

DOI: <https://doi.org/10.32782/2524-0072/2026-88-41>

UDC 005.334:338.48

DETERMINANTS OF DIGITAL RESILIENCE OF HOSPITALITY ENTERPRISES AND THE IMPACT OF WAR RISKS ON ITS PROVISION

ДЕТЕРМІНАНТИ ЦИФРОВОЇ СТІЙКОСТІ ПІДПРИЄМСТВА СФЕРИ ГОСТИННОСТІ ТА ВПЛИВ ВОЄННИХ РИЗИКІВ НА ЇЇ ЗАБЕЗПЕЧЕННЯ

Chupyr Olena

Doctor of Economic Sciences,
Professor of Entrepreneurship, Trade and the Tourism Industry,
Simon Kuznets Kharkiv National University of Economics
ORCID: <https://orcid.org/0000-0002-2560-894X>

Avanesova Nina

Doctor of Economic Sciences,
Professor of Management and Public Administration,
O. M. Beketov National University of Urban Economy in Kharkiv
ORCID: <https://orcid.org/0000-0003-3636-9769>

Чупир Олена Миколаївна

Харківський національний економічний університет імені Семена Кузнеця

Аванесова Ніна Едуардівна

Харківський національний університет міського господарства
імені О. М. Бекетова

This article examines the development of digital resilience in hospitality businesses amid military threats. It argues that, in times of war, digitalization becomes a factor for survival, whilst a purely instrumental approach to transformation has run its course, demonstrating the need to transition to the concept of digital resilience. The key finding is the systematization of determinants: external (martial law, digital inequality, communication instability, regulatory constraints) and internal (staff shortages, low digital literacy, resistance to change, lack of funding, cyber-vulnerability, complexity of IT integration). Risks and adaptation mechanisms have been identified for each. A distinction has been made between digital transformation (the process) and resilience (the characteristic). The identified determinants form the basis for diagnosing vulnerabilities. Further research will focus on developing a methodology for quantitatively assessing resilience.

Keywords: digital resilience, determinants of digital resilience, hospitality businesses, digital transformation, military threats, adaptive capacity, disruptive risks, business continuity.

У статті досліджено проблему формування цифрової стійкості підприємств гостинності в умовах воєнних загроз, що набуває особливої актуальності для українського бізнесу через перманентну нестабільність, руйнування інфраструктури, енергетичні обмеження, кадрові втрати та зміну споживацьких патернів. Кризи мають не лише деструктивний, а й стимулюючий потенціал, виступаючи точками біфуркації для оновлення бізнесу. Саме в періоди екзистенційних викликів найповніше розкривається значення цифрової трансформації як інструменту адаптації, а її детермінанти стають визначальними для виживання підприємства. У воєнний час цифровізація стає не інструментом сервісу, а фундаментальним чинником життєздатності, що забезпечує безперервність діяльності. Суто інструментальний підхід до цифрової трансформації вичерпав себе, що свідчить про необхідність переходу до концепції цифрової стійкості – здатності бізнесу зберігати функціональність у перманентних кризових умовах, а не обмежуватися впровадженням технологічних змін. Ключовим результатом є систематизація детермінант цифрової стійкості підприємств гостинності. Зовнішні фактори охоплюють воєнний стан, цифрову нерівність, нестабільність зв'язку та регуляторні обмеження. Внутрішні – кадровий дефіцит, низька цифрова грамотність, опір змінам, брак фінансування, кібервразливість та складність інтеграції ІТ. Для кожної детермінанти окреслено ризики у разі їх ігнорування та адаптаційні механізми, що дозволяють мінімізувати негативні наслідки та підвищити рівень цифрової стійкості, що створює підґрунтя для практичних рекомендацій. Розмежовано цифрову трансформацію (інструментальний процес



зміни бізнес-моделі) та цифрову стійкість (характеристика, що забезпечує безперервність і самовідновлення). Пріоритетом стають не лише операційна ефективність, а й довіра споживачів та капіталізація репутації у турбулентному середовищі. Ідентифіковані детермінанти слугують основою для діагностики цифрової стійкості підприємств, виявлення вразливостей і розроблення заходів адаптації до воєнних загроз. Подальші дослідження доцільно спрямувати на створення методики кількісного оцінювання стійкості та її апробацію на реальних кейсах в умовах війни.

