UDC 005.591.6:004.9:658.1
JEL: C43; L25; M15; O32
DOI: https://doi.org/10.32983/2222-4459-2026-7-180-197

# THE METHODOLOGY FOR ASSESSING AND DEVELOPING THE DIGITAL RESILIENCE INDEX AS A NEW DRIVER OF COMPETITIVENESS FOR A HIGH-TECH ENTERPRISE

©2026 KUCHKO O. O.

*UDC 005.591.6:004.9:658.1*
*JEL: C43; L25; M15; O32*

**Kuchko O. O. The Methodology for Assessing and Developing the Digital Resilience Index as a New Driver of Competitiveness for a High-Tech Enterprise**

*The rapid diffusion of digital technologies, the integration of artificial intelligence into managerial processes, and the growing dependence of high-tech enterprises on digital infrastructure are fundamentally reshaping traditional approaches to sustaining competitiveness. Despite these developments, contemporary research has not yet established a unified methodological framework for comprehensively assessing enterprise digital resilience as an integrated characteristic reflecting an organization's ability to ensure the continuity of digital processes, adapt to internal and external threats, and sustain innovation-driven development. In particular, limited attention has been devoted to the formalization of digital resilience as a quantitative composite indicator suitable for strategic management applications in high-tech enterprises. The aim of this study is to develop an original methodological approach for assessing the digital resilience of high-tech enterprises based on the Digital Resilience Index (DRI) and to substantiate the role of digital resilience as a key determinant of enterprise competitiveness. The methodological framework combines systems analysis, structural-functional analysis, comparative and logical methods, index-based analysis, and methods of scientific synthesis and conceptual modeling. The study proposes an original definition of digital resilience for high-tech enterprises, develops a conceptual architecture of its formation, and introduces the Digital Resilience Index (DRI), which integrates indicators related to digital infrastructure, artificial intelligence adoption, cyber resilience, business continuity, R&D capability, and the adaptability of enterprise management systems. A methodological procedure for calculating the index and interpreting its values is also developed. The scientific novelty of the research lies in the development of an original methodology for assessing the digital resilience of high-tech enterprises and in the introduction of the Digital Resilience Index (DRI) as a new strategic management instrument for innovation-driven development. The practical significance of the proposed approach lies in its applicability to the comprehensive assessment of enterprise digital resilience, the identification of critical digital vulnerabilities, and the support of managerial decision-making aimed at strengthening enterprise competitiveness.*
***Keywords:*** *digital resilience; Digital Resilience Index (DRI); high-tech enterprise; competitiveness; digital transformation; R&D capability; artificial intelligence.*
***Tabl.:*** *6.* ***Formulae:*** *9.* ***Bibl.:*** *20.*

***Kuchko Oleksii O.*** *– Postgraduate Student of the Department of Management and Finance, Mariupol State University (6 Preobrazhenska Str., Kyiv, 03037, Ukraine)*
***E-mail:*** *oleksii.kuchko@mu.edu.ua*
***ORCID:*** *https://orcid.org/0009-0002-6624-1440*

*УДК 005.591.6:004.9:658.1*
*JEL: C43; L25; M15; O32*

***Кучко О. О. Методологія оцінювання та формування Digital Resilience Index як нового фактора конкурентоспроможності High-Tech підприємства***

*Стрімке поширення цифрових технологій, інтеграція штучного інтелекту в управлінські процеси та зростання залежності високотехнологічних підприємств від цифрової інфраструктури істотно змінюють традиційні підходи до забезпечення їх конкурентоспроможності. Водночас у сучасних наукових дослідженнях відсутній єдиний методичний підхід до комплексного оцінювання цифрової стійкості підприємства як інтегральної характеристики його здатності забезпечувати безперервність цифрових процесів, адаптуватися до внутрішніх і зовнішніх загроз та підтримувати інноваційний розвиток. Недостатньо розробленими залишаються питання формалізації цифрової стійкості у вигляді кількісного інтегрального показника, придатного для використання у стратегічному управлінні високотехнологічними підприємствами. Метою статті є розроблення авторського методичного підходу до оцінювання цифрової стійкості high-tech підприємства на основі інтегрального Digital Resilience Index та обґрунтування ролі цифрової стійкості як чинника забезпечення конкурентоспроможності. Методологічну основу дослідження становлять системний, структурно-функціональний, порівняльний, логічний та індексний методи, а також методи узагальнення наукових підходів і концептуального моделювання. У результаті дослідження запропоновано авторське визначення цифрової стійкості високотехнологічного підприємства, розроблено архітектуру її формування та інтегральний Digital Resilience Index, що охоплює показники розвитку цифрової інфраструктури, інтеграції технологій штучного інтелекту, кіберстійкості, безперервності бізнес-процесів, функціонування R&D-центру та адаптивності системи управління. Запропоновано методичний підхід до розрахунку індексу та інтерпретації його значень. Наукова новизна полягає в розробленні авторської методології оцінювання цифрової стійкості високотехнологічного підприємства та формуванні Digital Resilience Index як нового інструменту стратегічного управління інноваційним розвитком. Практична цінність полягає в можливості використання запропонованої методики для комплексного оцінювання цифрової стійкості підприємств, виявлення критичних цифрових вразливостей і обґрунтування управлінських рішень щодо підвищення їх конкурентоспроможності.*
***Ключові слова:*** *цифрова стійкість; Digital Resilience Index; високотехнологічне підприємство; конкурентоспроможність; цифрова трансформація; R&D-центр; штучний інтелект.*
***Табл.:*** *6.* ***Формул:*** *9.* ***Бібл.:*** *20.*

***Кучко Олексій Олександрович*** *– аспірант, кафедра менеджменту та фінансів, Маріупольський державний університет (вул. Преображенська, 6, Київ, 03037, Україна)*
***E-mail:*** *oleksii.kuchko@mu.edu.ua*
***ORCID:*** *https://orcid.org/0009-0002-6624-1440*

The ongoing digital transformation of the global economy is fundamentally reshaping the determinants of enterprise competitiveness, particularly for firms whose activities are centered on the development and commercialization of innovations. Whereas financial resources, production capacity, and technological capabilities were traditionally regarded as the primary sources of competitive advantage, increased attention is now being paid to an enterprise's ability to ensure the uninterrupted operation of digital systems, rapidly adapt to technological change, effectively manage digital risks, and sustain innovation activities under conditions of heightened uncertainty. This capability is gradually emerging as a new strategic resource for the long-term development of high-tech businesses.

The widespread adoption of artificial intelligence, big data analytics, digital twins, cloud computing, the Industrial Internet of Things (IIoT), and automated management systems has significantly increased enterprises' dependence on digital infrastructure. At the same time, the range of factors capable of disrupting its operation continues to expand. These threats extend far beyond cyberattacks and technical failures of information systems. They also include disruptions in global supply chains for digital components, cloud platform outages, the loss of critical data, risks associated with artificial intelligence algorithms, geopolitical conflicts, energy crises, and other external factors that directly affect the enterprise's digital environment.

For high-tech enterprises, these developments are of particular significance. Their competitiveness increasingly depends on the efficient operation of digital platforms, R&D centers, knowledge management systems, digital customer interaction channels, automated production facilities, and analytical decision-support systems. A disruption affecting any of these components may result in the loss of competitive advantages, reduced innovation performance, increased operational risks, and diminished investment attractiveness.

Recent global developments have demonstrated that digital resilience is becoming one of the key determinants of economic security. The COVID-19 pandemic, the rapid digitalization of industrial processes, the accelerated deployment of generative artificial intelligence, the sharp increase in cyberattacks, and the wartime challenges faced by Ukraine have exposed the limitations of conventional enterprise management models. Organizational systems focused primarily on financial or operational efficiency have proved insufficient to ensure sustainable performance under conditions of large-scale digital disruptions. These developments have highlighted the need for a new managerial paradigm in which digital resilience is viewed not merely as a component of information security but as an independent strategic factor underpinning the long-term development of enterprises.

Contemporary economic literature increasingly examines digital resilience in connection with digital transformation, organizational adaptability, cyber resilience, business continuity, and digital risk management. Nevertheless, existing approaches remain fragmented. Some scholars emphasize the technological infrastructure of enterprises, others associate digital resilience primarily with cybersecurity, while still others consider it an element of digital transformation. As a result, substantial knowledge has been accumulated regarding individual aspects of the problem; however, no universally accepted framework currently exists for comprehensively assessing digital resilience as an integrated characteristic of enterprise development.

From the perspective of strategic management, this creates significant methodological challenges. The absence of reliable quantitative measures of digital resilience complicates the assessment of digital transformation outcomes, the evaluation of investments in digital infrastructure, benchmarking across enterprises, and evidence-based strategic decision-making. Although digital resilience is widely recognized as an important determinant of enterprise development, it remains insufficiently conceptualized and operationalized within economic research.

This challenge is particularly relevant for Ukrainian high-tech enterprises, which simultaneously pursue digital modernization, implement innovation projects, integrate into international production networks, and operate under heightened wartime and cyber threats. Under these circumstances, there is a growing need for a comprehensive methodological framework capable of assessing the level of digital resilience, identifying the most vulnerable components of the enterprise's digital ecosystem, and supporting the development of strategic priorities for its further advancement.

