

O. Yemets,

PhD in Economics, Associate Professor, Associate Professor of the Department of Entrepreneurship, Trade and Applied Economics,

Vasyl Stefanyk Precarpathian National University

ORCID ID: <https://orcid.org/0000-0003-1338-2880>

A. Shpak,

PhD in Economics, Assistant of the Department of Management and Marketing,

Vasil Stefanyk Precarpathian National University

ORCID ID: <https://orcid.org/0009-0002-4260-1683>

D. Kurii,

Higher education applicant degree of Doctor of Philosophy at the specialty of 051 "Economics", Vasil Stefanyk Precarpathian National University

ORCID ID: <https://orcid.org/0009-0003-8671-0782>

DOI: 10.32702/2306-6814.2025.11.102

ARTIFICIAL INTELLIGENCE IN THE ENTERPRISE ECONOMIC SECURITY SYSTEM: NEW OPPORTUNITIES FOR RISK MANAGEMENT

O. I. Ємець,

к. е. н., доцент, доцент кафедри підприємництва, торгівлі та прикладної економіки, Прикарпатський національний університет імені Василя Стефаника

A. Д. Шпак,

к. е. н., асистент кафедри менеджменту і маркетингу, Прикарпатський національний університет імені Василя Стефаника

Д. В. Курій,

здобувач вищої освіти ступеня доктора філософії за спеціальністю 051 Економіка, Прикарпатський національний університет імені Василя Стефаника

**ШТУЧНИЙ ІНТЕЛЕКТ У СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА:
НОВІ МОЖЛИВОСТІ УПРАВЛІННЯ РИЗИКАМИ**

In the current conditions of an unstable economic environment, increasing cyber threats, information saturation, and global competition ensure that enterprise economic security becomes especially relevant. Effective risk management now becomes a key element for a business's stable operation and strategic development. This article aims to explore the potential of artificial intelligence in the system of enterprise economic security, as well as to analyze new opportunities for its application in effective risk management. The study will provide an overview of the main directions for using AI technologies and identify the key advantages of integrating such solutions into managing the enterprise's economic security practice. The analysis shows that integrating artificial intelligence technologies into an enterprise economic security system is a promising approach to enhancing risk management effectiveness in a dynamic and unstable external environment. Despite significant initial costs associated with the implementation of relevant technological solutions, their practical application enables achieving a qualitatively new level of economic resilience and prompt response to threats. The main advantages of implementing AI in the enterprise's economic security system include: real-time risk and threat response, which minimizes damage from adverse events; reduction

of human errors and subjective bias, enhancing the objectivity and justification of managerial decisions; optimization of costs for auditing, monitoring, and data analysis through the automation of control and diagnostic procedures; and improved accuracy in forecasting risky situations and potential threats, enabling the enterprise to act proactively and reduce uncertainty in the business environment. Moreover, artificial intelligence enables the integration of disparate information flows, allowing the formation of a comprehensive picture of the enterprise's security status, enhances organizational adaptability to changes in the external environment, and contributes to the development of a proactive risk management system. The prospects for further research lie in a deeper analysis of the effectiveness of artificial intelligence applications in various areas of enterprise economic security, with a focus on adaptability, data integration, and proactive risk management in the context of digital transformation.

В умовах нестабільного економічного середовища, зростання кіберзагроз, інформаційного перевантаження та глобальної конкуренції питання забезпечення економічної безпеки підприємства набуває особливої актуальності. На сучасному етапі ефективне управління ризиками виступає визначальним елементом забезпечення стабільності функціонування та стратегічного розвитку підприємств. Метою цієї статті є дослідження потенціалу штучного інтелекту в системі забезпечення економічної безпеки підприємства, а також аналіз нових можливостей його застосування для підвищення ефективності управління ризиками. У процесі дослідження здійснено огляд основних напрямів застосування технологій штучного інтелекту, а також визначено ключові переваги їх інтеграції в практику управління економічною безпекою підприємства — тобто забезпечення його захищеності від внутрішніх і зовнішніх загроз, які можуть негативно вплинути на стабільне функціонування, розвиток, економічну стійкість та конкурентоспроможність. Аналіз довів, що впровадження технологій штучного інтелекту в систему економічної безпеки є перспективним напрямом підвищення ефективності управління ризиками в умовах динамічного та нестабільного зовнішнього середовища. Незважаючи на значні початкові витрати, практичне застосування таких рішень дозволяє досягти якісно нового рівня економічної стійкості підприємства та здатності оперативно реагувати на потенційні загрози. До основних переваг впровадження штучного інтелекту в систему економічної безпеки належать: оперативне реагування на ризики та загрози в режимі реального часу, що дозволяє мінімізувати збитки від негативних подій; зниження рівня людських помилок та впливу суб'єктивізму, що підвищує об'єктивність і обґрунтованість управлінських рішень; оптимізація витрат на аудит, моніторинг і аналітичну обробку даних завдяки автоматизації контрольних і діагностичних процедур; підвищення точності прогнозування ризикових ситуацій і потенційних загроз, що дає змогу підприємству діяти на випередження та зменшувати рівень невизначеності у бізнес-середовищі. Перспективи подальших досліджень полягають у поглибленому аналізі ефективності застосування штучного інтелекту в різних галузях економічної безпеки підприємства.

