Digital Technologies in the Economic Security Management System of Industrial Organizations: Business Process Modeling

Iryna Stankevych[1], Hanna Sakun[1], Inna Yatskevych[1], Oksana Vasylenko[2], Eduard Siemens[2] and Viktor Shevchenko[3]

[1]*Department of Management and Marketing, Odessa State Academy of Civil Engineering and Architecture, Didrikhsona Str. 4, 65029 Odesa, Ukraine*

[2]*Departments of Electrical Engineering, Mechanical Engineering and Engineering Management, Anhalt University of Applied Sciences, Bernburger Str. 57, 06366 Köthen, Germany*

[3]*Zammler LTD, Proviantska Str. 3, 01035 Kiyv, Ukraine*

arnika@ukr.net, sakun.anna@ukr.net, innav2018@gmail.com, {oksana.vasylenko, eduard.siemens}@hs-anhalt.de, shevchenko@zammler.com.ua

Keywords: Economic Security, Digital Technologies, Industry 4.0, Business Process Modeling, Industrial Organizations, ERP-System, Big Data Analytics, Blockchain.

Abstract: The development of the Industry 4.0 concept and the intensive digitalization of business processes of industrial organizations create qualitatively new conditions for managing their economic security. Traditional protection methods are becoming insufficiently effective in the face of rapidly changing threats associated with cyberattacks and data integrity risks. The purpose of the study is to develop theoretical and methodological principles and a practical model for integrating digital technologies into the economic security management system of industrial enterprises through the prism of business process modeling. The work uses a systems approach, a process approach, regression analysis and modeling methods. The authors propose a process-oriented model for ensuring economic security, which involves the use of technologies such as ERP systems, Big Data Analytics and blockchain to ensure transparency and continuity of critical business processes (for example, supply chain management and production). The results of the study show that the implementation of integrated digital solutions not only increases efficiency and productivity (up to 15-20%), but also significantly strengthens the ability of the enterprise to withstand internal and external threats through real-time monitoring and risk prediction. The practical significance of the work lies in the possibility of using the proposed model by industrial organizations to develop digital transformation strategies taking into account aspects of economic security.

1 INTRODUCTION

The contemporary global economy is defined by rapid digitalization and geopolitical volatility. For Ukrainian industrial organizations seeking competitiveness and sustainable development, embracing digital transformation – incorporating technologies like the Internet of Things, AI, Big Data, and Cloud Computing – is essential. This shift fundamentally optimizes business processes, making them more flexible, efficient, and cost-effective.

Crucially, this digital evolution simultaneously introduces a new generation of sophisticated threats, creating a critical gap in traditional economic security management. The problem lies in the fact that while digital technologies dramatically enhance operational efficiency, they simultaneously introduce significant vulnerabilities that traditional, reactive security models are ill-equipped to handle:

1) The extensive reliance on interconnected digital infrastructure and data creates a massive attack surface for cyber threats.
2) The sheer volume of data and complex information systems increases the risk of data manipulation, insider threats, and breaches, which can directly lead to significant financial and reputational damage.
3) Over-reliance on complex information systems creates potential single points of failure, turning technological dependence into a critical economic security risk.

The central challenge in the digital age is the mismatch between the rapidly evolving complexity of digital threats and the current, reactive approach to economic security. To ensure sustainable operations, security must transition from a simple protective function to a proactive, integrated strategy embedded directly into core business processes. Therefore, there is a critical need for methodological tools, such as business process modeling techniques, to enable industrial organizations to seamlessly integrate digital security mechanisms into their operational models, thereby effectively managing economic security within the complex digital economy.

2 LITERATURE REVIEW

The impact of digital transformation on businesses is a highly relevant and complex issue, making it a frequent subject of academic research. In recent decades, have studied how digital transformation affects the economy, politics, and culture, particularly focusing on artificial intelligence (AI), the Internet of Things (IoT), and big data [1] - [3], [11], [17]. Furthermore, [1] emphasize that to truly achieve innovative solutions in business digitalization, enterprises need to integrate blockchain, AI, and the industrial IoT, as the combined potential of these technologies is greater than their individual capabilities.

Digitalization is transforming businesses in two key ways: by boosting productivity and by paving the way for fully digital enterprises [5] - [8]. Across EU countries, the digital economy is increasingly driven by the use of data analytics and artificial intelligence (AI) to fuel economic growth and innovation [2]. This digital shift enables companies to optimize production, cut costs, and increase profits [9].

