

<https://doi.org/10.26565/2786-4995-2026-3-16>

UDC 005.21:004.9:658

Mykolenko Olena

*PhD in Economics, Associate Professor,
Faculty of Taxation, Accounting and Audit
State Tax University
31 Universytetska St., Irpin, 08205, Ukraine
e-mail: mykolenkohelen@gmail.com
ORCID ID: [0000-0002-1988-7401](https://orcid.org/0000-0002-1988-7401)*

Denchyk Iryna

*Senior Lecturer,
Education and Research Institute "Karazin Banking Institute"
V. N. Karazin Kharkiv National University,
4, Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: irina.denchik@karazin.ua
ORCID ID: [0000-0003-1594-1084](https://orcid.org/0000-0003-1594-1084)*

The role of digital technologies in building the organizational resilience of enterprises

Abstract. The object of the study is the process of building organizational resilience in enterprises under the influence of digital transformation amid martial law, economic instability, and increasing systemic risks. Under these conditions, digital technologies acquire strategic importance by enhancing the adaptability of organizational processes, ensuring business continuity, enabling timely managerial decision-making, and strengthening enterprises' capacity to respond to crisis-related disruptions.

Problem statement. The full-scale war has substantially transformed the operating environment of Ukrainian enterprises, intensifying infrastructure, workforce, logistics, energy, and cybersecurity risks. Under these conditions, digitalization extends beyond the automation of individual business processes and becomes a system-forming factor in organizational resilience, necessitating a reconsideration of its role within enterprise management systems. This perspective is consistent with the overall problem addressed in the article.

Unresolved issues. Despite the substantial body of research on digital transformation and organizational resilience, a comprehensive approach to identifying the mechanism through which organizational resilience is built remains insufficiently developed. Such an approach should consider the technological, managerial, human, and security-related components of digital transformation as a unified and interconnected system. Further research is required into the interaction among digital leadership, digital culture, employees' digital competencies, intelligent information systems, cyber resilience, and continuous learning and innovation, particularly in the context of prolonged systemic disruptions.

Purpose of the article. The purpose of the study is to determine the role of digital technologies in building the organizational resilience of enterprises under martial law and economic instability, as well as to substantiate strategic directions for the development of digital management practices, taking into account European and U.S. experience.

Main material. The methodological framework of the study is based on a comprehensive approach integrating the concepts of organizational resilience, digital transformation, and adaptive enterprise management. The research employs systems and comparative analysis, the structural-logical method, as well as methods of analysis, synthesis, systematization, and scientific generalization. The study identifies the specific features of the transformation of management models in Ukrainian enterprises under the impact of the war and systematizes the functional role of digital technologies in risk forecasting, managerial decision support, business process adaptability, business continuity, and cyber resilience. A comparative analysis of European and U.S. approaches to digitally enabled organizational resilience is conducted, and the possibilities for adapting these approaches to the Ukrainian context are substantiated. An adaptive system of digital organizational resilience for enterprises is proposed, integrating six interconnected components: digital leadership, digital culture, employees' digital competencies, intelligent information systems, cyber resilience, and continuous learning and innovation. Unlike fragmented approaches focusing on individual digital factors, the proposed system is based on their cyclical interaction and integration with human capital, organizational culture, and adaptive management mechanisms.

Conclusions. The study establishes that, under martial law and economic instability, digital transformation acquires strategic importance for building the organizational resilience of enterprises. The organizational resilience of a digitally transformed enterprise is determined not so much by the availability of individual technological solutions as by its ability to integrate digital technologies, management practices, human capital, organizational culture, and cyber-resilience mechanisms into a coherent adaptive system. The practical significance of the findings lies in the possibility of using the proposed system as a conceptual framework for developing digital transformation strategies for Ukrainian enterprises, enhancing their capacity to adapt to crisis-related disruptions, maintain business continuity, and remain competitive during the wartime economy and post-war recovery. Future research should focus on developing methodological tools for the quantitative assessment of digital organizational resilience and on the empirical validation of the proposed system.

Keywords: *organizational resilience, digital transformation, digital technologies, digital organizational resilience, adaptive management, digital leadership, digital culture, digital competencies, cyber resilience, business continuity.*

Formulas: –; Figures: 2; Tables: 2; References: 20.

JEL Classification: M15, O33, L21.

For citation: Mykolenko Olena, Denchyk Iryna. The role of digital technologies in building the organizational resilience of enterprises. *Financial and Credit Systems: Prospects for Development*. №3(22) 2026. P. 251-272. <https://doi.org/10.26565/2786-4995-2026-3-16>

Introduction. Amid increasing global economic instability, organizational resilience is evolving from a desirable competitive advantage into a key prerequisite for the effective functioning and development of enterprises [1]. For Ukrainian businesses, this issue has become particularly acute due to the full-scale war, which has fundamentally altered the business environment, intensified external uncertainty, and heightened the need for new management approaches. The destruction of production infrastructure, disruptions to logistics routes, the relocation of enterprises, labor shortages, persistent cyber threats, and energy-related risks have created a fundamentally new operating environment for Ukrainian enterprises, in which the ability to adapt rapidly to change has become a critical determinant of their viability [18].

Under these conditions, digital technologies can no longer be regarded merely as tools for automating individual business processes. They increasingly perform a system-forming function by ensuring business continuity, supporting real-time managerial decision-making, enabling rapid responses to crises, and maintaining organizational manageability regardless of the location of employees or production facilities [5; 9; 10]. Cloud services, artificial intelligence, big data analytics, digital platforms, enterprise resource planning (ERP) systems, digital document management, and cybersecurity tools are gradually becoming integral components of contemporary organizational resilience models [4; 8; 19].

Martial law has substantially transformed approaches to managing Ukrainian enterprises. Whereas digitalization was previously associated primarily with improving efficiency and competitiveness, it is now increasingly focused on enhancing adaptability, ensuring business continuity, and strengthening the capacity to recover rapidly from crisis-related disruptions. Under these conditions, the nature of management itself is also changing: traditional hierarchical models are giving way to more flexible digital management systems based on data utilization, predictive analytics, remote collaboration, and intelligent decision support [10; 18].

At the same time, the digital transformation of Ukrainian enterprises is taking place amid Ukraine's active integration into the European Union's single digital space. The harmonization of digital standards, participation in European digital development programs, and the implementation of approaches embedded in the Digital Decade 2030 and Industry 5.0 frameworks create new opportunities for modernizing enterprise management systems. Technological cooperation with the United States also plays an important role in this process, facilitating the adoption of advanced digital solutions in cybersecurity, artificial intelligence, cloud computing, supply chain management, and digital analytics. As a result, a new model of organizational resilience is emerging, built on the integration of digital innovation, adaptive management, and international

technological cooperation [14-16].

Literature review. Organizational resilience is becoming increasingly prominent in contemporary management research due to the growing instability of the business environment and the need to ensure business continuity amid crises and structural changes. In systematizing scholarly approaches to conceptualizing organizational resilience, Hillmann and Guenther [1] emphasize the multidimensional nature of the concept and the need to view it not only as an organization's ability to recover from adverse impacts but also as its capacity to adapt and develop under changing conditions. This perspective allows organizational resilience to be conceptualized as a dynamic organizational characteristic associated with an enterprise's ability to anticipate threats, respond to them, adapt its internal processes, and leverage accumulated experience for further development.

Digitalization has emerged as one of the key factors transforming the mechanisms through which organizational resilience is achieved. In contemporary literature, digital transformation is understood as a considerably broader phenomenon than the implementation of individual information technologies. Verhoef et al. [2] define it as a comprehensive process of organizational change encompassing technological solutions, business models, organizational structures, resources, and approaches to value creation. Wessel et al. [3] likewise distinguish digital transformation from traditional IT-enabled organizational transformation, emphasizing that digital transformation entails more fundamental changes in organizational identity, value propositions, and the ways in which enterprises operate. Accordingly, the impact of digitalization on organizational resilience should be examined not merely in terms of the use of individual digital tools but from the perspective of the systemic transformation of an enterprise's organizational capabilities.

A distinct stream of research focuses on determining how specific digital capabilities affect organizational performance and adaptability. In particular, Mikalef and Gupta [4] conceptualize an enterprise's artificial intelligence capability as a complex organizational capability developed through the combination of technological, human, and other resources and capable of positively influencing organizational creativity and performance. This perspective is particularly relevant to resilience research, as it demonstrates that the effects of digital technologies depend not only on their availability but also on an enterprise's ability to integrate technological resources with employee competencies and organizational processes.

The direct relationship between digital transformation and organizational resilience has been examined by Zhang, Long, and von Schaewen [5]. By combining PLS-SEM and fsQCA methods, the authors demonstrate that digital transformation contributes to enhancing organizational resilience; however, achieving this outcome depends on a set of interrelated conditions. This confirms the complex nature of the relationship between digitalization and resilience and highlights the need to consider not individual technologies in isolation, but rather the configuration of an enterprise's digital and organizational capabilities.

