УДК 658.15:338.24:004.9
JEL Classification: L26, M15, O33, G32

HREBENIKOVA O.[1], DENYSOVA T.[2]

STRATEGIC DIRECTIONS FOR IMPROVING THE MECHANISM OF MANAGING THE ECONOMIC SECURITY OF ENTREPRENEURSHIP IN THE CONTEXT OF INCREASING DIGITALIZATION OF SOCIO-ECONOMIC PROCESSES

DOI: https://doi.org/10.32620/cher.2025.4.02

Formulation of the problem. In the context of dynamic digitalization and increasing geopolitical threats, the issue of economic security of entrepreneurship becomes particularly acute. Modern enterprises face a complex of new risks where traditional protection methods no longer provide the necessary effectiveness. There is an urgent need to revise security management approaches to ensure the flexibility and adaptability of the business to the rapidly changing conditions of the digital economy and the state of war. *The purpose of the article* is to substantiate the theoretical and methodological foundations and develop strategic directions for improving the mechanism of economic security management of entrepreneurship in the context of dynamic digitalization and increasing geopolitical threats. *The object of the research* is the system of economic security management of business entities under digital transformations. *The methods used in the study* include general scientific methods: analysis and synthesis (for studying the theoretical basis and identifying digital risks), systems approach (for forming an ecosystem vision of security), methods of generalization (for systematizing protection technologies), and comparison. *The main hypothesis of the research* is the assumption that the integration of innovative digital tools into the management strategy and the development of digital competencies of the personnel are key factors in ensuring the enterprise's resilience against modern hybrid threats. *Presenting of the main material.* The article analyzes the impact of digitalization on the architecture of enterprise economic security. Key digital risks and wartime challenges are identified. The possibilities of using modern technologies, particularly blockchain and data analytics, to protect business processes are considered. The importance of forming a digital security culture and implementing proactive risk management methods is substantiated. Strategic directions are proposed, covering both technological and organizational aspects of protection. *Originality and practical significance of the research* lie in the development of strategic directions for improving the security management mechanism, which allow forming an adaptive protection system. The approaches proposed by the authors of the article can be used by enterprise managers to increase business resilience and gain competitive advantages in the digital environment. *Conclusions and prospects for further research:* the main digital threats to the economic security of the enterprise are identified, and it is proven that reliable protection is guaranteed by the integration of modern technologies (blockchain, artificial intelligence) into the management system. It is established that digital tools allow risks to be detected even before they occur (predictive approach). The

[1] **Гребенікова Олена Володимирівна,** канд. екон. наук, доцент, доцент кафедри менеджменту та бізнес-адміністрування, Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна.

Hrebenikova Olena, Candidate of Sciences (Economic), Associate Professor, Associate Professor of the Management and Business Administration Department, National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine.

ORCID ID: https://orcid.org/0000-0003-2695-4630

e-mail: o.grebenikova@khai.edu

[2] **Денисова Тетяна Володимирівна,** канд. техн. наук, доцент, доцент кафедри економіко-математичного моделювання, Харківський національний економічний університет імені Семена Кузнеця, м. Харків, Україна.

Denysova Tetiana, Candidate of Sciences (Technical), Associate Professor, Associate Professor of the Economic and Mathematical Modeling Department, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine.

ORCID ID: https://orcid.org/0000-0001-7254-0901

e-mail: tetiana.denysova@hneu.net

ЧАСОПИС ЕКОНОМІЧНИХ РЕФОРМ №4(60)/2025 ISSN 2221-8440

implementation of the proposed measures will allow enterprises not only to adapt to challenges but also to develop effectively. Further research should be directed to studying the tools for evaluating the effectiveness of digital security.

Keywords:
economic security, cybersecurity, strategic management, digital economy, digitalization, blockchain, artificial intelligence, geopolitical threats.

