ISSN 2786-5002 (online)
ISSN 2786-4995 (print)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені В. Н. КАРАЗІНА

ФІНАНСОВО-КРЕДИТНІ СИСТЕМИ: ПЕРСПЕКТИВИ РОЗВИТКУ

ЗБІРНИК НАУКОВИХ ПРАЦЬ

Випуск 3(22)2026

Заснований 2021р.

Харків – 2026

УДК 336.7:338.24

Збірник наукових праць «Фінансово-кредитні системи: перспективи розвитку» публікує наукові статті, які містять оригінальні результати розв'язання питаннь економіки, обліку, фінансів та банківської справи, управління та інформаційних технологій зазначених напрямків. Журнал виходить 4 рази на рік (березень, червень, вересень, грудень).

ISSN 2786-5002 (online) **ISSN 2786-4995 (print)**

Головний редактор:
Самородов Борис, Харківський національний університет імені В. Н. Каразіна, Україна
Заступник головного редактора:
Азаренкова Галина, Харківський національний університет імені В. Н. Каразіна, Україна
Відповідальний редактор:
Мірошник Олексій, Харківський національний університет імені В. Н. Каразіна, Україна
Технічний редактор:
Покровська Марія, Харківський національний університет імені В. Н. Каразіна, Україна

РЕДАКЦІЙНА КОЛЕГІЯ:

Абдул Азіз Абдул Рахман, Королівський університет, Бахрейн
Адамонене Рута, Університет Миколаса Ромеріса, Литва
Акімова Людмила, Національний університет водного господарства та природокористування, Україна
Бабічев Анатолій, Харківський національний університет імені В. Н. Каразіна, Україна
Балезентіс Томас, Литовський центр соціальних наук, Литва
Баранова Валерія, Харківський національний університет імені В. Н. Каразіна, Україна
Гороховатський Володимир, Харківський національний університет радіоелектроніки, Україна
Данкевич Андрій, Національний університет харчових технологій, Україна
Доерті Боб, професор, Школа бізнесу та суспільства Університету Йорк, Велика Британія
Житар Максим, Національний університет «Київський авіаційний інститут», Україна
Ільїч Людмила, Київський університет імені Бориса Грінченка, Україна
Карас Міхал, Технологічний університет у Брно, Чехія
Мельниченко Олександр, Гданський політехнічний університет, Польща
Нурул Мохаммад, Міжнародний університет Даффоділ, Бангладеш
Семеног Андрій, Сумський державний університет, Україна
Сергієнко Олена, Національний технічний університет «Харківський політехнічний інститут», Україна
Сіманавічіене Жанета, Університет Миколаса Ромеріса, Литва
Ткаченко Наталія, Київський національний університет імені Тараса Шевченка, Україна
Хусам-Алдін Нізар Аль-Малкаві, Британський університет в Дубаї, Об'єднані Арабські Емірати

Збірник наукових праць «Фінансово-кредитні системи: перспективи розвитку» внесений до категорії Б переліку фахових видань України (Наказ Міністерства освіти і науки України № 582 від 24.04.2024, Наказ Міністерства освіти і науки України № 928 від 11.06.2026): C1 Економіка (0311 Economics); C3 Міжнародні відносини (0312 Political sciences and civics, 0314 Sociology and cultural studies); D1 Облік і оподаткування (0411 Accounting and taxation); D2 Фінанси, банківська справа, страхування та фондовий ринок (0412 Finance, banking and insurance); D3 Менеджмент (0413 Management and administration; 0415 Secretarial and office work); D4 Публічне управління та адміністрування (0413 Management and administration); D5 Маркетинг (0414 Marketing and advertising); D7 Торгівля (0414 Marketing and advertising, 0416 Wholesale and retail sales).

Затверджено до друку рішенням Вченої ради Харківського національного університету імені В. Н. Каразіна (протокол № 17 від 05 жовтня 2026 року)

Усі права захищені. Передрук і переклади дозволяються лише зі згоди автора та редакції.
Редакція не завжди поділяє думку автора й не відповідає за фактичні помилки, яких він припустився.

Засновник:
Харківський національний університет імені В. Н. Каразіна,
майдан Свободи 4, м. Харків, 61022, Україна. **www.karazin.ua**

Сайт збірника: **https://periodicals.karazin.ua/fcs** Електронна адреса: **fcs.journal@karazin.ua**
Ідентифікатор медіа у Реєстрі суб'єктів у сфері медіа: R30-04477 (Рішення № 1538 від 09.05.2024 року Національної ради України з питань телебачення і радіомовлення. Протокол № 15)

© Харківський національний університет імені В. Н. Каразіна, 2026

Management of financial and credit systems and the socio-humanitarian component of their development

Viadrova Nadiia, Lytvynenko Alina, Fridman Olena, Lytvynenko Olena
Digital transformation of enterprise crisis management under economic instability 185

Kokorieva Olha, Safonova Yelizavieta
Responsible AI maturity model in the strategic management
of corporate social responsibility of enterprises 205

Kramarenko Anna
From theory to practice: the phenomenon of teaching entrepreneurship in EdTech 216

Misiura Ievgeniia, Novikova Tetyana, Khrystoforova Olena, Malafieiev Timur
Digital transformation of project management: current challenges and future prospects 230

Mykolenko Olena, Denchyk Iryna
The role of digital technologies in building the organizational resilience of enterprises.....251

Petrykiva Olha, Beregna Irina
Optimizing the management of primary care facilities in the face of crisis challenges 273

Stashchuk Dmytro, Aleksin Glib
Reconceptualizing value-based management: an integrated conceptual framework.....286

Управління фінансово-кредитними системами та соціально-гуманітарна компонента їх розвитку

Management of financial and credit systems and the socio-humanitarian component of their development

https://doi.org/10.26565/2786-4995-2026-3-12
UDC 005.334:004.9

Viadrova Nadiia
PhD in Economics, Associate Professor,
Associate Professor at the Department of Banking Business and Financial Technologies
V. N. Karazin Kharkiv National University
4 Svobody Square, Kharkiv, 61022, Ukraine
e-mail: 3000918@gmail.com
ORCID ID: 0000-0003-2386-3231
Lytvynenko Alina
PhD in Economics, Associate Professor,
Associate Professor at the Department of International Economic Relations and Business Security
Simon Kuznets Kharkiv National University of Economics
9a Nauky Avenue, Kharkiv, 61165, Ukraine
e-mail: alina.lytvynenko@hneu.net
ORCID ID: 0000-0003-0372-5130
Fridman Olena
PhD in Economics, Associate Professor,
Associate Professor at the Department of Management, Accounting and Business Communications
V. N. Karazin Kharkiv National University
4 Svobody Square, Kharkiv, 61022, Ukraine
e-mail: o.fridman@karazin.ua
ORCID ID: 0000-0002-7437-6372
Lytvynenko Olena
PhD in Economics, Associate Professor,
Associate Professor at the Department of Economics and Business
State Biotechnology University
44 Alchevskykh Street, Kharkiv, 61002, Ukraine
e-mail: o.litvinenko@btu.kharkov.ua
ORCID ID: 0000-0002-8360-4461

Digital transformation of enterprise crisis management under economic instability

Abstract. The full-scale war and economic instability have significantly altered the operating environment of Ukrainian enterprises and necessitated the transformation of traditional approaches to crisis management. Under these conditions, digital transformation is becoming an important component of crisis management strategy, ensuring business process continuity, real-time risk monitoring, and enhanced enterprise adaptability. The use of artificial intelligence, Big Data, cloud technologies, the Internet of Things, digital twins, and predictive analytics facilitates the transition from a reactive model of crisis management to a predictive and adaptive one. Digitalization is of particular importance in the context of Ukraine's post-war recovery and European integration. In the current environment, digital transformation has emerged as one of the key factors in ensuring enterprise resilience and long-term development.

© Viadrova Nadiia, Lytvynenko Alina, Fridman Olena, Lytvynenko Olena, 2026
This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0.

Problem statement. Despite the rapid development of digital technologies and their increasing adoption by enterprises, the integration of digital tools into crisis management systems remains insufficiently systematic. Technological solutions and traditional crisis management mechanisms are often considered separately, limiting enterprises' ability to anticipate crises, respond promptly to risks, and maintain economic resilience under conditions of high uncertainty.

Unresolved issues. Despite a substantial body of research on digitalization and crisis management, comprehensive approaches to developing a digital model of enterprise crisis management remain insufficiently elaborated. The relationships between an enterprise's level of digital maturity, its adaptability to crisis-related challenges, and the effectiveness of managerial decision-making in a highly turbulent environment require further investigation.

Purpose of the article. The purpose of the article is to provide a theoretical rationale and identify practical directions for the digitalization of enterprise crisis management in order to enhance enterprise resilience and adaptability under conditions of economic instability.

Main material. The study is based on systemic and comparative approaches to analyzing the digital transformation of enterprise crisis management under conditions of economic instability. The article examines enterprise digital maturity and digital resilience, contemporary risk management tools, and the potential of artificial intelligence, Big Data, ERP, CRM, cloud technologies, IoT, Digital Twin, and predictive analytics to ensure business process continuity and adaptability. Based on a synthesis of European and U.S. experience, the study substantiates the prospects for adapting these approaches to the Ukrainian context and proposes a five-level Digital Crisis Management Framework designed to support risk monitoring and forecasting, managerial decision-making, and the adaptive recovery of enterprises.