Ключові слова: цифрова стійкість, детермінанти цифрової стійкості, підприємства гостинності, цифрова трансформація, воєнні загрози, адаптаційні можливості, деструктивні ризики, безперервність бізнесу.

Statement of the problem. The issue of digital resilience becomes particularly relevant in times of crisis, when destabilizing factors threaten the very survival of businesses. Crises are two-sided: whilst destructive, they simultaneously stimulate renewal, acting as points of bifurcation that, for Ukrainian hospitality businesses, manifest in digital transformation, model optimization, service diversification, and a focus on new segments. The comprehensive impact of the crisis encompasses the creation of new competitive advantages, the implementation of flexible strategies, the acquisition of experience in risk response, the emergence of adaptive leaders, and the optimization of HR policies and financial flows. It is precisely during such periods that digital transformation reveals itself as a tool for adaptation, and its determinants become crucial for survival. War acts as a catalyst: restrictions on access to traditional sales channels are forcing businesses to scale up online services, implement contactless technologies, and adopt remote staff management.

Analysis of recent research and publications. In academic literature, distinct areas of research have emerged focusing on the operations of hospitality sector enterprises during a crisis. Firstly, the study by Bai S. and Yeliseyeva V. [1] confirms that digitalization (CRM, ERP, cloud services, analytics) has a positive impact on the resilience of businesses during wartime, helping them to remain competitive, whilst in the work by Bondar S. V. [2], the digitalization strategy is regarded as a necessary condition for the effective functioning of hospitality enterprises. Secondly, managerial aspects are being actively researched: crisis management in the hospitality sector is examined in the work by Danko N. I. and Kachanyuk E. O. [3], the specific features of management in crisis situations are highlighted in the study by Kish G. V. [5], and the issue of financial stability in the context of the digital economy is analysed by Tanklevska N. S. and Miroshnychenko V. O. [10]. Thirdly, the study by Nikitenko K. S. [8] identifies the key management challenges of digitalization in the HoReCa sector (unevenness,

fragmentation, staff incompetence, insufficient funding, weak cybersecurity), which serve as the basis for identifying internal determinants. Issues of financial security for enterprises in the digital environment are discussed in the works of Mekhed A. A. and Varnaliy Z. S. [7], as well as in the research by Susidenko V. T. and co-authors [9]. Certain aspects of the state's digital transformation and infrastructure resilience are highlighted in analytical reports by Vox Ukraine [4; 11].

Highlighting previously unresolved parts of the overall problem. Thus, existing research has yet to provide a systematic analysis of the determinants of digital resilience in hospitality businesses in the face of military threats, integrating external and internal factors, along with their associated risks and adaptive potential. This applies in particular to the specific nature of hospitality businesses' operations in the context of ongoing crises caused by military action.

Formation of the objectives of the article (task statement). The purpose of this study is to identify and substantiate the determinants of digital resilience in hospitality enterprises and to examine the influence of war-related risks on the conditions for its formation and maintenance in a turbulent economic environment.

Summary of the main research material. The digital transformation of domestic hospitality enterprises, intensified by the challenges of martial law, is developing along several interrelated lines and encompasses key aspects of operations: from management decisions and security to logistics and customer communication, leading to a systematic restructuring of the internal structure of business models. The implementation of digital technologies is ceasing to be merely a tool for automating routine operations and is evolving into a new operational paradigm, the foundation of which is adaptability, remote control of business processes, personalized interaction with consumers, and a comprehensive real-time analytical picture [9]. The authors [9] point out that the digital transformation of infrastructure in the hotel and restaurant sector is taking place through the