Key words: risk situation forecasting; potential of artificial intelligence; informational flows; soundness of managerial decisions.

Ключові слова: прогнозування ризикових ситуацій; потенціал штучного інтелекту; інформаційні потоки; обґрунтованість управлінських рішень.

PROBLEM STATEMENT

In the current conditions of an unstable economic environment, increasing cyber threats, information saturation, and global competition, the issue of ensuring the economic security of an enterprise becomes especially relevant. Effective risk management now becomes a key element for stable operation and strategic development of a business.

Traditional methods of risk assessment and response are increasingly proving insufficient for prompt detection and neutralization of dynamically changing threats. Primarily, these methods are based on statistical estimates,

manual analysis, and historical data. However, modern enterprises operate in a big data environment where information volumes are rapidly increasing, and its analysis requires high processing speed and adaptability. The human factor is unable to promptly process such a large number of variables without automation.

Moreover, threats to economic security are rapidly evolving: new forms of cybercrime, supply chain disruptions, geopolitical upheavals, regulatory changes, and more. Traditional experience-based methods often fail to anticipate new risks.

Table 1. Main areas and general characteristics of anomaly detection in data using AI

Main areas	Specifics of anomaly detection using AI	Technologies and methods for anomaly detection using AI
Financial transactions	AI systems can analyze payment transactions in real time, detecting attempts of double payments, fraudulent expenses, forged invoices, or transactions that do not correspond to typical behavior patterns of clients or counterparties.	Random Forest, clustering (K-means), Isolation Forest
Employee behavior	Internal threats are often associated with the human factor. Algorithms can monitor user activity within corporate networks: unusual login times, suspicious file movements, attempts to access confidential information, and so on.	Neural networks, behavioral modeling, anomaly detection models
Financial performance indicators of the enterprise	Detection of sudden fluctuations in revenue, expenses, profitability, turnover, or other key indicators may indicate internal disruptions, dishonest activities, or external influences (such as market manipulation).	Time series analysis, autoencoders, regression models

Source: compiled based on [3; 5—6].

Risk management methods are often implemented as distinct procedures or policies that lack integration into a cohesive system. This complicates the detection of intersystem threats and synergistic risk effects, which can lead to more widespread consequences. Overall, the processes of detection, assessment, and response in traditional systems take time, which can be critical in rapidly evolving crises or cyber incidents. In modern conditions, systems capable of operating in real-time have an advantage.

Thus, the existing limitations of traditional approaches highlight the need for advanced technological solutions, particularly the use of artificial intelligence, which can elevate risk management to a qualitatively new level.

In this context, innovative approaches based on the application of artificial intelligence (AI) draw special attention as they open new horizons for enhancing the adaptability and resilience of enterprises to internal and external challenges.

ANALYSIS OF RESEARCH AND PUBLICATIONS

Specific features of applying artificial intelligence in the economic security system of enterprises are discussed in the works of Khalina O., Shmagalo V. [5], Kolesnikov A. P. [2], Karapetyan O. M., Novakivskiy I. I., and Rachynska H. V. [3]. The works of the mentioned authors examine various aspects of implementing artificial intelligence technologies in the security systems of business entities, namely: real-time risk analysis, forecasting economic threats, cyber protection of information infrastructure, automation of internal control, and detection of anomalies in financial and operational processes. Novakivskiy I. I. and Rachynska H. V. [3] also pay significant attention to the impact of AI on transforming traditional approaches to security process management and ensuring the enterprise's adaptability to changes in the external environment.