Conclusions. The digital transformation of crisis management is defined as a comprehensive process of integrating advanced digital technologies into the strategic management system with the aim of enhancing enterprise adaptability, business process continuity, and economic resilience. A strategic priority for Ukrainian businesses is the development of Digital Economic Resilience through the use of artificial intelligence, predictive analytics, data-driven management, and integration into European digital ecosystems. The findings of the study can be used to improve crisis management systems and enhance the resilience and competitiveness of Ukrainian enterprises in the wartime and post-war economy.

Keywords: *digital transformation, crisis management, digital resilience, economic resilience, digital maturity, artificial intelligence, predictive analytics, risk management, digital technologies, economic instability.*

Formulas: –, figures: 2, tables: 2, references: 24.

JEL Classification: M15, M21, O33, L25.

For citation: Viadrova Nadiia, Lytvynenko Alina, Fridman Olena, Lytvynenko Olena. Digital transformation of enterprise crisis management under economic instability. Financial and Credit Systems: Prospects for Development. №3(22) 2026. P. 185-204. https://doi.org/10.26565/2786-4995-2026-3-12

Introduction. The full-scale war has transformed the operating environment of Ukrainian enterprises and, consequently, the very logic of crisis management. Whereas crises were previously regarded primarily as temporary deviations from normal development, instability has now become a persistent feature of the business environment. War-related risks, the destruction of production infrastructure, disruptions to logistics routes, energy instability, human capital shortages, cyber threats, and high market volatility have created a new type of crisis environment in which enterprises are required to address operational, financial, human resource, and security challenges simultaneously. Under these conditions, management effectiveness is increasingly determined not by the speed of response to a crisis, but by the ability to anticipate its development, manage uncertainty, and make data-driven decisions in real time.

In this context, digital transformation is no longer a separate dimension of technological modernization. It is becoming an integral component of an enterprise's crisis management strategy, as digital technologies enable business process continuity, real-time risk monitoring, remote management, the integration of production and financial flows, and the development of adaptive management models [1]. The use of artificial intelligence, Big Data, cloud platforms, digital twins, the Internet of Things (IoT), predictive analytics systems, and automated control systems is transforming the nature of crisis management, shifting it from a reactive model towards one focused on forecasting, prevention, and rapid adaptation [2, 3].

A distinctive feature of the current stage of Ukraine's economic development is that digitalization is taking place simultaneously with post-war recovery processes and Ukraine's integration into the European economic area. Fulfilling the commitments associated with the country's European integration path requires the harmonization of digital policy with European Union legislation, as well as the development of digital markets, cybersecurity, electronic identification, data governance, and digital services. For Ukrainian enterprises, this entails not only access to new markets and technologies but also the need to develop a fundamentally new management system capable of operating in accordance with European digital economy standards [4].

At the same time, the accelerated digital transformation of Ukrainian businesses is largely supported by international assistance programs aimed at developing digital infrastructure, supporting small and medium-sized enterprises, strengthening cyber resilience, fostering innovation, and promoting the digital recovery of the economy. As a result, digitalization is increasingly viewed not merely as a tool for automating individual business processes, but as one of the key factors in ensuring the economic resilience of enterprises under conditions of prolonged instability [5].

Literature review. Contemporary research increasingly conceptualizes the digital transformation of enterprises not as the implementation of individual information technologies, but as a comprehensive transformation of business models, management processes, and decision-making mechanisms. In this context, scholarly attention focuses on enterprises' readiness for digital change, the integration of information systems, the development of employees' digital competencies, and the capacity of businesses to respond promptly to changes in the external environment [1, 4-8]. Accordingly, an enterprise's digital maturity is determined not only by the extent to which digital technologies are adopted but also by its capacity to integrate them into strategic and operational management.

The relationship between digital transformation and enterprise resilience becomes particularly important under conditions of high uncertainty. Recent empirical studies confirm the positive impact of digital transformation on organizational resilience, particularly through the development of innovation capability and the capacity to respond rapidly to change [5]. This broadens the traditional understanding of digitalization: digital technologies serve not only as a means of improving operational efficiency but also as a factor in strengthening enterprise adaptability, enhancing its capacity to withstand external shocks, and enabling recovery following crisis-related disruptions.

A distinct strand of the contemporary academic discourse focuses on the digital transformation of crisis management. The literature indicates a gradual shift from the traditional crisis management model, primarily oriented towards responding to threats that have already materialized, to a preventive approach based on digital monitoring, data analysis, and the forecasting of potential crises [9, 14, 15]. Within this approach, digital technologies are integrated into risk identification, the assessment of alternative scenarios, and managerial decision support, thereby creating conditions for reducing the time lag between the emergence of a threat and the enterprise's response.

Advances in artificial intelligence and technologies for processing large volumes of data significantly expand the potential of this approach. AI-driven risk governance involves the use of artificial intelligence algorithms and predictive analytics to identify risks, improve the quality and justification of managerial decisions, and strengthen enterprises' strategic adaptability [2]. In this context, Big Data and Predictive Analytics enable a shift from the retrospective analysis of crisis phenomena towards forecasting their likelihood and modelling their potential consequences.

The use of Digital Twin technology also represents a promising direction in the digitalization of crisis management. Digital twins enable the creation of virtual models of physical assets,

production processes, and supply chains, allowing alternative scenarios to be tested without intervening in the real-world system. Recent studies associate the use of Digital Twin technology with enhanced supply chain resilience, improved process visibility, scenario modelling, and the early detection of potential disruptions [3, 22]. Combining digital twins with machine learning and deep learning technologies further expands the possibilities for forecasting crisis situations and supporting preventive managerial decision-making.

For Ukrainian enterprises, the digital transformation of crisis management acquires particular significance due to the simultaneous impact of economic, war-related, infrastructural, human resource, logistical, energy, and cyber risks. Studies of business operations under martial law highlight the growing importance of cyber resilience, digital support for enterprise relocation, remote human resource management, and the digitalization of logistics processes [10-13]. Under such conditions, digital technologies perform a dual function: they ensure the continuity of ongoing business processes while simultaneously providing tools that enable enterprises to adapt to structural changes in the external environment.

Contemporary European approaches to digital resilience provide an important theoretical context for the development of digital crisis management. European academic and regulatory discourse is characterized by increasing attention to digital sovereignty, cyber resilience, the development of digital ecosystems, and the integration of the digital and green transitions [16, 18-20]. The Industry 5.0 concept further broadens the understanding of digital transformation by integrating the principles of resilience, sustainability, and human-centricity [17]. Within this approach, technological modernization is regarded not as an end in itself but as a means of developing enterprises capable of maintaining viability and adapting to systemic crises.

Cyber resilience occupies a particularly important place in this context. The expansion of digital infrastructure simultaneously increases enterprises' dependence on information systems and creates new sources of risk. Contemporary approaches therefore involve integrating cybersecurity with crisis management mechanisms, ensuring business continuity, and facilitating recovery from digital incidents [19]. This indicates a gradual convergence of the concepts of digital resilience, risk management, and crisis management.

International experience also reveals differences between institutional and technological models of digital transformation. The European approach places greater emphasis on regulatory frameworks, digital sovereignty, cybersecurity, sustainability, and the development of digital ecosystems [16–20], whereas the U.S. approach is characterized by a stronger focus on technological leadership, the advancement of artificial intelligence, data analytics, and innovative digital solutions [21]. At the same time, recent research on digital sovereignty and artificial intelligence regulation demonstrates a gradual convergence of the technological and regulatory dimensions of digital policy [23]. For Ukraine, combining these approaches with European integration processes and the inclusion of Ukrainian enterprises in European digital ecosystems is of particular importance [24].

A synthesis of the literature makes it possible to identify several interrelated strands of contemporary research: the digital transformation of business and management processes [1, 4-8]; the relationship between digital transformation and organizational resilience [5]; the digitalization of crisis management [9, 14, 15]; the use of artificial intelligence, predictive analytics, and Digital Twin technologies in risk management systems [2, 3, 22]; the digital adaptation of enterprises to the specific challenges of the wartime environment [10-13]; and the development of digital and cyber resilience within European and international approaches [16-21, 23, 24].

At the same time, an analysis of the existing body of research indicates that these strands have largely developed in isolation from one another. Previous studies have provided substantial insights into the potential of individual digital technologies, the relationship between digitalization and organizational resilience, cybersecurity challenges, the digitalization of supply chains, and the

transformation of crisis management. However, a comprehensive approach that integrates digital risk monitoring, data integration and analytical processing, crisis scenario forecasting, intelligent decision support, and adaptive enterprise recovery into a single continuous crisis management cycle remains insufficiently developed.

This research gap is particularly relevant for enterprises operating under the simultaneous impact of war-related, economic, logistical, human resource, energy, and cyber threats. This necessitates the further development of the theoretical and methodological foundations of the digital transformation of crisis management and the establishment of an integrated model capable of facilitating a transition from predominantly reactive responses to crisis events towards continuous monitoring, early risk detection and forecasting, intelligent decision support, and the adaptive recovery of enterprise operations.

Purpose, objectives and research methods. The aim of the article is to advance the theoretical foundations and substantiate practical approaches to the digital transformation of enterprise crisis management under conditions of economic instability.

To achieve this aim, the study addresses the following objectives: to examine the contemporary challenges faced by enterprises operating under wartime conditions; to determine the role of digital technologies in ensuring business economic resilience; to analyze the impact of European integration and international support on the digital transformation of Ukrainian enterprises; and to propose directions for improving crisis management systems through the use of digital tools.

The methodological framework of the study is based on an interdisciplinary approach that integrates the concepts of the digital economy, crisis management, economic resilience theory, and risk management. The study employs systemic, process-based, and risk-oriented approaches, along with methods of comparative analysis, logical generalization, structural and functional analysis, scientific abstraction, and synthesis. These methods made it possible to comprehensively assess the impact of digital transformation on the effectiveness of enterprise crisis management under conditions of economic instability.

