VI міжнародна науково-практична конференція учених та студентів
«Цифрова економіка як фактор інновацій та сталого розвитку суспільства»
09-10 грудня 2025 р.

УДК 339.9:332.2:631.1
Oleksii DZIS, Postgraduate Student
Vinnytsia National Agrarian University, Ukraine
Supervisor: Svitlana KOLIADENKO, Dr. Sc. (Economics), Prof.

DIGITAL TECHNOLOGIES AS A MEANS OF ENHANCING THE ECONOMIC SECURITY OF AGRICULTURAL ENTERPRISES

Олексій ДЗІСЬ, аспірант
Вінницький національний аграрний університет, Україна
Науковий керівник: Світлана КОЛЯДЕНКО, докт. екон. наук, проф.

ЦИФРОВІ ТЕХНОЛОГІЇ ЯК ЗАСІБ ПІДВИЩЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ АГРАРНИХ ПІДПРИЄМСТВ

Economic security is one of the key prerequisites for sustainable development, ensuring the stability of economic systems and their ability to withstand both external and internal threats. Contemporary research commonly distinguishes several levels of economic security, including the global, international, national, regional, enterprise-level, and individual levels [1]. Each of these levels forms its own set of risks and response mechanisms; however, all of them are interconnected and exert a significant influence on one another. Of particular importance is the economic security of agricultural enterprises, as they constitute the foundation of national food security and contribute significantly to regional socio-economic stability and the well-being of the population. At the same time, enterprise economic security is a complex and multifaceted concept that encompasses a system of interrelated components, including financial, production, investment, human resource, information and technological, and other components. Each of these components reflects the level of protection of a specific area of activity, the enterprise's readiness to address particular risks and threats, and ultimately determines its overall potential for sustainable development.

Accordingly, enterprise economic security is defined as a state of protection of a business against threats that may lead to economic losses, bankruptcy, or a decline in competitiveness. It encompasses the management of financial risks, protection against unfair competition, cyber threats, and internal crises such as corruption and fraud, as well as ensuring the sustainable development of the enterprise. In the course of carrying out economic activities, it is essential to clearly define the objectives for which specific measures aimed at ensuring enterprise economic security are implemented. The overall goal of enterprise economic security can be formulated as ensuring the stable and efficient functioning of the enterprise in the present while preserving its growth potential in the future, even under conditions of risks, threats, and adverse factors. More specific objectives include ensuring financial stability and independence, maintaining a high competitive position, protecting trade secrets, optimizing the enterprise's potential, achieving technological leadership, and safeguarding proprietary and confidential business information. [3].

The survival of an enterprise and the feasibility of its operations directly depend on the successful achievement of the aforementioned objectives. Given the increasing number and severity of risks, as well as the rapid dynamics of the economy under conditions of globalization and digitalization, deliberate and purpose-driven implementation of measures and instruments to ensure enterprise economic security has become essential for every organization. It is evident that the implementation of economic security measures may vary significantly across enterprises and largely depends on the specific characteristics of a particular industry.

VI міжнародна науково-практична конференція учених та студентів
«Цифрова економіка як фактор інновацій та сталого розвитку суспільства»
09-10 грудня 2025 р.

Modern agricultural enterprises are undergoing a phase of active digital transformation driven by the rapid development of digital and information and communication technologies, changes in the organization of production processes, and the need to enhance competitiveness in the global market [4]. Digitalization has become not only a tool for production modernization but also a key driver of resource management optimization, automation of operational processes, and improvement of enterprises' forecasting capabilities. The advancement of digital technologies in agriculture, including the implementation of precision farming, IoT systems, and advanced analytical platforms, leads to the emergence of a new operational environment in which development opportunities expand while the complexity of risks to economic security simultaneously increases.

The implementation of digital technologies provides agricultural enterprises with broad opportunities to improve analytics, monitoring, and risk assessment systems, which is critically important for ensuring all key components of economic security. Digital tools enable an enhanced level of financial security at the enterprise level. The use of automated financial management systems, online banking, electronic document management, and analytical platforms contributes to reducing the likelihood of errors, fraud, and unauthorized access to financial information. Predictive analytics systems assist agricultural enterprises in modeling revenue and cost scenarios, assessing the impact of market fluctuations on financial performance, and increasing the effectiveness of strategic planning. The introduction of blockchain technologies in financial transaction chains ensures transparency in the movement of funds, reduces the risks of corrupt practices, and enhances trust among business partners and financial institutions.