СТРАТЕГІЧНІ НАПРЯМКИ ВДОСКОНАЛЕННЯ МЕХАНІЗМУ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМНИЦТВА В КОНТЕКСТІ ПІДВИЩЕННЯ ЦИФРОВАННОСТІ СОЦІАЛЬНО-ЕКОНОМІЧНИХ ПРОЦЕСІВ

Постановка проблеми. В умовах динамічної цифровізації та зростання геополітичних загроз питання економічної безпеки підприємництва набуває особливої гостроти. Сучасні підприємства стикаються з комплексом нових ризиків, де традиційні методи захисту вже не забезпечують необхідної ефективності. Виникає нагальна потреба у перегляді підходів до управління безпекою, щоб забезпечити гнучкість та адаптивність бізнесу до швидкозмінних умов цифрової економіки та воєнного стану. *Мета статті* – обґрунтування теоретико-методологічних засад і розробка стратегічних напрямів удосконалення механізму управління економічною безпекою підприємництва в умовах динамічної цифровізації та зростання геополітичних загроз. *Об'єктом дослідження* є система управління економічною безпекою суб'єктів підприємництва в умовах цифрових трансформацій. *Методи, використані в дослідженні:* у роботі застосовано загальнонаукові методи: аналізу та синтезу (для вивчення теоретичного базису та ідентифікації цифрових ризиків), системний підхід (для формування екосистемного бачення безпеки), методи узагальнення (для систематизації технологій захисту) та порівняння. *Основною гіпотезою дослідження* є припущення, що інтеграція інноваційних цифрових інструментів у стратегію управління та розвиток цифрових компетенцій персоналу є ключовими факторами забезпечення стійкості підприємства перед сучасними гібридними загрозами. *Виклад основного матеріалу.* У статті проаналізовано вплив цифровізації на архітектуру економічної безпеки підприємства. Ідентифіковано ключові цифрові ризики та виклики воєнного часу. Розглянуто можливості використання сучасних технологій, зокрема блокчейну та аналітики даних, для захисту бізнес-процесів. Обґрунтовано важливість формування цифрової культури безпеки та впровадження проактивних методів управління ризиками. Запропоновано стратегічні напрями, що охоплюють як технологічні, так і організаційні аспекти захисту. *Оригінальність та практична значимість дослідження* полягає в розробці стратегічних напрямів удосконалення механізму управління безпекою, які дозволяють сформувати адаптивну систему захисту. Запропоновані авторами статті підходи можуть бути використані керівниками підприємств для підвищення резильєнтності бізнесу та отримання конкурентних переваг у цифровому середовищі. *Висновки та перспективи подальших досліджень*: визначено головні цифрові загрози економічній безпеці підприємства та доведено, що надійний захист гарантує інтеграція сучасних технологій (блокчейн, штучний інтелект) у систему управління. Встановлено, що цифрові інструменти дозволяють виявляти ризики ще до їхнього настання (предиктивний підхід). Реалізація запропонованих заходів дозволить підприємствам не лише адаптуватися до викликів, але й ефективно розвиватися. Подальші дослідження доцільно спрямувати на вивчення інструментів оцінки ефективності цифрової безпеки.

Ключові слова:
економічна безпека, кібербезпека, стратегічне управління, цифрова економіка, цифровізація, блокчейн, штучний інтелект, геополітичні загрози.

Formulation of the problem. In the current context of global digital transformation, economic processes are undergoing a fundamental change, which creates new challenges for the economic security of entrepreneurship. Digitalization significantly influences business models, the competitive environment, and enterprise operations, generating both new opportunities and threats. The pace of innovation and technological change in the global economy is continually increasing, leading to new forms of competition, radical shifts in market structures, and transformation of value chains. The protection of digital assets, intellectual property, and data which are becoming key drivers of competitiveness in the modern economy has therefore acquired special significance.

The COVID-19 pandemic has significantly accelerated digitalization and demonstrated the critical importance of digital resilience for enterprises to ensure their continuous operation. The full-scale war in Ukraine highlighted the

ЧАСОПИС ЕКОНОМІЧНИХ РЕФОРМ № 4(60)/2025 ISSN 2221-8440

ЧАСОПИС ЕКОНОМІЧНИХ РЕФОРМ №4(60)/2025 ISSN 2221-8440

urgent need to secure enterprises' economic assets under conditions of military operations, where businesses face physical destruction of assets, cyberattacks as part of hybrid warfare, forced relocations, and the necessity of rapid adaptation to extreme conditions. Martial law posed unique challenges to Ukrainian enterprises regarding the preservation of digital infrastructure, protection of strategically critical data from cyberattacks, and continuity of business processes under air alerts and limited access to electricity. Ukrainian businesses have demonstrated an unprecedented level of digital resilience and adaptability, providing a unique experience in integrating security protocols under emergency conditions, which can offer valuable lessons for the global business community.