comprehensive integration of systems – enterprise resource planning, customer relationship management, sales operations, business analytics, and supply chain management – driven by a combination of factors: regulatory changes, new consumer practices, migration flows, staff shortages, and the challenges of martial law. The result of this process is the redesign of business models based on multi-channel approaches, a shift towards personalized service formats, cost optimization, digital document management, and enhanced cybersecurity. The achievement of digital resilience depends directly on the effectiveness of a business's digital transformation, particularly during times of crisis when resources are limited and the need for adaptability increases; therefore, it is crucial to analyze the determinants of digital transformation, which, in conditions of instability, act as key factors in ensuring an enterprise's digital resilience. When analyzing the determinants of digital transformation [2], specific triggers that directly prompt hotels to change should be identified: a decline in business activity, loss of competitive position, customer dissatisfaction, operational inefficiency, stricter security requirements, and the need to enter new markets. At the same time, the specifics of the industry are determined by consumer priorities, which shape three areas of innovation: creating unique experiences (exploratory innovation), enhancing functional utility (co-innovation through partnerships), and advancing services to ensure comfort and personalization. Digitalization is a key component in each of these areas, which necessitates its systematization within formal strategies. The formulation and implementation of such strategies are determined by a range of factors: alignment with the organization's strategic objectives and mission, the availability of internal resources (technical, financial, and human), the competitive environment and market trends, guest expectations and needs, the regulatory framework, and the pace of technological innovation. Taking these determinants into account is a prerequisite for developing an effective and adaptive digitalization strategy. The outlined determinants of digital transformation lay the foundation for an organization's resilience; however, transformation alone does not guarantee it. To achieve this, it is important that the technological solutions implemented ensure not only operational efficiency but also business continuity,

adaptability to change, and rapid recovery from crises – in other words, that they foster the enterprise's digital resilience. Before moving on to an analysis of the determinants of digital resilience in hospitality enterprises, it is necessary to outline the specific nature of the external environment in which they operate. Military threats, economic instability, logistical disruptions, cyberattacks, and staff shortages are placing unprecedented pressure on businesses, making digital resilience a critical factor for survival. It is precisely in such conditions that the determinants defining a business's ability to withstand threats, adapt, and recover take on particular significance. According to an analysis by the international platform MSG, the key sources of management crises are a combination of internal and external factors [5]. These include technological risks, in particular equipment failures or large-scale cyber incidents that could completely paralyze operational activities. Internal social and labor conflicts – such as strikes or deep-seated disagreements that undermine teamwork – pose a serious threat. A crisis may also arise from disorganization, when norms of subordination, professional ethics, or labor rights are violated. The immediate cause is often incompetent management that neglects its duties and makes ineffective decisions. Ethical violations form a separate category: corruption, data falsification, or fraud. The most acute phase is a financial crisis, leading to insolvency and the bankruptcy of the enterprise. Military threats have a significant negative impact on hospitality businesses' operations, underscoring the importance of digital resilience for their survival and development. War generates significant uncertainty, leading to disruptions in supply chains, instability in demand, restrictions on population mobility, and a decline in tourist flows. Under such conditions, rapid response to external changes is enabled by digital transformation tools, which serve as the foundation for a new-generation adaptive business architecture. Military threats significantly increase the risks to the information security of hospitality businesses. The intensity of cyberattacks is increasing, disrupting the operation of digital booking, management, and customer communication systems, which necessitates the strengthening of cyber defenses, the implementation of data backup, and the active use of cloud technologies to ensure the continuity of business processes even in the event of critical damage to physical

infrastructure. As the authors note [9], in the context of military threats, the disruption of the consumer market and regional disintegration, the need to establish a flexible information infrastructure takes on particular importance; such an infrastructure would ensure the timeliness of management decisions, personalized customer interaction, cybersecurity, and integration with government e-services. It has been established that the successful digitalization of the sector is possible only if technical solutions are aligned with businesses' real needs in crisis conditions. As already noted, war acts as a catalyst for digital transformation, with systemic and multidimensional impacts that encompass both operational and strategic levels of management. In this context, digital resilience emerges as an enterprise's inherent ability to adapt to extreme conditions by implementing flexible technological solutions. Strategic management of hospitality enterprises in the face of military threats is undergoing a radical transformation. Approaches to planning and decision-making are changing: analytical tools are becoming a key mechanism for instant risk assessment, adaptation to demand fluctuations, and rigorous resource optimization, which is critical given resource scarcity. Digital resilience is thus evolving from a tool for short-term survival into a fundamental competitive advantage. It forms the basis for the long-term competitiveness of hospitality businesses in today's environment, ensuring their viability and market leadership despite global instability. The hospitality industry is currently undergoing a radical transformation, driven by the synergy of global digital shifts and acute internal challenges – military conflict, economic instability, changes in consumer behavior, and a severe labor shortage. In these conditions, the introduction of digital technologies into the hospitality sector serves not only as a tool for process automation but also as a strategic safeguard for business viability in the turbulent environment. Digitalization not only enables increased revenue and personalized service but also takes management quality to a new level whilst optimizing costs. However, on the path to large-scale technological renewal of the sector, its implementation is hampered by several managerial barriers that hinder the systematic modernization of enterprises. Table 1 consolidates and systematizes the key determinants influencing the digital resilience of hospitality industry enterprises.