Addressing this research gap determines the relevance of the present study and provides the rationale for developing an original methodology for assessing the digital resilience of high-tech enterprises based on an integrated Digital Resilience Index (DRI). The proposed index is conceptualized as a strategic management instrument designed to evaluate the effectiveness of digital transformation, support innovation-driven development, and strengthen the long-term competitiveness of high-tech enterprises.

## LITERATURE REVIEW

The contemporary conception of digital resilience has evolved progressively through the development of organizational resilience theory, risk management, digital transformation, information security, and strategic management. Despite the substantial body of

scholarly research in these fields, no unified approach to defining the economic essence of enterprise digital resilience has yet been established. Most existing studies address only individual functional dimensions of the problem, highlighting the need for a comprehensive analysis of the current theoretical approaches.

The theoretical foundations of organizational resilience were established in the works of K. Bhamra, S. Dani, and K. Burnard, who conceptualize resilience as an organization's ability to maintain efficient performance, adapt to changes in the external environment, and recover from disruptive events [9]. The authors argue that resilience is determined not only by tangible resources but also by organizational learning, knowledge accumulation, managerial flexibility, and the capacity for continuous adaptation. Although these contributions remain fundamental, they were developed prior to the current stage of digital transformation and therefore do not account for the role of digital infrastructure and artificial intelligence in strengthening enterprise resilience.

A significant contribution to the development of the organizational resilience conception was made by K. Burnard, who proposed viewing resilience as an integrated characteristic of the management system that enables an organization not only to respond to crises but also to use them as opportunities for further development [10]. This perspective considerably broadened the traditional understanding of resilience. However, the author's analysis primarily focuses on organizational adaptation mechanisms while giving limited consideration to the digital components of modern enterprises. Consequently, the applicability of this conception to high-tech companies, whose performance largely depends on the efficiency of digital processes, remains constrained.

The analytical reports of the Organisation for Economic Co-operation and Development (OECD) have also made an important contribution to the contemporary understanding of digital resilience. In *OECD Enhancing the Digital Resilience of Businesses* and *OECD Digital Economy Outlook 2024*, digital resilience is recognized as one of the fundamental prerequisites for the functioning of the digital economy. Unlike earlier conceptions of organizational resilience, these reports emphasize not only post-crisis recovery but also the enterprise's capacity to sustain digital operations, manage data effectively, ensure cybersecurity, strengthen employees' digital competencies, and rapidly integrate emerging technologies into business activities [17; 18]. Nevertheless, the OECD recommendations are primarily macroeconomic in nature and are intended to support public policy in the field of digital development. They do not provide a methodological framework for the integrated assessment of digital resilience at the enterprise level, which limits their practical application in strategic management.

Another important area of contemporary research concerns the development of international standards for digital risk management and business continuity. ISO 22301:2019 establishes the requirements for business continuity management systems, focusing on organizational preparedness for disruptive events, the continuity of critical business processes, and the restoration of operations following disruptions [13]. The principal strength of this standard consists in its systematic approach to organizational resilience management. However, it does not adequately reflect the specific challenges associated with the digital transformation of high-tech enterprises and does not offer a methodology for the quantitative assessment of digital resilience.

Another internationally recognized standard, ISO/IEC 27001:2022, defines the requirements for information security management systems [14]. Its provisions are aimed at ensuring the confidentiality, integrity, and availability of information, managing information security risks, and continuously improving protective mechanisms. Despite its fundamental importance for modern enterprises, the standard addresses only one dimension of digital resilience. Information security represents a necessary, but not sufficient, condition for ensuring the sustainable development of an enterprise's digital ecosystem.

A substantial contribution to the advancement of digital risk management methodology has also been made by the U. S. National Institute of Standards and Technology (NIST). The updated *NIST Cybersecurity Framework 2.0* significantly expands the traditional cybersecurity approach by introducing an integrated system of interconnected risk management functions encompassing governance, risk identification, protection of digital assets, threat detection, incident response, and recovery [15]. However, the framework is primarily intended to evaluate cybersecurity performance and does not provide a mechanism for assessing digital resilience as an integrated characteristic of an enterprise's innovation-driven development.

The continued advancement of digital technologies has also led to the development of dedicated guidelines for the deployment of artificial intelligence systems. The *NIST AI Risk Management Framework 1.0* introduced a structured approach to managing AI-related risks by establishing principles for the reliability, safety, transparency, and governance of artificial intelligence systems [16]. This represents a significant step towards the responsible development of the digital economy. Nevertheless, the framework considers artificial intelli-

gence primarily from the perspective of AI-specific risk management and does not conceptualize it as an integral component of enterprise digital resilience.

A comprehensive assessment of global digital threats is regularly provided by the World Economic Forum. In its annual report, *Global Cybersecurity Outlook 2025*, the Forum identifies digital resilience as one of the principal determinants of enterprise competitiveness across industries [20]. The report emphasizes the interdependence of digital infrastructure, cybersecurity, human capital development, artificial intelligence adoption, and digital risk management. Of particular importance is the conclusion that competitive advantage is increasingly determined not by the degree of digitalization itself, but by an enterprise's ability to maintain the stable functioning of its digital ecosystem in an environment characterized by continuous external change. However, these findings remain largely analytical and have not yet been translated into a practical methodology for the strategic assessment of enterprise performance.

The issue of digital resilience has also attracted increasing attention within Ukrainian economic research. D. Bondarenko researches digital transformation as the foundation for modernizing enterprise management systems, emphasizing the integration of digital technologies into business processes and managerial practices [1; 2]. The author convincingly demonstrates that digitalization creates new opportunities for improving productivity. At the same time, the research primarily focuses on digital transformation processes, while the assessment of digital resilience remains beyond its scope.

V. Derhachova and Ya. Koleshnia examine digital transformation as a factor contributing to enterprise competitiveness, with particular attention to the evolution of business models, the development of digital services, and the digitalization of management processes [3]. The authors rightly argue that digital technologies are becoming an increasingly important source of competitive advantage. Nevertheless, their study does not propose methodological approaches for assessing or quantitatively measuring the level of digital resilience.

A similar perspective is reflected in the works of N. Tanklevska and V. Miroshnychenko, who explore digital transformation as a component of the strategic development of enterprises operating within the digital economy [7]. Their research substantiates the necessity of modernizing management systems through digital technologies and adapting enterprises to new economic conditions. However, digital resilience is addressed only indirectly through the efficiency of digital transformation, without the development of a dedicated methodological framework for its assessment.

M. Kostromskyi analyzes the digitalization of business processes as a factor enhancing enterprise performance [4]. Particular attention is given to digital platforms, management automation, and digital innovation. However, the study does not examine the interrelationships among digital infrastructure maturity, cyber resilience, R&D capabilities, and enterprise competitiveness, although these relationships are critically important for high-tech industries.

In the studies conducted by S. Onyshchenko, O. Ptashchenko and their co-authors, digital transformation is examined through the lens of enterprise innovation, digital business models, and advanced technological platforms [5; 6]. The researchers emphasize that digital technologies have become one of the principal drivers of enterprise development. Nevertheless, the proposed approaches rely predominantly on qualitative assessment criteria, which limits their applicability to strategic analysis and benchmarking across enterprises.

The literature review demonstrates that contemporary research has established a substantial theoretical foundation for researching digital transformation, organizational resilience, cybersecurity, and digital risk management. However, these research streams remain largely disconnected. While some studies focus on digital transformation and others address cyber resilience, business continuity, or information security, digital resilience as a comprehensive economic category has received comparatively limited scholarly attention. There is still no generally accepted framework defining its structure, no integrated system of interconnected assessment indicators, and no composite index capable of quantitatively measuring enterprise digital resilience and supporting strategic decision-making in innovation-driven development.

This research gap provides the rationale for developing the proposed methodology for assessing the digital resilience of high-tech enterprises based on the *Digital Resilience Index (DRI)*. The proposed index integrates the key components of an enterprise's digital ecosystem into a single composite indicator, thereby providing a methodological foundation for evidence-based strategic management and innovation-oriented decision-making.

## RESEARCH AIM

The ***aim*** of the present study is to develop an original methodology for assessing the digital resilience of high-tech enterprises based on the integrated Digital Resilience Index (DRI) and to substantiate its applicability as a strategic management tool for innovation-driven development and enhanced competitiveness in the context of the digital transformation of the economy.

To achieve this aim, the following research questions were formulated:

**RQ1.** Can digital resilience be regarded as an independent strategic determinant of the competitiveness of high-tech enterprises?

**RQ2.** Which components constitute enterprise digital resilience, and how do they interact within the enterprise's digital ecosystem?

**RQ3.** Is it possible to assess digital resilience comprehensively through a single integrated quantitative indicator?

**RQ4.** Which assessment criteria are most appropriate for determining the level of digital resilience and supporting strategic managerial decision-making?

In accordance with the research aim, the following hypothesis was formulated: digital resilience represents an integrated characteristic of a high-tech enterprise that emerges from the interaction of digital infrastructure, data management systems, artificial intelligence technologies, cyber resilience, innovation activities, and organizational adaptability. Furthermore, its level can be quantitatively assessed through the construction of an integrated index capable of reflecting an enterprise's preparedness to operate under conditions of continuous digital change.

