УДК 330.131.7:004.9:005.334

S. Muravskyi
R. Tolpezhnikov

METHODOLOGICAL APPROACHES TO ASSESSING ENTERPRISE ECONOMIC SECURITY IN THE CONTEXT OF DIGITAL TRANSFORMATION

The article provides an analysis of methodological approaches to assessing the economic security of enterprises in the context of digital transformation. Traditional approaches were largely developed before digital technologies became a central element of the business environment. As a result, they insufficiently reflect digital risks such as cyberattacks, data breaches, technological failures, and vulnerabilities arising from the use of cloud services, automation, artificial intelligence, and IoT systems. The paper highlights recent research trends that integrate digital factors into economic security assessment. Based on the analysis, the study proposes directions for modernizing existing methodologies. The findings emphasize the need to update traditional methodologies to ensure a more accurate and comprehensive assessment of enterprise economic security under conditions of accelerating digital transformation.

Keywords: *economic security, digital transformation, methodological approaches, digital risks, risk-oriented assessment, information security, cybersecurity frameworks, assessment indicators.*

DOI 10.34079/2518-1394-2025-15-30-136-145

Problem statement. Modern business is undergoing fundamental changes under the influence of the Fourth Industrial Revolution, which is characterized by widespread digitalization, the development of artificial intelligence, big data, and the Internet of Things (IoT). In this context, the issue of economic security goes far beyond the traditional protection of assets and ensuring financial stability. Modern enterprises face a combination of both traditional and emerging threats to economic security.

Digital transformation of business, on the one hand, opens new opportunities for improving efficiency, but on the other – creates new challenges in the field of security. In particular, the rapid introduction of digital technologies is accompanied by cyber threats and risks related to information security, data management, process automation, and other factors. Scientific publications of recent years demonstrate increased attention to the digital dimension of economic security. However, most existing methodologies either do not integrate the digital factor at all or include it only fragmentarily – primarily as components of information security (Дергалюк, 2023). At the same time, digital transformation affects all components of economic security: financial, personnel, operational, technological, and intellectual. This leads to the rise of complex and interrelated digital risks that cannot be adequately assessed using traditional approaches (Біличенко та Касьянова, 2023).

The aim of the study is to analyze existing methodological approaches to assessing enterprise economic security, identify their limitations in capturing digital transformation factors, and propose directions for integrating digital risks and cybersecurity considerations into assessment frameworks with a focus on the application of proactive risk management.

Analysis of recent research and publications. Recent years have seen active scientific research in the field of methodological support for enterprise economic security. A review of publications shows the absence of a unified approach: different researchers propose various classifications and methodologies, each with its advantages and limitations. Researchers such as Maltuz V., Maltuz O., Shylo Zh., Krechko M., Koptieva H., Hapeyeva O., Holovko R., and

others emphasize that no methodology has become a generally accepted standard, and the choice of approach depends on business specifics and available data (Малтіз, В. та Малтіз, О., 2022; Шило та Кречко, 2022; Коптєва, 2020; Гапєєва та Головко, 2025). Koptieva H. (2020) also notes that the economic security of an enterprise largely derives from the efficiency and resilience of its business processes. Scientific sources highlight a number of methodological approaches to assessing economic security, including (but not limited to) those described below.

Resource-functional approach. This approach involves assessing the components of the security system by functional areas or resource types (financial, personnel, technological, information security, etc.). For each area, indicator systems are developed regarding resource efficiency, followed by calculation of an integral indicator considering the weight of each group. The advantage of this approach is its comprehensive overview of all aspects of activity. However, the formalization of components and indicators may be subjective and fail to reflect enterprise-specific conditions (Ткаченко та Гречко, 2022).

Economic-mathematical approach. This approach is based on building a mathematical model of the enterprise's economic security level as a function of several variables. It may involve calculating an integral index or an econometric model that predicts security indicators depending on endogenous and exogenous factors. Although considered the most academically grounded, the approach requires reliable data and complex model development. For industrial enterprises, unifying indicators and ensuring comparability is particularly difficult (Насруллаєв, 2025).

Result-oriented approach**.** The result-oriented approach evaluates economic security by comparing actual performance indicators with planned or target values based on strategic and operational goals. A specific variation of this approach is the profit-investment model, where the key criterion of economic security is the ability to generate sufficient profit (net or reinvested profit) to ensure stable functioning and development. However, profit alone does not capture the full range of factors that shape an enterprise economic security, and matching it with overall performance efficiency overlooks structural vulnerabilities and non-financial risks. As a result, the approach may be insufficient in dynamic conditions, especially under digital transformation (Коптєва, 2020).