Research results. Digital transformation is increasingly viewed not as a process involving the implementation of individual information technologies, but as a fundamental transformation of an enterprise's operating model. Its essence lies in the transition from management based predominantly on managers' experience and intuition to data-driven management supported by digital platforms and analytical tools. Within such a system, digital technologies are integrated into all areas of enterprise activity, ranging from strategic planning to the operational control of business processes [6].

One of the key characteristics of a modern enterprise is its level of Digital Maturity. Unlike the level of digitalization, which reflects the number of technologies implemented, digital maturity indicates an enterprise's capacity to use digital solutions effectively to achieve its strategic objectives. It encompasses digital corporate culture, the integration of information systems, data management quality, the level of process automation, the development of employees' digital competencies, and readiness for organizational change. Digital maturity therefore determines how rapidly an enterprise can adapt to emerging challenges [5].

In recent years, the concept of Digital Resilience, which links digital transformation with economic and organizational resilience, has become particularly relevant. Digital resilience refers to an enterprise's capacity to maintain business continuity and adapt its business processes in the face of digital, information-related, and physical threats. The integration of digital systems, data monitoring and analytics, business process automation, and the use of advanced digital technologies, including ERP, WMS, IoT, BI, and DSS, play an important role in strengthening digital resilience by enhancing the speed, transparency, and evidence base of managerial decision-making [7].

Digital transformation also changes the competency requirements for managerial personnel. A modern manager not only coordinates the activities of organizational units but also acts as an integrator of digital technologies into the enterprise's business model. This requires the development of digital leadership, proficiency in analytical systems, an understanding of the capabilities of artificial intelligence, digital platform management, cyber risk assessment, and the use of technologies that support managerial decision-making. Managers' digital competencies are becoming an important intangible asset of the enterprise and a factor contributing to its competitiveness [8].

Digital Risk Management is also becoming increasingly important. Unlike traditional approaches, it is based on the continuous collection and analysis of data, automated identification of potential threats, the use of machine learning algorithms to forecast crisis scenarios, and real-time managerial decision support. This makes it possible to substantially reduce the time lag between the emergence of a risk and the response to it, which is critically important under conditions of war, financial market instability, and rapid changes in the business environment [6].

Digital transformation is shaping a new paradigm of crisis management in which an enterprise's competitive advantages are determined not so much by the volume of resources at its disposal as by its capacity to process information rapidly, anticipate risks, ensure business continuity, and adapt its business model to dynamic changes in the external environment. It is the integration of digital maturity, digital resilience, contemporary managerial competencies, and digital risk management that provides the foundation for developing an effective enterprise crisis management system under current conditions of economic instability.

Martial law has posed an unprecedented challenge to Ukrainian businesses, transforming not only the conditions of economic activity but also the very nature of managerial risks. Unlike traditional economic crises, contemporary challenges are multidimensional: physical threats are intertwined with digital, economic, human resource, and logistical challenges. This significantly increases the requirements for the speed of managerial decision-making, the adaptability of business processes, and enterprises' capacity to operate under conditions of persistent turbulence.

One of the most severe consequences of the war has been the physical destruction of production assets. The destruction of enterprises, warehouses, energy facilities, and transport infrastructure has resulted not only in the loss of tangible resources but also in the need to rapidly restore production processes at new locations. Under such conditions, the digitalization of critical information becomes essential, as it ensures the preservation of management data and technical documentation and enables the rapid restoration of operations regardless of an enterprise's physical location [9].

Alongside physical threats, cyber risks have become substantially more significant. Ukrainian enterprises are increasingly targeted by cyberattacks aimed at disrupting information systems, stealing data, or disabling digital infrastructure. With the widespread use of remote work, cloud services, and electronic document management, information security has become an integral component of crisis management. Accordingly, cyber resilience extends beyond the responsibilities of IT departments and becomes an essential element of strategic enterprise management [10].

Another characteristic phenomenon of the wartime period has been the large-scale relocation of enterprises. The transfer of production facilities to safer regions required the rapid migration of information systems, digital archives, production data, and communication channels. Experience in recent years has demonstrated that enterprises with higher levels of digital maturity have adapted to relocation considerably more easily, as their key business processes had already been integrated into the digital environment [11].

The problem of human resource availability has also become significantly more acute. The mobilization of employees, forced population migration, changes in the structure of the labor market, and psychological exhaustion among personnel have made it increasingly difficult for

enterprises to maintain stable operations. Under such conditions, digital tools for remote collaboration, business process automation, and the use of decision support systems partially compensate for human resource shortages by enhancing management productivity [12].

The closure of certain transport routes, changes in export infrastructure, unstable supplies of raw materials, and rising transportation costs compel enterprises to continuously reassess their logistics decisions. This encourages a transition towards digital supply chain management based on real-time route monitoring, risk forecasting, and the use of analytical platforms to optimize logistics flows.

Large-scale attacks on energy infrastructure have demonstrated the critical dependence of most enterprises on an uninterrupted electricity supply. This has increased the relevance of digital systems for monitoring energy consumption, automated management of production processes, information resource backup, and the use of cloud infrastructure, which ensures access to critical data even during prolonged power outages [13].

The contemporary business environment is characterized by the interconnectedness of physical, digital, and economic risks. Under such conditions, the effectiveness of crisis management is determined by an enterprise's capacity to respond to crisis events as well as by its level of digital readiness to operate under persistent uncertainty. The increasing complexity of risks necessitates a transformation of crisis management tools. Whereas digital technologies were previously used primarily to automate individual operations, they are now being integrated into enterprise strategic management systems and provide decision support at all management levels [9].

Cloud Computing has become one of the core technologies of contemporary crisis management. Migrating information resources to cloud environments ensures continuous access to corporate data regardless of employees' location, minimizes the risk of information loss, and facilitates enterprise relocation. Under wartime conditions, cloud infrastructure has become a key means of preserving management documentation, financial information, and production databases [14].

ERP systems play a key role in ensuring the integrity of business processes by integrating production, finance, procurement, logistics, human resource management, and warehouse operations within a unified information environment. Such integration enhances the transparency of enterprise operations, reduces the time required for managerial decision-making, and improves resource utilization in crisis situations. At the same time, Customer Relationship Management (CRM) systems enable enterprises to maintain stable communication with customers even when business operations are geographically dispersed. Customer behavior analysis, sales automation, service personalization, and digital interaction channels contribute to customer retention, which is an important factor in ensuring an enterprise's financial resilience [7].

A qualitatively new stage in the development of digital crisis management is associated with the use of artificial intelligence and Big Data analytics. Machine learning algorithms make it possible to identify hidden patterns, assess risks, forecast changes in demand, optimize resource utilization, and model alternative development scenarios. Combined with Big Data technologies, these capabilities facilitate the transition towards data-driven management, in which decisions are based on analytical models rather than solely on expert assessments. Predictive Analytics is becoming particularly important, as it enables enterprises not only to assess their current condition but also to anticipate potential crisis situations. The application of mathematical models, statistical methods, and artificial intelligence algorithms enables the early detection of risks, thereby substantially reducing the time interval between the emergence of a potential threat and the corresponding managerial response [2, 15].

One of the most promising areas of digital transformation is the use of Digital Twin technology. The creation of digital models of production facilities, technological processes, or logistics systems makes it possible to test different operational scenarios without intervening in

actual production processes. This provides opportunities to model the consequences of crisis situations, optimize resource utilization, plan the relocation of production facilities, and evaluate the effectiveness of alternative managerial decisions [3].

The analysis indicates that most of the challenges faced by Ukrainian enterprises under martial law are complex in nature and require integrated rather than isolated digital management solutions. The effectiveness of crisis management is determined not so much by the implementation of individual information technologies as by their capacity to ensure business process continuity, enable rapid responses to risks, and support managerial decision-making. To systematize the findings of the study, the relationship between key wartime challenges, digital tools, and expected managerial outcomes is summarized in Table 1.

Table 1. Relationship between Wartime Challenges, Digital Tools, and Crisis Management Outcomes at the Enterprise Level

Wartime challenge	Management problem	Digital tools	Crisis management effect	Key KPIs
Physical destruction of assets	Loss of production capacity, documentation, and information	Cloud technologies, Digital Twin, digital document management	Rapid recovery of operations, preservation of critical data	Recovery Time, information availability
Cyber threats	Risk of data loss and disruption of information systems	AI analytics, Big Data, cloud services, digital document management	Enhanced digital resilience, early threat detection	Number of cyber incidents, average response time
Enterprise relocation	Relocation of production and business processes	ERP, Cloud Computing, CRM	Business continuity and coordination of operations	Relocation time, duration of downtime
Human resource shortages	Reduced human resource capacity, employee overload	ERP, AI analytics, CRM	Automation of routine processes, increased labor productivity	Labor productivity, level of process automation
Disruption of logistics chains	Supply disruptions and delays in product delivery	ERP, Big Data, Predictive Analytics, IoT	Route optimization, delay forecasting	Lead Time, delivery timeliness
Energy instability	Production downtime, equipment disruptions	IoT, Predictive Analytics, Digital Twin	Energy consumption control, equipment failure forecasting	Downtime, energy efficiency, equipment utilization rate
High uncertainty in the external environment	Complexity of strategic planning	AI analytics, Big Data, Predictive Analytics	Support for scenario planning and risk forecasting	Forecast accuracy, decision-making speed

Source: systematized by the authors based on [3, 13, 15].