## RESEARCH METHODOLOGY

Achieving the research aim required the application of a complementary set of general scientific and specialized research methods that collectively enable a comprehensive analysis of digital resilience as an economic category and support the development of the proposed assessment methodology.

The theoretical foundation of the study is based on contemporary conceptions of digital transformation, organizational resilience, strategic management, innovation management, the digital economy, cyber resilience, and business continuity. The integration of these theoretical perspectives makes it possible to conceptualize digital resilience not as an isolated element of information security but as an integrated characteristic of a high-tech enterprise that determines its capacity for sustainable development within a digital environment.

A system approach was employed to examine digital resilience as the outcome of interactions among organizational, technological, informational, and managerial components of the enterprise. This approach provided the basis for developing an integrated model of digital resilience and identifying the relationships among its structural elements.

Structural and functional analysis was applied to examine the internal architecture of the digital ecosystem of a high-tech enterprise, determine the functional roles of its individual components, and assess their contribution to the overall level of digital resilience.

The method of scientific abstraction was used to clarify the economic essence of the concept of *digital resilience*, formulate the author's definition of enterprise digital resilience, and identify its principal characteristics.

Comparative analysis enabled a systematic comparison of contemporary international approaches, recommendations issued by international organizations, international standards, and the findings of Ukrainian scholars concerning enterprise digital resilience. This made it possible to identify their common features, conceptual differences, and methodological limitations.

The decomposition method was employed to divide digital resilience into interconnected components, each representing a specific dimension of the enterprise's digital ecosystem. This served as the basis for constructing the system of indicators used in the integrated assessment.

Conceptual modeling was applied to develop the proposed architecture of digital resilience for high-tech enterprises. The modeling process defined the structural components of digital resilience, established the logic of their interactions, and determined the role of each component within the system of strategic innovation management.

The proposed assessment methodology is based on the index method, which enables the aggregation of heterogeneous indicators into a single composite measure. The use of an integrated index makes it possible to avoid evaluating individual characteristics of digital activity in isolation and instead determine the overall level of enterprise digital resilience.

To establish the structure of the integrated indicator, an expert-analytical grouping method was employed, whereby individual indicators were combined into functionally homogeneous categories according to their substantive characteristics. This approach ensures the flexibility of the proposed index and allows its structure to be refined or expanded in accordance with the specific features of individual enterprises.

Indicator normalization was applied to transform variables measured in different units into a common evaluation scale, thereby enabling their subsequent aggregation into the integrated Digital Resilience Index.

The overall level of digital resilience was determined using the integrated assessment method, which combines normalized indicators through weighted aggregation. This approach is widely employed in contemporary research involving the construction of composite socioeconomic indices and provides an appropriate level of analytical reliability.

The empirical and informational basis of the research includes scholarly publications by Ukrainian and

international researchers, analytical reports published by the Organisation for Economic Co-operation and Development (OECD), the World Economic Forum (WEF), and the U.S. National Institute of Standards and Technology (NIST), international ISO standards, as well as recent studies addressing digital transformation, organizational resilience, cybersecurity, and the strategic management of high-tech enterprises.

The proposed methodology is conceptual in nature and is intended to serve as a framework for the strategic assessment of digital resilience in high-tech enterprises. Its practical implementation involves the development of a system of indicators, the determination of weighting coefficients, the construction of the calculation algorithm for the integrated Digital Resilience Index (DRI), and the establishment of an interpretation scale, which constitute the main focus of the subsequent sections of this study.

## RESULTS

The rapid digitalization of production processes, the widespread adoption of artificial intelligence technologies, the development of digital platforms, computer-aided design systems, digital twins, cloud computing, and intelligent analytics have fundamentally reshaped the understanding of the factors that determine the competitiveness of modern high-tech enterprises. While traditional economic theory regarded tangible resources, production capacity, financial capital, and technological innovation as the principal sources of competitive advantage, the digital economy increasingly shifts this focus towards digital assets, information resources, and an organization's ability to operate effectively under conditions of continuous technological change.

This transformation can be explained by the fact that virtually all key business processes of high-tech enterprises are now integrated into a unified digital ecosystem. Product design, research and development, production planning, logistics management, customer interaction, financial planning, marketing, after-sales services, and strategic management increasingly rely on digital platforms and large-scale data resources. Under these conditions, enterprise performance depends not only on the quality of individual digital technologies but also on the ability of the entire digital ecosystem to operate continuously despite the influence of internal or external disruptive factors.

Consequently, the conception of digital resilience extends far beyond the traditional understanding of information security. While information security primarily focuses on protecting information assets and cyber resilience concentrates on resisting cyber threats, digital resilience encompasses a much broader range of organizational processes. It reflects an enterprise's ability to ensure the continuous creation of economic value regardless of changes occurring within its digital environment.

In our view, this characteristic fundamentally distinguishes digital resilience from related conceptions. Rather than describing a specific functional area, digital resilience reflects the degree of coordination and coherence across the entire digital system. From this perspective, an enterprise is viewed as a complex multi-level socioeconomic system in which every digital component performs its own functions while simultaneously influencing the efficiency of the others. The failure or insufficient development of even a single critical component may trigger cascading disruptions throughout the entire digital ecosystem.

This interdependence is particularly evident in high-tech enterprises, where business performance largely depends on research and development activities. The efficiency of R&D units is determined not only by the qualifications of researchers or the availability of financial resources but also by rapid access to information, the quality of digital databases, the use of machine learning models, computer-aided design systems, digital simulation technologies, and collaborative digital platforms. Disruptions affecting any of these elements can significantly reduce innovation performance regardless of the enterprise's scientific and technological capabilities.

Digital resilience also plays a critical role in the speed and quality of managerial decision-making. Contemporary high-tech enterprises operate in an environment characterized by continuous technological change, evolving market requirements, and shifting customer behavior. Managerial decisions increasingly rely on big data analytics, predictive models, artificial intelligence algorithms, and digital decision-support systems. Loss of access to these resources, or a significant deterioration in their performance, inevitably reduces an enterprise's ability to respond promptly to external changes, thereby weakening its competitive position.

In the contemporary literature, digital resilience is frequently equated with digital maturity. In our opinion, such an interpretation is methodologically inaccurate. Digital maturity reflects the extent to which digital technologies have been adopted and integrated into enterprise operations. Digital resilience, in contrast, characterizes the ability of these technologies to sustain the continuous creation of economic value even under conditions of digital disruptions, organizational failures, or external crises. An enterprise may demonstrate a high level of digital maturity through the extensive implementation of advanced informa-

tion systems while remaining vulnerable to cyberattacks, data loss, infrastructure failures, or errors in artificial intelligence algorithms. Conversely, an enterprise with a lower degree of digitalization may exhibit a substantially higher level of digital resilience owing to a well-balanced digital architecture, efficient risk management practices, and a high degree of organizational adaptability.

The relationship between digital resilience and digital transformation is equally open to debate. A considerable proportion of contemporary studies implicitly treat digital transformation as the ultimate objective of enterprise development. We argue, however, that digital transformation represents the process through which an enterprise moves towards a new technological state, whereas digital resilience reflects the quality and sustainability of the outcomes achieved through that process. In other words, digital transformation answers the question of how actively an enterprise adopts digital technologies, while digital resilience evaluates how effectively and securely the resulting digital system performs after implementation.

For this reason, digital resilience should be regarded not merely as a property of digital infrastructure but as a strategic productive asset of the enterprise. Unlike traditional assets, its economic value is not embodied in physical form but in its capacity to ensure the stable operation of digital processes, sustain innovation performance, reduce losses arising from digital risks, accelerate managerial decision-making, and create the conditions necessary for long-term competitive advantage. Accordingly, digital resilience should be recognized as an independent object of strategic management requiring systematic assessment, continuous monitoring, and purposeful development.

Within this context, an important methodological question arises. If digital resilience represents a strategic enterprise asset, it must be expressed not only qualitatively but also quantitatively. Without an appropriate measurement framework, it is impossible to compare enterprises, evaluate the effectiveness of digital investments, assess the outcomes of digital transformation, or forecast changes in competitiveness. This consideration served as the conceptual foundation for developing the proposed architecture of digital resilience and the integrated *Digital Resilience Index (DRI)*.

The literature review indicates that existing interpretations of digital resilience have largely evolved within separate research domains. OECD publications emphasize the resilience of the digital economy and the development of digital competencies [17; 18]. ISO standards focus primarily on business continuity and information security management [13; 14]. NIST frameworks address cybersecurity and artificial intelligence risk management [15; 16]. At the same time, the studies conducted by Ukrainian scholars mainly investigate enterprise digital transformation, the digitalization of business processes, and the development of digital business models [1–7]. Despite these different perspectives, all of these approaches share a common limitation: digital resilience is examined through individual functional dimensions rather than as an integrated economic characteristic of the enterprise.