The importance of the interaction between an enterprise's internal capabilities and its external environment is further supported by the findings of Xie et al. [6], who investigated the role of business networks in building organizational resilience in the digital era during the COVID-19 pandemic. Their findings demonstrate that the digital environment transforms not only an enterprise's internal processes but also the mechanisms through which it interacts with partners and other participants in business networks. Thus, digital resilience is not built in isolation within an enterprise; it also depends on the enterprise's ability to leverage external relationships, information flows, and network resources to respond to crises.

Considerable attention in the academic literature has also been devoted to the digital maturity of enterprises. Robertson et al. [7], examining small and medium-sized retail enterprises during the COVID-19 pandemic, identified a relationship between digital maturity and organizational resilience. Digitally mature enterprises were found to be better prepared to adapt their business processes and maintain operations under significant external constraints. This suggests that digital maturity can be regarded as a prerequisite for transforming digital technologies

from a collection of individual tools into a systemic resource for organizational adaptation.

This line of research is further developed by Trieu et al. [8], who link information technology capabilities to organizational ambidexterity, resilience, and the performance of small and medium-sized enterprises. Their findings demonstrate the importance of an enterprise's ability to simultaneously maintain current operational efficiency while creating opportunities to explore new solutions and adapt to change. Accordingly, information technologies acquire strategic significance when they support not only operational activities but also organizational flexibility and an enterprise's capacity to reconfigure itself in response to changes in the external environment.

Recent studies have also deepened the understanding of the mechanisms through which digital transformation influences organizational resilience. Browder, Dwyer, and Koch [9] demonstrate that digital transformation can contribute to the renewal of organizational adaptation mechanisms and enhance enterprises' capacity to respond to change. In turn, Awad and Martín-Rojas [10] emphasize the mediating role of organizational learning and innovation. Their findings indicate that the positive impact of digital transformation on resilience is largely realized through an organization's ability to acquire new knowledge, translate it into new managerial and technological solutions, and sustain innovation activities. This provides a basis for considering continuous learning and innovation as important components of a digitally oriented system of organizational resilience.

Recent research provides further evidence of the strengthening relationship between digital transformation and organizational resilience. Wang and Jia [11] directly examine the impact of digital transformation on organizational resilience, whereas Koh, Toh, and Yuen [12], drawing on organizational information processing theory, focus on the factors contributing to the development of organizational digital resilience. This perspective is particularly important because digitalization simultaneously expands an enterprise's information-processing and analytical capabilities while increasing its dependence on digital infrastructure, data quality, information systems, and its capacity to manage digital risks.

At the same time, digital technologies have considerable potential to enhance the resilience of interorganizational processes. In particular, using blockchain-coordinated supply chains as an example, Lohmer, Bugert, and Lasch [13] demonstrate the potential of digital technologies to support the resilience of complex networked systems and mitigate the propagation of the adverse effects of disruptions throughout supply chains. This broadens the understanding of digital resilience from the intraorganizational level to the level of digital ecosystems and interorganizational interactions.

Another important direction in contemporary discourse is the transition toward a human-centric model of digital transformation. Within the Industry 5.0 framework, resilience, alongside sustainability and human-centricity, is identified as one of the fundamental principles guiding the development of European industry [14; 15]. This approach implies that technological transformation should combine improvements in efficiency with human capital development, organizational adaptability, and the capacity of organizations to operate under conditions of systemic disruption. Accordingly, employees' digital competencies and their ability to interact effectively with emerging technologies are becoming important components of organizational resilience.

The strategic importance of digital capabilities is also reflected in European digital policy. The Digital Decade 2030 programme envisages the systematic development of digital skills, digital infrastructure, the digital transformation of businesses, and the digitalization of public services [16], while the European Digital Innovation Hubs network provides institutional mechanisms to support the digital transformation of enterprises, particularly small and medium-sized enterprises [17]. Taken together, these initiatives create an environment in which enterprises' digital maturity is increasingly associated with their competitiveness, adaptability, and long-term resilience.

For Ukraine, the relationship between digital transformation and resilience is of particular

importance. The OECD study [18] explicitly considers the digital transformation of businesses in the context of strengthening Ukraine's resilience. Amid prolonged security, economic, and infrastructure risks, digital technologies are becoming essential not only for the modernization of enterprises but also for maintaining business continuity, adapting to disruptions in traditional ways of organizing work, and creating the conditions necessary for recovery.

As the use of digital technologies expands, cyber resilience is becoming increasingly important. Within the NIST methodological framework, cyber resilience is considered in terms of a system's ability to anticipate adverse conditions, withstand them, recover from them, and adapt in the face of attacks, failures, or other disruptions [19]. For modern enterprises, this means that digital transformation without appropriate cyber risk management can simultaneously create new opportunities and introduce additional vulnerabilities. Therefore, cyber resilience should be regarded as an integral component of the overall organizational resilience system of a digitally transformed enterprise.

Recent studies further confirm the need to examine the intermediate organizational mechanisms through which this impact occurs. Zhang, Li, and Zhao [20] investigate the relationship between digital transformation and organizational resilience, taking into account the role of innovation capability and flexible response. This approach demonstrates that digital technologies create the potential for resilience; however, the realization of this potential depends on an enterprise's ability to transform digital resources into specific adaptive and innovative capabilities.

Thus, the literature review indicates an emerging and robust scholarly consensus regarding the positive relationship between digital transformation and organizational resilience [5-12; 20]. At the same time, existing studies predominantly focus on individual mechanisms underlying this relationship, including digital maturity [7], information technology capabilities [8], organizational adaptation [9], learning and innovation [10], information processing [12], and innovation capability and flexible response [20]. The resilience of digital supply chains [13], human-centric digital transformation [14; 15], and cyber resilience [19] are also examined as distinct areas of research.

Nevertheless, a comprehensive approach to identifying the mechanism through which organizational resilience is built remains insufficiently developed, particularly one in which the technological, managerial, human, and security-related components of digital transformation are considered as a unified and interconnected system. In particular, further research is needed to explore the interaction among digital leadership, digital culture, employees' digital competencies, intelligent information systems, cyber resilience, and continuous learning and innovation in strengthening an enterprise's ability to anticipate threats, adapt, recover, and transform. Examining these interrelationships is particularly relevant for enterprises operating under conditions of prolonged systemic disruption, where digital technologies serve not only to enhance efficiency but also as an infrastructural foundation for business continuity and adaptability.

Purpose, objectives and research methods. The purpose of the study is to determine the role of digital technologies in building the organizational resilience of enterprises under martial law and economic instability, as well as to substantiate strategic directions for the development of digital management practices, taking into account European and U.S. experience.

To achieve this aim, the following research objectives were defined: to synthesize contemporary theoretical approaches to understanding organizational resilience and determine the role of digital transformation in strengthening it; to examine the specific features of the transformation of management models in Ukrainian enterprises under the impact of the war; to determine the potential of digital technologies to enhance adaptability, ensure business continuity, and strengthen enterprises' capacity to respond to crisis-related challenges; to analyze international digital transformation practices and the approaches adopted by the European Union and the United States to digitally enabled organizational resilience; to identify opportunities for adapting international experience to the Ukrainian context and substantiate strategic directions for building the digital organizational resilience of Ukrainian enterprises.

The methodological framework of the study is based on a comprehensive approach integrating the concepts of organizational resilience, digital transformation, and adaptive enterprise management. The study is grounded in the principles of systems thinking, interdisciplinarity, and risk-oriented analysis, which make it possible to consider digital transformation not as a set of isolated technological changes but as an integral component in building a comprehensive system of enterprise resilience.

To address the research objectives, the following methods were employed: systems analysis to examine organizational resilience as an integrated system and determine the role of digital technologies in building it; comparative analysis to compare the approaches adopted in Ukraine, the European Union, and the United States to digitally enabled enterprise resilience and identify opportunities for adapting international experience to Ukrainian conditions; the structural-logical method to establish relationships among digital technologies, management processes, adaptability, and organizational resilience; methods of analysis, synthesis, and systematization to examine contemporary scholarly approaches to digital transformation and organizational resilience and organize the factors shaping their interaction; and scientific generalization to formulate the authors' conclusions, substantiate an adaptive system of digital organizational resilience, and identify strategic directions for enhancing enterprise resilience under wartime economic conditions.

The information base of the study comprises recent scholarly publications on organizational resilience, digital transformation, and adaptive management; regulatory and strategic documents of the European Union; analytical materials published by international organizations, particularly the OECD; and NIST methodological documents on cyber resilience.

The scientific novelty of the study lies in advancing the theoretical understanding of the role of digital technologies in building the organizational resilience of enterprises by conceptualizing them not merely as tools for automating and improving the efficiency of individual business processes, but as a system-forming factor in building enterprise resilience under wartime economic conditions. The proposed approach conceptualizes digital transformation as the foundation for developing an adaptive management system that integrates technological, managerial, human, and security-related components and strengthens enterprises' capacity to respond to crisis-related challenges, maintain business continuity, adapt to and recover from destabilizing impacts, and integrate into the European digital economic space.