Indicator (threshold) approach. This approach relies on identifying threshold values for certain indicators – deviations from these values signal deterioration in economic security. Indicators typically include financial, operational, and resource metrics, categorized into critical, acceptable, and optimal levels. Its advantages include simplicity, ease of diagnostics, and suitability for monitoring systems. However, challenges include difficulty in defining universal thresholds for different industries and the failure to capture dynamic threats – particularly digital ones – that evolve faster than norms can be updated (Шило та Кречко, 2022).

Financial state assessment approach. This is one of the most common practical approaches. It evaluates liquidity, solvency, financial stability, profitability, business activity, and capital structure to determine the enterprise's ability to meet obligations, ensure operational continuity, and create financial reserves. Its primary limitation is its orientation exclusively toward financial results, excluding operational, technological, and digital risks (Малтіз, В. та Малтіз, О., 2022).

Program-target approach. This approach views economic security as a result of programs, strategic plans, and measures aimed at threat mitigation. Its limitation is the resource-intensive nature of implementation and insufficient reflection of digital-specific risks (Шило та Кречко, 2022).

Risk-Oriented Approaches. Modern research increasingly highlights risk-management-based approaches to assessing security. These approaches involve identifying, analyzing, and managing key risks, including financial, operational, legal, and – in the context of digital

transformation – cyber risks. They often rely on real-time threat monitoring, incident response analytics, and integrated risk-management platforms (Гапєєва та Головко, 2025).

Traditional approaches largely overlook digital factors. They usually assume stable information environments and thus fail to account for cyber threats, data loss, IoT vulnerabilities, cloud dependencies, and other risks inherent to digitalized operations.

Presenting main material. Analysis of recent publications shows that most traditional methodologies for assessing economic security were developed during periods when digital technologies were not a dominant factor of the business environment. As a result, many approaches implicitly assume a stable information environment or treat it as secondary. For example, indicator-based or financial assessment methods focus primarily on economic and financial indicators (profitability, liquidity, etc.) and may overlook digital risks such as cyberattacks or IT system failures.

However, some approaches initially incorporated elements related to information security. The resource–functional approach, which structures economic security into functional components, usually includes information security as one of the key subsystems alongside financial, personnel, and technological components. This means that the assessment includes the degree of protection of information resources, data security systems, cybersecurity, etc. (Ткаченко та Гречко, 2022). Nevertheless, the level of detail varies, and often the digital factor is represented by only a few indicators (e.g., presence of a security policy, number of security breaches), which do not reflect the complexity of cyber risks.

In recent years, a growing number of studies have focused specifically on the intersection between digital transformation and economic security. The digital factor includes several elements: digital assets (data, software platforms), digital processes (online operations, automated production), new risks (cyber threats, data leaks, technical failures), new opportunities (Big Data analytics, artificial intelligence). Some modern methodological approaches attempt to integrate these elements. The implementation of advanced digital technologies can improve security but simultaneously requires mitigation of new digital risks (Kukhar, Kravchyk and Brechko, 2023).

Digital transformation restructures the economic security system of an enterprise as well. New risk groups emerge (which previously were not as significant): technological, operational, managerial, financial, and privacy-related. These risks negatively affect core subsystems of security: financial, technological, informational, personnel, and intellectual components (Біличенко та Касьянова, 2023). For example, a cyberattack (a technological risk) can simultaneously cause: financial losses, operational shutdown of IT systems, leakage of confidential information, reputational damage and personnel turnover. Thus, digital risks have a cross-functional nature that traditional narrow methodologies cannot fully capture.