Such fragmentation considerably limits the practical applicability of existing approaches within strategic management. Enterprise managers may obtain information about the development of individual digital components, yet they lack an integrated perspective on their combined contribution to competitiveness and innovation performance. Assessing the level of cybersecurity does not reflect the efficiency of digital infrastructure; a high degree of digital maturity does not necessarily indicate an enterprise's ability to operate under conditions of large-scale digital disruptions; and the intensity of digital transformation alone does not demonstrate the organization's capacity to sustain stable digital operations over the long term.

Within the resource-based view of strategic management, sustainable competitive advantage is traditionally associated with the development of strategic resources capable of generating lasting economic value. According to this perspective, a strategic resource should be valuable, difficult for competitors to imitate, capable of supporting long-term competitive advantages, and effectively integrated into the enterprise's value creation system. In the digital economy, these characteristics increasingly describe not individual digital technologies but the enterprise's ability to ensure the efficient functioning of its entire digital ecosystem. From this perspective, digital resilience should be regarded as a strategic organizational capability that determines an enterprise's readiness for continuous development under conditions of technological uncertainty.

This interpretation differs fundamentally from the conventional understanding of digital resilience as merely a component of information security or cybersecurity. Although protecting digital infrastructure is unquestionably essential for modern enterprises, it represents only one dimension of digital resilience. Even a highly secure digital environment cannot ensure the efficient utilization of digital technologies in the absence of advanced data management systems, adequate digital competencies among employees, the integration of artificial intelligence into managerial processes, efficient R&D activities, or an adaptive organizational structure. Consequently, digital resilience

emerges through the interaction of a much broader range of organizational, technological, informational, and managerial factors than those traditionally examined within the field of information security.

It is equally important to distinguish digital resilience from digital maturity. In most contemporary studies, digital maturity is used to evaluate the extent of digital technology adoption, the level of business process automation, and the progress of digital transformation within an organization [1–3; 7]. However, extensive implementation of digital technologies does not necessarily imply that an enterprise is capable of maintaining their efficient operation during disruptive events or adapting rapidly to technological change. A high level of digital maturity may coexist with excessive dependence on specific information systems, insufficient cyber resilience, or limited organizational adaptability. Under such circumstances, digital transformation creates additional opportunities for enterprise development while simultaneously increasing exposure to digital risks.

In our view, digital resilience should be defined as an integrated economic characteristic of a high-tech enterprise that reflects its ability to ensure the continuous functioning of its digital ecosystem, sustain innovation-driven development, adapt promptly to technological change, and minimize the adverse effects of digital risks on business performance. This definition combines technological, organizational, informational, and economic dimensions of enterprise development and, unlike existing approaches, conceptualizes digital resilience as an independent object of strategic management.

This interpretation necessitates a transition from the qualitative description of digital resilience to its quantitative assessment. If digital resilience directly influences enterprise competitiveness, it should be evaluated through a comprehensive indicator that integrates the key characteristics of the digital ecosystem and enables both longitudinal and cross-enterprise comparisons. This reasoning served as the conceptual foundation for developing the proposed architecture of digital resilience and the integrated *Digital Resilience Index (DRI)*.

Defining digital resilience as an integrated economic characteristic naturally raises the question of its internal structure. Any integrated conception must consist of clearly identified components connected through stable functional relationships. Only under these conditions can it be formalized, quantitatively assessed, and incorporated into strategic management practices. Accordingly, the next stage of the study involved the development of the proposed architecture of digital resilience for high-tech enterprises.

Current research provides only limited guidance regarding the structural composition of digital resilience. International ISO standards and NIST frameworks describe individual functional areas of digital governance, while the OECD primarily focuses on the development of the digital economy and digital competencies. At the same time, most Ukrainian studies examine digital transformation processes within enterprises [1–7; 13–18]. However, no conceptual model has yet been proposed that integrates all key components of enterprise digital activity into a unified analytical framework. In our opinion, such a model should serve as the foundation for the subsequent quantitative assessment of digital resilience.

The proposed architecture was developed on the basis of three fundamental principles:

- Digital resilience is determined not by individual technologies but by the efficiency of their interaction within the enterprise's digital ecosystem.
- Each structural component must directly contribute to the enterprise's ability to ensure the continuity of digital processes and sustain innovation-driven development.
- Every component should be quantitatively measurable, thereby enabling the subsequent construction of the integrated *Digital Resilience Index (DRI)*.

Based on these principles, digital resilience is conceptualized as a multi-level system composed of interconnected functional blocks. Each block represents a distinct dimension of the enterprise's digital ecosystem; however, only their combined interaction determines the overall level of digital resilience.

Digital infrastructure occupies a central position within the proposed architecture. It provides the technological environment that supports the operation of all enterprise information systems. This component encompasses corporate networks, data centers, cloud services, production information systems, digital platforms, the Industrial Internet of Things (IIoT), digital twins, and other technological solutions that ensure the functioning of business processes. An insufficient level of digital infrastructure development inevitably constrains the efficient utilization of all other digital technologies, regardless of their technological sophistication.

The second structural component is the data management system. Within the digital economy, data have become one of the most valuable strategic resources, while the quality of managerial decision-making increasingly depends on the completeness, reliability, timeliness, and accessibility of information. Consequently, enterprise digital resilience is directly influenced by the efficiency of data collection, storage, organization, integration, protection, and utilization

processes. This extends beyond the technical management of information resources to include the establishment of a unified data governance framework that supports production, research, and managerial activities.

The next component comprises artificial intelligence and predictive analytics. In the high-tech sector, machine learning algorithms, generative artificial intelligence, and advanced analytics are becoming integral elements of production management, demand forecasting, logistics optimization, R&D support, and strategic planning. However, the mere adoption of artificial intelligence does not automatically indicate a high level of digital resilience. What is essential is its efficient integration into managerial decision-making processes, the reliability of AI algorithms, the quality of training data, continuous monitoring of model performance, and the capability to adapt AI systems rapidly to changing conditions. For this reason, the level of AI integration is proposed as a separate structural component of digital resilience.

A distinctive feature of the proposed architecture is the inclusion of the enterprise's R&D capability as an independent component. Most existing models of digital transformation pay limited attention to the contribution of research and development to digital resilience. In our view, such an approach is insufficient, particularly for high-tech enterprises. R&D centers contribute not only to the creation of new products and technologies but also to the continuous renewal of the enterprise's digital ecosystem, adaptation to technological change, and implementation of innovative digital solutions. The more rapidly an enterprise can integrate emerging technologies into its business processes, the greater its capacity to sustain digital resilience over the long term.

Another functional component is cyber resilience and digital risk management. Unlike the conventional approach, which considers cybersecurity as an independent area of activity, the proposed model incorporates cyber resilience into the overall architecture of digital resilience. This integration reflects the fact that digital risks influence virtually every component of the enterprise's digital ecosystem. Loss of access to digital services, data breaches, failures of information systems, or external cyber incidents directly affect production processes, R&D activities, logistics, financial management, and customer interactions. Therefore, any assessment of digital resilience that excludes cyber resilience cannot provide an objective representation of the enterprise's actual level of preparedness.

An equally important component is digital human capital. Experience gained from digital transformation initiatives demonstrates that the efficiency of even the most advanced technologies largely depends on employees' ability to use them effectively. Digital competencies, readiness to adopt new digital tools, proficiency in working with artificial intelligence systems, data literacy, and the ability to operate within a digital environment directly influence the performance of the entire digital ecosystem. Consequently, human capital should not be regarded as an external factor affecting digital resilience but rather as one of its fundamental structural components.

The proposed architecture captures the interdependence of all key dimensions of digital activity within a high-tech enterprise and provides a conceptual foundation for their subsequent formalization. It establishes the basis for developing a system of quantitative indicators, determining the relative importance of individual components, and constructing the integrated *Digital Resilience Index (DRI)*, which enables a comprehensive assessment of enterprise digital resilience. The next stage of the study focuses on identifying the factors that influence the development of digital resilience and justifying their inclusion in the proposed integrated assessment model.

The development of any integrated assessment model requires the prior identification of the factors that directly influence the phenomenon under examination. In this context, it is essential to distinguish between the structural components of digital resilience and the factors that shape its development. Whereas the architecture reflects the internal structure of digital resilience, the influencing factors represent the economic, organizational, technological, and institutional processes that determine the level of development of each structural component. Accordingly, the development of the proposed system of influencing factors constitutes a necessary prerequisite for constructing the methodology for the quantitative assessment of digital resilience.

The literature indicates that most existing studies concentrate on individual groups of determinants. Research on digital transformation primarily examines the level of business process digitalization, the degree of production automation, or the adoption of advanced information technologies [1–7]. Studies in the field of cybersecurity focus mainly on digital risk management, the protection of information infrastructure, and the continuity of digital services [13–16]. Research addressing enterprise innovation emphasizes the roles of R&D, human capital, and the development of organizational capabilities [8–12]. Despite this substantial body of work, the contemporary literature has yet to establish a comprehensive classification of the factors that determine digital resilience.

In our view, this gap can be explained by the fact that digital resilience results from the simultaneous

interaction of numerous heterogeneous processes that differ in their origins, rates of change, and degree of managerial controllability. Consequently, traditional classifications based solely on technological or organizational criteria fail to provide a comprehensive understanding of the mechanisms underlying the formation of digital resilience.