AI has significantly upgraded digital tools, turning them from simple communication methods into sophisticated instruments for data analysis, automation, and industrial decision-making. This is seen in applications like voice assistants, image recognition, autonomous vehicles, robotics, and predictive analytics [11]. Complementing this, Blockchain technology provides a secure, transparent, and trustworthy base for business intelligence by ensuring data integrity and transparency. Its combination with AI is creating novel solutions in critical areas such as supply chain management, finance, and enterprise production structures [10].

While digitalization fosters financial accessibility, broader economic opportunities, and innovation, it also generates regulatory uncertainty, cybersecurity risks, and technological limitations. To strengthen economic security and trust within the digital economy, [3], [12], [14] advocate for prioritizing measures such as regulatory clarity, risk-based regulation, robust cybersecurity, and enhanced consumer education.

Digital transformation significantly increases the efficiency of industrial enterprise management through automation, data analytics, and process integration into a single digital ecosystem, which allows you to optimize business processes, reduce costs, speed up decision-making, and increase the competitiveness of the enterprise [15] - [18]. The practical application of digital technologies at industrial enterprises allows for faster response to market changes, improved product quality, and effective resource management.

The extensive research on digital transformation has not yet fully clarified how digital technologies influence the security of economic and private organizations. Because current methods for measuring economic security don't adequately address the digital environment's unique characteristics, it's crucial to develop comprehensive, integrated approaches. These new methods must merge conventional financial metrics with specialized indicators for cybersecurity and digital system resilience.

3 METHODOLOGY

To achieve the goal, a systematic and process-oriented approach was used. Economic security is considered as an integrated system that encompasses financial, human resources, information and management components. Business process modeling was carried out based on the Business Process Modeling Notation methodology with an emphasis on critical control points, where digital technologies introduce the greatest changes and risks. The business model for economic security management is proposed to be implemented through the integration of three key digital circuits into the standard business process of an industrial organization [16]. The entire cycle is a dynamic system where ERP provides Continuity and process control; Big Data Analytics provides Forecasting and detection of hidden threats; and Blockchain guarantees Transparency and immutability of data in the supply chain. The entire cycle is aimed at transforming risk information into a tangible economic advantage, strengthening the enterprise's ability to withstand threats in real time (see Fig. 1).

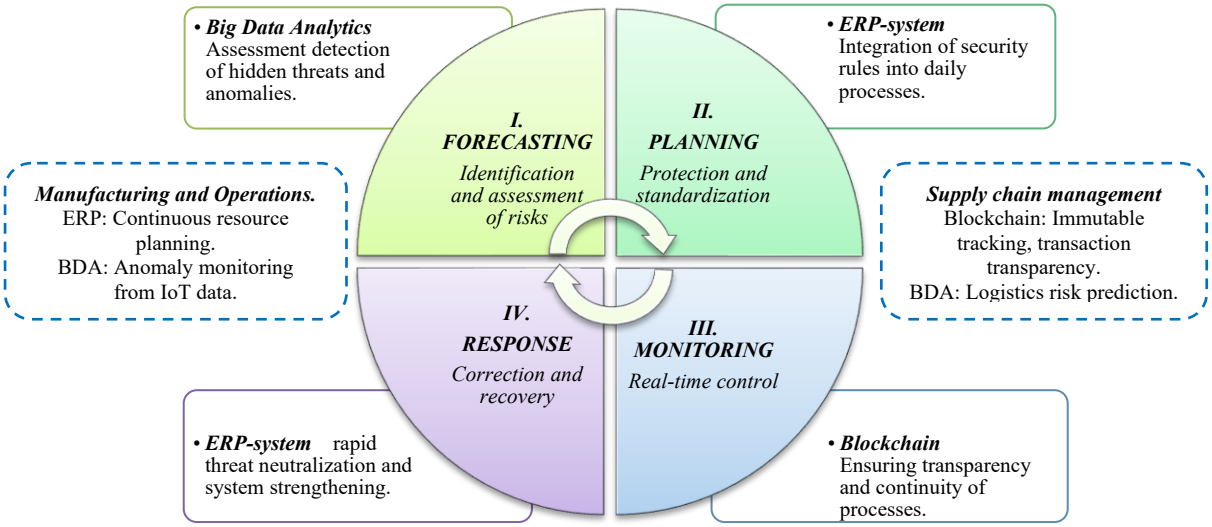

Figure 1: Process-oriented model of economic security of industrial organizations.