Analysis of recent research and publications. Geopolitical conflicts and global economic instability increase the vulnerability of businesses to cyberattacks, information manipulations, and strategic economic threats. The growing dependence of enterprises on digital platforms, cloud services, and global information systems creates new risks associated with possible failures, data leaks, or interferences in the operation of digital infrastructure. In such conditions, traditional approaches to managing corporate economic security require substantial rethinking and improvement, since they are unable to effectively respond to the challenges of the digital era in conditions of heightened geopolitical and military threats. The formation of a new mechanism for managing economic security should be based on the principles of adaptability, proactivity, and systemic integration of security functions into the general strategy of digital transformation of the enterprise, with a special emphasis on resilience in conditions of crisis situations and external shocks.

The issues of economic security of entrepreneurship in the conditions of digitalization are actively researched in modern scientific literature, which reflects the relevance of this direction for the theory and practice of management. Theoretical and methodological aspects of transforming the concept of economic security in the conditions of the digital economy are investigated in the works of Z. S. Varnaliy [1] and S. I. Melnyk [2], who emphasize the necessity of expanding the traditional understanding of economic security taking into account new digital threats. The authors of the monograph [3] develop a systemic approach to economic security, integrating the digital dimension as an integral component of the modern security system of the enterprise.

The evolution of these perspectives in a global context is explored in the works of Xiaojuan Jiang [4]. The researcher proposes the concept of «digital economic security», which reflects the specifics of ensuring business resilience in conditions of digital transformation. In turn, a group of researchers led by A. Bharadwaj [5] examines the issue of integrating digital strategy and business security, emphasizing the necessity of a holistic approach to managing digital risks.

In the works of O. Kravchenko, O. Havryliuk, O. Chelombitko, S. Boiko [6], V. Proskura, T. Chernychko, D. Veretskyi [7], V. Y. Bakai [8], O. Obramych [9], Yu. Nieustroiev, T. Yehorova-Hudkova, V. Ostrianko [10], I. I. Kulchytskyi [11], A. Chaikina, O. Maslii, A. Cherviak [12], and A. V. Harahulia [13], special attention is paid to the issues of digitalization and cybersecurity as components of economic security.

A significant contribution to the development of mechanisms for managing the economic security of enterprises in the conditions of digital transformation was made by Ukrainian scientists S. V. Saloid [14], N. S. Pryimak, O. V. Deviatkova [15], O. M. Liashenko [16], V. V. Baidala, A. V. Yakymovska [17], and M. O. Hutnichenko [18], who proposed conceptual models for adaptive security management by integrating digital monitoring and response tools.

In the international scientific discourse, significant attention is paid to blockchain technologies as a tool for ensuring security. Research by T. Kukman and S. Gričar [19] demonstrates the potential of blockchain for protecting intellectual property and ensuring the transparency of supply chains. The work of R. Rahul [20] reveals methodological aspects of integrating blockchain into economic security management systems. The authors of the study [21] analyze the role of public-private partnership in ensuring cybersecurity and protecting critical infrastructure, while L. Judijanto [22] investigates the influence of regulatory mechanisms on the development of economic security systems in the digital era.

The analysis of scientific publications indicates the active development of theoretical and methodological foundations of managing the economic security of entrepreneurship in the conditions of digitalization. At the same time, there is a need for systematization and deepening of research regarding the formation of a compre-

hensive mechanism for managing economic security, which would integrate traditional approaches and innovative digital tools, take into account the specifics of business functioning in conditions of geopolitical instability and military conflicts, and also ensure the flexibility and adaptability of the enterprise to the rapidly changing conditions of the digital economy.

The purpose of this research is the substantiation of theoretical and methodological foundations and the development of strategic directions for improving the mechanism of managing the economic security of entrepreneurship in the conditions of dynamic digitalization and increasing geopolitical threats.

Presentation of the main material. The existing scientific developments form a theoretical basis for further research, however, they require development in the direction of practical implementation and adaptation to the specific conditions of functioning of Ukrainian enterprises during the war and post-war recovery.

Digitalization of socio-economic processes causes the emergence of new challenges in the system of managing the economic security of business entities. Classical threats are significantly transformed under the influence of the integration of digital technologies, which determines the necessity of modification of existing mechanisms of ensuring economic stability. Among the key risks, the following can be highlighted:

- escalation of cyber threats, in particular unauthorized access to digital assets, confidential data, and trade secrets;
- exacerbation of competitive struggle in the digital environment;
- acceleration of technological obsolescence;
- growth of dependence on digital platforms and ecosystems;
- vulnerability of intellectual property rights in the context of liberalization of information flows;
- complexity of timely adaptation to rapid technological changes;
- growth of the level of dependence of operational activity on the functioning of digital infrastructure.