The data presented in Table 1 demonstrate that contemporary digital technologies increasingly function not as isolated automation tools but as components of an integrated system for ensuring enterprise economic resilience. At the same time, a clear cause-and-effect relationship can be observed between wartime challenges and digital solutions: the higher the level of digital integration of business processes, the lower the time losses associated with crisis response, operational recovery, and managerial decision-making.

It is particularly noteworthy that the same digital technology can simultaneously address several management challenges. For example, cloud services ensure business continuity during relocation, enhance the protection of corporate information, and provide a foundation for remote collaboration among employees. Similarly, artificial intelligence, predictive analytics, and Big Data technologies are used not only for data analysis but also for the early detection of risks, support for scenario planning, and improvement of the evidence base for managerial decision-making.

In recent years, digital transformation has increasingly been regarded in European Union countries as an integral component of economic security and strategic autonomy. While the initial stages of digitalization focused primarily on the automation of production and the development of electronic services, contemporary European policy is oriented towards building resilient digital ecosystems capable of ensuring business continuity during global crises. Successive crises have intensified the EU's focus on digital resilience, security, and strategic autonomy [16].

One of the conceptual directions of contemporary European industrial policy is Industry 5.0, which complements the principles of production automation with human-centricity, resilience, and sustainability. Unlike Industry 4.0, which focused primarily on the digitalization of production processes, the new model is oriented towards strengthening enterprises' capacity to adapt to crisis-related challenges, rapidly reconfigure production systems, and effectively use digital technologies to support managerial decision-making. In this context, digitalization is regarded not as an end in itself but as an instrument for enhancing organizational resilience [17].

An important element of the European model is the concept of Digital Sovereignty. Its essence lies in ensuring the independence of critical digital infrastructure, protecting data, developing domestic digital platforms, and reducing technological dependence on external providers. For enterprises, this entails the need to integrate cybersecurity, data governance, digital identification, and secure cloud services into the overall corporate governance system [16].

European practice also demonstrates the gradual convergence of digital transformation with the principles of sustainable development and the green transition. Digital technologies are used not only to increase productivity but also to monitor environmental performance, manage resource efficiency, enhance corporate governance transparency, and facilitate engagement with stakeholders. Digitalization is therefore becoming an instrument for achieving long-term economic resilience rather than merely improving operational efficiency [18].

EU countries place particular emphasis on cybersecurity as an integral component of crisis management. Contemporary enterprises integrate cybersecurity mechanisms throughout all stages of digital transformation, thereby minimizing the risks of business process disruptions and strengthening enterprise resilience to external digital threats [19].

At the same time, the effectiveness of the European model is largely supported by the development of digital ecosystems in which enterprises, research institutions, public authorities, and technology companies jointly create digital services, exchange data, and develop innovative solutions. The ecosystem-based approach is increasingly regarded as one of the key factors contributing to the competitiveness of the European economy [20].

Unlike the European model, which relies substantially on regulatory mechanisms and sustainability principles, the U.S. approach is primarily oriented towards the rapid adoption of technological innovations and the use of data as a strategic resource. Particular emphasis is placed on the development of digital platforms, artificial intelligence, cloud technologies, and predictive analytics systems, which enable enterprises to adapt rapidly to changes in the external environment [21].

Artificial intelligence is one of the key drivers of digital transformation. Contemporary AI solutions are applied to the automated analysis of financial risks, assessment of consumer behavior, optimization of production processes, support for strategic planning, and identification of potential crisis situations. The use of machine learning algorithms enables enterprises to continuously improve forecasting models based on accumulated data, thereby substantially increasing the accuracy of managerial decision-making [6].

Predictive Crisis Analytics technologies have undergone particularly rapid development. Unlike traditional risk management, they are based on the continuous analysis of large volumes of structured and unstructured data obtained from internal information systems, financial markets,

logistics networks, open information sources, and digital platforms. This makes it possible to develop scenarios for the evolution of crisis events even before their evident manifestations emerge.

In contemporary global supply chain management practices, digital technologies are increasingly used to enhance supply chain transparency, resilience, and adaptability. Following the COVID-19 pandemic and amid geopolitical conflicts, particular attention has been paid to developing transparent digital supply chains and integrating ERP platforms, IoT systems, blockchain technologies, and predictive analytics to enable the timely identification of risks and supplier diversification [22].

An important component of the U.S. model is the development of comprehensive enterprise cyber resilience. Cybersecurity is integrated not only into IT infrastructure but also into corporate governance, strategic planning, and operational risk management. This approach involves continuous testing of information systems, the use of artificial intelligence technologies to detect cyber threats, automated incident response, and continuous staff training [23].

For Ukraine, the digital transformation of crisis management is of strategic importance not only in the context of post-war recovery but also as an integral component of the European integration process. At the same time, the mechanical adoption of European or U.S. models is unlikely to produce the expected results. A considerably more promising approach is to develop a national model of digital resilience adapted to the specific characteristics of the wartime economy and the structure of Ukrainian business. A key priority is the harmonization of digital standards with the European Union regulatory framework. This includes the development of electronic identification, data governance, cybersecurity, digital document management, the use of cloud infrastructure, and the integration of advanced digital services into enterprise operations. The alignment of standards will contribute not only to the development of the domestic digital market but also to the broader participation of Ukrainian companies in European production and technology networks.

Ukraine’s participation in European digital initiatives, particularly the Digital Europe Programme, provides significant opportunities by supporting the development of supercomputing technologies, artificial intelligence, Digital Innovation Hubs, digital skills, and cybersecurity. For Ukrainian enterprises, this creates additional opportunities to access advanced technologies, international expertise, collaborative projects, and financial instruments for development.

Another promising direction is the integration of Ukrainian enterprises into European digital platforms and sectoral ecosystems. The use of shared digital services, data exchange platforms, e-commerce tools, and digital interaction technologies can enhance business process transparency, accelerate access to European markets, and strengthen the competitive position of Ukrainian companies. The development of digital partnerships among businesses, government authorities, universities, research institutions, and international technology companies is also of particular importance. Such partnerships can facilitate the accelerated adoption of innovations, the development of digital competencies, the dissemination of best management practices, and the formation of a national digital resilience ecosystem [24].

A comparative analysis of international models indicates that the digitalization of crisis management follows different conceptual trajectories. In European Union countries, an institutional approach based on digital resilience, regulatory frameworks, and ecosystem-based cooperation predominates, whereas the U.S. model is oriented towards technological leadership and the extensive use of artificial intelligence and data analytics.

For Ukraine, the development of a hybrid model combining the regulatory advantages of the European approach with the technological flexibility of the U.S. model appears appropriate (Table 2).

Table 2. Comparative Characteristics of Crisis Management Digitalization Models: The EU and U.S. Experience and Prospects for Ukraine

Criterion	European Union	United States	Ukraine (Prospective Model)
Strategic objective	Digital resilience of the economy and sustainable development	Technological leadership and competitiveness	Enhancing business resilience under wartime conditions and during post-war recovery
Conceptual framework	Industry 5.0, Digital Sovereignty, ESG	AI-driven Management, Data-driven Enterprise	Digital Resilience Management
Priority approach	Regulatory and ecosystem-based	Innovation- and technology-driven	Integrated risk-oriented approach
Key digital tools	Cloud services, digital ecosystems, cybersecurity, digital platforms	AI, Machine Learning, Big Data, Predictive Analytics, IoT	ERP, CRM, AI, Big Data, Digital Twin, cloud technologies
Risk management	Preventive, in accordance with European standards	Predictive, based on analytics and data	Combination of predictive analytics and scenario planning
Cyber resilience	Integrated into national digital policy	Integrated into corporate governance	Development of corporate cyber resilience in accordance with EU standards
Supply chain management	Digital platforms and cross-border cooperation	AI-based optimization and digital monitoring	Logistics diversification and digital supply control
Role of the state	Establishment of digital rules and financing of innovation	Promotion of innovation through the market and private sector	Legislative harmonization and digital support for businesses
Expected outcome	Resilient digital economy	High business adaptability	Competitive and digitally resilient enterprise

Source: generalized and systematized by the authors based on [17, 23, 24].

International experience demonstrates that contemporary crisis management is increasingly extending beyond the boundaries of traditional risk management. In EU countries, it is based on digital resilience, integrated ecosystems, and regulatory frameworks for cybersecurity, whereas the U.S. model emphasizes technological leadership, data analytics, and artificial intelligence. For Ukraine, the most promising approach is to combine these models by integrating European regulatory standards and digital platforms with advanced AI solutions, predictive analytics, and digital tools for managerial decision support [6, 23].

Figure 1 illustrates the logic of integrating international experience into Ukrainian practice.

The proposed conceptual model demonstrates that the effective digital transformation of crisis management in Ukraine should be based not on the replication of individual international practices but on their integration in accordance with national conditions. European experience should primarily be applied to harmonize digital regulation, strengthen cyber resilience, and develop digital ecosystems, whereas the U.S. approach is particularly valuable due to its extensive use of artificial intelligence, predictive analytics, and data-driven management.

The synergy of these approaches provides the foundation for the authors' Digital Resilience Management model, which integrates enterprise digital maturity, intelligent risk management, business process continuity, and digital resilience. Unlike traditional crisis management, the proposed model is oriented not only towards responding to crisis events but also towards developing an adaptive management system capable of anticipating risks, rapidly reconfiguring business processes, and maintaining enterprise competitiveness in the wartime and post-war economy.

The analysis of contemporary approaches to crisis management, enterprise digital transformation, and business practices under martial law indicates that existing management models only partially address current challenges. Most of them focus either on minimizing the consequences of crises or on automating individual business processes. By contrast, the contemporary environment is characterized by highly dynamic change, multi-level risks, and the need for continuous managerial decision-making based on large volumes of data. This necessitates

the development of an integrated digital crisis management model combining forecasting, analytics, and adaptive management technologies [6].