Digital and information technologies significantly strengthen the physical and technogenic security of enterprises [5]. Digital video surveillance systems, motion and access sensors, and territory security control systems make it possible to substantially reduce the risks of unauthorized access, theft, or damage to property. Infrastructure condition monitoring systems enable the timely detection of technogenic threats associated with the operation of warehouses, grain elevators, and production facilities. In addition, digital technologies allow for remote monitoring of compliance with storage standards, temperature regimes, and the technical condition of equipment, which significantly reduces the likelihood of incidents that could negatively affect the economic security of the enterprise.

From the perspective of the environmental component of economic security, digital technologies also represent a powerful and effective tool. Agricultural enterprises are able to conduct comprehensive monitoring of the environmental impact of their production activities, track the consumption of water and energy resources, and control compliance with environmental regulations and standards. Geographic information system (GIS)–based analysis enables the assessment of land conditions, the forecasting of the outcomes of agronomic decisions, and the reduction of anthropogenic environmental pressure. Precision application technologies for fertilizers and plant protection products reduce environmental risks, minimize resource consumption, and contribute to the rationalization of production activities in the environmental dimension.

Cybersecurity plays a pivotal role in ensuring the information and technological component of the economic security of agricultural enterprises, as modern production processes are increasingly dependent on digital systems, network infrastructure, and data flows. Given the extensive use of IoT devices, automated monitoring systems, resource management platforms, and analytical solutions, agricultural enterprises become potentially vulnerable to cyberattacks, data loss or distortion, and disruptions to critical technological processes [6]. Ensuring an adequate level of cybersecurity makes it possible to maintain data integrity and availability, guarantees the uninterrupted operation of digital systems, and minimizes the risks

of unauthorized interference, which is a necessary condition for the stability of the technological infrastructure and the enhancement of the overall level of enterprise economic security.

References:

1 Ivashchenko, O. V. (2013). Financial and economic security of an enterprise. Bulletin of Odesa National University. Economics, 18(1–1), 142–145. http://nbuv.gov.ua/j-pdf/Vonu_econ_2013_18_1(1)_33.pdf

2. Nebava, M. I., & Mironova, Yu. V. (2017). Economic security of the enterprise [Textbook]. Vinnytsia: Vinnytsia National Technical University.

3. Hrybinenko, O. M., & Shahoian, S. M. (2017). The essence and ways of ensuring the economic security of the enterprise. Scientific Bulletin of Kherson State University, (22), 98–100.

4. Koliadenko, S. V. (2016). Digital economy: Prerequisites and stages of development in Ukraine and worldwide. Economics. Finance. Management: Topical Issues of Science and Practice, (6), 105–112.

5. Zelisko, N., Raiter, N., Markovych, N., Matskiv, H., & Vasylyna, O. (2024). Improving business processes in the agricultural sector considering economic security, digitalization, risks, and artificial intelligence. Ekonomika APK, 31(3), 10–21. https://doi.org/10.32317/2221-1055.2024030.10

6. Koliadenko, S. V., & Dzis, O. V. (2024). Information and technological component of the economic security of agricultural enterprises in the context of digitalization. Economics, Finance, Management: Topical Issues of Science and Practice, 3(69).

УДК 008; 005; 330.65

Nataliia GAVKALOVA,

Doctor of Economy, Head of the Department of Public Administration and Economic Policy of the Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine; Dr.hab., Professor Warsaw University of Technology (Poland)

Oleh KUNITSYN,

PhD student of the Department of Public Administration and Economic Policy of the Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine

RESHAPING ARCHETYPES OF SOCIAL INSTITUTIONS IN UKRAINE: THE DANGERS OF AI IN WARTIME INFORMATION MANIPULATIONS

The russian aggression to Ukraine has revealed not only the physical devastations of war, but also an intensified struggle over truth and symbolic order [1]. The study investigates how information manipulation during the invasion, especially with the rise of generative AI and synthetic data, reshapes the archetypes of social institutions in Ukraine. Social institutions such as family, community solidarity, volunteer networks and civic trust function through deep symbolic archetypes that guide expectations of protection, moral authority, unity, and truth [2;3]. During the war, disinformation, staged reports, fake news, deepfakes and fabrications have long been tools of manipulation. Recently, however, generative AI technologies and synthetic data offer new scales, modalities, and sophistication to these practices [4;5]. This research seeks to understand how these emerging AI-enabled forms affect trust, legitimacy, identity and resilience of Ukrainian social institutions.

The objective of the study is to analyze how generative AI and synthetic data act as instruments of information manipulation that exploit, distort or undermine archetypes of social institutions in Ukraine during wartime. This includes identifying which archetypes are most