Within the framework of this study, the factors influencing digital resilience are classified according to their economic nature and the character of managerial influence. This approach not only systematizes the relevant determinants but also identifies the opportunities available to enterprises for managing them within the process of strategic development.

The first group comprises technological factors that determine the technological foundation of the enterprise's digital ecosystem. These include the level of digital infrastructure development, the adoption of cloud technologies, the integration of production information systems, the implementation of digital twins, the Industrial Internet of Things (IIoT), production automation systems, and artificial intelligence technologies. Collectively, these factors define the enterprise's technological capability and determine its potential for digital modernization. However, the findings of the present analysis indicate that even a highly developed technological infrastructure cannot, by itself, ensure an adequate level of digital resilience in the absence of other essential conditions.

The second group consists of information-related factors that characterize the quality of corporate data management. Within the digital economy, data have effectively become one of the principal productive resources, making their efficient management increasingly critical for managerial decision-making, forecasting accuracy, R&D performance, and the efficiency of digital services. This category includes the completeness, timeliness, reliability, integration, standardization, and accessibility of information resources, together with the existence of data management systems and the use of advanced analytical platforms.

A separate category comprises innovation-related factors that determine the long-term adaptability of the enterprise's digital ecosystem. Unlike technological factors, which describe its current state, innovation factors reflect its future development potential. They include the intensity of R&D investment, the speed of technology adoption, the digital activity of research units, the efficiency of technology transfer, the use of open innovation practices, and participation in international innovation ecosystems. These factors largely determine an enterprise's capacity to sustain digital resilience over the medium and long term.

The next category includes organizational and managerial factors. Their importance is often underestimated, although management quality ultimately determines how effectively all other enterprise resources are utilized. This group comprises the level of digital integration of business processes, organizational adaptability, digital leadership, corporate governance maturity, managerial responsiveness, cross-functional collaboration, and the development of a strategic digital management system. Even when enterprises possess comparable technological capabilities, organizational mechanisms frequently determine the speed and efficiency with which they respond to changes in the external environment.

A distinct group is formed by human capital factors associated with the development of digital competencies. Under contemporary conditions, the competitiveness of high-tech enterprises increasingly depends on employees' ability to interact effectively with digital technologies, utilize advanced data analytics, work with artificial intelligence systems, and rapidly master new digital solutions. Accordingly, this category includes employees' digital competencies, the intensity of professional training, the proportion of personnel engaged in digital projects, readiness for organizational change, the level of digital culture, and competencies related to data management.

Risk-related factors constitute another essential category, reflecting the enterprise's ability to withstand the adverse effects of digital threats. These encompass not only cyber incidents but also data loss, failures of critical digital infrastructure, dependence on specific software providers, technological incompatibility among information systems, disruptions affecting digital platforms, and insufficient reliability of artificial intelligence algorithms. Unlike most existing approaches, the proposed framework does not treat risk factors as an independent management domain. Instead, they are integrated into the overall digital resilience assessment because they directly influence virtually every component of the enterprise's digital ecosystem.

The proposed classification differs fundamentally from existing approaches. Rather than describing isolated characteristics of enterprise digital activity, it establishes a multi-level system of interconnected factors, each of which can be represented by a set of quantitative indicators. This feature provides the basis for the mathematical formalization of the model and the subsequent development of the integrated *Digital Resilience Index (DRI)*.

At the same time, the contribution of individual factors to digital resilience is not uniform. The experience of high-tech enterprises demonstrates that certain components of the digital ecosystem perform

system-forming functions, whereas others play supporting or compensatory roles. Consequently, the factors incorporated into the integrated index cannot be assigned equal weights. Their relative importance should be determined according to their economic significance, their influence on the continuity of digital processes, their interdependence with other components of the digital ecosystem, and their contribution to the creation of long-term competitive advantages.

The proposed digital resilience architecture provides the conceptual foundation for subsequent quantitative assessment. Its practical application requires the development of a system of indicators reflecting the condition of each structural component of the enterprise's digital ecosystem. Importantly, these indicators should capture the economic outcomes generated by digital technologies rather than the technologies themselves, thereby ensuring the universality of the model regardless of enterprise characteristics or the maturity of specific technological solutions.

The review of existing methodologies demonstrates that most of them evaluate individual dimensions of digital development, including digital maturity, automation, business process digitalization, or cybersecurity [1–7; 13–18]. To date, however, the scientific literature has not proposed a comprehensive system of indicators specifically designed to assess the digital resilience of high-tech enterprises.

In the proposed methodology, the selection of indicators was based on four criteria: economic relevance, quantitative measurability, data availability, and the absence of redundancy. These criteria minimize subjectivity while ensuring the comparability of assessment results across enterprises.

According to the proposed architecture, digital resilience is assessed through six functional dimensions:

- digital infrastructure;
- data management system;
- artificial intelligence and predictive analytics;
- R&D capability;
- digital human capital;
- cyber resilience and digital risk management.

Each dimension is represented by a system of individual indicators that are normalized and aggregated into a composite group score. These group scores subsequently serve as the basis for calculating the integrated *Digital Resilience Index (DRI)*, which reflects the overall level of digital resilience of a high-tech enterprise.

The construction of the integrated digital resilience indicator requires a transition from a qualitative description of the enterprise's digital ecosystem to its quantitative assessment. Accordingly, each of the six functional dimensions of the proposed architecture is represented by a set of individual indicators reflecting the most significant aspects of enterprise digital development.

The selection of indicators was guided by the OECD recommendations on measuring digital transformation, the NIST approaches to digital risk assessment, the ISO principles of business continuity management, and contemporary methodologies for evaluating the innovation performance of high-tech enterprises [8–18]. At the same time, the proposed indicator system does not replicate any existing methodology. Instead, it has been developed in accordance with the original conceptualization of digital resilience proposed in this study.

Only those indicators that satisfy three criteria were included in the integrated model: they capture economically significant dimensions of digital resilience, can be measured using available information, and do not duplicate the content of other indicators. This approach ensures that the model remains both analytically informative and methodologically parsimonious.

The proposed system of indicators is presented in *Tbl. 1*.

The proposed framework comprises thirty individual indicators that collectively capture the technological, informational, innovative, human capital, and security dimensions of enterprise digital resilience. However, the direct use of their absolute values is methodologically inappropriate because the indicators differ in measurement units, value ranges, and scales. Consequently, they cannot be aggregated directly into a single integrated measure.

The proposed indicator system is inherently heterogeneous, as the individual indicators differ not only in measurement units and ranges but also in the direction of their influence on enterprise digital resilience. Under these conditions, direct aggregation would be methodologically inappropriate. To ensure comparability, all individual indicators are normalized by transforming them onto a common dimensionless scale ranging from 0 to 1.

For *benefit indicators*, where higher values contribute positively to digital resilience, the following normalization formula is applied:

$$z_i = \frac{x_i - x_{\min}}{x_{\max} - x_{\min}},$$

where: $z_i$ – normalized value of the $i$-th indicator;

$x_i$ – observed value of the indicator;

$x_{\min}$ – minimum value of the indicator within the observed sample;

$x_{\max}$ – maximum value of the indicator within the observed sample.

**Table 1**

**System of Indicators for Calculating the Digital Resilience Index (DRI)**

| Functional Dimension | Core Indicators |
|---|---|
| Digital infrastructure | Level of production process digitalization; share of cloud services; digital infrastructure availability ratio; level of information systems integration; degree of production automation |
| Data management | Completeness of corporate data; data quality; information update speed; level of database integration; use of Business Intelligence |
| Artificial intelligence and predictive analytics | Share of business processes utilizing AI; number of AI models deployed in production; forecasting accuracy; use of predictive analytics; level of automated decision-making |
| R&D capability and innovation potential | R&D expenditure intensity; share of digital innovation projects; speed of new technology implementation; number of digital patents; commercialization rate of research outcomes |
| Digital human capital | Employees' digital competency level; proportion of personnel completing digital training; availability of IT specialists; digital culture; workforce readiness for technological change |
| Cyber resilience and digital risk management | Number of critical cyber incidents; average recovery time for digital services; compliance with information security standards; efficiency of data backup systems; maturity of digital risk management |

**Source:** developed by the author based on the literature review [1–18].

For *cost indicators*, where higher values negatively affect digital resilience, inverse normalization is employed:

$$z_i = \frac{x_{\max} - x_i}{x_{\max} - x_{\min}}.$$

This normalization procedure provides a consistent interpretation of all indicators, whereby values approaching one indicate a higher level of performance with respect to the corresponding dimension of digital resilience.

Following normalization, an integrated score is calculated for each functional dimension. For this purpose, a weighted additive model is employed:

$$S_j = \sum_{i=1}^{n} w_i z_i,$$

where: $S_j$ – integrated score of the $j$-th functional dimension;

$w_i$ – weight assigned to the $i$-th indicator;

$z_i$ – normalized value of the $i$-th indicator;

$n$ – number of indicators included in the corresponding functional dimension.

The weighting coefficients satisfy the following normalization constraint:

$$\sum_{i=1}^{n} w_i = 1.$$

The resulting composite scores for the six functional dimensions are subsequently used to calculate the integrated measure of enterprise digital resilience.

