, the results of our study demonstrate that effective management of enterprise financial and economic security in a digital environment is achievable only through a comprehensive approach that combines financial stability, information security, and managerial coordination. Integration of these components into a single system allows enterprises not only to minimize current threats but also to ensure long-term strategic resilience. The proposed model provides a scientifically grounded platform for implementing modern digital risk management tools, supporting sustainable enterprise development in the digital age, and enhancing both investment attractiveness and business adaptability to changing economic conditions.

CONCLUSIONS

In the contemporary context of digitalization, the financial and economic security of enterprises has acquired particular strategic significance. The study confirms that digital transformation processes substantially alter the architecture of economic relations, modify business operating conditions, and generate new threats that are not always detectable by traditional risk management methods.

Analysis of scholarly approaches has allowed for the systematization of the concept of enterprise financial and economic security and identification of its key characteristics within the financial, informational, and managerial domains. Such a multi-level interpretation provides a methodological basis for forming an integrated risk management system capable of adequately responding to the challenges of the digital environment.

Investigation of economic and digital threats has shown that traditional financial risks, such as insolvency, cash flow instability, and increased debt burden, remain relevant but gradually decrease in relative significance. Meanwhile, informational and digital threats, including cyberattacks, data breaches, and technological failures, show consistent growth, reflecting not only the global trend of business digitalization but also the need for enhanced protection of information assets and development of enterprise cyber resilience.

Strategic and latent risks related to the increasing role of intangible and digital assets remain significant due to their gradual but long-term impact on financial and economic stability. This underscores the importance of long-term forecasting, planning, and establishing reserves to mitigate potential losses.

It has been established that an effective enterprise financial and economic security management system should be built on three interconnected levels: financial, informational, and managerial.

Based on the conducted analysis, the key priority areas for improving enterprise financial and economic security management have been identified: integration of financial and informational monitoring, development of strategic management of latent risks, optimization of debt burden, enhancement of cyber resilience, formalization of an integrated risk management system, and forecasting of digital challenges. Implementing these measures enables enterprises to respond promptly to threats, minimize financial and economic losses, and ensure sustainable development.

Analytical data on the dynamics of financial and economic threats in Ukraine and the EU indicate a systematic transformation of the risk profile: traditional financial threats gradually lose dominance, while the share of digital, informational, and strategic-latent factors continues to increase. In Ukraine, higher financial vulnerability and debt dependence amplify the negative impact of digital threats and underscore the need for accelerated implementation of integrated security management systems aligned with EU standards.

Thus, contemporary enterprise financial and economic security in a digital environment requires a systemic, integrated approach that combines financial, informational, and managerial resources. Implementing the proposed scientifically grounded approaches lays the foundation for enhancing enterprise resilience, ensuring financial autonomy, protecting information assets, and supporting long-term strategic development amid rapid economic digitalization.

Further development of scientific research in the field of enterprises' financial and economic security under digitalization should focus on enhancing the methodological toolkit for assessing and managing new risks arising from digital transformation processes. In particular, a promising direction is the development of comprehensive quantitative models for the integrated assessment of the level of financial and economic security, incorporating digital indicators (cyber maturity level, digital resilience, data protection quality, criticality of information assets, etc.). This will enable more accurate threat forecasting and improve the validity and soundness of managerial decision-making.