At the same time, a comprehensive study of the potential of artificial intelligence in the economic security system of enterprises—which simultaneously encompasses

risk management, analytical data processing, cybersecurity, and internal control—remains a relevant area of scientific research.

FORMULATION OF THE ARTICLE'S OBJECTIVES

This article aims to explore the potential of artificial intelligence in the economic enterprise security system, as well as to analyze new opportunities for its application in effective risk management. In the course of the research, an overview of the main areas of application of artificial intelligence technologies will be conducted, and the key advantages of integrating such solutions into the practice of enterprise economic security management will be identified—namely, ensuring protection against internal and external threats that may negatively affect stable operations, development, economic resilience, and competitiveness.

THE PAPER MAIN BODY

Economic security encompasses an enterprise's ability to withstand internal and external threats and maintain stability, competitiveness, and development potential. The main risks are formed across the following areas [1—2; 4]:

- Financial (including fraudulent transactions, financial market instability, currency fluctuations, decreased asset liquidity, credit risks);
- Informational (including confidential information leaks, cyberattacks, employee sabotage, and insufficient protection of information infrastructure);
- Personnel (including employee dishonesty, staff turnover, lack of qualified specialists, internal espionage);
- Reputational risks (including the spread of negative information, public conflicts, failure to meet obligations to counterparties, and scandals related to management).

AI enables the automation of monitoring, data analysis, and risk forecasting processes through a range of tools currently used in economic security, including anomaly detection systems, predictive analytics, Big data processing, cybersecurity, and automation of internal control [6].

So, one of the key tools for using artificial intelligence in the enterprise economic security system is anomaly detection, which we interpret as the identification of atypical or suspicious actions that may indicate potential threats, breaches, or fraud.

Based on this tool, machine learning algorithms process large volumes of structured and unstructured data. They are trained on historical data and form an understanding of the system's or users' "normal" behavior [5—6]. Any deviations from established patterns are automatically identified as anomalies that require the attention of security specialists. The main areas and general specifics of anomaly detection in data using AI are presented by us in Table 1.

Thanks to the application of such systems and their associated machine-learning algorithms, an enterprise can respond to threats promptly and predict or prevent their occurrence. For example, in a manufacturing enterprise, an artificial intelligence system can detect anomalous activity in the procurement system—such as placing an order for raw materials that significantly exceeds the average monthly consumption or using an unusual supplier with whom the enterprise has not previously collaborated. Such actions may indicate internal abuses, staff errors, or attempts at fraudulent activities and, accordingly, trigger internal control mechanisms or block the operation pending verification.

Among the tools for using artificial intelligence in the economic security system of an enterprise, we highlight predictive analytics, which we interpret as the ability to assess the likelihood of risks arising before they become actual. This enables enterprises to respond to threats and to act proactively, reducing their impact or preventing them altogether. Based on this tool, AI models analyze historical data, identify trends, correlations, and cyclical patterns, and use these to develop predictive scenarios. Unlike traditional statistical methods, intelligent algorithms are capable of processing large volumes of unstructured information (such as reports, news, and social media [3]), which significantly expands analytical capabilities. The main capabilities of AI predictive analytics in the economic security system of an enterprise are presented in Table 2.

Table 2. Main areas and general characteristics of predictive analytics using AI

Main areas	Specifics of historical data analysis	Technologies used for predictive analytics
Risk probability assessment	Systems can calculate the probability of a partner's default, supply chain disruption, or mass employee turnover based on behavioral, market, and internal data.	Machine learning Deep learning Time series analysis Natural language processing (NLP)
Scenario modeling	Simulation modeling allows for the assessment of the consequences of internal decisions (such as changing suppliers, workforce reduction, entering new markets) and external factors (such as exchange rate fluctuations, political risks, changes in legislation).	
Identification of hidden threats	AI is capable of detecting patterns that are not obvious to humans or that traditional risk management methods fail to identify.	

Source: compiled based on [3; 6].

A company can use a predictive model to: assess the risk of losing a key client; forecast a partner's bankruptcy; model the impact of political instability on supply chains; and early detect signs of a market crisis.

Thus, AI-based predictive analytics enables a shift from reactive to proactive risk management, which is one of the conditions for achieving the enterprise's sustainable economic security.