This cross-functional impact of digital risks is not merely theoretical but has been demonstrated in multiple real-world incidents. A notable example illustrating the limitations of traditional assessment approaches is the Colonial Pipeline ransomware attack. In May 2021, Colonial Pipeline, which transports 45 % of East Coast fuel, suffered a ransomware attack forcing a six-day shutdown (TechTarget, 2021). Attackers accessed the network through a compromised VPN password lacking multi-factor authentication. The company paid a $ 4.4 million ransom, while US President declared a state of emergency as fuel shortages affected 17 states (Insurica, 2024). Traditional economic security assessments (evaluating financial ratios and operational metrics) would likely have shown satisfactory results prior to the attack. However, these methodologies failed to detect the absence of basic cybersecurity controls. Experts confirmed the attack was preventable but essential protective measures were not in place. This demonstrates that enterprises can exhibit strong conventional security indicators while giving rise to critical digital vulnerabilities detectable only through cyber-specific

assessment metrics. The Colonial Pipeline case, along with similar incidents across various industries, reinforces the arguments regarding the underestimation of digital threats.

International organizations also highlight the underestimation of digital threats by businesses, especially small and medium enterprises. The Organisation for Economic Co-operation and Development (OECD) reports that small firms are significantly less likely to implement formal cybersecurity measures than large enterprises. Only a small share of micro-enterprises maintain cybersecurity policies, whereas the proportion is much higher among large businesses (OECD, 2021). The World Economic Forum (WEF) in its annual Global Risks Report consistently ranks cyber risks among the most serious global business threats. Rising geopolitical tensions further increase the likelihood of large-scale cyberattacks (World Economic Forum, 2023). Those reports signal the necessity of integrating the digital factor into economic security assessment.

Some recent methodologies directly incorporate digital elements, especially within risk-oriented frameworks. These include: probabilistic approach (evaluates the likelihood of risk events and expected losses), value-at-risk (determines the maximum potential loss within a given confidence interval), scenario-based approach (models alternative developments of events and their consequences for the enterprise), risk matrix (classifies threats by probability and level of impact). International practice increasingly employs frameworks such as COSO ERM and NIST Cybersecurity Framework, which offer integrated assessment of operational, financial, and digital risks based on uncertainty management and cyber resilience principles (Kukhar, Kravchyk and Brechko, 2023). Recent studies also highlight approaches based on digital maturity and stress testing, which assess an enterprise's sensitivity to extreme events, including technical failures or cyber incidents (Blakyta, Bogma, Bolduieva, Lukyanov and Shtuler, 2023). These modern approaches are most adaptive to the digital economy because they systematically incorporate new types of threats created by digital transformation.

Table 1

Table summarizes the consideration of digital factors across different methodological approaches

Approach	Essence	Consideration of the Digital Factor
Resource-functional	Assessment of the state of individual security components (financial, personnel, technological, informational, etc.) followed by integration of results	Partially – information security is included, but digital risks are insufficiently detailed
Economic-mathematical	Calculation of an integral safety index or econometric model based on a set of indicators	Partially – digital variables may be integrated, but initially not assumed
Result-oriented	Security is assessed based on the ability of an enterprise to generate profit and reinvest it into development and protection	No – ignores digital infrastructure, data, cyber risks
Indicator (threshold)	Assessment of the degree to which actual indicators meet planned and strategic targets	No – digital risks are not included
Financial condition-based	Measurement of safety using liquidity, solvency, capital structure, etc.	No – digital factors are excluded
Program-target	Assessment through the implementation of strategic programs and planned measures	Partially – digitalization can be integrated at a strategic level
Risk-oriented	Identification, assessment, and management of risks	Yes – some approaches integrate digital risks

Overall, the current methodological landscape for assessing the economic security of enterprises can be described as transitional. It is gradually shifting from fragmented, narrowly

focused approaches toward more comprehensive and integrated models that better reflect the realities of the digital age. Many traditional methodologies still do not fully account for the "digital dimension" (see Table 1), although recent research increasingly identifies this gap and offers solutions aimed at updating or expanding established approaches. Newer studies begin to fill this void by proposing methodological adjustments or by developing new frameworks centered on digital risks and the consequences of digital transformation. Another critical area for enhancement is the adoption of a proactive risk management approach rather than a purely reactive one.

One of the key directions for improving classical methodologies is the modernization of the resource-functional approach. This modernization requires a more detailed examination of the information-technological component of economic security. In practical terms, this involves conducting deeper diagnostics of the enterprise's information security, including the state of its IT infrastructure, network protection mechanisms, backup and redundancy systems, and the digital competencies of personnel. The methodological tools used to assess this component can be significantly strengthened by adopting internationally recognized cybersecurity frameworks such as the NIST Cybersecurity Framework, which provides structured standards for evaluating cybersecurity maturity and resilience. Their integration into the assessment process would allow economic security evaluations to reflect both technological preparedness and vulnerability to cyber threats.