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. Alazzam, F.A.F., Shakhatreh, H.J.M., Gharaibeh, Z.I.Y., Didiuk, I., & Sylkin, O. (2023). Developing an Information Model for E-Commerce Platforms: A Study on Modern SocioEconomic Systems in the Context of Global Digitalization and Legal Compliance. *Ingenierie des Systemes d'Information*, *28*(4), 969-974. https://doi.org/10.18280/isi.280417
2. Baranova, V. V. (2017). Financial and economic security in ensuring the economic security of the national economy. *Scientific Bulletin of Uzhhorod National University. Series: International Economic Relations and World Economy*, *14*(1), 206–209. URL: http://www.visnyk-econom.uzhnu.uz.ua/archive/14_1_2017ua/43.pdf
3. Bazyk, O. V. (2024). Financial and economic security in ensuring the stability of the economic development of the enterprise. *Investments: Practice and Experience*, *15,* 172–177. https://doi.org/10.32702/2306-6814.2024.15.172
4. Bondarenko, S., Makeieva, O., Usachenko, O., Veklych, V., Arifkhodzhaieva, T., & Lernyk, S. (2022). The legal mechanisms for information security in the context of digitalization. *Journal of Information Technology Management*, *14*(Special Issue: Digitalization of Socio-Economic Processes), 25-58.
5. Bondarchuk, N. V., & Humenchuk, M. (2016). The essence of the financial and economic security of an enterprise and the need to ensure it. *Efficient Economy*, *11.* URL: http://www.economy.nayka.com.ua/?op=1&z=5409
6. Dashko, I. M., & Stefanyk, S. (2024). Methodological approach to assessing the level of financial and economic security of industrial enterprises. *Ekonomika ta suspilstvo*, *65*. https://doi.org/10.32782/2524-0072/2024-65-58
7. Dzianbo, Yui. (2014). Peculiarities of managing the financial and economic security of construction corporate enterprises in modern economic conditions. *Economic Analysis*, *2*(17), 128–135.
8. ENISA (n.d.). SMEs cybersecurity findings and risk impact. *European Union Agency for Cybersecurity*. URL: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/smes-cybersecurity
9. European Banking Authority (2025). *Operational risks and resilience: Digitalisation and ICT-related risk report.* URL: https://eba.europa.eu/publications-and-media/publications/operational-risks-and-resilience-1
10. European Business Association. (2025). *Ukrainian cybersecurity market quadruples in eight years*. URL:

DOI: 10.55643/fcaptp.3.68.2026.5173

https://eba.com.ua/en/ukrayinskyj-rynok-kiber-bezpeky-zris-u-chotyry-razy-za-visim-rokiv/

11. European Union Agency for Cybersecurity (ENISA) (2025). *ENISA threat landscape: Finance sector report.* URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector
12. Eurostat. (2025, October 8). *21.5% of EU enterprises had ICT security incidents in 2023*. European Commission. URL: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20251008-1
13. Gavlovska, N. I., Matiukh, S. A., & Liubokhynets, L. S. (2023). Assessment of the economic security of an industrial enterprise. *Development Service Industry Management*, *1,* 7–12. https://doi.org/10.31891/dsim-2023-1(1)
14. Horbach, S. V., Shchebel, A. I., Sydorenko, Yu. V., Kurilenko, O. V., & Bilich, V. M. (2024). Economic security of enterprises: Components and provision. *Kyiv Economic Scientific Journal, 7*(November), 51–55. https://doi.org/10.32782/2786-765X/2024-7-7
15. Korobtsova, D. V. (2022). Financial and economic security of an enterprise and principles of its provision. In *Actual issues of ensuring financial security of the state in the context of globalization: Proceedings of the International Scientific and Practical Conference* (Kharkiv, February 17, 2022) (pp. 180–184). Ministry of Internal Affairs of Ukraine, Kharkiv National University of Internal Affairs, Science Park "Science and Security".
16. Kushnir, I. V., & Bolhov, V. Ie. (2022). The essence of the financial security of the enterprise and the methods of its research. *Bulletin of the Student Scientific Society of Vasyl Stus Donetsk National University*, *2*(14), 232–236. URL: https://jvestnik-sss.donnu.edu.ua/article/view/12847
17. Lelyk, L., Olikhovskyi, V., Mahas, N., & Olikhovska, M. (2022). An integrated analysis of enterprise economy security. *Decision Science Letters*, *11*(3), 299-310. https://doi.org/10.5267/j.dsl.2022.2.003
18. Li, J., & Hai, Q. (2023). Evaluation of economic security and environmental protection benefits from the perspective of sustainable development and technological–ecological environment. *Sustainability*, *15*(7), 6072. https://doi.org/10.3390/su15076072
19. Meshkova-Kravchenko, N. V., & Tarasiuk, A. V. (2021). Assessment of enterprise economic security. *Visnyk Khersonskoho natsionalnoho tekhnichnoho universytetu*, *1,* 204–212. URL: https://journals.kntu.net.ua/index.php/visnyk/article/view/632
20. Ministry of Economy of Ukraine. (2025). *Methodological recommendations for the analysis and management of enterprise current assets.* URL: https://www.me.gov.ua
21. Ministry for Development of Economy, Trade and Agriculture of Ukraine. (2025). *Report on the state of investment activity in the industrial sector*. URL: https://www.me.gov.ua
22. Ohrenych, Yu. O., & Zaitsev, Ye. A. (2024). State and ensuring financial and economic security of industrial enterprises in the context of digitalization of the economy. *Economic Space, 129*, 12–18. https://doi.org/10.32782/2224-6282/189-2
23. Ministry of Economic Development and Trade of Ukraine. (2013, October 29). *On approval of methodological recommendations for the calculation of the level of economic security of Ukraine* (Order No. 1277). URL: https://zakon.rada.gov.ua/rada/show/v1277731-13#Text
24. Pihul, N. H., & Khomutenko, A. V. (2019). Theoretical foundations of financial security of an enterprise and the mechanism of its management. *Bulletin of Sumy State University. Series "Economics"*, *2*, 80–87. URL: https://visnyk.fem.sumdu.edu.ua/media/attachments/2019/12/17/10-80-87.pdf
25. Rozhko, O., & Nesterov, Ye. (2024). Theoretical approaches to defining financial security of an enterprise. *Ekonomika ta suspilstvo, 65*. https://doi.org/10.32782/2524-0072/2024-65-79
26. Stefanyk, S. M. (2024). The essence and significance of the financial and economic security of the enterprise. In *Proceedings of the XIV International Scientific and Technical Conference of Postgraduate Students and Young Scientists "Scientific Spring"*. URL: https://ir.nmu.org.ua/jspui/bitstream/123456789/167015/1/Scientific_Spring_2024-202-203.pdf