The listed determinants are not mutually exclusive – they are strongly correlated

(the complexity of IT integration is often a consequence of financial constraints and low digital literacy). However, for applied analysis, it is advisable to consider them separately, as each requires distinct response measures. The determinants discussed do not exhaust the full complexity of the situation. According to strategic reports [12; 13], Ukraine's current digital landscape indicates that the potential of classical digital transformation as a purely instrumental process has been exhausted. In the context of military destabilization and growing cyber threats [4; 11], there is a need to rethink the architecture of business-consumer interaction, which brings the concept of digital resilience to the fore – the ability of a business to maintain functionality, adapt, and recover in the face of ongoing crises. The authors of [6] interpret digital modernization as the integration of technology into the economy – a «tool for breakthrough development».

Building on this approach, we argue that, in times of crisis, technological integration is not an end in itself but a means of fostering digital resilience – the ability to function amid nonlinear, crisis-driven changes.

In this sense, the priority is not only operational efficiency, but also maintaining consumer trust and capitalizing on reputation in a turbulent environment. Whereas in the traditional approach, digitalization is a means of optimizing costs, in the proposed approach, it becomes the foundation for building a secure space for customer interaction, where technological solutions strengthen market trust.

Traditional approaches to business continuity and cyber resilience [7] focus on internal technological stability, ignoring the customer experience during a crisis, which creates a gap between technological readiness and market viability and highlights the need to broaden approaches to take into account the specific nature of the hospitality sector, where the customer experience is a determining factor in competitiveness. Competitiveness in the hospitality sector is shifting from formalized plans to dynamic organizational capabilities shaped by market interaction. A key role is to integrate an understanding of customer needs into all aspects of operations, based on the collection and analysis of consumer behavior data, thereby transforming standard service into a personalized guest experience. The identified determinants provide a basis for understanding operating conditions during a crisis; however, to gain a comprehensive understanding of the

Table 1

Determinants of digital resilience of hospitality enterprises in conditions of military threats

Determinants	Impact on the company's operations	Destructive (risks)	Adaptive (capabilities)
1	2	3	4
<i>The imposition of martial law and mobilization measures (external determinants)</i>	A decline in tourist numbers and a fall in demand due to security threats; disruptions to logistics chains and supply chain failures; a shortage of skilled staff resulting from mobilization and migration; and restrictions on business operations due to curfews and legal prohibitions.	A decline in the customer base due to reduced tourist activity and security threats; logistical disruptions; staff shortages resulting from mobilization and migration; and restrictions on operations due to curfews and legal prohibitions.	The shift to remote work and flexible employment, the expansion of online services and contactless customer service technologies, resource allocation and alternative logistics, the involvement of internally displaced persons, and government support programs.
<i>A severe shortage of skilled workers against the backdrop of migration trends (internal determinants)</i>	Damage to reputation due to inconsistent service and declining customer loyalty; loss of competitive advantage due to an inability to scale operations and implement digital tools; constraints on long-term development due to a lack of human resources to implement strategic initiatives.	Chronic staff overload, leading to burnout and exhaustion; a shortage of specialists with the necessary skills for digitalization; staff turnover, which jeopardizes operational continuity, and a decline in service quality due to excessive workloads on employees.	Automation of routine processes (chatbots, online booking) to reduce the workload on staff; development of digital skills through training; flexible working arrangements (outsourcing, remote working); support for mental health (rotation, workload management).
<i>Insufficient digital literacy among staff (internal determinant)</i>	Low returns on digital investments, the persistence of manual processes with overlapping functions, and limited operational flexibility, which together lead to a loss of competitive advantage and a reduced ability to adapt to market changes.	Resistance to automation (reluctance to adapt, sabotage, psychological barriers); the persistence of manual practices; ineffective automation due to the superficial use of IT tools without integration into processes.	Ongoing staff training; engaging staff in the change process by communicating the benefits of automation and using motivational strategies; phased implementation through pilot projects, followed by scaling up.
	A slowdown in digital transformation, which widens the technological gap with competitors, and operational inefficiency due to the continued use of	Transformation held back by resistance from management or staff; reliance on manual processes; low adaptability due to	Involving senior management and key staff in the planning of the transformation, demonstrating the benefits of automation to different
<i>Resistance to organizational change (internal determinant)</i>	costly manual procedures; a loss of competitiveness resulting from an inability to deliver the required levels of service quality, speed, and flexibility.	Inflexibility in management and production makes it difficult to respond to market changes.	levels of management; phased implementation through pilot projects, followed by scaling up; fostering a culture of change through communication, training, and incentive schemes.