Research results. In the digital economy, resilience is increasingly derived not from material resources but from an enterprise's digital capabilities. While a decade ago digitalization was viewed primarily as a means of enhancing productivity, today it increasingly determines an organization's ability to respond rapidly to change, reconfigure business processes, and ensure business continuity under conditions of high uncertainty [5; 9-11; 20].

One of the key indicators of an enterprise's readiness to address such challenges is its digital maturity. Digital maturity reflects not the extent to which individual digital solutions have been implemented, but rather the degree to which digital technologies are integrated into the strategic management system. Enterprises with a high level of digital maturity use data as a basis for managerial decision-making, rapidly scale digital services, integrate business processes within a unified information system, and are capable of promptly reconfiguring their organizational structures in response to changing operating conditions [7]. For Ukrainian enterprises, this is particularly important in the context of production relocation, remote work, and continuous changes in the market environment.

At the same time, even the most advanced technologies cannot ensure resilience without an adequate level of employees' digital competencies. The effectiveness of digital transformation depends not only on investments in software and equipment but also on employees' readiness to work with digital platforms, use analytical tools, collaborate in virtual environments, and rapidly adapt to new technological solutions [7; 8; 12]. Under these conditions, continuous employee learning, the development of digital leadership, and the cultivation of a data-driven culture are

becoming strategic priorities of contemporary management.

An enterprise's digital culture is also an important component of organizational resilience. It reflects the organization's readiness for continuous change, openness to innovation, support for experimentation, cross-functional collaboration, and the integration of digital technologies as a natural part of everyday operations. A strong digital culture facilitates the rapid dissemination of new management practices and significantly reduces the time required for an enterprise to adapt to crisis situations.

The adaptability of organizational processes is becoming particularly important. Modern digital platforms, ERP and CRM systems, business intelligence tools, artificial intelligence technologies, digital document management, and cloud computing enable enterprises to rapidly reconfigure their production and management processes without significant organizational losses [4; 8-10]. As a result, digitalization not only enhances the efficiency of individual operations but also creates a fundamentally new quality of management based on rapid decision-making, flexible resource reallocation, and continuous monitoring of changes in the external environment.

Under current conditions, digital technologies should be regarded not as auxiliary automation tools but as a strategic resource for building enterprise organizational resilience. The levels of digital maturity and digital competencies, together with the development of digital culture and the adaptability of business processes, determine an organization's ability to operate effectively under wartime economic conditions, integrate into the European digital space, and maintain long-term competitiveness.

The full-scale war has become a catalyst for the profound transformation of management approaches in Ukrainian enterprises. Whereas most companies previously developed their strategies based on the assumption of a predictable market environment, the ability to operate under conditions of persistent turbulence has now become a critical determinant of organizational effectiveness. Martial law has substantially altered the nature of risks: they have become multidimensional, interconnected, and capable of rapidly spreading across production, financial, human resources, information, and logistics domains [18]. Under these conditions, organizational resilience is no longer a characteristic of individual business processes but assumes a systemic nature, determining an enterprise's ability to maintain its operations even in the absence of stable external conditions.

One of the most significant challenges has been the destruction of production infrastructure. Damage to production facilities, warehouse complexes, transport hubs, and critical infrastructure has forced enterprises to reconsider traditional approaches to organizing production. The spatial concentration of assets, which had long provided cost efficiencies, has emerged as a source of increased risk. In response, models involving the geographical diversification of production, the establishment of backup production facilities, and the use of cloud-based IT infrastructure and digital platforms are becoming increasingly widespread, enabling enterprises to coordinate their activities regardless of their physical location [18].

The relocation of enterprises has gradually evolved from an emergency measure into a distinct area of strategic management. The transfer of production facilities to safer regions has been accompanied by the need to rapidly restore production processes, integrate new suppliers, reconfigure logistics, and establish cooperation with local communities. At the same time, relocation has demonstrated the importance of the digital integration of business processes. Enterprises that had implemented ERP systems, digital document management, cloud services, and electronic communication platforms before the outbreak of the full-scale war were able to adapt to new operating conditions considerably faster while maintaining organizational manageability even in the face of fundamental changes in their organizational structures [9; 18].

Enterprises' human resource systems have also been significantly affected. The mobilization of employees, internal and external migration, shortages of qualified professionals, and the widespread adoption of remote and hybrid work have transformed traditional approaches to human

capital management. Competition for skilled professionals increasingly depends not only on remuneration but also on opportunities to work remotely, use modern digital tools, and engage in continuous professional development. These developments highlight the need to strengthen employees' digital competencies, foster digital leadership, and develop new approaches to organizing team collaboration.

At the same time, Ukrainian businesses face cyberattacks targeting information systems, attempts to steal data, attacks on cloud infrastructure, and disruptions to digital services. Under these conditions, cybersecurity is no longer solely a technical function of IT departments but is becoming an integral component of the overall corporate governance system. Consequently, the level of cyber resilience increasingly determines the overall organizational resilience of an enterprise [19].

The closure of certain transport routes, changes in export logistics, instability in maritime transportation, fluctuations in transportation costs, and the need to reorient operations toward European markets have forced enterprises to reconsider their approaches to supply chain management. In response, digital platforms for shipment monitoring, predictive analytics systems, artificial intelligence technologies, and digital inventory management tools have become important instruments for maintaining the flexibility of logistics processes and enabling rapid responses to changes in the external environment.

Energy-related risks have emerged as an additional source of instability, directly affecting the continuity of production activities. Large-scale attacks on energy infrastructure have highlighted the need to establish backup power sources, optimize energy consumption, and implement digital systems for monitoring the use of energy resources.

These factors have substantially increased uncertainty in the business environment. Unlike traditional crises, in which enterprises could estimate the timeframe for the recovery of economic activity, the current environment is characterized by highly dynamic change and limited predictability. This requires managers to move away from rigid strategic planning toward scenario-based management, continuous risk monitoring, and the use of digital analytics to support managerial decision-making.

As a result, martial law has created new requirements for enterprise management systems. The speed of managerial decision-making has become one of the key characteristics of a modern organization. Competitive advantage is increasingly determined not by the volume of available resources but by the ability to rapidly analyze information, assess alternative scenarios, and quickly adapt operations to changes in the external environment. Consequently, digital information and analytical systems, Big Data technologies, and artificial intelligence tools are increasingly being integrated into the strategic management of enterprises.

Figure 1 presents the conceptual framework for the transformation of organizational resilience in contemporary Ukrainian enterprises.

Digital team collaboration enables the coordination of employees' activities regardless of their physical location. The use of corporate digital platforms, collaborative tools, digital document management systems, and project management systems helps maintain the integrity of the organizational structure even when employees are geographically dispersed. This mode of interaction is gradually transforming organizational culture by strengthening horizontal communication, accelerating information exchange, and increasing employee involvement in decision-making processes [2; 3; 9].

The widespread adoption of remote work has increased the importance of remote management. Modern managers are increasingly assuming the role of coordinators within the enterprise's digital ecosystem, ensuring the synchronization of team activities, monitoring task performance, and maintaining strategic communication through digital channels. This significantly changes the requirements for managerial competencies, increasing the importance of digital leadership, data literacy, and change management.