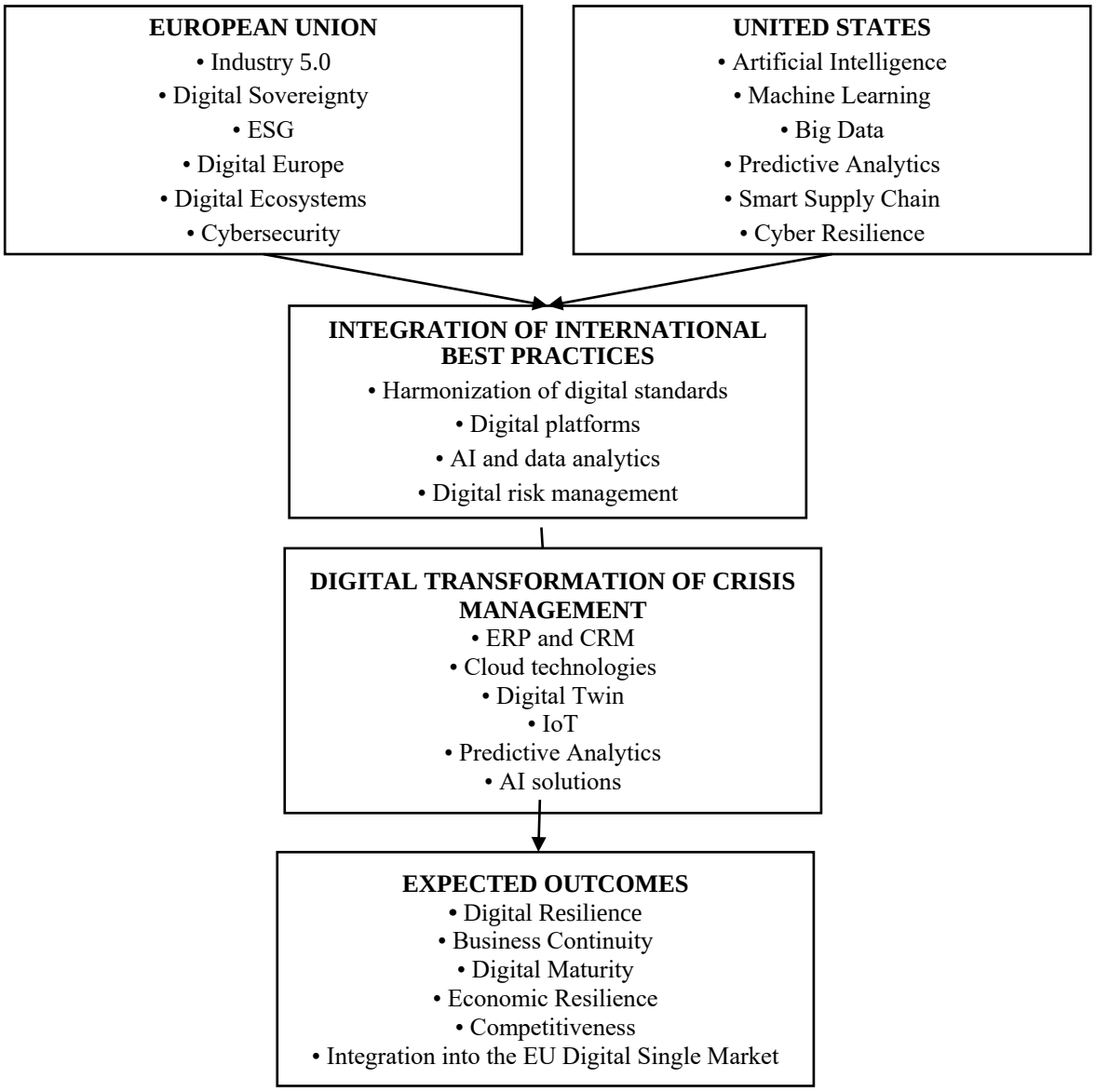

Figure 1. Conceptual Model for Integrating International Experience into the Digital Transformation of Crisis Management in Ukrainian Enterprises
Source: developed by the authors.

For this purpose, a five-level Digital Crisis Management Framework (DCMF) is proposed, which conceptualizes crisis management as a continuous, digitally enabled risk management cycle. Unlike traditional models, the proposed framework involves continuous data exchange across all management levels and the use of artificial intelligence tools to support managerial decision-making. A fundamental feature of the framework is its adaptability: the outcomes of implemented managerial decisions generate new datasets that are subsequently used for further system learning and the refinement of forecasts.

The first level of the framework is the Risk Monitoring Layer, which ensures the continuous collection of information from the enterprise's internal and external environments. Data sources include ERP systems, CRM platforms, IoT devices, financial indicators, logistics services, information on cyber incidents, market indicators, and open information sources. At this stage, an

enterprise digital risk profile is developed, enabling potential threats to be identified before they escalate into a crisis.

The second level, the Digital Analytics Layer, focuses on the integration and processing of the collected data. This level is primarily based on Big Data technologies, Business Intelligence (BI), and advanced analytics tools. Their application enables the visualization of key enterprise performance indicators, the identification of hidden patterns and interrelationships among risks, and the detection of critical deviations in business processes. At this stage, information is transformed into knowledge required for strategic management.

The third level, the Predictive Crisis Layer, represents a key distinction between the proposed framework and conventional crisis management systems. The use of artificial intelligence algorithms, machine learning, and predictive analytics makes it possible to model alternative development scenarios, estimate the probability of crisis situations, assess potential financial losses, and forecast the impact of external factors on enterprise operations. An Early Warning System operates simultaneously, automatically signalling critical changes in key indicators and triggering additional analysis.

The fourth level, the Decision Intelligence Layer, ensures the transformation of analytical information into practical managerial actions. At this stage, the results of predictive analytics are integrated with decision support systems, digital KPI monitoring dashboards, and ERP platforms. Management is thus able to rapidly evaluate alternative response scenarios, analyze their economic consequences, and select the most effective managerial decisions depending on the level of risk and the enterprise's available resources.

The fifth level, the Adaptive Recovery Layer, is aimed at ensuring long-term economic resilience. Its distinctive feature is the application of continuous improvement principles, whereby the outcomes of crisis management measures are continuously evaluated through digital KPI monitoring. Based on the results obtained, the system automatically adjusts the parameters of predictive models, updates risk assessment criteria, and adapts decision-support algorithms. In this way, a mechanism is established that enables the enterprise to continuously adapt to changes in the external environment.

The proposed framework is based on the end-to-end integration of digital technologies (Figure 2).

ERP systems provide a unified information environment for the enterprise; Big Data technologies accumulate large volumes of structured and unstructured data; BI analytics transform these data into a system of management indicators; artificial intelligence generates predictive scenarios; and digital KPI monitoring enables the evaluation of the effectiveness of implemented crisis management decisions. The Early Warning System serves as an integrating element, combining monitoring, forecasting, and rapid response within a unified information and analytical environment.

The scientific novelty of the proposed model lies in the transition from the reactive logic of crisis management to a model of continuous digital risk management. Unlike traditional approaches, the Digital Crisis Management Framework (DCMF) is not limited to responding to crisis events that have already materialized; instead, it enables their early prediction, intelligent analysis of cause-and-effect relationships, automated decision support, and the adaptive recovery of enterprise operations. This approach is consistent with contemporary trends in the development of the digital economy, the concept of Digital Resilience, and the principles of Industry 5.0, thereby providing a methodological foundation for developing a new architecture of crisis management for Ukrainian enterprises in the wartime and post-war economy.

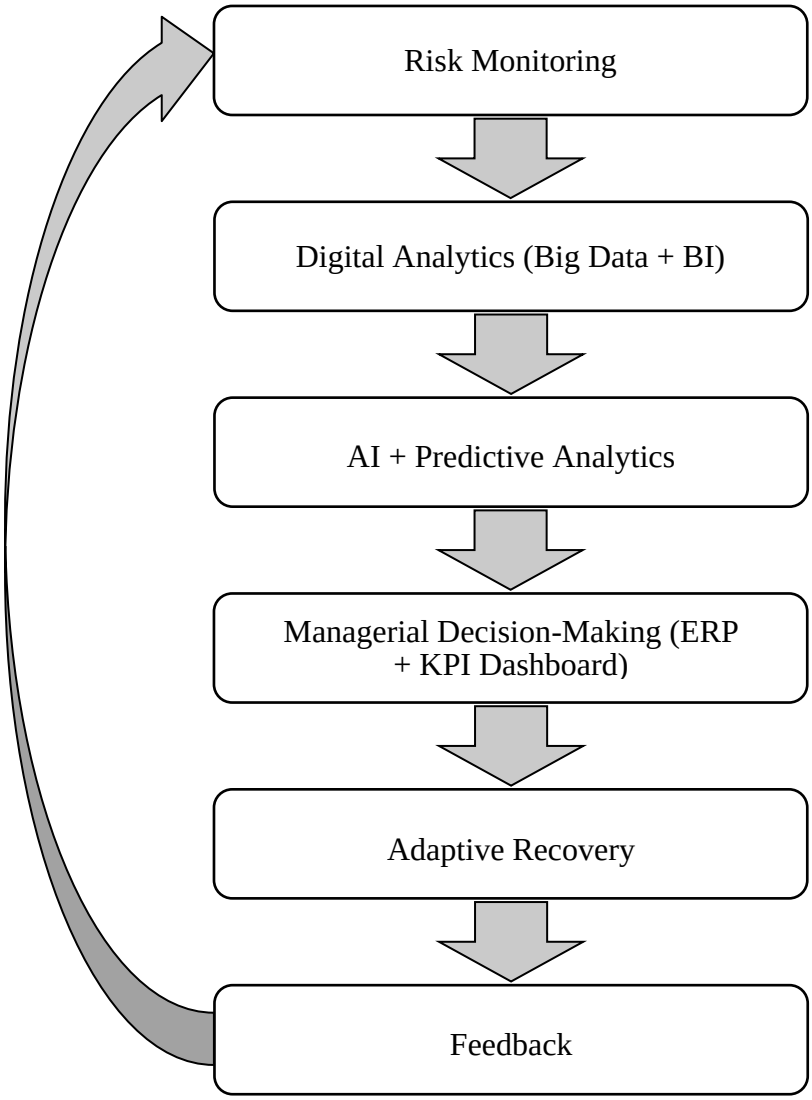

Figure 2. Five-Level Digital Crisis Management Framework
Source: compiled by the authors.