The business model allows you to adjust, change the system, eliminate its shortcomings before it is physically implemented, allows you to reduce the costs of creating a system, makes it possible to evaluate work based on results, helps to achieve mutual understanding between all project participants. At the same time, it should be understood that various modeling languages are used to model the business processes of organizations, each of which cannot always be adapted, especially to complex industrial organizations [15].

4 RESULTS AND DISCUSSION

The digital economy, which includes new digital industries and old ones revamped by technology, is a major driver of both economic growth and social change. This current phase of development is often called the Fourth Industrial Revolution because it features rapid changes and close interaction between production and digital technologies, leading to more intellectualized labor [9].

The exponential growth of data volumes generated by enterprises poses a challenge to traditional methods of information processing and requires the development of new innovative solutions. Digital transformation is more than just adopting new technologies like AI, the Internet of Things (IoT), cloud computing, blockchain (for things like cryptocurrency), augmented/virtual reality, and biometrics. According to [2], it fundamentally requires a complete overhaul of a business's management system, from setting strategic goals to putting them into action. This includes developing and launching new business ideas and often revising those original goals. For this transformation to succeed, an organization must be flexible and able to quickly adapt to change, effectively using these new digital tools to tackle complex problems. While offering many benefits, this process also brings new challenges: businesses must constantly keep up with rapid technological changes, enhance cybersecurity, and manage vast amounts of data.

The use of formalized business process models (BPMN, IDEF0, ARIS) made it possible to carry out a structural decomposition of the activities of industrial enterprises, accurately identifying critical control points and potential bottlenecks where threats to economic security may arise, and thus develop mechanisms for preventive risk prevention. Additionally, the use of statistical analysis of the dynamics of digitalization of Ukrainian enterprises for 2020–2025 (growth from 28% to 55%) in combination with Eurostat data on EU countries (growth from 61% to 82%) creates a benchmarking base for assessing the digital divide and substantiating the need to implement integrated digital solutions (such as ERP, BDA, Blockchain) as a significant factor in strengthening ES and increasing competitiveness. Both data series demonstrate a stable and predictable linear growth of digitalization, as confirmed by $R^2 > 0.99$. This suggests that the selected linear regression model is

very well suited to describe digitalization trends in both the EU and Ukraine over this time interval (see Fig. 2) [5], [19].

The European industrial sector is currently experiencing major shifts due to a mix of global and internal pressures. These factors include the complete digitalization of society, greater environmental awareness, an aging workforce, a shortage of skilled labor, and changes in international trade leading to increased competition, particularly from Asia. To survive, European industry must adapt to these new realities [5].

Merging digital tools with reality lets us build virtual models that accurately reflect real-world conditions. This enables firms to test and improve products earlier, leading to significant cost reductions. Moreover, when industrial enterprises prioritize fast learning, innovation, and flexible operations, they can quickly adjust to the market, keep costs low, improve how they're managed, and ensure stable economic security.

Digital transformation drives industrial growth, using technologies like AI and robotics to increase productivity and lower costs. Critically, a firm's economic security is now less isolated and more dependent on its position within the entire network of economic relationships [14].

We will model the impact of the implementation of digital technologies on the financial indicators of Novikon LLC in order to quantitatively assess productivity growth, cost reduction and risks to determine additional profit, ROI and payback period of investments [15], [20]. The calculation results shown in Table 1 show that the digitalization of business processes in Novikon LLC provides a quick payback of investments (1.3–1.7 years) and a high level of profitability (ROI 58–80%), which indicates a significant potential for increasing the efficiency and economic security of the enterprise through the implementation of digital technologies.

The obtained calculation results confirm the high economic feasibility of digitalization, because even in a conservative scenario, the implementation of IT solutions provides a quick payback and a significant increase in profitability. This indicates that business process automation effectively optimizes costs and increases productivity, although the final benefit significantly depends on the accuracy of the initial parameters - margin, OPEX level and ERP implementation cost.

Optimizing digital tool selection requires assessing an enterprise's size, production specifics, and available budget [18]. The foundation for robust cyber threat protection lies in a holistic approach that integrates multiple tools and mandates continuous personnel training. Industrial enterprises employ a broad spectrum of digital defenses to ward off cyberattacks, with the principal tools being highlighted in Figure 3.

Digital process automation uses technologies to minimize common manual errors, leading to highly accurate and reliable task completion. Beyond accuracy, these technologies also enhance collaboration among participants, boost work efficiency, and cut labor costs. However, the impact of digital technologies varies greatly depending on the industry and a company's current readiness for digital transformation. For instance, goods-producing enterprises have longer production cycles, which means their return on investment (ROI) from digital technologies takes more time. Despite this, they actually implement a broader range of digital optimization and automation technologies in their production processes compared to service-providing companies.