The proposed *Digital Resilience Index (DRI)* is defined as follows:

$$DRI = \sum_{j=1}^{6} \alpha_j S_j,$$

where: *DRI* – Digital Resilience Index;

$S_j$ – integrated score of the $j$-th functional dimension;

$\alpha_j$ – weight assigned to the corresponding functional dimension;

$$\sum_{j=1}^{6} \alpha_j = 1.$$

The integrated model consists of six functional dimensions:

$$DRI = \alpha_1 I + \alpha 2 D + \alpha_3 A + \alpha_4 R + \alpha_5 H + \alpha_6 C,$$

where: $I$ – Digital Infrastructure;

$D$ – Data Management;

$A$ – Artificial Intelligence and Predictive Analytics;

$R$ – R&D Capability;

$H$ – Digital Human Capital;

$C$ – Cyber Resilience and Digital Risk Management.

The proposed model is intentionally designed to be flexible, allowing the set of individual indicators to be refined or adapted to the specific characteristics of particular industries without altering the overall structure of the integrated index. At the same time, maintaining a common framework of

functional dimensions ensures the comparability of assessment results across enterprises and provides a methodological foundation for cross-industry benchmarking and comparative analysis.

A critical stage in constructing an integrated index is the determination of weighting coefficients for the individual functional dimensions. The literature offers several approaches for this purpose, including equal weighting, expert judgment, the Analytic Hierarchy Process (AHP), entropy-based methods, and statistical techniques such as principal component analysis. Each approach possesses specific advantages and limitations; therefore, the choice of weighting method should be aligned with the objectives of the study and the availability of relevant data.

In this study, the Analytic Hierarchy Process (AHP) is proposed as the most appropriate approach because it combines expert judgment with a formal procedure for testing the consistency of pairwise comparisons. The application of AHP makes it possible to account for differences in the economic significance of individual functional dimensions, avoid the unrealistic assumption of equal importance, and enhance the methodological robustness of the integrated assessment of digital resilience.

The determination of weighting coefficients represents one of the most important stages in developing the integrated indicator. Assigning equal weights offers the simplest solution; however, this approach implicitly assumes that all dimensions of digital resilience contribute equally to enterprise performance, an assumption that is inconsistent with the operational characteristics of high-tech enterprises. In practice, disruptions affecting digital infrastructure or data management systems typically produce substantially greater economic consequences than temporary declines in digital culture or the intensity of employee training. Consequently, the application of equal weighting may distort the overall assessment of digital resilience.

To determine the weighting coefficients, the present study employs the Analytic Hierarchy Process (AHP) developed by Thomas L. Saaty. This method is widely used in the construction of composite indices, the evaluation of complex socioeconomic systems, and multi-criteria decision support. Its principal advantage lies in combining expert evaluation with a mathematical assessment of judgment consistency, thereby providing a more rigorous and objective basis for determining weights than subjective assignment alone.

The AHP procedure involves pairwise comparisons of the functional dimensions using Saaty's nine-point scale. The resulting comparison matrix is then used to derive the priority vector and calculate the consistency ratio of expert judgments. If the consistency ratio does not exceed the recommended threshold of 0.10, the resulting weighting coefficients are considered sufficiently reliable for subsequent calculations.

Considering the proposed architecture of digital resilience, digital infrastructure and data management exert the greatest influence on the integrated assessment because they constitute the operational foundation for all other components of the enterprise's digital ecosystem. R&D capability and cyber resilience are likewise characterized by high economic significance, as they determine the enterprise's long-term adaptability and its ability to withstand digital risks. Although digital human capital and artificial intelligence play an essential role, their effectiveness depends to a considerable extent on the maturity of the underlying digital infrastructure.

Based on the results of the expert evaluation, the weighting coefficients presented in *Tbl. 2* are proposed.

**Table 2**

**Weighting Coefficients of the Functional Dimensions of the Digital Resilience Index (DRI)**

| Functional Dimension | Symbol | Weight |
|---|---|---|
| Digital Infrastructure | I | 0.22 |
| Data Management | D | 0.18 |
| Artificial Intelligence and Predictive Analytics | A | 0.14 |
| R&D Capability | R | 0.17 |
| Digital Human Capital | H | 0.13 |
| Cyber Resilience and Digital Risk Management | C | 0.16 |
| Total | | 1.00 |

**Source:** developed by the author.

The proposed weighting scheme reflects the system-forming role of digital infrastructure and information resources in ensuring enterprise digital resilience. At the same time, the differences among the weighting coefficients remain moderate, which is consistent with the principle of comprehensive assessment and prevents any single functional dimension from dominating the integrated index.

The weighting coefficients were derived using the Analytic Hierarchy Process (AHP) based on pairwise comparisons of the functional dimensions according to Saaty's nine-point scale. The resulting pairwise comparison matrix is presented in *Tbl. 3*.

The calculations yielded a consistency ratio (CR) of 0.08, which is below the recommended threshold of 0.10. This result indicates an acceptable level of consistency in the expert judgments and confirms the suit-

ability of the derived weighting coefficients for subsequent calculations.

**Table 3**

**Pairwise Comparison Matrix of the Functional Dimensions of the Digital Resilience Index (DRI)**

| Functional Dimension | I | D | A | R | H | C |
|---|---|---|---|---|---|---|
| I | 1 | 2 | 3 | 2 | 3 | 2 |
| D | 1/2 | 1 | 2 | 1 | 2 | 1 |
| A | 1/3 | 1/2 | 1 | 1/2 | 2 | 1 |
| R | 1/2 | 1 | 2 | 1 | 2 | 2 |
| H | 1/3 | 1/2 | 1/2 | 1/2 | 1 | 1/2 |
| C | 1/2 | 1 | 1 | 1/2 | 2 | 1 |

**Source:** developed by the author using Saaty's Analytic Hierarchy Process (AHP).

Incorporating the estimated weighting coefficients, the integrated digital resilience index is expressed as follows:

$$DRI = 0.22\text{I} + 0.18D + 0.14A + 0.17R + 0.13H + 0.16C.$$

The value of the *Digital Resilience Index (DRI)* ranges from 0 to 1. Values approaching 1 indicate a greater capacity of the enterprise to ensure the stable operation of its digital ecosystem, maintain business continuity, and adapt effectively to technological change.

However, the numerical value of the integrated index alone does not provide sufficient insight into the actual level of enterprise digital resilience. For practical application, the assessment results must be supported by an appropriate interpretation framework.

To illustrate the calculation procedure, consider the integrated assessment of the Digital Infrastructure functional dimension. Following the normalization of the five individual indicators, the resulting values are 0.82, 0.76, 0.81, 0.77, and 0.79. Assuming equal contributions of the individual indicators within the functional dimension, the integrated score is calculated as follows:

$$I = \frac{0.82 + 0.76 + 0.81 + 0.77 + 0.79}{5} = 0.79.$$

The integrated scores for the remaining functional dimensions are calculated using the same procedure and are subsequently aggregated into the overall Digital Resilience Index (DRI) in accordance with the proposed model (*Tabl. 4*).

The interpretation scale was developed with reference to widely accepted approaches used in constructing composite indices in socioeconomic research, whereby the range of possible values is divided into several levels representing qualitatively different states of the phenomenon under investigation. This approach facilitates the practical application of the methodology and allows it to be used both for internal performance monitoring and for comparative benchmarking across enterprises.

The proposed interpretation scale not only facilitates the practical interpretation of the Digital Resilience Index (DRI) but also provides a foundation for strategic managerial decision-making. Determining the level of digital resilience enables managers to identify the most vulnerable components of the enterprise's digital ecosystem, evaluate their influence on overall organizational performance, and establish evidence-based priorities for digital modernization. Furthermore, the integrated index supports benchmarking across enterprises, monitoring changes over time, and assessing the efficiency of digital transformation strategies.

To examine the practical applicability of the proposed methodology, the Digital Resilience Index (DRI) was calculated using a representative high-tech enterprise as an illustrative case. The application of the model involved determining the values of the individual indicators, normalizing the data, calculating the integrated scores for each functional dimension, and deriving the overall index value. The results enabled an assessment of the enterprise's level of digital resilience, the identification of the most vulnerable components of its digital ecosystem, and the determination of priorities for further improvement.

To further validate the methodology, an illustrative application was performed using a hypothetical high-tech enterprise. The calculations followed the proposed algorithm, including the normalization of individual indicators, the estimation of integrated scores for each functional dimension, and the calculation of the final Digital Resilience Index (DRI) (*Tbl. 5*).

According to the proposed interpretation scale, the calculated value of DRI = 0.721 corresponds to a High level of digital resilience. This result indicates that the enterprise has established the essential components of a resilient digital ecosystem, demonstrates a substantial capacity to adapt to technological change, and is capable of maintaining the continuity of its critical business processes within the digital environment.

To evaluate the robustness of the proposed model, a sensitivity analysis of the Digital Resilience Index (DRI) was conducted by systematically varying the values of individual functional dimensions while holding all remaining parameters constant. Specifically, the value of each functional dimension was increased and decreased by 10% in separate simulation scenarios (*Tbl. 6*).