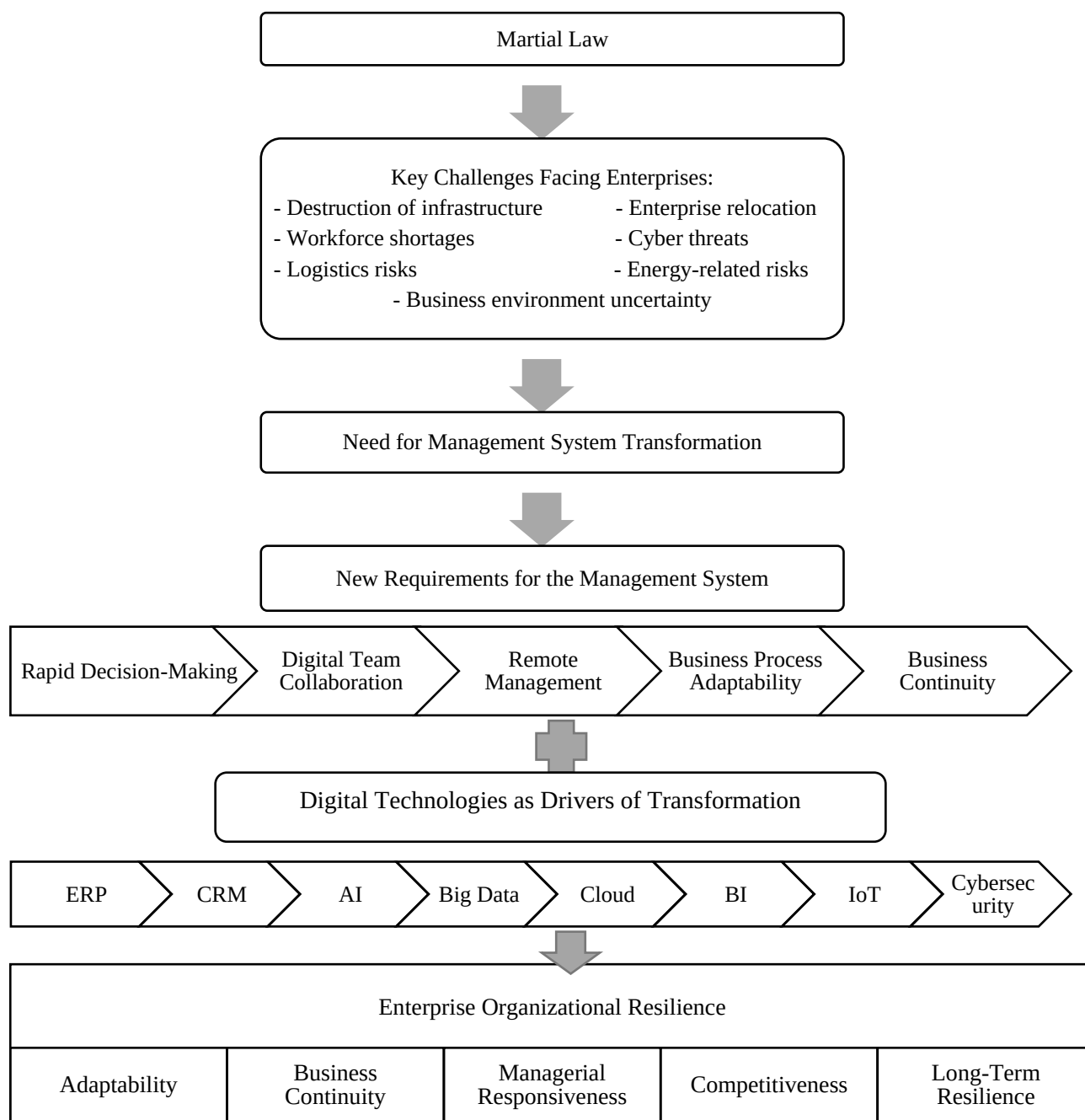


Fig. 1. Transformation of Organizational Resilience in Ukrainian Enterprises under Martial Law
Source: compiled by the authors.

The new business environment also places greater demands on business process adaptability. Organizations must be prepared to rapidly modify production routes, supply structures, customer interaction formats, and internal procedures without significantly compromising operational efficiency. Such flexibility can be achieved through the integration of ERP, CRM, and BPM systems, cloud services, business process automation technologies, and digital analytics.

A logical outcome of these transformations is a reconsideration of the concept of Business Continuity. Whereas it was previously viewed primarily as a set of contingency measures designed to address emergencies, it is now evolving into a strategic principle of enterprise operations. Its implementation requires not only crisis response plans but also the development of digital infrastructure capable of supporting critical business processes regardless of external circumstances.

Consequently, the organizational resilience of a modern enterprise is increasingly determined by the extent to which digital technologies are integrated into its corporate governance system, thereby ensuring operational continuity, the adaptability of organizational processes, and the capacity to operate under conditions of prolonged uncertainty.

Contemporary digital transformation is changing the role of technology within enterprise management systems. Whereas technologies were previously used primarily to automate individual operations, they now form the foundation of organizational resilience by enabling the timely identification of risks, supporting managerial decision-making, enhancing business process flexibility, and ensuring business continuity (Table 1).

Table 1. Functional Role of Digital Technologies in Building Enterprise Organizational Resilience

Functional Area	Digital Technologies	Impact on Organizational Resilience
Risk forecasting and managerial decision support	Artificial Intelligence (AI), Machine Learning	Analysis of large datasets, forecasting of crisis situations, optimization of managerial decisions, and reduced response time to risks.
Early detection of crises	Big Data, Predictive Analytics	Monitoring of the external environment; forecasting changes in demand, financial risks, logistics disruptions, and other sources of instability.
Ensuring business continuity	Cloud Computing	Secure data storage, remote access to information, and support for enterprise operations regardless of the location of employees or production facilities.
Crisis scenario modelling	Digital Twin	Creation of digital enterprise models to test alternative development scenarios without posing risks to actual operations.
Adaptive business process management	ERP, CRM, BPM systems	Integration of business processes, increased management transparency, rapid resource reallocation, and coordination of activities across organizational units.
Transparency and reliability of business processes	Blockchain	Information protection, verification of transaction authenticity, increased trust among supply chain participants, and minimized risk of data falsification.
Protection of digital infrastructure	Cybersecurity systems, Zero Trust, SIEM, Multi-Factor Authentication	Protection of corporate data, ensuring the continuity of digital services, strengthening enterprise cyber resilience, and minimizing the consequences of cyberattacks.

Source: systematized by the authors based on [2; 4; 8; 13; 18; 19; 20].

The analysis of Table 1 demonstrates that modern digital technologies perform functions that extend far beyond the traditional automation of business processes. They are increasingly integrated into strategic management systems, enabling timely risk forecasting, providing information support for managerial decision-making, facilitating digital interaction among organizational units, and enhancing the adaptability of organizational processes. Under these conditions, digitalization is becoming one of the key factors in building enterprise organizational resilience.

For Ukrainian enterprises, the integrated use of digital technologies is of particular importance. The highest level of organizational resilience is achieved not through the implementation of individual digital solutions but through their integration into a unified digital management ecosystem that combines analytical tools, information platforms, managerial decision-support systems, and cybersecurity solutions. This approach is consistent with current European trends in the development of the digital economy and creates the conditions necessary to enhance the competitiveness of Ukrainian enterprises under martial law and during post-war recovery.

Building enterprise organizational resilience is currently regarded as one of the priority areas of economic policy in the world's leading economies. At the same time, approaches to digital transformation differ considerably. While European Union countries focus on developing a digital

economy oriented toward sustainable development, social responsibility, and technological sovereignty, the U.S. model is based on the accelerated adoption of innovation, the development of artificial intelligence, platform-based business models, and data-driven management [4; 19]. For Ukraine, which is simultaneously undergoing digital transformation, wartime adaptation, and European integration, combining the most effective elements of both models is of particular importance (Table 2).

Table 2. Comparative Characteristics of European and U.S. Approaches to Digitally Enabled Enterprise Organizational Resilience

Area	European Approach	U.S. Approach	Implications for Ukraine
Development concept	Industry 5.0 – human-centricity, resilience, sustainable development	AI-driven Management – intelligent management, automated decision-making	Combining digital efficiency with a socially responsible business orientation
Strategic priority	Digital sovereignty	Technological leadership and innovation	Reducing technological dependence and developing domestic digital infrastructure
Enterprise management	ESG, digital responsibility	Data-driven Decision Making	Developing a data-driven management system aligned with sustainable development principles
Innovation ecosystem	European Digital Innovation Hubs (EDIH)	Digital ecosystems and corporate innovation platforms	Integrating Ukrainian enterprises into international digital innovation networks
Security	Cybersecurity, protection of critical infrastructure	Cyber Resilience, Zero Trust, proactive cyber risk management	Strengthening enterprise cyber resilience under martial law
Business organization	Digital transformation of production	Platform-based business models	Developing digital services and new value creation models
Logistics	Integrated EU digital transport system	AI-driven supply chain optimization	Building resilient logistics networks and diversifying supply sources
Long-term strategy	Digital Decade 2030	Investment in breakthrough digital technologies	Aligning Ukraine's digital policy with EU standards while leveraging U.S. technological expertise

Source: systematized by the authors based on [4; 14–19].

The European model of digital transformation is based on the Industry 5.0 concept, which views digital technologies as a means of enhancing productivity, strengthening resilience, promoting environmental responsibility, and fostering human-centric development. Considerable attention is devoted to digital autonomy, the development of European Digital Innovation Hubs, the implementation of ESG principles, and the achievement of the strategic objectives of the Digital Decade 2030, which are aimed at enhancing business digital maturity, developing digital competencies, and protecting digital infrastructure. This approach provides a systemic perspective on organizational resilience as the outcome of a balanced combination of technological, economic, and social factors [14; 15].

The U.S. model is characterized by a significantly faster pace of innovation adoption and a strong orientation toward technological leadership. Its key priorities include AI-driven management systems, data-driven decision-making, the development of digital platforms, the scaling of cloud services, and the creation of digital ecosystems. Particular importance is attached to the concept of cyber resilience, which encompasses not only the protection of information infrastructure but also an enterprise's ability to maintain business continuity even in the event of large-scale cyberattacks or other digital threats. Considerable emphasis is also placed on the use of artificial intelligence for risk forecasting, supply chain optimization, and real-time managerial decision support [4; 19].