Discussion. The findings of the study confirm that the digital transformation of crisis management should be understood more broadly than the implementation of individual digital technologies for the automation of management processes. Its fundamental significance lies in transforming the very logic of crisis management – from a predominantly reactive response to threats that have already materialized towards continuous risk monitoring, crisis scenario forecasting, data-driven decision support, and the adaptive recovery of enterprise operations. In this context, the proposed five-level Digital Crisis Management Framework (DCMF) systematizes digital tools according to the successive stages of crisis management and establishes a closed-loop management cycle incorporating a feedback mechanism.

The findings are consistent with contemporary studies demonstrating a positive relationship between digital transformation and enterprise resilience. In particular, previous research has established that digital transformation contributes to organizational resilience through the development of innovation capability and the capacity for rapid response [5], supporting the proposition advanced in this study that digital maturity provides a foundation for enhancing enterprise adaptability. At the same time, the findings of the present study extend this approach by specifying the managerial mechanism through which such adaptability can be achieved, namely

through the interconnected processes of monitoring, analytics, forecasting, decision-making, and recovery.

The proposed approach is also consistent with the growing trend towards the intelligent management of risks. Research on AI-driven risk governance demonstrates the potential of artificial intelligence and predictive analytics for risk identification and strategic decision support [2]. Studies on Digital Twin technologies, in turn, demonstrate the potential of digital modelling to enhance supply chain resilience and analyze alternative crisis development scenarios [3, 22]. Within the proposed DCMF, these technologies are considered not in isolation but as interconnected components of a unified information and analytical cycle. The integrative nature of the framework makes it possible to combine data collection, analytical processing, risk forecasting, and the subsequent transformation of analytical results into specific managerial actions.

The findings also further elaborate existing academic approaches to the digitalization of crisis management [9, 14, 15]. While previous studies predominantly consider digital technologies either as a factor contributing to greater crisis management effectiveness or as a set of tools for its transformation, the proposed framework structures these technologies according to the functional logic of a continuous crisis management cycle. Importantly, the final element of the DCMF is not merely the recovery of enterprise operations but adaptive recovery, the outcomes of which are fed back into the system to refine the parameters of subsequent monitoring, forecasting, and decision-making. Crisis management thus acquires the characteristics of a system capable of accumulating information from previous crisis impacts and using it to enhance preparedness for future threats.

The findings are particularly significant in the context of Ukrainian enterprises. Unlike crisis environments shaped predominantly by economic or market fluctuations, the current operating environment in Ukraine is characterized by the simultaneous impact of physical, energy-related, logistical, human resource, financial, and cyber threats [10-13]. Under such conditions, the use of isolated digital solutions is insufficient to ensure an adequate level of resilience. The practical value of the proposed framework lies specifically in its capacity to integrate heterogeneous information sources and digital technologies into a unified system for early risk detection and managerial decision support. This makes it possible to view digital transformation not only as a component of technological development but also as an element of an enterprise's strategic preparedness to operate under conditions of prolonged instability.

The comparison of European and U.S. approaches also indicates that the direct transfer of any single international model to the Ukrainian context would be inappropriate. The European approach emphasizes digital resilience, cybersecurity, digital sovereignty, ecosystem-based collaboration, and the principles of Industry 5.0 [16-20], whereas the U.S. experience is characterized by a stronger orientation towards technological leadership, the use of artificial intelligence, data analytics, and innovative digital solutions [21]. The findings suggest that a hybrid approach combining the institutional and security foundations of the European model with technological flexibility and data-driven management tools is particularly promising for Ukraine. Such an orientation simultaneously addresses the need to strengthen the resilience of Ukrainian businesses and facilitate their further integration into European digital ecosystems [24].

At the same time, the proposed Digital Crisis Management Framework (DCMF) has several limitations that define the boundaries within which the findings should be interpreted. First, the framework is conceptual in nature and was developed through the systematization of academic approaches, comparative analysis of international experience, and synthesis of the specific characteristics of enterprise operations under conditions of war and economic instability. The framework was not empirically tested on a sample of Ukrainian enterprises within the scope of this study; therefore, the effectiveness of individual DCMF levels and the strength of the relationships between them require further quantitative validation. In addition, the practical applicability of the framework may vary depending on enterprise size, industry, level of digital maturity, availability of financial resources, data quality, and the digital competencies of managerial personnel.

A further limitation is that the implementation of artificial intelligence, Big Data, Digital Twin, and predictive analytics does not in itself guarantee greater effectiveness of crisis management. The effectiveness of these technologies depends on the quality and completeness of data, the degree of integration among information systems, the reliability of digital infrastructure, the level of cybersecurity, and management's ability to correctly interpret the outputs of analytical models. Accordingly, an enterprise's digital maturity should be regarded as an important prerequisite for the practical application of the proposed framework rather than merely as an outcome of digital transformation.

Future research should focus on the empirical validation of the DCMF across enterprises representing different types of economic activity and varying levels of digital maturity. A promising direction is the development of a system of quantitative indicators for each level of the framework and the assessment of their effects on crisis response time, business process recovery time, risk forecasting accuracy, operational continuity, and enterprise economic resilience. This would facilitate the transition from a conceptual framework to a methodological toolkit for assessing the effectiveness of digital crisis management and identifying the conditions under which the integration of digital technologies generates the greatest resilience benefits for enterprises.

Conclusions. The proposed model of the digital transformation of crisis management demonstrates that the future development of Ukrainian enterprises will be determined not so much by the scale of digitalization of individual business processes as by their capacity to integrate digital technologies into strategic management systems. Under current conditions, digital transformation is no longer an independent dimension of enterprise modernization but is becoming one of the key instruments for ensuring economic resilience. Development priorities should therefore focus on strengthening enterprise adaptability to external risks rather than solely on the automation of operational activities.

One of the key directions is the broader implementation of artificial intelligence technologies. While AI is currently used primarily to automate individual business functions, its role is expected to increasingly shift towards intelligent support for strategic management. Machine learning algorithms, generative artificial intelligence, agentic systems, and predictive models have the potential to substantially improve the quality of risk assessment, accelerate managerial decision-making, and enable the rapid modelling of alternative enterprise development scenarios.

Another promising direction is the more extensive use of European digital platforms and business support programmes. The integration of Ukrainian enterprises into European Union digital services, participation in international innovation projects, and the use of Digital Innovation Hubs and instruments available under the Digital Europe Programme will facilitate the accelerated adoption of advanced technologies, the development of digital competencies, and stronger international cooperation.

At the same time, integration into the European digital market requires the harmonization of corporate management approaches. This involves the digital transformation of corporate governance, the implementation of advanced electronic document management systems, digital performance monitoring dashboards, performance and risk management tools, as well as the application of the principles of transparency, accountability, and data-driven management. In this context, digital technologies are becoming not only instruments of automation but also the foundation of a qualitatively new model of corporate management.

In summary, the development of Digital Economic Resilience should become a strategic priority for Ukrainian enterprises. Its essence lies not only in the use of advanced information technologies but also in an enterprise's capacity to rapidly adapt to crisis-related challenges, maintain business process continuity, effectively use data for managerial decision-making, and integrate into international digital ecosystems. Such a model will contribute to the long-term competitiveness of Ukrainian businesses under wartime conditions and throughout post-war development.