Continued from Table 1

1	2	3	4
<i>Financial and strategic funding shortfall (internal determinant)</i>	Low return on investment due to the lack of a systematic strategy; operational constraints resulting from the continued use of manual procedures; loss of competitive advantage due to technological backwardness; low resilience to crises due to the lack of flexible digital tools.	A slowdown in technological modernization due to a lack of resources and the absence of a strategy; limited flexibility from piecemeal digitalization; and fragmented IT solutions that reduce return on investment.	Developing a long-term digital strategy that takes into account the specific characteristics of the sector, phased, scalable investment, securing alternative sources of funding (government programs, grants, partner investments), and focusing resources on priority areas.
<i>Regional digital inequality (exogenous determinant)</i>	Limited competitiveness due to a technology gap; a shrinking customer base due to poor online market coverage; operational instability resulting from reliance on external infrastructure quality; difficulties scaling the business in regions with weak technological infrastructure.	Inconsistent service standards due to technological limitations; poor coverage of the online market due to limited access to digital sales and communication channels; an uneven playing field that puts businesses in remote areas at a distinct disadvantage.	The use of mobile and satellite technologies to establish a basic digital presence, local digital optimization of internal processes that do not require a constant internet connection, partnerships with operators to expand coverage and with flexible service delivery through a gradual build-up of digital capabilities.
<i>Cyber vulnerability and information security systems (internal determinants)</i>	Disruption to operations caused by the failure of critical systems; financial losses arising from system recovery and penalties; reputational risks due to data breaches; weakening of market positions due to a loss of trust.	Operational disruptions caused by cyberattacks or security system failures; leaks of confidential data and damage to reputation; financial losses resulting from downtime and system recovery; loss of trust among customers and partners.	Comprehensive cyber security (firewalls, antivirus software, intrusion detection); regular security audits and system updates; data backup via cloud technologies; staff training in cyber hygiene; standardized incident response procedures.
<i>The complexity of selecting and integrating IT solutions (internal determinant)</i>	Low return on investment due to the lack of a systematic strategy; piecemeal automation that fails to deliver the expected operational benefits; difficulties in scaling the business due to the fragmentation of IT tools; loss of competitive advantage as a result of falling behind technologically.	Inefficient use of resources due to a lack of assessment of the viability of investments, the dispersal of investments across unrelated systems, piecemeal implementation without system integration, and the inability to scale up and achieve comprehensive automation.	The introduction of practices for the preliminary assessment of the economic viability of digital solutions, the use of integrated platforms rather than individual tools, phased, scalable implementation, and expert guidance in selecting IT tools.

End of Table 1

1	2	3	4
<i>Instability of telecommunications infrastructure and electricity supply (external determinants)</i>	Disruption to business continuity due to a lack of connectivity; loss of online bookings and customer inquiries as a result of digital service outages; unavailability of cloud services; financial losses due to downtime and a decline in service quality.	Loss of contact with customers and the inability to process bookings and payments; system failures due to a lack of internet and power supply; unavailability of cloud data, resulting in a loss of control over processes; disruption to coordination between departments; and forced downtime.	Backup power supply (generators, batteries, solar panels); alternative communication channels (satellite internet, Starlink, various providers); standalone booking systems with offline access; local data backup; continuity of critical services during power cuts.
<i>Regulatory constraints and legal uncertainty in the field of digitalization (external determinants)</i>	Rising operational costs for legal support; delays in the roll-out of digital services; risks of reputational damage in the event of data protection breaches; reduced competitiveness due to limited ability to integrate digital solutions with government e-services.	Rising costs of legal support and auditing, difficulties in implementing digital tools due to changes in legislation, the risk of fines for data protection law breaches, and a slowdown in digital transformation due to legal uncertainty.	Engaging legal advisers to support digital projects; implementing compliance management systems; using industry data protection standards (ISO/IEC 27001) as the basis for internal regulatory frameworks; participating in public consultations on regulatory policy in the digital sector.