In Ukraine, certain elements of international experience are already being gradually integrated into national digital policy and corporate governance practices. Digital document management, cloud technologies, digital services, and advanced cybersecurity solutions are being

actively implemented, while cooperation with the European Union is expanding within digital transformation and innovation development programmes. At the same time, businesses are showing increasing interest in the use of artificial intelligence, predictive analytics, digital platforms, and tools for automating management processes [18].

Nevertheless, the pace of digital transformation remains uneven. The main barriers include limited investment resources, disparities in the level of digital maturity among enterprises, shortages of professionals with digital competencies, the high costs of implementing advanced information systems, and persistent risks associated with military hostilities and cyberattacks. Small and medium-sized enterprises face additional challenges related to the complexity of integrating digital platforms and limited access to innovation infrastructure.

Post-war economic recovery provides an opportunity for a qualitatively new stage in the modernization of Ukrainian enterprises. A promising direction is the development of an integrated model of digital organizational resilience that combines European principles of sustainable development, digital responsibility, and technological autonomy with U.S. approaches to the use of artificial intelligence, data analytics, and digital platforms.

The experience of Ukrainian enterprises operating under martial law demonstrates that traditional approaches to ensuring organizational resilience are becoming increasingly inadequate in addressing contemporary challenges. Practice shows that the isolated implementation of digital technologies does not guarantee an enterprise's ability to respond effectively to crises. Instead, the determining factor is the extent to which digital solutions are integrated into strategic management systems, corporate culture, and managerial decision-making processes.

In view of the above, the authors propose a concept of enterprise digital organizational resilience – the Adaptive System of Digital Organizational Resilience – which conceptualizes organizational resilience as the outcome of the interaction among six interconnected management components. Unlike existing approaches, the proposed model is based not on individual digital technologies but on their integration with human capital, organizational culture, and adaptive management mechanisms.

The starting point of the model is digital leadership, which determines the strategic direction of an enterprise's digital transformation. Its function extends beyond making managerial decisions regarding the implementation of digital technologies to fostering organizational readiness for continuous change, developing innovative thinking, and promoting a culture of openness to digital transformation. Digital leadership coordinates all other components of the model and defines the enterprise's strategic development priorities.

The next component is digital culture, which shapes the organization's internal environment. It is characterized by openness to innovation, employees' readiness to operate in a digital environment, the development of horizontal communication, knowledge sharing, and the integration of digital technologies into everyday activities. Without a well-established digital culture, even the most advanced information systems are unlikely to produce the expected managerial outcomes.

Under current conditions, digital competencies are becoming a key component of an enterprise's organizational capital. These competencies encompass not only proficiency in specialized software but also the ability to work with large datasets, use digital services, apply artificial intelligence tools, and interact effectively in digital environments. The level of digital competencies directly influences the speed at which an enterprise can adapt to emerging challenges.

The functional foundation of the model is formed by intelligent information systems that integrate ERP, CRM, and BPM platforms, business intelligence systems, cloud services, artificial intelligence technologies, and predictive analytics. These systems enable the collection, processing, and analysis of information, support managerial decision-making, facilitate the rapid reallocation of resources, and enhance the adaptability of business processes.

An integral component of the model is cyber resilience, which ensures the protection of digital infrastructure, corporate data, and information resources. Under current conditions, cyber

resilience encompasses both technical cybersecurity measures and organizational procedures for managing cyber risks, backing up information resources, continuously monitoring the digital environment, and rapidly restoring critical services following cyberattacks or other emergencies.

The final component of the model is continuous learning and innovation, which ensures its dynamic nature. The continuous development of digital competencies, adoption of new technologies, advancement of innovative management approaches, and accumulation of organizational experience enable an enterprise to adapt to changes in the external environment in a timely manner.

The cyclical architecture of the model, presented in Fig. 2, more accurately reflects the dynamic nature of organizational resilience.

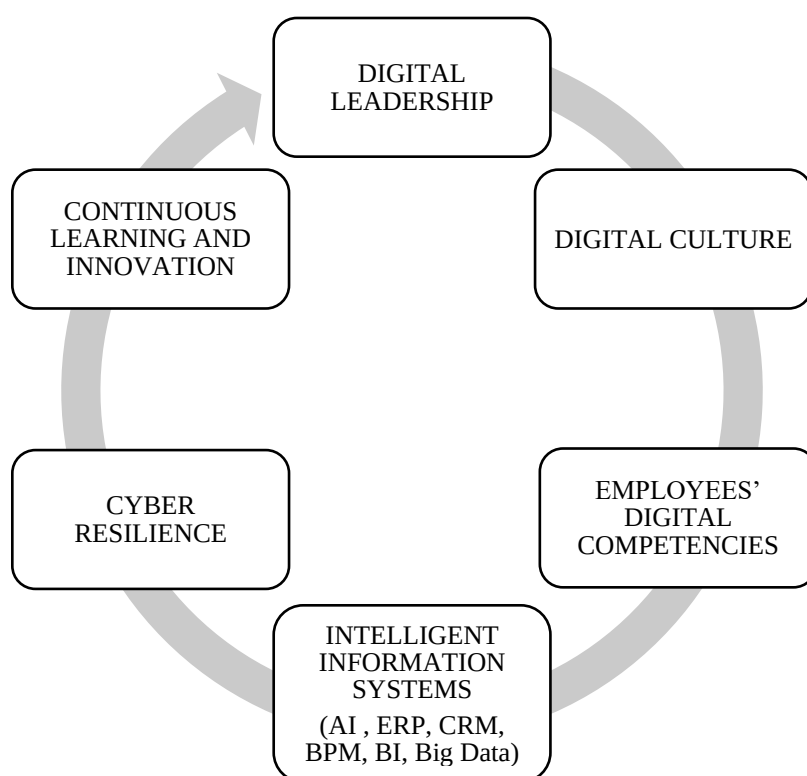


Fig. 2. Digital Model of Enterprise Organizational Resilience
Source: developed by the authors.

A key feature of the proposed concept is the continuous interaction among all its components. Digital leadership defines the strategic directions for the development of digital culture; digital culture facilitates the development of employees' digital competencies; a high level of digital competencies enables the effective use of intelligent information systems; information systems require robust cyber resilience; and the outcomes of their operation provide a foundation for continuous learning and further innovation. In turn, accumulated experience and newly acquired knowledge are fed back into the management system, initiating a new cycle of enterprise digital transformation.

From this perspective, organizational resilience is viewed not as a static outcome of individual management measures but as a continuous process involving the interaction of digital technologies, human capital, organizational culture, and adaptive management. The practical value of the proposed model lies in its potential use as a conceptual framework for developing digital transformation strategies for Ukrainian enterprises, strengthening their resilience to crisis-related disruptions, and ensuring competitiveness under wartime economic conditions and during post-war recovery.

The experience of recent years has demonstrated that digital transformation can no longer be regarded as a separate area of enterprise modernization. Under martial law, it is evolving into a strategic mechanism for ensuring organizational resilience, determining an enterprise's ability to adapt to crises, maintain business continuity, and integrate into the international economic environment. At the same time, the further development of digital resilience requires not the isolated automation of individual processes but a systemic transformation of the enterprise management model.

The first strategic direction involves integrating artificial intelligence technologies into the corporate governance system. At the current stage, AI should be regarded not merely as a tool for automating individual operations but as a foundation for intelligent managerial decision support. The use of machine learning algorithms, predictive analytics, and generative artificial intelligence creates opportunities for modelling crisis scenarios, forecasting changes in the market environment, optimizing resource utilization, and accelerating managerial responses. In the future, AI is expected to form the foundation of adaptive enterprise management.

The second strategic direction is the development of digital leadership, which is gradually becoming one of the key competencies of modern managers. Managing digital change requires the ability to operate under conditions of uncertainty, use analytical data in strategic decision-making, coordinate cross-functional teams, and foster a culture of continuous innovation.

Organizational resilience is determined not only by technological capabilities but also by employees' readiness to embrace change, operate effectively in a digital environment, and rapidly adapt to new conditions. Corporate culture plays a crucial role in integrating digital technologies into the enterprise's day-to-day operations, fostering innovation, and enhancing the effectiveness of team collaboration.

An important strategic priority for Ukraine is the expanded use of European Union digital platforms. The participation of Ukrainian enterprises in European digital initiatives, cooperation with European Digital Innovation Hubs, and the use of cloud infrastructure, digital services, and innovation support tools will contribute to accelerating the digital modernization of businesses. At the same time, this will facilitate the harmonization of management practices with European standards and enhance the competitiveness of Ukrainian enterprises in international markets.