References

1. Lytvynenko, O. D., Lytvynenko, A. O., & Morozova, N. L. (2025). Impact of digital economy on business development in Ukraine. *Business Inform*, (5), 176–183. DOI: https://doi.org/10.32983/2222-4459-2025-5-176-183 [in Ukrainian]
2. Liberato lo Conte, D., Sancetta, G., Cucari, N., & Escobar, O. (2026). AI-driven risk governance for SMEs: From predictive analytics to strategic competitiveness. *Strategic Change*. DOI: https://doi.org/10.1002/jsc.70097
3. Liu, C., Wang, Y., Purvis, L., & Potter, A. (2026). Can digital twin technology enhance supply-chain resilience? A systematic literature review. *Sustainability*, 18(5), Article 2361. DOI: https://doi.org/10.3390/su18052361
4. Pasko, M., Lisna, I., Morozova, N. L., & Denchyk, I. (2025). Readiness of Ukrainian business for digital transformation: Drivers and barriers. *Financial and Credit Systems: Prospects for Development*, 1(16), 125–137. DOI: https://doi.org/10.26565/2786-4995-2025-1-10 [in Ukrainian]
5. Zhang, J., Li, H., & Zhao, H. (2025). The impact of digital transformation on organizational resilience: The role of innovation capability and agile response. *Systems*, 13(2), Article 75. DOI: https://doi.org/10.3390/systems13020075
6. Babenko, M. V., Pyvavar, I. V., Morozova, N. L., & Lytvynenko, A. V. (2026). Managerial decision-making in the context of digital transformation. *Business Inform*, (1), 576–588. DOI: https://doi.org/10.32983/2222-4459-2026-1-576-588 [in Ukrainian]
7. Zahorodniuk, O. V., & Dmytryk, I. O. (2024). The role of BPM, CRM and ERP systems in the digital transformation of Ukrainian business. *Collected Works of Uman National University of Horticulture*, 104(2), 191–201. DOI: https://doi.org/10.32782/2415-8240-2024-104-2-191-201 [in Ukrainian]
8. Grinko, A., Hrynko, P., & Daudova, G. (2025). Philosophy of developing a competency-based model of organizational personnel in the digital economy. *Current Problems of Sustainable Development*, 2(2), 34–46. DOI: https://doi.org/10.60022/2(2)-4S [in Ukrainian]
9. Yursha, O., Koval, S., & Melnyk, L. (2024). Transformation of enterprises' crisis management in the digital economy paradigm. *Central Ukrainian Scientific Bulletin. Economic Sciences*, 12(45), 201–213. DOI: https://doi.org/10.32515/2663-1636.2024.12(45).201-213 [in Ukrainian]
10. Kraus, K. M., Kraus, N. M., & Shtepa, O. V. (2022). Digital transformation of cybersecurity at the micro level under martial law. *Innovation and Sustainability*, (3), 26–37. Retrieved from: https://ir.lib.vntu.edu.ua/handle/123456789/37434 [in Ukrainian]
11. Safonik, N. P., Kovalchuk, A. M., & Kostiunik, O. V. (2026). Transformation of business models of relocated enterprises under intellectualization and digitalization: Investment and organizational aspects. *Current Problems of Sustainable Development*, 3(4), 91–99. DOI: https://doi.org/10.60022/3(4)-11S [in Ukrainian]
12. Kotkovskyi, V. R., Samorodov, B. V., & Chkheailo, A. A. (2024). Human resource management in wartime: Motivation, ways and methods of effective use of personal potential. *Sustainable Economic Development*, 3(50), 228–235. DOI: https://doi.org/10.32782/2308-1988/2024-50-34 [in Ukrainian]
13. Misiura, Ie. Yu. (2026). Logistics in the context of digitalization in Ukraine. *Business Inform*, (1), 100–109. DOI: https://doi.org/10.32983/2222-4459-2026-1-100-109 [in Ukrainian]
14. Lisnyi, A. (2026). Digital transformation as a mechanism for anti-crisis management of enterprises in the conditions of unstable markets. *Economy and Society*, (84). DOI: https://doi.org/10.32782/2524-0072/2026-84-119 [in Ukrainian]
15. Piankova, O., & Rula, O. (2025). The impact of digital transformations on the effectiveness of crisis management in international companies. *Economy and Society*, (72). DOI: https://doi.org/10.32782/2524-0072/2025-72-155 [in Ukrainian]
16. Adler-Nissen, R., & Eggeling, K. A. (2024). The discursive struggle for digital sovereignty: Security, economy, rights and the cloud project Gaia-X. *Journal of Common Market Studies*. DOI: https://doi.org/10.1111/jcms.13594
17. Ivanov, D. (2023). The Industry 5.0 framework: Viability-based integration of the resilience, sustainability, and human-centricity perspectives. *International Journal of Production Research*, 61(5), 1683–1695. DOI: https://doi.org/10.1080/00207543.2022.2118892
18. Bianchini, S., Damioli, G., & Ghisetti, C. (2023). The environmental effects of the "twin" green and digital transition in European regions. *Environmental and Resource Economics*, 84, 877–918. DOI: https://doi.org/10.1007/s10640-022-00741-7
19. Ristvej, J., Tonhauser, M., Chovanec, D., Kubás, J., Kollár, B., et al. (2025). Cyber resilience conceptual model for European Union NIS2 standards implementation in Slovakia. *Scientific Reports*, 15, Article 26902. DOI: https://doi.org/10.1038/s41598-025-12829-3
20. Crupi, A., Del Sarto, N., Di Minin, A., Gregori, G. L., Lepore, D., Marinelli, L., & Spigarelli, F. (2020). The digital transformation of SMEs—A new knowledge broker called the digital innovation hub. *Journal of Knowledge Management*, 24(6), 1263–1288. DOI: https://doi.org/10.1108/JKM-11-2019-0623
21. National Institute of Standards and Technology. (2025). *NIST strategy for American technology leadership in the 21st century*. Retrieved from: https://www.nist.gov/director/strategic-priorities
22. Ashraf, M., Eltawil, A., & Ali, I. (2024). Disruption detection for a cognitive digital supply chain twin using hybrid deep learning. *Operational Research*, 24, Article 23. Retrieved from: https://link.springer.com/article/10.1007/s12351-024-00831-y
23. Papyshev, G., & Chan, K. J. D. (2026). AI regulatory strategies for digital sovereignty: The role of geopolitics and technological disparities. *Electronic Markets*, 36(1), Article 8. DOI: https://doi.org/10.1007/s12525-025-00870-z
24. Serhiienko, O., Smorodin, A., & Silichova, T. (2025). Digital transformation as a catalyst for European integration processes development. *Actual Problems of Innovative Economy*, (4), 103–111. DOI: https://doi.org/10.36887/2524-0455-2025-4-24 [in Ukrainian]

Received: 12.05.2026 *Accepted: 15.09.2026*
Received after review: 30.08.2026 *Published: 05.10.2026*

Authors Contribution: *All authors have contributed equally to this work*
Conflict of Interest: *The authors declare no conflict of interest*

Declaration on the use of artificial intelligence

During the preparation of this article, the artificial intelligence tool Grammarly was used to check for grammatical and spelling errors. The concept, content, scientific novelty, and research results belong to the authors. The final version of the article was reviewed, revised, and edited by the authors.

Вядрова Надія
к.е.н., доцент, доцент кафедри банківського бізнесу
та фінансових технологій,
Харківський національний університет імені В. Н. Каразіна,
майдан Свободи, 4, Харків, 61022, Україна
e-mail: 3000918@gmail.com
ORCID ID: 0000-0003-2386-3231
Литвиненко Аліна
к.е.н., доцент, доцент кафедри міжнародних економічних відносин та безпеки бізнесу,
Харківський національний економічний університет імені Семена Кузнеця,
проспект Науки, 9а, Харків, 61165, Україна
e-mail: alina.lytvynenko@hneu.net
ORCID ID: 0000-0003-0372-5130
Фрідман Олена
к.е.н., доцент, доцент кафедри менеджменту,
обліку та бізнес-комунікацій,
Харківський національний університет імені В. Н. Каразіна,
майдан Свободи, 4, Харків, 61022, Україна
e-mail: o.fridman@karazin.ua
ORCID ID: 0000-0002-7437-6372
Литвиненко Олена
к.е.н., доцент, доцент кафедри економіки та бізнесу,
Державний біотехнологічний університет,
вулиця Алчевських, 44, Харків, 61002, Україна
e-mail: o.litvinenko@btu.kharkov.ua
ORCID ID: 0000-0002-8360-4461

Цифрова трансформація антикризового менеджменту підприємств в умовах економічної нестабільності

Анотація. Повномасштабна війна та економічна нестабільність суттєво змінили умови функціонування українських підприємств і зумовили трансформацію традиційних підходів до антикризового менеджменту. За таких умов цифрова трансформація стає важливою складовою антикризової стратегії, забезпечуючи безперервність бізнес-процесів, оперативний моніторинг ризиків та підвищення адаптивності підприємств. Використання штучного інтелекту, Big Data, хмарних технологій, Інтернету речей, цифрових двійників і прогнозної аналітики сприяє переходу від реактивної моделі антикризового управління до прогнозної та адаптивної. Особливого значення цифровізація набуває в контексті післявоєнного відновлення та європейської інтеграції України. У сучасних умовах цифрова трансформація виступає одним із ключових чинників забезпечення стійкості та довгострокового розвитку підприємств.

Постановка проблеми. Попри активний розвиток цифрових технологій та їх упровадження в діяльність підприємств, інтеграція цифрових інструментів у систему антикризового менеджменту залишається недостатньо системною. Технологічні рішення та традиційні механізми антикризового управління часто розглядаються відокремлено, що обмежує можливості підприємств щодо прогнозування криз, оперативного реагування на ризики та забезпечення економічної стійкості в умовах високої невизначеності.

Нерозв'язані аспекти. Незважаючи на значну кількість досліджень у сфері цифровізації та антикризового менеджменту, недостатньо розробленими залишаються комплексні підходи до формування цифрової моделі антикризового управління підприємствами. Подальшого дослідження потребують взаємозв'язки між рівнем цифрової зрілості підприємства, його адаптивністю до кризових викликів та ефективністю прийняття управлінських рішень у високотурбулентному середовищі.

Мета статті. Метою статті є теоретичне обґрунтування та визначення практичних напрямів цифровізації антикризового менеджменту підприємств для підвищення їх стійкості й адаптивності в умовах економічної нестабільності.

Основний матеріал. Дослідження ґрунтується на системному та порівняльному підходах до аналізу цифрової трансформації антикризового менеджменту підприємств в умовах економічної нестабільності. У статті досліджено цифрову зрілість і цифрову стійкість підприємств, сучасні інструменти управління ризиками, а також можливості використання штучного інтелекту, Big Data, ERP, CRM, хмарних технологій, IoT, Digital Twin і прогнозної аналітики для забезпечення безперервності та адаптивності бізнес-процесів. На основі узагальнення європейського й американського досвіду обґрунтовано перспективи його адаптації до українських умов та запропоновано п'ятирівневу модель Digital Crisis Management Framework, орієнтовану на моніторинг і прогнозування ризиків, підтримку управлінських рішень та адаптивне відновлення підприємств.