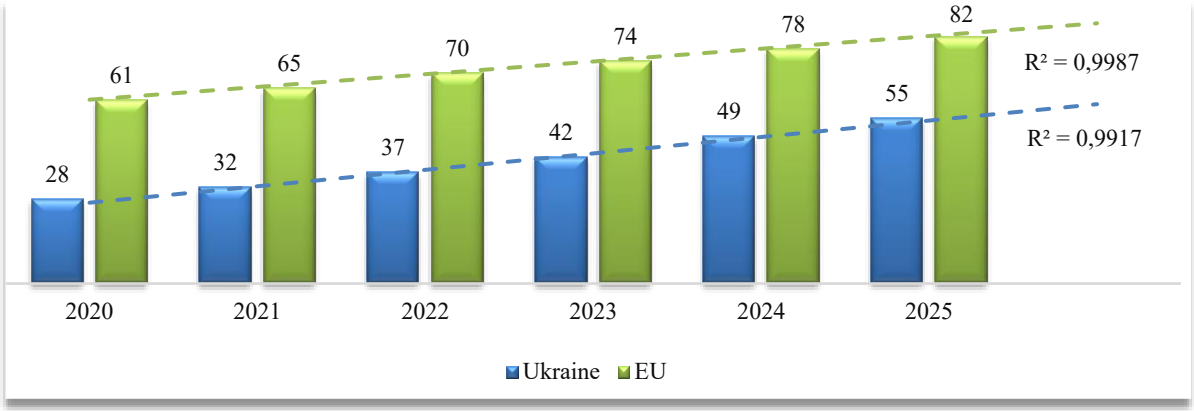

Figure 2: Digitalization of Ukrainian and EU industrial enterprises, % (2020–2025) [5].

Table 1: Scenario analysis for the digitalization model of economic security management using the example of Novicon LLC.

Indicator	Conservative	Average	Optimistic
CAPEX (₴)	500000	1500000	3000000
ΔR (%)	0,05	0,1	0,15
ΔOPEX (%)	0,07	0,12	0,18
ΔLoss (%)	0,3	0,5	0,7
R_0 (₴)	19097100	19097100	19097100
GP_0 (₴)	5729130	5729130	5729130
NP_0 (₴)	266800	266800	266800
$OPEX_0$ (₴)	5462330	5462330	5462330
$Loss_0$ (₴)	381942	381942	381942
R_1 (₴)	20052955	21006810	21961665
GP_1 (₴)	6015887	6302043	6588500
$OPEX_1$ (₴)	5083964	4811850	4476713
$Loss_1$ (₴)	267360	190971	114583
NP_1 (₴)	664563	1299222	1997204
ΔNP (₴)	397763	1032422	1730404
ROI (%)	0,796	0,688	0,577
Payback (y)	1,26	1,45	1,73