Another essential enhancement relates to indicator-based and economic-mathematical approaches. To adequately capture the influence of digital transformation, the set of indicators used within these methodologies could be expanded to include metrics that reflect digital and cybersecurity-related aspects (Насруллаєв, 2025). Such indicators might include the number of cybersecurity incidents detected over a given period, the average recovery time of IT systems after failures, the proportion of the IT budget directed toward security, or the presence of relevant certifications such as ISO 27001. Establishing benchmark or threshold values for these indicators makes it possible not only to evaluate traditional financial or operational vulnerabilities but also to detect emerging digital threats proactively.

A further avenue for improvement lies in strengthening methodologies that historically did not incorporate explicit risk evaluation. These methodologies should be supplemented with elements of digital risk management. The assessment of economic security must therefore include the identification of digital risks, their qualitative and quantitative evaluation, and the introduction of continuous monitoring practices (Біличенко та Касьянова, 2023). This encompasses risks such as cyberattacks, ransomware, data breaches, cloud service disruptions, vulnerabilities in AI systems, and failures of IoT-enabled processes. Such an expanded evaluation should analyze both the probability of risks and their financial and operational consequences, while also incorporating real-time monitoring supported by analytical tools or digital dashboards. In practice, this can take the form of a digital risk module integrated into the broader system of economic security assessment.

In addition to integrating new risk factors, there is a broad consensus that enterprises should move toward a proactive risk management approach in economic security. Historically, many organizations have been reactive – addressing risks and threats only after they manifest. Proactive risk management, by contrast, is an ongoing, forward-thinking process that identifies potential risks before problems arise. It seeks to minimize disruptions by taking preventive actions and preparedness measures so that threats are mitigated before they snowball into major challenges. Some international frameworks reinforce the importance of proactivity. The COSO ERM emphasizes integrating risk with strategy and performance and addressing emerging risks, while the NIST Framework explicitly highlights continuous govern / identify / protect activities to prevent and prepare for cybersecurity incidents. Rather than being purely reactive, it guides organizations to anticipate and address risks head-on, turning potential challenges into

opportunities where possible (Kukhar, Kravchyk and Brechko, 2023). It embeds risk management into organizational governance and strategy, encouraging continuous risk scanning and early action. This standard's principles – such as continual monitoring, periodic review, and integration of risk considerations into decision-making – all serve to institutionalize proactivity. In practice, a proactive approach might include establishing early warning systems (for instance, key risk indicators that trigger alerts when conditions met) and conducting regular scenario analyses to imagine future threat possibilities. Companies like Accenture have noted that in recent years firms are investing more in predictive analytics, artificial intelligence, and threat intelligence to bolster their proactive risk identification capabilities. Such tools can scan for emerging patterns and allow management to respond before an incident fully unfolds (Accenture, 2024).

Digital transformation also provides opportunities to enhance the assessment process itself. Instead of relying solely on periodic manual evaluations, enterprises can transition to automated monitoring systems capable of continuously gathering and analyzing relevant data. These systems can aggregate information from business-process digital platforms, cybersecurity tools, and external threat intelligence sources, enabling real-time identification of deviations from acceptable values. As modern security dashboards increasingly combine financial, operational, and technological indicators, they embody the recommendations found in recent methodological research advocating the development of integrated digital platforms for economic security analysis (Насруллаєв, 2025). This shift transforms the assessment process from a reactive one into a proactive system capable of anticipating and flagging potential threats at early stages.

The assessment of economic security should be supported by broader organizational and strategic measures aimed at enhancing digital resilience. Although such measures apply more directly to ensuring security than to assessing it, incorporating them into methodological frameworks – whether through quantitative indicators or qualitative criteria – makes it possible to more comprehensively evaluate an enterprise's preparedness for digital threats. Research in the field emphasizes the importance of implementing integrated automated management systems, adopting cloud technologies to strengthen IT infrastructure resilience, investing in the digital competencies of personnel and regular cybersecurity training, establishing partnerships for information exchange related to cyber threats, and fostering a corporate culture of adaptability and innovation (Біличенко та Касьянова, 2023). These organizational practices significantly influence the success of digital transformation and must therefore be reflected in any holistic methodology for assessing economic security.