Source: compiled by the author [1; 3; 8; 10]

mechanism of resilience, it is necessary to trace the logic of its development from basic tools to strategic outcomes.

Conclusions. This study has identified a set of determinants that influence the level of digital resilience of hospitality enterprises in the face of military threats. In a crisis context, digitalization ceases to serve a purely optimization-oriented function and becomes a fundamental prerequisite for maintaining operational capability, shifting the focus from efficiency to business continuity. It has been established that the determinants of digital resilience are heterogeneous in origin: external factors necessitate the establishment of backup management circuits, whilst internal factors are characterized by structural interdependence,

whereby staff shortages hinder technological adoption and low digital literacy negates the potential of automation solutions. A key conceptual finding is the distinction between digital transformation – as a process of changing the business model – and digital resilience – as a systemic property that ensures continuity and self-recovery. The «risk-adaptation» matrix developed enables a shift from localized fault diagnosis to a comprehensive resilience audit, which has practical significance for management decisions in the hospitality sector. A promising direction for further research is the development of methodological tools for quantitatively measuring the level of digital resilience among enterprises in the sector.

REFERENCES:

1. Bai S., Yelisieiev V. (2025) Tsyfrovizatsiia u zabezpechenni stiikosti torhovelnykh pidpriemstv [Digitalization in ensuring the sustainability of retail businesses]. *SCIENTIA FRUCTUOSA* no. 4, pp. 38-54.
2. Bondar S.V. (2024) Formuvannia stratehii tsyfrovizatsii subiekta hotelnoho biznesu [Developing a digitalization strategy for a hotel business]. *Ekonomika ta suspilstvo*, no. 60. Available at: <https://economyandsociety.in.ua/index.php/journal/article/view/359>
3. Danko N.I., Kachaniuk Ye. O(2025) Stratehiia rozvytku pidpriemstv sfery hostynnosti v Ukraini v umovakh kryzy [A development strategy for hospitality businesses in Ukraine during the crisis]. *Biznes-Inform*, no. 8, pp. 517-525.