**Table 4**

**Interpretation Scale for the Digital Resilience Index (DRI)**

| DRI Value | Level of Digital Resilience | Interpretation |
|---|---|---|
| 0.00–0.20 | Critically Low | The digital ecosystem is unstable. There is a high probability of business disruption even under relatively minor internal or external disturbances. Comprehensive digital modernization is required |
| 0.21–0.40 | Low | Individual digital solutions have been implemented; however, they remain insufficiently integrated. A high level of digital risk reduces overall enterprise performance |
| 0.41–0.60 | Moderate | The fundamental components of the digital ecosystem are in place; however, structural constraints continue to limit digital resilience and organizational adaptability |
| 0.61–0.80 | High | The enterprise maintains the efficient operation of its digital ecosystem, adapts rapidly to technological change, and ensures the continuity of critical business processes |
| 0.81–1.00 | Strategic | Digital resilience constitutes a major source of competitive advantage. The digital ecosystem demonstrates a high degree of adaptability, scalability, and the capacity to sustain long-term innovation-driven development |

**Source:** developed by the author based on the synthesis of previous research [1–20].

**Table 5**

**Results of Calculating the Functional Dimensions of the Digital Resilience Index (DRI)**

| Functional Dimension | Symbol | Integrated Score | Weight | Weighted Score |
|---|---|---|---|---|
| Digital Infrastructure | I | 0.79 | 0.22 | 0.174 |
| Data Management | D | 0.72 | 0.18 | 0.130 |
| Artificial Intelligence and Predictive Analytics | A | 0.68 | 0.14 | 0.095 |
| R&D Capability | R | 0.75 | 0.17 | 0.128 |
| Digital Human Capital | H | 0.63 | 0.13 | 0.082 |
| Cyber Resilience and Digital Risk Management | C | 0.70 | 0.16 | 0.112 |
| Digital Resilience Index (DRI) | | | | 0.721 |
| Functional Dimension | Symbol | Integrated Score | Weight | Weighted Score |

**Source:** calculated by the author.

**Table 6**

**Results of the Sensitivity Analysis of the Digital Resilience Index (DRI)**

| Simulation Scenario | DRI Value |
|---|---|
| Baseline value | 0.721 |
| 10% increase in the R&D Capability score | 0.734 |
| 10% increase in the Digital Human Capital score | 0.729 |
| 10% decrease in the Cyber Resilience score | 0.710 |
| 10% decrease in the Digital Infrastructure score | 0.704 |

**Source:** developed by the author.

The results demonstrate that the Digital Resilience Index (DRI) is most sensitive to changes in Digital Infrastructure, R&D Capability, and Cyber Resilience and Digital Risk Management. These findings support the proposed weighting scheme and confirm that the model exhibits an appropriate level of robustness with respect to moderate variations in the values of individual functional dimensions.

The integrated assessment also makes it possible to identify structural imbalances that remain concealed when individual indicators of digital development are analyzed in isolation. In particular, the highest scores were recorded for Digital Infrastructure and R&D Capability, indicating that the enterprise possesses a well-developed technological foundation and a strong capacity to implement emerging digital solutions. By contrast, comparatively lower scores were observed for Digital Human Capital, highlighting the need to strengthen professional development programs, enhance employees' digital competencies, and foster a stronger digital organizational culture.

The practical application of the proposed methodology confirms that the integrated indicator not only determines the overall level of enterprise digital resilience but also identifies the specific functional dimensions that constrain its further development. Unlike conventional measures of digital maturity or digitalization, the Digital Resilience Index (DRI) is designed to evaluate the balance and coherence of the enterprise's digital ecosystem, thereby substantially expanding its analytical value for strategic management.

## DISCUSSION

The findings support the proposition that digital resilience should be regarded as an independent economic category integrating the technological, informational, organizational, and innovation-related dimensions of high-tech enterprise development. Unlike existing approaches, which primarily focus on digital transformation, digital maturity, or cybersecurity, the proposed model provides a comprehensive assessment of an enterprise's ability to maintain the continuous operation of its digital ecosystem while sustaining long-term competitiveness.

An important advantage of the proposed methodology is its flexibility and broad applicability. Although the overall structure of the integrated index remains unchanged, the set of individual indicators can be adapted to the characteristics of specific industries, enterprise sizes, or technological environments. This flexibility enables the model to serve as an instrument for internal strategic analysis, inter-enterprise benchmarking, monitoring the outcomes of digital transformation initiatives, and supporting investment decision-making.

Nevertheless, the proposed model has several limitations. First, the determination of weighting coefficients relies on expert judgment, introducing a degree of subjectivity despite the consistency verification provided by the Analytic Hierarchy Process. Second, the availability and quality of corporate data may affect the calculation of certain indicators. Future research should therefore focus on validating the proposed model using empirical data from high-tech enterprises across different industries, statistically verifying the weighting coefficients through multivariate analytical techniques, and investigating the relationships between digital resilience and financial performance, innovation outcomes, and market competitiveness.

## CONCLUSIONS

This study proposes an original conceptualization of digital resilience as an integrated economic characteristic of a high-tech enterprise that reflects its ability to ensure the stable operation of its digital ecosystem, adapt to technological change, and sustain long-term innovation-driven development. Unlike existing approaches, digital resilience is conceptualized not as a component of cybersecurity or digital transformation but as an independent determinant of competitive advantage.

An original architecture of digital resilience has been developed, comprising six interconnected functional dimensions: Digital Infrastructure, Data Management, Artificial Intelligence and Predictive Analytics, R&D Capability, Digital Human Capital, and Cyber Resilience and Digital Risk Management. Based on this architecture, a system of quantitative indicators has been established to enable a comprehensive assessment of the enterprise's digital ecosystem.

The study also proposes a methodology for calculating the Digital Resilience Index (DRI), incorporating the normalization of individual indicators, the estimation of integrated scores for each functional dimension, the application of weighting coefficients derived using the Analytic Hierarchy Process, and the calculation of the overall integrated index. In addition, an interpretation scale has been developed to classify enterprise digital resilience levels and facilitate the application of assessment results in strategic management.

The illustrative application of the proposed methodology confirms its practical suitability for the comprehensive assessment of digital resilience in high-tech enterprises. The Digital Resilience Index (DRI) enables not only the evaluation of the overall maturity of the enterprise's digital ecosystem but also the identification of structural imbalances, the determination of strategic priorities for digital modernization, and the assessment of the effectiveness of digital transformation initiatives.

The practical significance of the proposed methodology lies in its potential application by managers of high-tech enterprises in designing digital development strategies, managing innovation activities, substantiating investments in digital technologies, and monitoring the effectiveness of digital transformation. Furthermore, the proposed approach provides a methodological foundation for future research in the field of the strategic management of enterprise digital development. ■

## BIBLIOGRAPHY


1. Бондаренко Д. В. Методичний підхід до оцінки цифровізації підприємств будівельної галузі. *Бізнес Інформ*. 2024. № 6. С. 93–103. DOI: https://doi.org/10.32983/2222-4459-2024-6-93-103
2. Бондаренко Д. В. Теоретичні засади цифрових трансформацій в компаніях. *Економіка та суспільство*. 2024. Вип. 64. DOI: https://doi.org/10.32782/2524-0072/2024-64-39