In summary, modernization of traditional methodological approaches should not replace or disregard existing conceptual foundations but rather enrich and adapt them to contemporary conditions. The indicator approach can be updated by expanding the range of indicators, the resource-functional approach can evolve by strengthening the information-technological subsystem, economic-mathematical models can incorporate digital variables, program-target methodologies can embed cybersecurity objectives, and risk-oriented approaches can be supplemented with advanced tools for digital risk analysis and real-time monitoring. Such an integrative strategy preserves the methodological strengths accumulated over previous decades while enabling the assessment of economic security to correspond to the challenges and opportunities created by digital transformation.

Conclusions. The study conducted provides a comprehensive review of modern methodological approaches to assessing the economic security of enterprises and analyzes how these approaches incorporate the digital factor in an era of rapid digital transformation. The literature review covering the period 2020-2025 demonstrates that researches have proposed a wide range of approaches – from indicator-based and resource-oriented methods to integral and risk-oriented models. The scientific community generally agrees that no universal assessment

methodology currently exists. Each approach possesses distinct advantages and limitations, and its applicability depends on the specific characteristics of the enterprise and the objectives of the assessment. At the same time, recent years have seen a clear trend toward methodological integration and a growing emphasis on risk-based assessment tools.

Regarding the integration of the digital factor, several important conclusions arise. Traditional methodologies largely did not focus on digital threats because they were developed before the widespread adoption of digital technologies. Nevertheless, some approaches – particularly functional and systemic ones – have included information security as a component of economic security, although often in a simplified or incomplete form. Present-day research highlights the necessity to rethink existing criteria: cybersecurity, data protection, continuity of digital processes, and the level of digital maturity of the enterprise are increasingly becoming critical indicators of its overall economic security. Emerging risks – ranging from cyberattacks to failures of artificial intelligence systems – have the potential to inflict losses comparable to, or even greater than, traditional financial or operational threats. Consequently, modern economic security assessments must systematically incorporate these factors. Equally important is the incorporation of proactive risk management practices. Relying solely on retrospective analysis can leave enterprises flat-footed in the face of fast-moving crises. By adopting proactive, continuous risk management – as advocated by some modern frameworks – enterprises can detect early warning signs and reinforce their defenses before threats fully materialize.

This article proposes several general directions for integrating the digital factor and proactive risk management into existing methodological approaches. These include expanding indicator systems to incorporate cybersecurity metrics; enhancing the analysis of the information-technological component within functional and systemic models; embedding risk-oriented procedures such as identification and continuous monitoring of risks; introducing automated analytical tools capable of real-time monitoring; and including organizational measures aimed at strengthening digital resilience. These improvements allow traditional methodologies to be updated without discarding their conceptual foundations, thus creating a synergistic effect: preserving methodological continuity while simultaneously addressing the challenges posed by digital transformation. Enterprises that adopt such modernized approaches will be better positioned to identify vulnerabilities, mitigate digital risks, and ensure sustainable development under conditions of ongoing technological change. Consequently, integrating the digital factor into methodological frameworks is not merely desirable but essential for achieving a realistic, comprehensive, and accurate assessment of economic security in today's digital economy.

Бібліографічний список

Біличенко, М. та Касьянова, Н., 2023. Вплив цифрової трансформації на формування системи економічної безпеки підприємства. *Бізнес Інформ*, 7(546), с.83-91. DOI: 10.32983/2222-4459-2023-7-83-91

Гапєєва, О. та Головко, Р., 2025. Особливості формування економічної безпеки підприємств. *Академічні візії*, 40. DOI:10.5281/zenodo.14917627

Дергалюк, Б., 2023. Вплив цифрової трансформації на забезпечення економічної безпеки підприємства. *Економічний вісник НТУУ «Київський політехнічний інститут»*, 26, с.65-68. DOI:10.20535/2307-5651.26.2023.287057

Коптєва, Г., 2020. Класифікація підходів до оцінки економічної безпеки підприємства. *Східна Європа: Економіка, Бізнес та Управління*, 2(25), с.221-229. DOI:10.32782/easterneurope.25-32

Малтіз, В. та Малтіз, О., 2022. Діагностика рівня економічної безпеки підприємства. *Economic Synergy*, 1-2, с.132-140. DOI:10.53920/ES-2022-1;2-10

Насруллаєв, Р., 2025. Методичні підходи до оцінки економічної безпеки підприємства. *Бізнес Інформ*, 7(569), с.338-344. DOI:10.32983/2222-4459-2025-7-338-344