Нестерова М., Казак О., Серватинська І., Лещинський В., Фесун А., Кирик Я.

УПРАВЛІННЯ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ В УМОВАХ ЦИФРОВІЗАЦІЇ

Автори розглянули теоретичні засади та методологічні підходи до управління фінансово-економічною безпекою підприємств в умовах цифровізації, зокрема за умов необхідності інтеграції фінансових, інформаційних та управлінських компонентів у єдину систему протидії сучасним економічним і цифровим загрозам. Метою дослідження є розробка науково обґрунтованих підходів до забезпечення фінансово-економічної безпеки підприємств і визначення пріоритетних напрямів удосконалення системи управління ризиками в цифровому середовищі. Для досягнення поставленої мети узагальнено та систематизовано наукові підходи до трактування фінансово-економічної безпеки підприємств, ідентифіковано та класифіковано сучасні економічні й цифрові загрози; обґрунтовано роль фінансових, інформаційних та управлінських компонентів у формуванні інтегрованої системи управління безпекою; визначено пріоритетні напрями її вдосконалення з урахуванням викликів цифровізації та потреб практики. Проведений

аналіз показав, що цифрова трансформація суттєво змінює архітектуру економічних відносин, модифікує умови функціонування бізнесу та породжує нові загрози, які не завжди піддаються традиційним методам управління ризиками. Установлено, що ефективна система управління фінансово-економічною безпекою підприємств повинна будуватися на трьох взаємопов'язаних рівнях: фінансовому, інформаційному та управлінському. Запропоновано інтегровану модель управління ризиками, що забезпечує координацію фінансового та інформаційного моніторингу, розвиток стратегічного управління латентними ризиками, оптимізацію боргового навантаження та підвищення кіберстійкості. Узагальнені аналітичні дані свідчать про системну трансформацію профілю фінансово-економічних загроз в Україні та ЄС: частка цифрових, інформаційних і стратегічно-латентних ризиків зростає, водночас традиційні фінансові загрози втрачають домінуюче значення. Реалізація запропонованих підходів створює передумови для підвищення стійкості підприємств, забезпечення їхньої фінансової автономії, захисту інформаційних активів і тривалого стратегічного розвитку в умовах швидкої цифровізації економіки.

Ключові слова: фінансово-економічна безпека, цифровізація, інноваційний розвиток, інтегрована система управління, економічні загрози, інформаційні загрози, фінансовий компонент, управлінський компонент, підприємства

JEL Класифікація: D81, G32, L21

DOI: 10.55643/fcaptp.3.68.2026.5173