The further development of the digital economy is impossible without the systematic enhancement of employees' digital competencies. The demand for professionals capable of working with data, artificial intelligence systems, digital platforms, and cybersecurity tools is steadily increasing. Therefore, enterprises should move from occasional employee training toward establishing systems of continuous professional development that integrate corporate training, digital learning platforms, and micro-credentials.

The digitalization of HR processes is also becoming increasingly important, transforming approaches to human capital management. The use of HR analytics, digital recruitment platforms, competency management systems, and data-driven employee assessment tools enables enterprises to respond rapidly to workforce challenges, ensure effective human resource planning, and maintain organizational flexibility.

Under current conditions, strengthening digital cyber resilience is becoming one of the key strategic directions for enterprise development. The increasing scale of digitalization is accompanied by growing cyber risks, which are particularly significant for enterprises operating under martial law. Cybersecurity should therefore be integrated into the overall strategic management system of an enterprise, encompassing not only the technical protection of information resources but also the development of organizational mechanisms for cyber risk management, digital infrastructure redundancy, and employee preparedness to respond to cyber incidents.

The development of digital business ecosystems also facilitates the integration of enterprises, suppliers, customers, financial institutions, research organizations, and public institutions within a unified digital environment. Unlike traditional models of interaction, digital

ecosystems create opportunities for rapid information exchange, the shared use of digital resources, the implementation of innovative projects, and enhanced resilience of value chains.

The final strategic direction is the integration of Ukrainian enterprises into European digital value chains. Post-war economic recovery creates new opportunities for Ukrainian businesses to enter the European digital market, participate in international production networks, and engage in joint innovation projects. The implementation of this strategic direction requires the harmonization of digital standards, the development of information system interoperability, improvements in enterprises' digital maturity, and the active use of advanced digital platforms.

The strategic development of digital organizational resilience should be based on a comprehensive combination of technological, managerial, and workforce transformations. Only the systemic integration of digital technologies, human capital, an innovation-oriented culture, and international partnerships can ensure the long-term competitiveness of Ukrainian enterprises amid global economic instability and post-war reconstruction.

Discussion. The findings confirm the perspective established in the contemporary academic literature that digital transformation is positively associated with organizational resilience; however, the mechanism underlying this relationship is more complex than the direct implementation of individual digital technologies. The need identified in this study for the systemic integration of digital solutions into strategic and operational management is consistent with the findings of Zhang, Long, and von Schaewen [5], who demonstrate that enhanced organizational resilience results from a combination of interrelated digital and organizational conditions. This is also consistent with the findings of Wang and Jia [11] regarding the relationship between digital transformation and organizational resilience. At the same time, the present study extends these perspectives by conceptualizing digitalization not merely as a factor that enhances adaptability but as a system-forming foundation of organizational resilience that integrates technological, managerial, human resource, and security dimensions.

The identified role of digital maturity in enabling enterprises to rapidly reconfigure business processes and maintain business continuity is consistent with the findings of Robertson et al. [7], who established the positive contribution of digital maturity to the organizational resilience of small and medium-sized enterprises under crisis conditions. At the same time, the findings of the present study broaden the interpretation of digital maturity: for enterprises operating under wartime economic conditions, it is reflected not only in the level of technological development but also in the capacity to ensure remote management, facilitate digital collaboration among geographically dispersed teams, rapidly reallocate resources, maintain access to critical information, and ensure the continuity of critical business processes.

The findings are also consistent with those of Trieu et al. [8] regarding the role of information technology capabilities and organizational ambidexterity in building enterprise resilience. The analysis confirms that digital technologies acquire strategic significance when they support not only the efficiency of current operations but also the rapid reconfiguration of business processes in response to changes in the external environment. For Ukrainian enterprises, this capability assumes particular importance due to the need to respond simultaneously to infrastructure destruction, relocation, workforce shortages, logistics and energy-related risks, cyber threats, and overall uncertainty in the business environment. In this context, digitalization performs a dual function: it supports ongoing operational activities while simultaneously creating opportunities for the adaptive transformation of the enterprise.

The findings regarding the importance of digital leadership, digital culture, and employees' digital competencies complement the technology-oriented perspective on digital resilience. This is consistent with the approach of Mikalef and Gupta [4], according to which the organizational impact of artificial intelligence depends on an enterprise's ability to combine technological and human resources. At the same time, the findings indicate that under conditions of high uncertainty, the human and managerial components perform not merely a supporting but an integrative function:

digital leadership sets the strategic direction of transformation, digital culture fosters organizational readiness for change, and digital competencies enable employees to effectively utilize the enterprise's technological potential.

An important finding is the confirmation of the role of continuous learning and innovation as a mechanism for maintaining the dynamic nature of organizational resilience. This finding is consistent with Awad and Martín-Rojas [10], who identify organizational learning and innovation as important mechanisms through which digital transformation affects organizational resilience, as well as with Browder, Dwyer, and Koch [9], who associate digital transformation with the renewal of an organization's adaptive capabilities. In the proposed model, this relationship is cyclical: the knowledge and experience accumulated through organizational activities provide the foundation for the further development of digital competencies, the improvement of information systems, and a new cycle of organizational adaptation.

The identified role of cyber resilience also warrants particular attention. The expansion of digital infrastructure simultaneously creates new opportunities for adaptation and increases an enterprise's dependence on the uninterrupted functioning of information systems. This is consistent with the approach of Koh, Toh, and Yuen [12], who examine organizational digital resilience from the perspective of an organization's capacity to process information effectively, as well as with the NIST systems approach to cyber resilience [19]. The findings suggest that, for enterprises operating under wartime economic conditions, cyber resilience should be integrated into the overall corporate governance system, as disruptions to the availability of digital services, data compromise, or the loss of information infrastructure directly affect an enterprise's ability to maintain critical operations.

The proposed approach is also consistent with the contemporary European concept of Industry 5.0, in which resilience is considered in conjunction with human-centricity and sustainable development [14; 15]. At the same time, the comparison of European and U.S. approaches demonstrates the value of using them not as alternatives but as complementary frameworks for Ukrainian enterprises. European principles of human-centricity, digital responsibility, technological autonomy, and digital competence development can be combined with an emphasis on artificial intelligence, data-driven management, digital platforms, and cyber resilience. Such a combination is particularly relevant to Ukraine, where digital transformation must simultaneously strengthen the current resilience of businesses and create a foundation for their post-war modernization and integration into the European digital space.

The scientific significance of the findings lies in the transition from a fragmented interpretation of the digital determinants of organizational resilience to their systemic conceptualization. Unlike studies that separately emphasize digital maturity [7], information technology capabilities [8], adaptation mechanisms [9], organizational learning and innovation [10], digital drivers [12], or innovation capability and response flexibility [20], the proposed Adaptive System of Digital Organizational Resilience integrates digital leadership, digital culture, employees' digital competencies, intelligent information systems, cyber resilience, and continuous learning and innovation into a unified cyclical system. It is the interaction among these components, rather than their development in isolation, that is regarded as the foundation of an enterprise's ability to anticipate threats, respond to crisis-related disruptions, adapt, maintain business continuity, and develop new capabilities for future growth. This directly corresponds to the architecture of the authors' model presented in the research results.

At the same time, the findings are subject to certain limitations. The study is predominantly theoretical and conceptual in nature, and the proposed Adaptive System of Digital Organizational Resilience requires further empirical validation. Moreover, the relative importance of individual components of the system may vary depending on enterprise size, industry, level of digital maturity, and the nature of crisis-related disruptions. Therefore, future research should focus on operationalizing the proposed components, developing appropriate indicators, and quantitatively

assessing the nature and strength of the relationships among them.

Conclusions. The study establishes that, under martial law and economic instability, digital transformation acquires strategic importance for building the organizational resilience of enterprises. Digital technologies serve not only to automate individual business processes but also to provide information and analytical support for management, enhance the adaptability of organizational processes, facilitate remote collaboration and rapid resource reallocation, ensure business continuity, and strengthen enterprises' capacity to respond to multidimensional crisis-related disruptions.

The effectiveness of digital technologies in strengthening organizational resilience is determined by the extent to which they are integrated into the enterprise management system. Artificial intelligence and predictive analytics enhance risk forecasting and managerial decision support; cloud technologies ensure access to information resources and business continuity; ERP, CRM, and BPM systems support the adaptability and coordination of business processes; Big Data technologies facilitate the early detection of changes in the external environment; blockchain can enhance the transparency and reliability of interorganizational interactions; while advanced cybersecurity tools strengthen the resilience of digital infrastructure. The integrated use of these technologies creates the conditions for moving from fragmented digitalization toward an integrated digital management ecosystem. The article systematizes the functional roles of these technologies according to their impact on organizational resilience.

The study demonstrates that the specific operating conditions of Ukrainian enterprises during the full-scale war have significantly broadened the scope of organizational resilience. Infrastructure destruction, enterprise relocation, workforce shortages, logistics and energy-related risks, cyber threats, and high levels of uncertainty require a shift from predominantly reactive crisis management measures toward an adaptive management system based on digital collaboration, scenario-based management, real-time data analysis, and business continuity. Under these conditions, digital maturity becomes not merely an indicator of an enterprise's technological development but a prerequisite for its ability to maintain organizational manageability and continue operating amid prolonged systemic disruptions.