The mentioned factors determine the actualization of tasks of preventing cybercrime, in particular counteracting unauthorized penetration into corporate databases, which is a priority direction of activity of the system of economic security of the enterprise.

The modern understanding of the economic security of entrepreneurship should be based on the principles of dynamic resilience, which envisages not only protection against threats, but also the ability to effectively use the opportunities of the digital environment for development.

The digital transformation of mechanisms of managing the economic security of the enterprise covers several key directions. Firstly, it is the implementation of digital technologies for monitoring and analysis of threats to economic security. Secondly, it is the development of systems of information protection and cybersecurity for the preservation of digital assets of the enterprise. Thirdly, it is the formation of digital competencies of personnel involved in the processes of managing economic security. These directions correspond to the tasks of the system of economic security regarding the formation of effective informational-analytical support and intensive use of the innovative toolkit.

An important aspect of the transformation of mechanisms of managing economic security in the digital era is also the integration of these mechanisms with the general system of enterprise management. Management of economic security should become an integral part of general management, aimed at the optimization of main production processes and ensuring the competitiveness of the enterprise. This requires the development and implementation of integrated management systems, which ensure effective interaction of various functional subsystems of the enterprise and allow responding promptly to changes in the internal and external environment.

The main strategic directions for improving the mechanism of managing economic security, their essence and expected results are presented in Table 1.

One of the key strategic directions of improving the mechanism of managing the economic security of entrepreneurship in the conditions of digitalization is the implementation of innovative technologies. This direction envisages the use of modern information technologies for the automation of processes of monitoring, analysis, and forecasting of threats to economic security, transforming traditional approaches to the protection of business processes and creating new opportunities for ensuring stability and competitiveness.

ЧАСОПИС ЕКОНОМІЧНИХ РЕФОРМ № 4(60)/2025 ISSN 2221-8440

ЧАСОПИС ЕКОНОМІЧНИХ РЕФОРМ №4(60)/2025 ISSN 2221-8440

Table 1 – Main strategic directions for improving the mechanism of managing economic security in the conditions of digitalization

Strategic direction	Key measures	Expected results
Development of digital competencies and organizational security culture	1. Implementation of programs for the development of digital skills of personnel. 2. Formation of cybersecurity culture at all levels of the organization. 3. Creation of a system of continuous learning and adaptation to digital innovations. 4. Development of mechanisms of personnel motivation regarding compliance with security protocols.	1. Increasing resilience to social engineering and the human factor in security incidents. 2. Growth of the efficiency of using digital protection tools. 3. Formation of a proactive approach to detection and prevention of threats.
Integration of security systems with business processes based on digital technologies	1. Implementation of intelligent systems for monitoring and early detection of threats. 2. Automation of processes of response to security incidents. 3. Integration of security systems into a single digital contour of enterprise management. 4. Development of adaptive models of risk management based on data analytics.	1. Reduction of the time of detection and neutralization of threats. 2. Optimization of costs for ensuring security. 3. Increasing transparency and manageability of the security system.
Transition to a proactive model of ensuring economic security	1. Implementation of predictive analytics for forecasting threats. 2. Development of response scenarios to potential crisis situations. 3. Creation of a system of continuous assessment and adaptation of the security strategy. 4. Formation of mechanisms of stress testing of the business model.	1. Reduction of the probability of realization of critical threats. 2. Increasing the strategic flexibility of the enterprise. 3. Reduction of potential losses from security incidents.
Development of the ecosystem approach to economic security	1. Creation of industry alliances on security issues. 2. Formation of joint platforms for data exchange on threats. 3. Development of security standards for digital ecosystems. 4. Development of public-private partnership in the sphere of cybersecurity.	1. Increasing the collective resilience of the entrepreneurial environment. 2. Optimization of resources for counteracting systemic threats. 3. Formation of joint mechanisms of response to crisis situations.