4. Derzhavna tsyfrova transformatsiia ta stiikist infrastruktury: analiz 2022-2025 rokiv (2025) [Government Digital Transformation and Infrastructure Resilience: Analysis for 2022–2025]. *Vox Ukraine*. Available at: <https://voxukraine.org/digital-transformation-analysis-2025>
5. Kish H. V. (2025) Osoblyvosti menedzhmentu hotelnykh pidpriemstv v umovakh kryzovykh sytuatsii [Features of hotel management in times of crisis]. *Naukovyi visnyk Odeskoho natsionalnoho ekonomichnoho universytetu*, no. 6 (331), pp. 103-110.
6. Liashenko V. I., Vyshnevskiy O. S. (2018) Tsyfrova modernizatsiia ekonomiky Ukrainy yak mozhlyvist proryvnoho rozvytku: monohrafiia [The Digital Modernization of Ukraine's Economy as an Opportunity for Breakthrough Development: A Monograph]. Kyiv: National Academy of Sciences of Ukraine, Institute of Industrial Economics, 252 p. (in Ukrainian).
7. Mekhed A. A., Varnalii Z. S. (2021) Finansova bezpeka pidpriemstv v umovakh tsyfrovoi ekonomiky [Financial security of businesses in the digital economy]. *Visnyk universytetu bankivskoi spravy*, no. 3, pp. 55-61.
8. Nikitenko K. S. (2025) Upravlinski vyklyky tsyfrovizatsii v hotelno-restorannomu biznesi Ukrainy [Management challenges of digitalization in Ukraine's hotel and restaurant sector]. *Ekonomichnyi prostir*, no. 202, pp. 196-201.
9. Susidenko V. T., Hushtan T. V., Kahanets-Havrylko L. P., Vakula I. (2025) Suchasni informatsiini systemy v hotelno-restorannomu biznesi [Modern information systems in the hotel and restaurant industry]. *Akademichni vizii*, no. 41. Available at: <https://academy-vision.org/index.php/av/article/download/1844/1712>
10. Tanklevska N. S., Miroshnychenko V. O. (2024) Finansova stiikist pidpriemstv v umovakh tsyfrovoi ekonomiky [The financial stability of businesses in the digital economy]. *Biznes-Inform*, no. 3, pp. 249-255.
11. Transformatsiia landshaftu kiberzahroz ta infrastrukturna stiikist Ukrainy 2025: analitychnyi ohliad (2025) [The Changing Landscape of CyberThreats and Ukraine's Infrastructure Resilience 2025: An Analytical Review]. *Vox Ukraine*. Available at: <https://voxukraine.org/>
12. Tsyfrova transformatsiia ekonomiky Ukrainy: vyklyky ta priorytety 2026: analit. dop. (2026). Kyiv: NISD, 84 p. (in Ukrainian).
13. Chystydokhid ukrainskykh turystychnykh kompanii zris na tretynu v pershomu pivrichchi 2024 roku (2024) [The net income of Ukrainian travel companies rose by a third in the first half of 2024]. *Diia. Biznes. Doslidzhennia YouContro* Available at: <https://surl.li/nsygpw>

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бай С., Єлісєєв В. Цифровізація у забезпеченні стійкості торговельних підприємств. *SCIENTIA FRUC-TUOSA* 2025. №4. С. 38-54.
2. Бондар С. В. Формування стратегії цифровізації суб'єкта готельного бізнесу. *Економіка та суспільство*. 2024. № 60. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/3592>
3. Дanyкo Н. І., Качанюк Є. О. Стратегія розвитку підприємств сфери гостинності в Україні в умовах кризи. *Бізнес-Інформ*. 2025. №8. С. 517-525.
4. Державна цифрова трансформація та стійкість інфраструктури: аналіз 2022-2025 років. *Vox Ukraine*. 2025. URL: <https://voxukraine.org/digital-transformation-analysis-2025>
5. Кіш Г. В. Особливості менеджменту готельних підприємств в умовах кризових ситуацій. *Науковий вісник Одеського національного економічного університету*. 2025. № 6 (331). С. 103-110.
6. Ляшенко В. І., Вишневецький О. С. Цифрова модернізація економіки України як можливість проривного розвитку: монографія. Київ, 2018. 252 с.
7. Мехед А. А., Варналій З. С. Фінансова безпека підприємств в умовах цифрової економіки. *Вісник університету банківської справи*. 2021 № 3. С. 55-61.
8. Нікітенко К. С. Управлінські виклики цифровізації в готельно-ресторанному бізнесі України. *Економічний простір*. 2025. № 202. С. 196-201.
9. Сусіденко В. Т., Гуштан Т. В., Каганець-Гаврилко Л. П., Вакула І. Сучасні інформаційні системи в готельно-ресторанному бізнесі. *Академічні візії*. 2025. № 41. URL: <https://academy-vision.org/index.php/av/article/download/1844/17>
10. Танклевська Н. С., Мірошніченко В. О. Фінансова стійкість підприємств в умовах цифрової економіки. *Бізнес-Інформ*. 2024. № 3. С. 249-255.
11. Трансформація ландшафту кіберзагроз та інфраструктурна стійкість України 2025 : аналітичний огляд. *Vox Ukraine*. 2025. URL: <https://voxukraine.org/>
12. Цифрова трансформація економіки України: виклики та пріоритети 2026: аналіт. доп. Київ : НІСД, 2026. 84 с.

13. Чистий дохід українських туристичних компаній зріс на третину в першому півріччі 2024 року. *Дія. Бізнес. Дослідження YouControl*. URL: <https://surl.li/nsygpw>

Дата надходження статті: 23.06.2026

Дата прийняття статті до публікації: 18.08.2026

Дата публікації статті: 28.08.2026