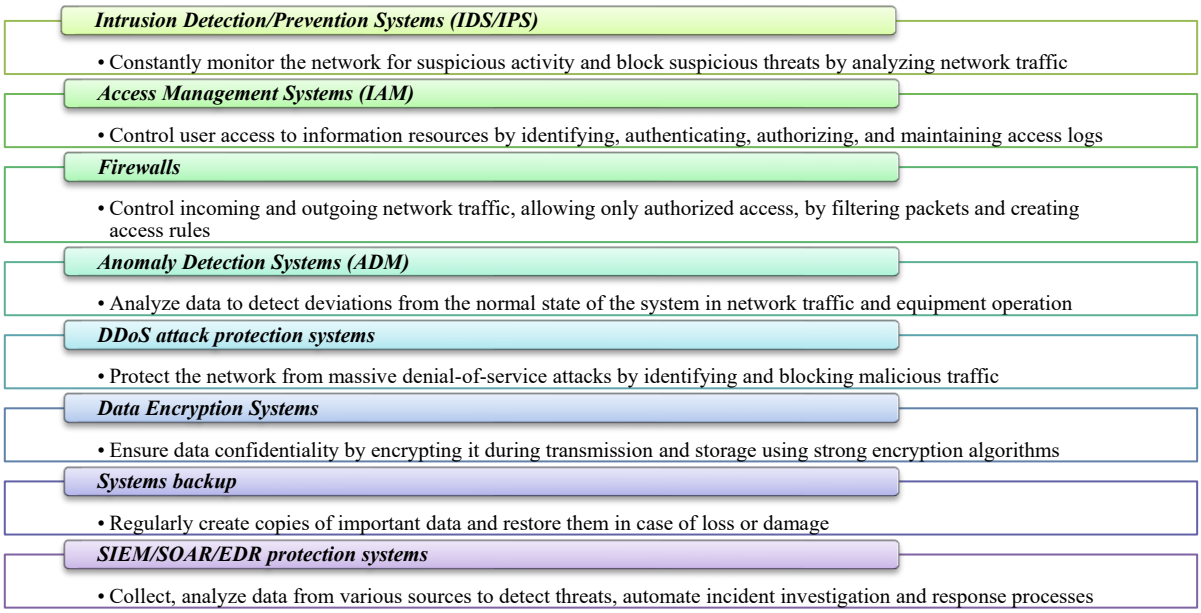

Figure 3: Digital enterprise security tools.

5 CONCLUSIONS

Digital transformation is essential for modern industrial progress, driving efficiency, product innovation, and market responsiveness to secure competitive advantages. However, this transition is inherently complicated by a heightened risk landscape, including serious concerns regarding privacy violations and the proliferation of information technology fraud and cybercrime. This study was specifically designed to support the industry's digital transformation by systematically assessing the current state of digital tool utilization in economic security management and identifying critical areas for improvement in cyber protection.

The core contribution is the affirmation that economic security management must adapt to the comprehensive operational changes introduced by digitalization across all production and value-

creation stages. The research results confirm the need for industrial enterprises to:

1) Recognize that the benefits of digital growth are inseparable from increased security risks;
2) Systematically analyze the profound, cross-functional changes digitalization introduces.

Ultimately, the study validates the crucial requirement for integrating modern cyber protection strategies, demonstrating that while digital technologies optimize operations and enhance transparency, addressing the pressing problem of economic security in this digitized environment remains a vital necessity for all enterprises, demanding further scientific and practical investigation.

ACKNOWLEDGMENTS

We acknowledge support by the German Research Foundation (Deutsche Forschungsgemeinschaft, DFG) and the Open Access Publishing Fund of Anhalt University of Applied Sciences.

REFERENCES

[1] A. A. Khan, A. A. Laghari, P. Li, M. A. Dootio, and S. Karim, "The collaborative role of blockchain, artificial intelligence, and industrial internet of things in digitalization of small and medium-size enterprises," Scientific Rep., vol. 13, no. 1, Jan. 2023. Accessed: Nov. 29, 2025. [Online]. Available: https://doi.org/10.1038/s41598-023-28707-9

[2] I. Mihus and S. K. Gupta, "The main trends of the development of the digital economy in the EU countries," in The Development of Innovations and Financial Technology in the Digital Economy, Scientific Center Innovative Res., 2023, pp. 23–41. Accessed: Nov. 29, 2025. [Online]. Available: https://doi.org/10.36690/diftde-2023-23-41

[3] I. O. Hubarieva, S. A. Buka, and N. V. Bielikova, "Assessing the level of digitalization of the economy of Ukraine and the EU member states," Probl. Econ., vol. 4, no. 58, pp. 14–21, 2023. Accessed: Nov. 29, 2025. [Online]. Available: https://doi.org/10.32983/2222-0712-2023-4-14-21

[4] I. V. Yatskevych and N. D. Maslii, "'Smart factories' as a promising direction for digitalization of enterprises," Bus. Inform, vol. 10, no. 525, pp. 363–367, 2021. Accessed: Nov. 29, 2025. [Online]. Available: https://doi.org/10.32983/2222-4459-2021-10-363-367

[5] European Commission, "Eurostat." Accessed: Nov. 29, 2025. [Online]. Available: https://ec.europa.eu/eurostat/data/database

[6] M. F. Arroyabe, C. F. A. Arranz, I. F. d. Arroyabe, and J. C. F. d. Arroyabe, "The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges," Technolog. Forecasting Social Change, vol. 199, p. 123051, Feb. 2024. Accessed: Nov. 29, 2025. [Online]. Available: https://doi.org/10.1016/j.techfore.2023.123051

[7] M. Zamora Iribarren, C. L. Garay-Rondero, I. Lemus-Aguilar, and R. E. Peimbert-García, "A review of industry 4.0 assessment instruments for digital transformation," Appl. Sci., vol. 14, no. 5, p. 1693, Feb. 2024. Accessed: Nov. 29, 2025. [Online]. Available: https://doi.org/10.3390/app14051693