Ткаченко, Т. та Гречко, А., 2022. Узагальнення методичних підходів оцінювання економічної безпеки промислових підприємств. *Економічний вісник НТУУ «Київський політехнічний інститут»*, 22, с.79-82. DOI:10.20535/2307-5651.22.2022.260154

Шило, Ж. та Кречко, М., 2022. Методи оцінки рівня економічної безпеки підприємства: підходи до оцінювання та забезпечення економічної безпеки. *Вісник Національного університету водного господарства та природокористування, серія «Економічні науки»*, 2(98), с.278-288. DOI:10.31713/ve2202224

Accenture, 2024. *Accenture Risk Study: 2024 Edition. Hyper-disruption demands constant reinvention.* [online] Available at: <https://www.accenture.com/content/dam/accenture/final/accenture-com/document-2/Accenture-Risk-Study-2024-Edition.pdf>

Blakyta, H., Bogma, O., Bolduieva, O., Lukyanov and V., Shtuler, I., 2021. Modeling enterprises` economic security in crisis conditions. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, 4, pp.116-121. DOI: 10.33271/nvngu/2021-4/116

Insurica, 2024. *Cyber case study: Colonial Pipeline ransomware attack*. [online] Available at: <https://insurica.com/blog/colonial-pipeline-ransomware-attack>

Kukhar, O., Kravchuk, Y. and Brechko, O., 2023. Digital transformation as a factor in ensuring economic security of enterprises. *Baltic Journal of Economic Studies*, 9(5), pp.143-152. DOI: 10.30525/2256-0742/2023-9-5-143-152

Organisation for Economic Co-operation and Development (OECD), 2021. *The Digital Transformation of SMEs*, OECD Studies on SMEs and Entrepreneurship. DOI: 10.1787/bdb9256a-en

TechTarget, 2022. *Colonial Pipeline hack explained: Everything you need to know*. [online] Available at: <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know>

World Economic Forum, 2023. *Global risk report*. [online] Available at: <https://www.weforum.org/publications/global-risks-report-2023>

References

Accenture, 2024. *Accenture Risk Study: 2024 Edition. Hyper-disruption demands constant reinvention.* [online] Available at: <https://www.accenture.com/content/dam/accenture/final/accenture-com/document-2/Accenture-Risk-Study-2024-Edition.pdf>

Bilychenko, M. and Kasianova N., 2023. Vplyv tsyfrovoi transformatsii na formuvannia systemy ekonomichnoi bezpeky pidpryiemstva [The impact of digital transformation on the formation of the enterprise's economic security system]. *Biznes Inform*, 7(546), pp.83-91. DOI:10.32983/2222-4459-2023-7-83-91 (in Ukrainian).

Blakyta, H., Bogma, O., Bolduieva, O., Lukyanov and V., Shtuler, I., 2021. Modeling enterprises` economic security in crisis conditions. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, 4, pp.116-121. DOI: 10.33271/nvngu/2021-4/116

Deraglyuk, B., 2023. Vplyv tsyfrovoi transformatsii na zabezpechennia ekonomichnoi bezpeky pidpryiemstva [Impact of digital transformation on ensuring the economic security of the enterprise]. *Ekonomichnyi visnyk NTUU "Kyivskyi politekhnichnyi instytut",* 26, pp.65-68. DOI: 10.20535/2307-5651.26.2023.287057 (in Ukrainian).

Hapeyeva, O. and Holovko, R., 2025. Osoblyvosti formuvannia ekonomichnoi bezpeky pidpryiemstv [Peculiarities of Forming the Economic Security of Enterprises]. *Akademichni vizii,* 40. DOI: 10.5281/zenodo.14917627 (in Ukrainian).

Insurica, 2024. *Cyber case study: Colonial Pipeline ransomware attack*. [online] Available at: <https://insurica.com/blog/colonial-pipeline-ransomware-attack>

Koptieva, H., 2020. Klasyfikatsiia pidkhodiv do otsinky ekonomichnoi bezpeky pidpryiemstva [Classification of approaches to assessing the economic security of an enterprise]. *Skhidna Yevropa: Ekonomika, Biznes ta Upravlinnia,* 2(25), pp.221-229. DOI: 10.32782/easterneurope.25-32 (in Ukrainian).