Source: developed by the authors based on the materials [4] – [9]

The main strategic directions of the application of innovative technologies for ensuring the economic security of enterprises at the modern stage of the development of digital technologies are:

- artificial intelligence and machine learning, which allow automating the processes of threat detection, analyzing large volumes of data for risk forecasting, and optimizing managerial decision-making at enterprises. Algorithms can detect anomalies in financial operations, predict potential crisis situations, and form recommendations regarding risk minimization;
- blockchain technologies, which ensure transparency and security of financial transactions, protect intellectual property, and create immutable records of business operations. This is especially important for confirming the authenticity of documents and preventing fraud;
- cloud computing, which provides flexible and scalable solutions for data storage with a high level of protection, ensures access to infor-

mation from any point of the world and reduces costs for IT infrastructure.

The opportunities and practical recommendations regarding the application of modern innovative technologies in the system of the economic security of entrepreneurship are presented in Table 2.

Table 2 – Innovative technologies in the system of the economic security of entrepreneurship

Type of innovative technologies	Opportunities for application	Practical recommendations
Artificial intelligence (AI) and machine learning	Intelligent analysis of anomalies in business processes. Automated detection of fraudulent actions. Forecasting of security incidents based on historical data. Optimization of the allocation of protection resources.	Implementation of pilot projects using AI for risk analysis. Development of hybrid decision-making models (human and AI). Gradual integration of AI solutions into existing security systems.
Blockchain technologies	Protection of the integrity of critical data. Ensuring the transparency of supply chains. Protection of intellectual property. Secure execution of smart contracts.	Identification of business processes for which the use of blockchain is appropriate. Assessment of the cost-benefit ratio of implementation. Integration with existing security systems.
Big Data technologies	Comprehensive analysis of the external environment and threat detection. Assessment of reputational risks based on social media analysis. Monitoring of market anomalies and the competitive environment. Creation of dynamic risk profiles.	Development of data architecture for effective analysis of security threats. Formation of interdisciplinary teams of analysts. Ensuring ethical use of data and compliance with privacy requirements.

Source: developed by the authors based on the materials [4] – [13], [19] – [22]

An important aspect of implementing innovative technologies is the development of cybersecurity systems that ensure the protection of an enterprise's information assets against both external and internal threats. Contemporary cybersecurity systems effectively address tasks such as preventing infiltration by competitors' economic intelligence structures, counteracting unauthorized access to the enterprise's virtual databases for criminal purposes, and ensuring the protection of confidential information and trade secrets. The implementation of these systems requires the development of appropriate organizational and technical solutions, as well as training personnel in the fundamentals of cybersecurity. Contemporary cybersecurity systems employ behavioural analysis, biometric authentication, and multi-layered protection mechanisms. Zero Trust architecture technologies involve continuous verification of all users and devices, which significantly strengthens the security of corporate networks.

The development of information and analytical support for the economic security system is an important strategic direction for improving the mechanism of management of the economic security of entrepreneurship in the context of digitalization. This direction entails the creation of an effective system for collecting, analyzing, and utilizing information to make managerial decisions aimed at ensuring economic security. The foundation of such a system should be comprehensive monitoring of the enterprise's external and internal environment, which ensures the timely identification of threats and opportunities to enhance the level of economic security. Effective information and analytical support enables the economic security system to perform tasks such as assessing and analyzing the enterprise's key risks, as well as forecasting its level of protection.

ЧАСОПИС ЕКОНОМІЧНИХ РЕФОРМ № 4(60)/2025 ISSN 2221-8440

ЧАСОПИС ЕКОНОМІЧНИХ РЕФОРМ №4(60)/2025 ISSN 2221-8440

The integration of digital tools into preventive and crisis management mechanisms is an important direction for improving the mechanism of management of the economic security of entrepreneurship in the context of digitalization. This direction involves the implementation of digital technologies to enhance the efficiency of threat detection and prevention for economic security, as well as to minimize the consequences of crises that have already occurred. Digital tools enable the automation of threat monitoring and analysis, ensuring timely detection of potential issues and facilitating the development of preventive measures. This is especially important in the context of digitalization, where the speed of changes in the external environment significantly increases, and traditional monitoring methods no longer provide the required operational efficiency.

The formation of a digital security ecosystem for entrepreneurship is an important direction for improving the mechanism of management of economic security in the context of digitalization. The foundation of such an ecosystem is the effective exchange of information on threats and security incidents, as well as the joint development and implementation of methods and tools to counter these threats. This approach allows enterprises to receive up-to-date information on new types of threats and effective methods for their neutralization, which is especially important in the context of the rapid development of digital technologies and the continuous evolution of cyber risks.