[8] M. Z. Yaqub and A. Alsabban, "Industry-4.0-enabled digital transformation: Prospects, instruments, challenges, and implications for business strategies," Sustainability, vol. 15, no. 11, p. 8553, May 2023. Accessed: Nov. 29, 2025. [Online]. Available: https://doi.org/10.3390/su15118553

[9] N. Mironova, H. Koptieva, I. Liganenko, A. Sakun, and D. Chernyak, "Modeling the selection of innovative strategy for development of industrial enterprises," WSEAS Trans. Bus. Econ., vol. 19, pp. 278–291, Jan. 2022. Accessed: Nov. 29, 2025. [Online]. Available: https://doi.org/10.37394/23207.2022.19.26

[10] R. H. Chowdhury, "Blockchain and AI: Driving the future of data security and business intelligence," World J. Adv. Res. Rev., vol. 23, no. 1, pp. 2559–2570, Jul. 2024. Accessed: Nov. 29, 2025. [Online]. Available: https://doi.org/10.30574/wjarr.2024.23.1.2273

[11] O. Peter, A. Pradhan, and C. Mbohwa, "Industrial internet of things (IIoT): Opportunities, challenges, and requirements in manufacturing businesses in emerging economies," Procedia Comput. Sci., vol. 217, pp. 856–865, 2023. Accessed: Nov. 29, 2025. [Online]. Available: https://doi.org/10.1016/j.procs.2022.12.282

[12] L. Shostak, A. Fedoniuk, and O. Pomazun, "Kiberbezpeka v systemi formuvannia biznes-modeli pidpryiemstva v umovakh tsyfrovoi ekonomiky," Ekonomika ta susp-vo, no. 64, Jun. 2024. Accessed: Nov. 29, 2025. [Online]. Available: https://doi.org/10.32782/2524-0072/2024-64-37

[13] M. V. Vereskun, V. M. Kolosok, and E. V. Kolosok, "Vplyv tsyfrovoi transformatsii na upravlinnia promyslovymy pidpryiemstvamy," Pidpryiemnytstvo i torhivlia, no. 30, pp. 11–16, Jul. 2021. Accessed: Nov. 29, 2025. [Online]. Available: https://doi.org/10.36477/2522-1256-2021-30-02

[14] NOVIKON. Accessed: Nov. 29, 2025. [Online]. Available: https://novikon.ua/

[15] O. V. Sakun, I. V. Stankevych, and H. O. Sakun, "Using the big data tool to increase the efficiency of logistics activities of enterprises in the conditions of digital transformation," Tsyfr. ekonomika ta ekon. bezpeka, no. 4 (13), pp. 122–129, Jun. 2024. Accessed: Nov. 29, 2025. [Online]. Available: https://doi.org/10.32782/dees.13-18

[16] O. Hapieieva, R. Holovko, and V. Vitiutin, "Ekonomichna bezpeka pidpryiemstva v umovakh didzhytalizatsii," Nauk. perspektyvy, no. 9(39), Oct. 2023. Accessed: Nov. 29, 2025. [Online]. Available: https://doi.org/10.52058/2708-7530-2023-9(39)-322-333

[17] R. Buhrimenko and P. Smirnova, “Vplyv rozvytku tsyfrovoi transformatsii na diialnist pidpryiemstva,” Ekonomika ta susp-vo, no. 59, Jan. 2024. Accessed: Nov. 29, 2025. [Online]. Available: https://doi.org/10.32782/2524-0072/2024-59-29

[18] S. V. Kyrylenko, “Systema ekonomichnoi bezpeky v umovakh tsyfrovoi ekonomiky,” J. Strategic Econ. Res., no. 1, pp. 40–47, Jun. 2024. Accessed: Nov. 29, 2025. [Online]. Available: https://doi.org/10.30857/2786-5398.2024.1.4

[19] Ministry of Digital Transformation of Ukraine, “Tsyfrovizatsiia rehioniv i hromad: Pershi vymiriuvannia 2025 roku.” Accessed: Nov. 29, 2025. [Online]. Available: https://thedigital.gov.ua/news/technologies/tsifrovizatsiya-regioniv-i-gromad-pershi-vimiryuvannya-2025-roku

[20] Opendatabot, “36501757 – TOV NOVIKON.” Accessed: Nov. 29, 2025. [Online]. Available: https://opendatabot.ua/c/36501757