3. Derhachova V. V., Koleshnia Ya. O. Digital transformation of industrial enterprises as a transformation of business models and corporate thinking. *Економічний вісник НТУУ «Київський політехнічний інститут»*. 2024. № 28. С. 46–50. DOI: https://doi.org/10.20535/2307-5651.28.2024.302773
4. Костромський М. В. Адаптація організаційної культури виробничих підприємств до викликів цифрової трансформації. *Бізнес Інформ*. 2024. № 11. С. 333–339. DOI: https://doi.org/10.32983/2222-4459-2024-11-333-339
5. Онищенко С. В., Маслій О. А., Пантась В. В. Ділова активність бізнесу в Україні: цифрова трансформація та сталий розвиток. *Економіка і регіон*. 2024. № 1. С. 136–146. DOI: https://doi.org/10.26906/EiR.2024.1(92).3321
6. Птащенко О. В., Кириленко О. П., Курцев О. Ю. Вплив цифрових трансформацій на розвиток сучасного економічного простору: людський капітал, інклюзія, безпека. *Бізнес Інформ*. 2024. № 7. С. 180–190. DOI: https://doi.org/10.32983/2222-4459-2024-7-180-190
7. Танклевська Н. С., Мірошниченко В. О. Фінансова стійкість підприємств в умовах цифрової економіки. *Бізнес Інформ*. 2024. № 3. С. 249–255. DOI: https://doi.org/10.32983/2222-4459-2024-3-249-255
8. Трубніков А. Цифрова трансформація менеджменту як драйвер післявоєнного відновлення промислових підприємств України. *Modeling the Development of the Economic Systems*. 2024. № 4. С. 394–399. DOI: https://doi.org/10.31891/mdes/2024-14-51
9. Bhamra R., Dani S., Burnard K. Resilience: The conєcept, a literature review and future directions. *International Journal of Production Research*. 2011. Vol. 49. Iss. 18. P. 5375–5393. DOI: https://doi.org/10.1080/00207543.2011.563826
10. Burnard K., Bhamra R. Organisational resilience: Development of a conceptual framework for organisational responses. *International Journal of Production Research*. 2011. Vol. 49. Iss. 18. P. 5581–5599. DOI: https://doi.org/10.1080/00207543.2011.563827
11. Regulation (EU) 2022/2554 of 14 December 2022 on Digital Operational Resilience for the Financial Sector (Digital Operational Resilience Act – DORA). European Parliament, & Council of the European Union. Luxembourg : Publications Office of the European Union, 2022. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
12. ISO 22301:2019. Security and resilience – Business continuity management systems – Requirements. International Organization for Standardization. Geneva: ISO, 2019. URL: https://www.iso.org/standard/75106.html
13. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. International Organization for Standardization. Geneva : ISO, 2022.
14. Cyber Resilience of Systems and Networks / Linkov, I., & Kott, A. (Eds.). Cham : Springer, 2019. DOI: https://doi.org/10.1007/978-3-319-77492-3
15. National Institute of Standards and Technology. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. Gaithersburg, MD : NIST, 2023.
16. National Institute of Standards and Technology. *Cybersecurity Framework (CSF 2.0)*. Gaithersburg, MD : NIST, 2024.
17. OECD. *Enhancing Resilience by Boosting Digital Business Transformation in Ukraine*. Paris : OECD Publishing, 2024. DOI: https://doi.org/10.1787/4b13b0bb-en
18. OECD. *OECD Digital Economy Outlook 2024. Volume 2: Strengthening Connectivity, Innovation and Trust*. Paris : OECD Publishing, 2024. DOI: https://doi.org/10.1787/3adf705b-en
19. Saurin T. A., Patriarca R., Hegde S., Rayo M. The influence of digital technologies on resilient performance: Contributions, drawbacks, and a research agenda. *Applied Ergonomics*. 2024. Vol. 118. Art. 104290. DOI: https://doi.org/10.1016/j.apergo.2024.104290
20. World Economic Forum. *Global Cybersecurity Outlook 2025*. Geneva : World Economic Forum, 2025.

**REFERENCES**

Bhamra R., Dani S. & Burnard K. (2011). Resilience: The concept, a literature review and future directions. *International Journal of Production Research, 18*(49), 5375–5393. https://doi.org/10.1080/00207543.2011.563826

Bondarenko D. V. (2024). Metodychnyi pidkhid do otsinky tsyfrovizatsii pidpryiemstv budivelnoi haluzi [Methodological approach to assessing the digitalization of construction enterprises]. *Biznes Inform, 6*, 93–103. https://doi.org/10.32983/2222-4459-2024-6-93-103

Bondarenko D. V. (2024). Teoretychni zasady tsyfrovykh transformatsii v kompaniiakh [Theoretical foundations of digital transformations in companies]. *Ekonomika ta suspilstvo, 64*. https://doi.org/10.32782/2524-0072/2024-64-39

Burnard K. & Bhamra R. (2011). Organisational resilience: Development of a conceptual framework for organisational responses. *International Journal of Production Research, 18*(49), 5581–5599. https://doi.org/10.1080/00207543.2011.563827

Derhachova V. V. & Koleshnia Ya. O. (2024). Digital transformation of industrial enterprises as a transformation of business models and corporate thinking. *Ekonomichnyi visnyk NTUU «Kyivskyi politekhnichnyi instytut», 28*, 46–50. https://doi.org/10.20535/2307-5651.28.2024.302773

European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2554 of 14 December 2022 on Digital Operational Resilience for the Finan-

cial Sector (Digital Operational Resilience Act – DORA). Luxembourg: Publications Office of the European Union. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
International Organization for Standardization. (2019). *ISO 22301:2019. Security and resilience – Business continuity management systems – Requirements*. Geneva: ISO. https://www.iso.org/standard/75106.html
International Organization for Standardization (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. Geneva: ISO.
Kostromskyi M. V. (2024). Adaptatsiia orhanizatsiinoi kultury vyrobnychykh pidpryiemstv do vyklykiv tsyfrovoi transformatsii [Adaptation of the organizational culture of manufacturing enterprises to the challenges of digital transformation]. *Biznes Inform, 11*, 333–339. https://doi.org/10.32983/2222-4459-2024-11-333-339
Linkov, I. & Kott, A. (2019). *Cyber Resilience of Systems and Networks*. Cham: Springer. https://doi.org/10.1007/978-3-319-77492-3
National Institute of Standards and Technology (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. Gaithersburg, MD: NIST.
National Institute of Standards and Technology (2024). *Cybersecurity Framework (CSF 2.0)*. Gaithersburg, MD: NIST.
OECD (2024). *Enhancing Resilience by Boosting Digital Business Transformation in Ukraine*. Paris: OECD Publishing. https://doi.org/10.1787/4b13b0bb-en
OECD (2024). *OECD Digital Economy Outlook 2024. Volume 2: Strengthening Connectivity, Innovation and Trust*. Paris: OECD Publishing. https://doi.org/10.1787/3adf705b-en
Onyshchenko S. V., Maslii O. A. & Pantas V. V. (2024). Dilova aktyvnist biznesu v Ukraini: tsyfrova transformatsiia ta stalyi rozvytok [Business activity in Ukraine: digital transformation and sustainable development]. *Ekonomika i rehion, 1*, 136–146. https://doi.org/10.26906/EiR.2024.1(92).3321
Ptashchenko O. V., Kyrylenko O. P. & Kurtsev O. Yu. (2024). Vplyv tsyfrovykh transformatsii na rozvytok suchasnoho ekonomichnoho prostoru: liudskyi kapital, inkliuziia, bezpeka [Impact of digital transformations on the development of the modern economic space: human capital, inclusion, security]. *Biznes Inform, 7*, 180–190. https://doi.org/10.32983/2222-4459-2024-7-180-190
Saurin T. A., Patriarca R., Hegde S. & Rayo M. (2024). The influence of digital technologies on resilient performance: Contributions, drawbacks, and a research agenda. *Applied Ergonomics, 118*. https://doi.org/10.1016/j.apergo.2024.104290
Tanklevska N. S. & Miroshnychenko V. O. (2024). Finansova stiikist pidpryiemstv v umovakh tsyfrovoi ekonomiky [Financial stability of enterprises in the digital economy]. *Biznes Inform, 3*, 249–255. https://doi.org/10.32983/2222-4459-2024-3-249-255
Trubnikov A. (2024). Tsyfrova transformatsiia menedzhmentu yak draiver pisliavoiennoho vidnovlennia promyslovykh pidpryiemstv Ukrainy [Digital transformation of management as a driver of post-war recovery of industrial enterprises of Ukraine]. *Modeling the Development of the Economic Systems, 4*, 394–399. https://doi.org/10.31891/mdes/2024-14-51
World Economic Forum (2025). *Global Cybersecurity Outlook 2025*. Geneva: World Economic Forum.

Дослідження не отримувало зовнішнього фінансування.

Автор заявляє про відсутність конфлікту інтересів.

Під час підготовки роботи автор використав CODEX (ChatGPT) з моделлю 5.6 SOL Extra High з метою первинного пошуку джерел і подібних досліджень на тему статті. Автор перевірив і відредагував отримані матеріали.

Стаття надійшла до редакції / Received: 12.07.2026
Статтю прийнято до публікації / Accepted: 26.07.2026
Оприлюднено / Published: 18.08.2026



УДК 332.7+338.5
JEL: R31; R41
DOI: https://doi.org/10.32983/2222-4459-2026-7-197-206

# ГЕОІНФОРМАЦІЙНА ОЦІНКА ВПЛИВУ ТРАНСПОРТНОЇ ДОСТУПНОСТІ НА ВАРТІСТЬ ЖИТЛОВОЇ НЕРУХОМОСТІ

©2026 **ПОМОРЦЕВА О. Є., В'ЮННИК І. С., ЗАМІРЕЦЬ К. І., ЛУК'ЯНОВА А. О.**

*УДК 332.7+338.5*
*JEL: R31; R41*

**Поморцева О. Є., В'юнник І. С., Замірець К. І., Лук'янова А. О. Геоінформаційна оцінка впливу транспортної доступності на вартість житлової нерухомості**

*У статті розглядається актуальна проблема оцінки впливу транспортної доступності на формування просторової диференціації ринкової вартості житлової нерухомості в межах міських територій. Предметом дослідження є вернакулярні райони Салтівського житлового масиву в місті Харкові. Метою статті є розробка та застосування геоінформаційного підходу до інтегральної оцінки пішохідної доступності громадського транспорту, а також аналіз її впливу на вартість житла. Основними завданнями дослідження є просторове моделювання зон пішохідної доступності до станцій метрополітену та зупинок наземного громадського транспорту, розрахунок інтегрального індексу транспортної доступності для кожного вернакулярного району та аналіз впливу цих показників на ринкову вартість нерухомості. У ході дослідження розроблено та реалізовано геоінформаційний підхід із використанням програмного забезпечення QGIS. На основі відкритих просторових даних сформовано точковий шар об'єктів транспортної інфраструктури – зупинок метрополітену та наземного громадського транспорту. Побудовано буферні зони*