An important component of the digital security ecosystem is the partnership between enterprises and specialized organizations that provide services in the field of economic security. These organizations can supply enterprises with up-to-date information on threats, conduct security system audits, provide consulting services, and so forth. Such partnerships enable enterprises to gain access to expert knowledge and resources that they cannot provide on their own. They also contribute to the formation of standards and best practices in the field of economic security, which can be implemented within enterprises.

The digital security ecosystem also involves cooperation with government bodies responsible for ensuring economic security at the national level. Such cooperation may include the exchange of information on threats, joint development of mechanisms to counter these threats, as well as participation in the formation of the regulatory framework in the field of economic security. Government bodies can also provide enterprises with information on the overall state of economic security in the country and the main trends in this area, which helps enterprises better prepare for potential threats. This form of interaction aligns with the principles of economic security management, which involve the engagement of various actors to enhance the overall level of security.

Conclusions and prospects for further research. The intensification of digitalization of socio-economic processes creates fundamentally new challenges for the economic security of entrepreneurship, requiring a systemic rethinking and improvement of management mechanisms. The proposed strategic directions make it possible to form an adaptive economic security system capable not only of countering the threats of the digital age but also of leveraging new opportunities to strengthen competitiveness.

The key success factors in implementing strategic changes are: the integration of security functions into the enterprise's overall digital strategy, the development of digital competencies and a security culture, a proactive approach to risk management, the utilization of the potential of innovative technologies, and ecosystem-based interaction with partners and stakeholders.

The implementation of the proposed strategic directions will enable enterprises not only to adapt to the challenges of the digital economy but also to gain competitive advantages through enhancing the resilience and adaptability of their business models.

References

1. Varnaliy, Z. S. (2020). *Economic and financial security of Ukraine in the conditions of globalization* : monohrafiia / Kyiv. nats. un-t im. Tarasa Shevchenka. Kyiv: Znannia Ukrainy, 423.

2. Melnyk, S. I. (2020). *Management of financial security of enterprises: theory, methodology, practice* : monohrafiia. Lviv: Rastr-7, 384.

3. Sytnyk, H. V., Blakyta, H. V., Huliaieva, N. M., et al. (2020). *Economic security of entrepreneurship in Ukraine* : monohrafiia. Kyiv: Kyiv. nats. torh.-ekon. un-t, 284 s.

4. Jiang, X. (2020). Digital economy in the post-pandemic era. *Journal of Chinese Economic and Business Studies*, 18(4), 333-339. https://doi.org/10.1080/14765284.2020.1855066.

5. Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., and Venkatraman, N. (2022). Digital Business

Strategy: Toward a Next Generation of Insights. *MIS Quarterly*, 37(2), 471-482.

6. Kravchenko, O., Havryliuk, O., Chelombitko, O., and Boiko, S. (2024). Management of economic security of enterprises in the conditions of the digital economy. *Adaptyvne upravlinnia: teoriia i praktyka. Seriia Ekonomika*, 19(38). https://doi.org/10.33296/2707-0654-19(38)-12.

7. Proskura, V., Chernychko, T., and Veretskyi, D. (2024). Modern approaches to determining the level of economic security of the enterprise in the conditions of digitalization. *Tsyfrova ekonomika ta ekonomichna bezpeka*, 4(13), 61-67. https://doi.org/10.32782/dees.13-9.

8. Bakay, V. Y. (2020). Ensuring the economic security of the enterprise based on the use of digital technologies. *Visnyk Khmelnytskoho natsionalnoho universytetu. Ekonomichni nauky*, 4(1), 32-35. https://doi.org/10.31891/2307-5740-2020-284-4-5.

9. Obramych, O. (2024). Peculiarities of forming digital security at the enterprise. *Ekonomika ta suspilstvo*, (68). https://doi.org/10.32782/2524-0072/2024-68-20.

10. Neustroiev, Yu. H., Yehorova-Hudkova, T. I., and Ostrianiko, V. V. (2020). Analysis of the influence of digitalization of the economy on the state's economic security system. *Vcheni zapysky Universytetu «KROK»*, 4(60), 202-209. https://doi.org/10.31732/2663-2209-2020-60-202-209.

11. Kulchytskyi, I. I. (2024). Digital economy and economic security of the enterprise: management strategies. *Aktualni pytannia ekonomichnykh nauk*, (6). https://doi.org/10.5281/zenodo.14575016.