Kukhar, O., Kravchuk, Y. and Brechko, O., 2023. Digital transformation as a factor in ensuring economic security of enterprises. *Baltic Journal of Economic Studies*, 9(5), pp.143-152. DOI: 10.30525/2256-0742/2023-9-5-143-152.

Maltuz, V. and Maltuz, O., 2022. Diahnostyka rivnia ekonomichnoi bezpeky pidpryiemstva [Diagnostics of the economic security of enterprise]. *Economic Synergy,* 1-2, pp.132-140. DOI:10.53920/ES-2022-1;2-10 (in Ukrainian).

Nasrullayev, R., 2025. Metodychni pidkhody do otsinky ekonomichnoi bezpeky pidpryiemstva [Methodical approaches to the assessment of economic security of enterprises]. Biznes Inform, 7(569), pp.338-344. DOI:10.32983/2222-4459-2025-7-338-344 (in Ukrainian).

Organisation for Economic Co-operation and Development (OECD), 2021. *The Digital Transformation of SMEs*, OECD Studies on SMEs and Entrepreneurship. DOI: 10.1787/bdb9256a-en.

Shylo, Zh. and Krechko, M., 2022. Metody otsinky rivnia ekonomichnoi bezpeky pidpryiemstva: pidkhody do otsiniuvannia ta zabezpechennia ekonomichnoi bezpeky [Methods for assessing the level of economic security of an enterprise: approaches to evaluation and ensuring economic security]. *Visnyk Natsionalnoho universytetu vodnoho hospodarstva ta pryrodokorystuvannia, seriia "Ekonomichni nauky",* 2(98), pp.278-288. DOI:10.31713/ve2202224 (in Ukrainian).

TechTarget, 2022. Colonial Pipeline hack explained: Everything you need to know. [online] Available at: <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know>.

Tkachenko, T. and Hrechko, A., 2022. Uzahalnennia metodychnykh pidkhodiv otsiniuvannia ekonomichnoi bezpeky promyslovykh pidpryiemstv [Generalization of methodological approaches to assessing the economic security of industrial enterprises]. Ekonomichnyi visnyk NTUU "Kyivskyi politekhnichnyi instytut", 22, pp.79-82. DOI:10.20535/2307-5651.22.2022.260154 (in Ukrainian).

World Economic Forum, 2023. Global risk report. [online] Available at: <https://www.weforum.org/publications/global-risks-report-2023>.

Стаття надійшла до редакції 05.12.2025

Муравський С.
Толпежніков Р.

МЕТОДИЧНІ ПІДХОДИ ДО ОЦІНЮВАННЯ ЕКОНОМОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Стаття присвячена комплексному аналізу методичних підходів до оцінювання рівня економічної безпеки підприємства в умовах цифрової трансформації. Здійснено систематизацію традиційних методологій – ресурсно-функціонального, економіко-математичного, індикаторного, програмно-цільового, фінансово-аналітичного та ризик-орієнтованого підходів – з акцентом на те, наскільки вони враховують цифрові ризики та виклики. Показано, що більшість існуючих методик були сформовані до епохи активної цифровізації, тому недостатньо охоплюють такі загрози, як кібератаки,

витоки даних, вразливість IT-інфраструктури, залежність від хмарних сервісів, збої автоматизованих систем та інші цифрові фактори.

На основі аналізу наукових публікацій визначено сучасні тенденції інтеграції цифрового виміру в оцінювання економічної безпеки, зокрема розвиток ризик-орієнтованих підходів, використання міжнародних кібербезпекових стандартів, впровадження показників цифрової стійкості та застосування інструментів цифрової аналітики. У статті запропоновано напрями модернізації класичних методик шляхом розширення системи індикаторів, поглиблення оцінки інформаційно-технологічної складової, включення цифрових ризиків у моделі оцінювання та впровадження автоматизованих систем моніторингу.

Отримані результати підкреслюють необхідність оновлення методичного апарату оцінювання економічної безпеки підприємств у відповідь на зростання ролі цифрових технологій та появу нових типів загроз. Модернізовані підходи забезпечують більш повне, реалістичне й адаптивне відображення стану економічної безпеки в умовах цифрової трансформації.

Ключові слова: *економічна безпека, цифрова трансформація, методичні підходи, цифрові ризики, ризик-орієнтоване оцінювання, інформаційна безпека, кібербезпека, індикатори оцінювання, цифрова стійкість.*