Висновки. Цифрова трансформація антикризового менеджменту визначається як комплексний процес інтеграції сучасних цифрових технологій у систему стратегічного управління, спрямований на підвищення

адаптивності, безперервності бізнес-процесів та економічної стійкості підприємств. Стратегічним пріоритетом для українського бізнесу є формування цифрової економічної стійкості (Digital Economic Resilience) на основі використання штучного інтелекту, прогнозної аналітики, управління на основі даних та інтеграції до європейських цифрових екосистем. Результати дослідження можуть бути використані для вдосконалення систем антикризового менеджменту та підвищення стійкості й конкурентоспроможності українських підприємств в умовах воєнної та післявоєнної економіки.

Ключові слова: *цифрова трансформація, антикризовий менеджмент, цифрова стійкість, економічна стійкість, цифрова зрілість, штучний інтелект, прогнозна аналітика, управління ризиками, цифрові технології, економічна нестабільність.*

Формули: -, рис.: 2, табл.: 2, бібл.: 24.

JEL Classification: M15, M21, O33, L25.

Для цитування: Viadrova Nadiia, Lytvynenko Alina, Fridman Olena, Lytvynenko Olena. Digital transformation of enterprise crisis management under economic instability. Фінансово-кредитні системи: перспективи розвитку. №3(22) 2026. С. 185-204. https://doi.org/10.26565/2786-4995-2026-3-12

Список літератури

1. Lytvynenko O. D., Lytvynenko A. O., Morozova N. L. Impact of Digital Economy on Business Development in Ukraine. *Business Inform.* 2025. No. 5. P. 176–183. DOI: https://doi.org/10.32983/2222-4459-2025-5-176-183.
2. Liberato lo Conte D., Sancetta G., Cucari N., Escobar O. AI-Driven Risk Governance for SMEs: From Predictive Analytics to Strategic Competitiveness. *Strategic Change*. 2026. DOI: https://doi.org/10.1002/jsc.70097.
3. Liu C., Wang Y., Purvis L., Potter A. Can Digital Twin Technology Enhance Supply-Chain Resilience? A Systematic Literature Review. *Sustainability*. 2026. Vol. 18(5). Article 2361. DOI: https://doi.org/10.3390/su18052361
4. Pasko M., Lisna I., Morozova N. L., Denchyk I. Readiness of Ukrainian business for digital transformation: drivers and barriers. *Фінансово-кредитні системи: перспективи розвитку*. 2025. № 1(16). С. 125–137. DOI: https://doi.org/10.26565/2786-4995-2025-1-10.
5. Zhang J., Li H., Zhao H. The Impact of Digital Transformation on Organizational Resilience: The Role of Innovation Capability and Agile Response. *Systems*. 2025. Vol. 13, No. 2. Article 75. DOI: https://doi.org/10.3390/systems13020075
6. Babenko M. V., Pyvavar I. V., Morozova N. L., Lytvynenko A. V. Managerial Decision-Making in the Context of Digital Transformation. *Бізнес Інформ*. 2026. № 1. С. 576–588. DOI: https://doi.org/10.32983/2222-4459-2026-1-576-588
7. Загороднюк О. В., Дмитрик І. О. The role of BPM, CRM and ERP systems in the digital transformation of Ukrainian business. Збірник наукових праць Уманського національного університету садівництва. 2024. Вип. 104. Ч. 2. С. 191–201. DOI: https://doi.org/10.32782/2415-8240-2024-104-2-191-201.
8. Грінько А. П., Гринько П. Л., Даудова Г. В. Філософія формування компетентнісної моделі персоналу організацій в умовах цифрової економіки. *Актуальні проблеми сталого розвитку*. 2025. Т. 2(2). С. 34–46. DOI: https://doi.org/10.60022/2(2)-4S
9. Юрша О. М., Коваль С. Ю., Мельник Л. М. Трансформація антикризового управління підприємствами в парадигмі цифрової економіки. *Центральноукраїнський науковий вісник. Економічні науки*. 2024. № 12(45). С. 201–213. DOI: https://doi.org/10.32515/2663-1636.2024.12(45).201-213.
10. Краус К. М., Краус Н. М., Штепа О. В. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability*. 2022. № 3. С. 26–37. DOI: https://ir.lib.vntu.edu.ua/handle/123456789/37434.
11. Сафонік Н. П., Ковальчук А. М., Костюнік О. В. Трансформація бізнес-моделей релокованих підприємств в умовах інтелектуалізації та цифровізації: інвестиційні та організаційні аспекти. *Актуальні проблеми сталого розвитку*. 2026. DOI: https://doi.org/10.60022/3(4)-11S
12. Котковський В., Самородов Б., Чхеайло А. Управління людськими ресурсами в умовах війни: мотивація, шляхи і способи ефективного застосування особистісного потенціалу. *Сталий розвиток економіки*. 2024. № 3(50). С. 228–235. DOI: https://doi.org/10.32782/2308-1988/2024-50-34
13. Місюра Є. Ю. Logistics in the Context of Digitalization in Ukraine / Логістика в умовах цифровізації в Україні. *Бізнес Інформ*. 2026. № 1. С. 100–109. DOI: https://doi.org/10.32983/2222-4459-2026-1-100-109.
14. Лісний А. Цифрова трансформація як механізм антикризового управління підприємствами в умовах нестабільних ринків. *Економіка та суспільство*. 2026. № 84. DOI: https://doi.org/10.32782/2524-0072/2026-84-119.
15. П'янкова, О., Рула, О. Вплив цифрових трансформацій на ефективність антикризового управління в міжнародних компаніях. *Економіка та суспільство*. 2025 (72). DOI: https://doi.org/10.32782/2524-0072/2025-72-155.
16. Adler-Nissen R., Eggeling K. A. The Discursive Struggle for Digital Sovereignty: Security, Economy, Rights and the Cloud Project Gaia-X. *Journal of Common Market Studies*. 2024. DOI: https://doi.org/10.1111/jcms.13594
17. Ivanov D. The Industry 5.0 framework: viability-based integration of the resilience, sustainability, and human-centricity perspectives. *International Journal of Production Research*. 2023. Vol. 61, No. 5. P. 1683–1695. DOI: https://doi.org/10.1080/00207543.2022.2118892
18. Bianchini S., Damioli G., Ghisetti C. The environmental effects of the "twin" green and digital transition in European regions. *Environmental and Resource Economics*. 2023. Vol. 84. P. 877–918. DOI: https://doi.org/10.1007/s10640-022-00741-7.
19. Ristvej J., Tonhauser M., Chovanec D., Kubás J., Kollár B., et al. Cyber resilience conceptual model for European Union NIS2 standards implementation in Slovakia. *Scientific Reports*. 2025. Vol. 15. Article 26902. DOI: https://doi.org/10.1038/s41598-025-12829-3

20. Crupi A., Del Sarto N., Di Minin A., Gregori G. L., Lepore D., Marinelli L., Spigarelli F. The digital transformation of SMEs – a new knowledge broker called the digital innovation hub. *Journal of Knowledge Management*. 2020. Vol. 24, No. 6. P. 1263–1288. DOI: https://doi.org/10.1108/JKM-11-2019-0623
21. National Institute of Standards and Technology. NIST Strategy for American Technology Leadership in the 21st Century. 2025. URL: https://www.nist.gov/director/strategic-priorities.
22. Ashraf M., Eltawil A., Ali I. Disruption Detection for a Cognitive Digital Supply Chain Twin Using Hybrid Deep Learning. 2023. URL: https://link.springer.com/article/10.1007/s12351-024-00831-y.
23. Papyshev G., Chan K. J. D. AI regulatory strategies for digital sovereignty: The role of geopolitics and technological disparities. *Electronic Markets*. 2026. Vol. 36, No. 1. Article 8. DOI: https://doi.org/10.1007/s12525-025-00870-z
24. Serhiienko O., Smorodin A., Silichova T. Digital transformation as a catalyst for European integration processes development. *Actual Problems of Innovative Economy*. 2025. No. 4. P. 103–111. DOI: https://doi.org/10.36887/2524-0455-2025-4-24

Стаття надійшла до редакції 12.05.2026 *Статтю рекомендовано до друку 15.09.2026*
Стаття надійшла після рецензування 30.08.2026 *Статтю опубліковано 05.10.2026*

Внесок авторів: *всі автори зробили рівний внесок у цю роботу*
Конфлікт інтересів: *автори повідомляють про відсутність конфлікту інтересів*

Декларація про використання штучного інтелекту

Під час підготовки цієї статті було використано інструменти штучного інтелекту Grammarly для перевірки граматичних та орфографічних помилок. Задум, зміст, наукова новизна та результати дослідження належать авторам. Остаточний текст статті був перевірений, опрацьований та відредагований авторами.

Наукове видання

ФІНАНСОВО-КРЕДИТНІ СИСТЕМИ: ПЕРСПЕКТИВИ РОЗВИТКУ

Збірник наукових праць

Випуск 3(22)2026

Українською та англійською мовами

Підписано до друку 05.10.2026. Формат 60х84/8.
Обл.-вид. арк. 37,54. Ум. друк. арк. 30,04. Наклад 100 пр.
Замовлення № 30/26.

Видавець і виготовлювач
Харківський національний університет імені В. Н. Каразіна.
61022, Харків, майдан Свободи, 4, **www.karazin.ua**
Свідоцтво суб'єкта видавничої справи ДК № 3367 від 13.01.09

Видавництво Харківського національного університету імені В. Н. Каразіна