The scientific novelty of the findings lies in advancing the theoretical understanding of digital technologies as a system-forming factor of organizational resilience and in substantiating the Adaptive System of Digital Organizational Resilience, which integrates six interconnected components: digital leadership, digital culture, employees' digital competencies, intelligent information systems, cyber resilience, and continuous learning and innovation. Unlike approaches in which individual technological or organizational factors are considered in isolation, the proposed system is cyclical in nature: the interaction among its components facilitates the continuous accumulation of organizational experience, the development of digital capabilities, and the emergence of a new cycle of enterprise adaptation and transformation. This cyclical nature is identified in the article as a fundamental feature of the authors' concept.

The comparative analysis of international experience demonstrates the value for Ukraine of combining the European principles of Industry 5.0, human-centricity, resilience, digital responsibility, and technological autonomy with approaches focused on the active use of artificial intelligence, data-driven management, digital platforms, and cyber resilience. On this basis, the study identifies strategic directions for developing the digital organizational resilience of Ukrainian enterprises, including the integration of AI into corporate governance, the development of digital leadership and culture, the systematic enhancement of employees' digital competencies, the digitalization of HR processes, the strengthening of cyber resilience, the development of digital business ecosystems, and the integration of enterprises into European digital value chains. As these strategic directions have been substantiated in detail in the main body of the study, they are summarized here rather than reiterated in full.

The practical significance of the proposed approach lies in the potential application of the

Adaptive System of Digital Organizational Resilience as a conceptual framework for developing digital transformation strategies for Ukrainian enterprises, identifying priorities for strengthening their digital and managerial capabilities, and preparing them to operate under conditions of prolonged crisis-related disruptions and post-war recovery.

Future research should focus on developing methodological tools for the quantitative assessment of digital organizational resilience, establishing a system of indicators for evaluating the six components of the proposed model, and empirically validating the model across enterprises representing different types of economic activity and levels of digital maturity. Further research should also examine the impact of generative artificial intelligence, digital ecosystems, and platform-based business models on enterprise organizational resilience in the context of Ukraine's post-war recovery and its further integration into the European digital economic space.

References

- Hillmann, J., & Guenther, E. (2021). Organizational resilience: A valuable construct for management research? *International Journal of Management Reviews*, 23(1), 7–44. DOI: <https://doi.org/10.1111/ijmr.12239>
- Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889–901. DOI: <https://doi.org/10.1016/j.jbusres.2019.09.022>
- Wessel, L., Baiyere, A., Ologeanu-Taddei, R., Cha, J., & Blegind Jensen, T. (2021). Unpacking the difference between digital transformation and IT-enabled organizational transformation. *Journal of the Association for Information Systems*, 22(1), 102–129. DOI: <https://doi.org/10.17705/1jais.00655>
- Mikalef, P., & Gupta, M. (2021). Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. *Information & Management*, 58(3), Article 103434. DOI: <https://doi.org/10.1016/j.im.2021.103434>
- Zhang, J., Long, J., & von Schaeven, A. M. E. (2021). How does digital transformation improve organizational resilience? Findings from PLS-SEM and fsQCA. *Sustainability*, 13(20), Article 11487. DOI: <https://doi.org/10.3390/su132011487>
- Xie, X., Wu, Y., Palacios-Marqués, D., & Ribeiro-Navarrete, S. (2022). Business networks and organizational resilience capacity in the digital age during COVID-19. *Technological Forecasting and Social Change*, 177, Article 121548. DOI: <https://doi.org/10.1016/j.techfore.2022.121548>
- Robertson, J., Botha, E., Walker, B., Wordsworth, R., & Balzarova, M. (2022). Fortune favours the digitally mature: The impact of digital maturity on the organisational resilience of SME retailers during COVID-19. *International Journal of Retail & Distribution Management*, 50(8/9), 1182–1204. DOI: <https://doi.org/10.1108/IJRDM-10-2021-0514>
- Trieu, H. D. X., Nguyen, P. V., Nguyen, T. T. M., Vu, H. T. M., & Tran, K. T. (2023). Information technology capabilities and organizational ambidexterity facilitating organizational resilience and firm performance of SMEs. *Asia Pacific Management Review*, 28(4), 544–555. DOI: <https://doi.org/10.1016/j.apmr.2023.03.004>
- Browder, R. E., Dwyer, S. M., & Koch, H. (2024). Upgrading adaptation: How digital transformation promotes organizational resilience. *Strategic Entrepreneurship Journal*, 18(1), 128–164. DOI: <https://doi.org/10.1002/sej.1483>
- Awad, J. A. R., & Martín-Rojas, R. (2024). Digital transformation influence on organisational resilience through organisational learning and innovation. *Journal of Innovation and Entrepreneurship*, 13, Article 69. DOI: <https://doi.org/10.1186/s13731-024-00405-4>
- Wang, Z., & Jia, J. (2025). Digital transformation and organizational resilience. *Finance Research Letters*, 78, Article 107165. DOI: <https://doi.org/10.1016/j.frl.2025.107165>
- Koh, L. Y., Toh, S. E., & Yuen, K. F. (2026). The influence of digital drivers on organisational digital resilience: An organisational information processing theory perspective. *Technology in Society*, 86, Article 103283. DOI: <https://doi.org/10.1016/j.techsoc.2026.103283>
- Lohmer, J., Bugert, N., & Lasch, R. (2020). Analysis of resilience strategies and ripple effect in blockchain-coordinated supply chains: An agent-based simulation study. *International Journal of Production Economics*, 228, Article 107882. DOI: <https://doi.org/10.1016/j.ijpe.2020.107882>
- Breque, M., De Nul, L., & Petridis, A. (2021). *Industry 5.0: Towards a sustainable, human-centric and resilient European industry*. Publications Office of the European Union. DOI: <https://doi.org/10.2777/308407>
- European Commission. (2022). *Industry 5.0, a transformative vision for Europe: Governing systemic transformations towards a sustainable industry*. Publications Office of the European Union. Retrieved from: https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/industry-50-transformative-vision-europe_en
- European Parliament, & Council of the European Union. (2022). Decision (EU) 2022/2481 of 14 December 2022 establishing the Digital Decade Policy Programme 2030. *Official Journal of the European Union*, L 323, 4–26. Retrieved from: <https://eur-lex.europa.eu/eli/dec/2022/2481/oj/eng>
- European Commission. (n.d.). *European Digital Innovation Hubs (EDIHs)*. Shaping Europe's Digital Future. Retrieved from: <https://digital-strategy.ec.europa.eu/en/policies/edihhs>
- OECD. (2024). *Enhancing resilience by boosting digital business transformation in Ukraine*. OECD Publishing. DOI: <https://doi.org/10.1787/4b13b0bb-en>
- Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach* (NIST Special Publication 800-160, Vol. 2, Rev. 1). National Institute of Standards and

Technology. DOI: <https://doi.org/10.6028/NIST.SP.800-160v2r1>

20. 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>

Received: 04.04.2026

Accepted: 11.09.2026

Received after review: 07.08.2026

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.

Миколенко Олена

кандидат економічних наук, доцент
Факультет податкової справи, обліку та аудиту
Державний податковий університет
вул. Університетська, 31, Ірпінь, 08205, Україна
e-mail: mykolenkohelen@gmail.com
ORCID ID: [0000-0002-1988-7401](https://orcid.org/0000-0002-1988-7401)

Денчик Ірина

старший викладач
Навчально-науковий інститут «Каразінський банківський інститут»
Харківський національний університет імені В. Н. Каразіна
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: irina.denchik@karazin.ua
ORCID ID: [0000-0003-1594-1084](https://orcid.org/0000-0003-1594-1084)

Роль цифрових технологій у формуванні організаційної стійкості підприємств

Анотація. Об'єктом дослідження є процес формування організаційної стійкості підприємств під впливом цифрової трансформації в умовах воєнного стану, економічної нестабільності та посилення системних ризиків. Цифрові технології в таких умовах набувають стратегічного значення, забезпечуючи адаптивність організаційних процесів, безперервність діяльності, оперативність прийняття управлінських рішень та здатність підприємств реагувати на кризові впливи.

Постановка проблеми. Повномасштабна війна суттєво трансформувала умови функціонування українських підприємств, посиливши інфраструктурні, кадрові, логістичні, енергетичні та кібербезпекові ризики. За таких умов цифровізація виходить за межі автоматизації окремих бізнес-процесів і перетворюється на системоутворюючий чинник організаційної стійкості, що зумовлює необхідність переосмислення її ролі в системі управління підприємством. Такий підхід відповідає загальній постановці проблеми, закладеній у статті.