12. Chaikina, A., Masliy, O., and Cherviak, A. (2024). Modern drivers of increasing economic security of the country in the conditions of digital transformation. *Stalyi rozvytok ekonomiky*, 2(49), 307-313. https://doi.org/10.32782/2308-1988/2024-49-49.

13. Harahulia, A. V. (2024). *Management of financial and economic security of business in the system of the global information environment* (Doctoral dissertation). Admiral Makarov National University of Shipbuilding, Mykolaiv.

14. Saloid, S. V. (2017). Mechanism of economic security management of the enterprise: theoretical aspect. *Ekonomichnyi visnyk Natsionalnoho tekhnichnoho universytetu Ukrainy «Kyivskyi politekhnichnyi instytut»*, (14), 250-254.

15. Pryimak, N. S., Devyatkova, O. V. (2022). Strategic management of economic security of the enterprise: theoretical foundations and tools. *Visnyk DonNUET. Seriia: Ekonomichni nauky*, 1(76), 37-45. https://doi.org/10.33274/2079-4819-2022-76-1-37-45.

16. Liashenko, O. M. (2015). Conceptualization of economic security management of the enterprise (2nd ed., rev.). NISD. Retrieved from https://niss.gov.ua/sites/default/files/2015-10/lyashenko_1_druk-43fc7.pdf (Access date: 12 September 2025)

17. Baydala, V. V., Yakymovska, A. V. (2023). Strategic management of economic security of enterprises. *Ukrainskyi zhurnal prykladnoi ekonomiky ta tekhniky*, 8(3), 241-245. https://doi.org/10.36887/2415-8453-2023-3-36.

18. Hutnichenko, M. O. (2024). Mechanism of economic security management of the enterprise. *Aktualni problemy staloho rozvytku*, 1(2), 7-12. https://doi.org/10.60022/2(2)-1SD.

19. Kukman, T., Gričar, S. (2025). Blockchain for Quality: Advancing Security, Efficiency, and Transparency in Financial Systems. *FinTech*, 4(1), 7. https://doi.org/10.3390/fintech4010007.

20. Ranjan, R. (2020). Integrating blockchain principles into enterprise systems: potential gains and associated risk. *International Journal of Innovation Studies*, 4(3), 57-67.

21. Sharma, M., Sajud, E., Goklani, N., and Chaubey, K. (2025). Public-Private Partnerships in Cybersecurity: A Strategic Approach to National Threat Management. *Journal of Electrical Systems*, 21(1), 974-988. https://doi.org/10.52783/jes.9148.

22. Judijanto, L. (2025). Challenges of economic law in the global and digital era: analysing regulation, data protection, and cybersecurity through a literature review. *International Journal of Financial Economics*, 2(1), 144-152.

Перелік використаних джерел

1. Варналій З. С. *Економічна та фінансова безпека України в умовах глобалізації* : монографія / Київ. нац. ун-т ім. Тараса Шевченка. Київ : Знання України, 2020. 423 с.

2. Мельник С. І. *Управління фінансовою безпекою підприємств: теорія, методологія, практика*: монографія. Львів: Растр, 2020. 384 с.

3. *Економічна безпека підприємництва в Україні* : монографія / Г. В. Ситник, Г. В. Блакита, Н. М. Гуляєва та ін. Київ : Київ. нац. торг.-екон. ун-т, 2020. 284 с.

4. Jiang X. Digital economy in the post-pandemic era. *Journal of Chinese Economic and Business Studies*. 2020. Vol. 18, No. 4. P. 333–339. https://doi.org/10.1080/14765284.2020.1855066.

5. Bharadwaj A., El Sawy O. A., Pavlou P. A., Venkatraman N. Digital Business Strategy: Toward a Next Generation of Insights. *MIS Quarterly*. 2022. Vol. 37, № 2. P. 471-482.

ЧАСОПИС ЕКОНОМІЧНИХ РЕФОРМ № 4(60)/2025 ISSN 2221-8440

6. Управління економічною безпекою підприємств в умовах цифрової економіки / О. Кравченко, О. Гаврилюк, О. Челомбітько, С. Бойко. *Адаптивне управління: теорія і практика. Серія Економіка*. 2024. Т. 19, Вип. 38. https://doi.org/10.33296/2707-0654-19(38)-12.

7. Проскура В., Черничко Т., Верецький Д. Сучасні підходи до визначення рівня економічної безпеки підприємства в умовах цифровізації. *Цифрова економіка та економічна безпека*. 2024. № 4 (13). С. 61-67. https://doi.org/10.32782/dees.13-9.

8. Бакай В. Й. Забезпечення економічної безпеки підприємства на основі використання цифрових технологій. *Вісник Хмельницького національного університету*. *Економічні науки.* 2020. № 4, Т. 1. С. 32-35. https://doi.org/10.31891/2307-5740-2020-284-4-5

9. Обрамич О. Особливості формування цифрової безпеки на підприємстві. *Економіка та суспільство*. 2024. Вип. 68. https://doi.org/10.32782/2524-0072/2024-68-20.

10. Нєустроєв Ю. Г., Єгорова-Гудкова Т. І., Острянко В. В. Аналіз впливу цифровізації економіки на систему економічної безпеки держави. *Вчені записки Університету «КРОК»*. 2020. № 4 (60). С. 202-209. https://doi.org/10.31732/2663-2209-2020-60-202-209.

11. Кульчицький І. І. Цифрова економіка та економічна безпека підприємства: стратегії управління. Актуальні питання економічних наук. 2024. Вип. 6. https://doi.org/10.5281/zenodo.14575016.

12. Чайкіна А., Маслій О., Черв'як А. Сучасні драйвери підвищення економічної безпеки країни в умовах цифрової трансформації. *Сталий розвиток економіки*. 2024. № 2 (49). С. 307-313. https://doi.org/10.32782/2308-1988/2024-49-49.

13. Гарагуля А. В. Управління фінансово-економічною безпекою бізнесу в системі глобального інформаційного середовища : дис. … д-ра філос. : 073 «Менеджмент» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв, 2024. 207 с.

14. Салоїд С. В. Механізм управління економічною безпекою підприємства: теоретичний аспект. *Економічний вісник Національного технічного університету України «Київський політехнічний інститут»*. 2017. № 14. С. 250-254.

15. Приймак Н. С., Дев'яткова О. В. Стратегічне управління економічною безпекою підприємства: теоретичні основи та інструментарій. *Вісник ДонНУЕТ. Серія: Економічні науки.* 2022. № 1 (76). С. 37-45. https://doi.org/10.33274/2079-419-2022-76-1-37-45.

16. Ляшенко О. М. *Концептуалізація управління економічною безпекою підприємства* : монографія. 2-ге вид., переробл. Київ : НІСД, 2015. 348 с.

17. Байдала В. В., Якимовська А. В. Стратегічне управління економічною безпекою підприємств. *Український журнал прикладної економіки та техніки*. 2023. Т. 8, № 3. С. 241-245. https://doi.org/10.36887/2415-8453-2023-3-36.

18. Гутніченко М. О. Механізм управління економічною безпекою підприємства. *Актуальні проблеми сталого розвитку*. 2024. Т. 1, № 2. С. 7-12. https://doi.org/10.60022/2(2)-1SD.

19. Kukman T., Gričar S. Blockchain for Quality: Advancing Security, Efficiency, and Transparency in Financial Systems. *FinTech*. 2025. Vol. 4, № 1. P. 7. https://doi.org/10.3390/fintech4010007.

20. Ranjan R. Integrating blockchain principles into enterprise systems: potential gains and associated risk. *International Journal of Innovation Studies*. 2020. Vol. 4, № 3. P. 57-67.

21. Sharma M., Sajud E., Goklani N., Chaubey K. Public-Private Partnerships in Cybersecurity: A Strategic Approach to National Threat Management. *Journal of Electrical Systems*. 2025. Vol. 21, № 1. P. 974-988. https://doi.org/10.52783/jes.9148.

22. Judijanto L. Challenges of economic law in the global and digital era: analysing regulation, data protection, and cybersecurity through a literature review. *International Journal of Financial Economics*. 2025. Vol. 2, № 1. P. 144-152.

Стаття надійшла до редакції : 27.09.2025 р.

Стаття прийнята до друку: 27.10.2025 р.

Стаття опублікована: 30.12.2025 р.

Бібліографічний опис для цитування :

Hrebenikova O., Denysova T. Strategic directions for improving the mechanism of managing the economic security of entrepreneurship in the context of increasing digitalization of socio-economic processes. *Часопис економічних реформ*. 2025. № 4(60). С. 12–20.