Нероз'язані аспекти. Незважаючи на значний науковий доробок щодо цифрової трансформації та організаційної стійкості, недостатньо розробленим залишається комплексний підхід до визначення механізму формування організаційної стійкості підприємств, у межах якого технологічні, управлінські, людські та безпекові компоненти цифрової трансформації розглядаються як єдина взаємопов'язана система. Потребує подальшого дослідження взаємодія цифрового лідерства, цифрової культури, цифрових компетентностей персоналу, інтелектуальних інформаційних систем, кіберстійкості та безперервного навчання й інновацій, особливо в умовах тривалих системних потрясінь.

Мета статті. Метою дослідження є визначення ролі цифрових технологій у формуванні організаційної стійкості підприємств в умовах воєнного стану та економічної нестабільності, а також обґрунтування стратегічних напрямів розвитку цифрових управлінських практик з урахуванням європейського та американського досвіду.

Основний матеріал. Методологічну основу дослідження становить комплексний підхід, що інтегрує концепції організаційної стійкості, цифрової трансформації та адаптивного управління підприємствами. Використано системний і порівняльний аналіз, структурно-логічний метод, методи аналізу, синтезу, систематизації та наукового узагальнення. У роботі визначено особливості трансформації моделей управління українськими підприємствами під впливом війни та систематизовано функціональну роль цифрових технологій у забезпеченні прогнозування ризиків, підтримки управлінських рішень, адаптивності бізнес-процесів, безперервності діяльності та кіберстійкості. Проведено порівняльний аналіз європейського й американського підходів до цифрового забезпечення організаційної стійкості та обґрунтовано можливості їх адаптації до українських умов. Запропоновано адаптивну систему цифрової організаційної стійкості підприємства, яка інтегрує шість взаємопов'язаних компонентів: цифрове лідерство, цифрову культуру, цифрові компетентності персоналу, інтелектуальні інформаційні системи, кіберстійкість, безперервне навчання та інновації. На відміну від фрагментарного підходу до окремих цифрових чинників, запропонована система ґрунтується на їх циклічній взаємодії та інтеграції з людським капіталом, організаційною культурою й адаптивними механізмами управління.

Висновки. У результаті дослідження встановлено, що цифрова трансформація в умовах воєнного стану та економічної нестабільності набуває стратегічного значення для формування організаційної стійкості підприємств. Організаційна стійкість цифровізованого підприємства визначається не тільки наявністю окремих технологічних рішень, скільки здатністю інтегрувати цифрові технології, управлінські практики, людський капітал, організаційну культуру та механізми кіберстійкості в цілісну адаптивну систему. Практичне значення отриманих результатів полягає в можливості використання запропонованої системи як

концептуальної основи для формування стратегій цифрової трансформації українських підприємств, підвищення їхньої здатності адаптуватися до кризових впливів, підтримувати безперервність діяльності та забезпечувати конкурентоспроможність у період воєнної економіки й післявоєнного відновлення. Подальші дослідження доцільно спрямувати на розроблення методичного інструментарію кількісного оцінювання цифрової організаційної стійкості та емпіричну апробацію запропонованої системи.

Ключові слова: організаційна стійкість, цифрова трансформація, цифрові технології, цифрова організаційна стійкість, адаптивне управління, цифрове лідерство, цифрова культура, цифрові компетентності, кіберстійкість, безперервність діяльності.

Формул: –; рис.: 2; табл.: 2; бібл.: 20.

Для цитування: Mykolenko Olena, Denchyk Iryna. The role of digital technologies in building the organizational resilience of enterprises. *Фінансово-кредитні системи: перспективи розвитку*. №3(22) 2026. С. 251-272. <https://doi.org/10.26565/2786-4995-2026-3-16>

Список літератури

1. Hillmann J., Guenther E. Organizational resilience: A valuable construct for management research? *International Journal of Management Reviews*. 2021. Vol. 23, No. 1. P. 7–44. DOI: <https://doi.org/10.1111/ijmr.12239>
2. Verhoef P. C., Broekhuizen T., Bart Y., Bhattacharya A., Dong J. Q., Fabian N., Haenlein M. Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*. 2021. Vol. 122. P. 889–901. DOI: <https://doi.org/10.1016/j.jbusres.2019.09.022>
3. Wessel L., Baiyere A., Ologeanu-Taddei R., Cha J., Blegind Jensen T. Unpacking the difference between digital transformation and IT-enabled organizational transformation. *Journal of the Association for Information Systems*. 2021. Vol. 22, No. 1. P. 102–129. DOI: <https://doi.org/10.17705/1jais.00655>
4. Mikalef P., Gupta M. Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. *Information & Management*. 2021. Vol. 58, No. 3. Article 103434. DOI: <https://doi.org/10.1016/j.im.2021.103434>
5. Zhang J., Long J., von Schaewen A. M. E. How does digital transformation improve organizational resilience? Findings from PLS-SEM and fsQCA. *Sustainability*. 2021. Vol. 13, No. 20. Article 11487. DOI: <https://doi.org/10.3390/su132011487>
6. Xie X., Wu Y., Palacios-Marqués D., Ribeiro-Navarrete S. Business networks and organizational resilience capacity in the digital age during COVID-19. *Technological Forecasting and Social Change*. 2022. Vol. 177. Article 121548. DOI: <https://doi.org/10.1016/j.techfore.2022.121548>
7. Robertson J., Botha E., Walker B., Wordsworth R., Balzarova M. Fortune favours the digitally mature: The impact of digital maturity on the organisational resilience of SME retailers during COVID-19. *International Journal of Retail & Distribution Management*. 2022. Vol. 50, No. 8/9. P. 1182–1204. DOI: <https://doi.org/10.1108/IJRDM-10-2021-0514>
8. Trieu H. D. X., Nguyen P. V., Nguyen T. T. M., Vu H. T. M., Tran K. T. Information technology capabilities and organizational ambidexterity facilitating organizational resilience and firm performance of SMEs. *Asia Pacific Management Review*. 2023. Vol. 28, No. 4. P. 544–555. DOI: <https://doi.org/10.1016/j.apmr.2023.03.004>
9. Browder R. E., Dwyer S. M., Koch H. Upgrading adaptation: How digital transformation promotes organizational resilience. *Strategic Entrepreneurship Journal*. 2024. Vol. 18, No. 1. P. 128–164. DOI: <https://doi.org/10.1002/sej.1483>
10. Awad J. A. R., Martín-Rojas R. Digital transformation influence on organisational resilience through organisational learning and innovation. *Journal of Innovation and Entrepreneurship*. 2024. Vol. 13. Article 69. DOI: <https://doi.org/10.1186/s13731-024-00405-4>
11. Wang Z., Jia J. Digital transformation and organizational resilience. *Finance Research Letters*. 2025. Vol. 78. Article 107165. DOI: <https://doi.org/10.1016/j.frl.2025.107165>
12. Koh L. Y., Toh S. E., Yuen K. F. The influence of digital drivers on organisational digital resilience: An organisational information processing theory perspective. *Technology in Society*. 2026. Vol. 86. Article 103283. DOI: <https://doi.org/10.1016/j.techsoc.2026.103283>
13. Lohmer J., Bugert N., Lasch R. Analysis of resilience strategies and ripple effect in blockchain-coordinated supply chains: An agent-based simulation study. *International Journal of Production Economics*. 2020. Vol. 228. Article 107882. DOI: <https://doi.org/10.1016/j.ijpe.2020.107882>
14. Breque M., De Nul L., Petridis A. Industry 5.0: Towards a Sustainable, Human-Centric and Resilient European Industry. Luxembourg: Publications Office of the European Union, 2021. DOI: <https://doi.org/10.2777/308407>
15. European Commission. Industry 5.0, a Transformative Vision for Europe: Governing Systemic Transformations towards a Sustainable Industry. Luxembourg: Publications Office of the European Union, 2022. URL: https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/industry-50-transformative-vision-europe_en
16. European Parliament, Council of the European Union. Decision (EU) 2022/2481 of 14 December 2022 establishing the Digital Decade Policy Programme 2030. *Official Journal of the European Union*. 2022. L 323. P. 4–26. URL: <https://eur-lex.europa.eu/eli/dec/2022/2481/oj/eng>
17. European Commission. European Digital Innovation Hubs (EDIHs). Shaping Europe's Digital Future. URL: <https://digital-strategy.ec.europa.eu/en/policies/edihs>

18. OECD. Enhancing Resilience by Boosting Digital Business Transformation in Ukraine. Paris: OECD Publishing, 2024. DOI: <https://doi.org/10.1787/4b13b0bb-en>
19. Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160, Vol. 2, Rev. 1. 2021. DOI: <https://doi.org/10.6028/NIST.SP.800-160v2r1>
20. 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>
Стаття надійшла до редакції 04.04.2026 *Статтю рекомендовано до друку 11.09.2026*
Стаття надійшла після рецензування 07.08.2026 *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.