Every day, terabytes of structured and unstructured data are generated, including financial documentation, reports, market research, customer feedback, information from social media, and user activities in digital systems [2—3]. Accordingly, one of the tools for using artificial intelligence in the enterprise economic security system is big data processing. Thanks to AI, it is possible to integrate and analyze information from diverse sources: market, internal, and competitive (see Table 3).

Big data processing with the use of AI enables an enterprise to quickly adapt to changes in the external environment, make informed decisions, and strengthen its economic security through continuous monitoring and analysis of key risk factors. For example, artificial intelligence

Table 3. Main areas and general characteristics of big data processing using AI

Main areas	Specifics of Big Data processing	Technologies used for Big Data processing
Internal sources ¹	Integration of data from accounting systems, PRM, ERP, and operational activity logs. Analysis of internal processes, costs, employee efficiency, and financial flows.	SQL, Python, Power BI, Machine Learning (ML), Neural Networks
External sources ²	Collection and analysis of market information, stock quotes, economic indicators, data about competitors, suppliers, and partners.	API requests, web scraping, BigQuery, Spark, cloud platforms (AWS, Azure)
Information environment ³	Processing of news texts, social media, and customer feedback. Detection of sentiment, trends, reputation threats, information campaigns, or fake attacks.	Natural Language Processing (NLP), sentiment analysis, text classifiers

Source: compiled based on [2—3; 5].

Table 4. Key areas and general specifics of cybersecurity provision using AI

Main areas	Cybersecurity provision specifics	Technologies used to enhance cybersecurity
Real-time attack detection	Thanks to machine learning, systems can recognize new, previously unknown types of attacks — including zero-day exploits — by analyzing deviations from the normal behavior of network devices and users.	ML algorithms, IDS/IPS, anomaly detection, behavioral analytics
Identification and blocking of unauthorized access	AI analyzes user behavior patterns such as login locations, activity times, and typical actions. Atypical or suspicious authorization attempts are automatically blocked or flagged as threats.	UEBA (User and Entity Behavior Analytics), multi-factor authentication, SIEM
Malware analysis	Deep learning algorithms enable the identification of malicious files even without exact signature descriptions by classifying them based on behavioral characteristics.	Deep learning, sandboxing, anti-malware engines з AI-модулями
Cyber risk forecasting	Based on the history of attacks, system behavior, and external cyber environment (e.g., industry threats), AI models the likelihood of future threats and vulnerabilities.	Predictive analytics, threat intelligence, risk modeling with AI
Log and security event analysis	AI tools are capable of processing millions of security events per day, identifying the most critical ones for prompt response.	SIEM-системи (Splunk, IBM QRadar), log mining, correlation engines з AI

Source: compiled based on [2; 5].

analyzes large volumes of data from social media and news sources to predict potential risks for the enterprise related to reputational threats or changes in market conditions.

In the context of digitalization of business processes, cybersecurity has become a key component of an enterprise's economic security [1—2]. Artificial intelligence (AI) plays an increasingly important role in protecting the information infrastructure by enabling proactive threat detection, rapid incident response, and minimizing the impact of attacks across several core areas highlighted in Table 4.

For example, business entities with large branch networks implement AI to automatically analyze corporate system login logs. By timely detecting suspicious activity

during non-working hours from unusual geolocation, the system blocks a potential attack at the authorization stage, which helps prevent data leakage. Thus, AI enhances the level of enterprise cybersecurity and reduces dependence on human factors by automating monitoring, analysis, and response to information threats.

Internal control is a fundamental element of an enterprise's economic security, ensuring compliance with standards, regulatory requirements, and financial discipline. In the context of digitalization, the automation of basic control areas using Robotic Process Automation (RPA) and Intelligent Systems (IS) is gaining increasing importance, according to the specifics presented in Table 5.

Table 5. Key areas and general specifics of internal control automation using AI

Main areas	Specifics of internal control automation	Technologies used for internal control automation
Financial reporting	Detection of errors, inaccuracies, and discrepancies in financial documents.	RPA, OPR, ML models for report verification
Contract control	Automatic verification of legal terms, deadlines, risky clauses, and inconsistencies with company policy.	NLP, contract analytics, rule-based engines
Procurement and payments	Identification of duplicate invoices, suspicious transactions, and payment delays.	ERP systems with built-in AI modules
Regulatory compliance	Detection of violations of standards (e.g., financial monitoring, tax regulations).	Compliance AI, regulatory rule engines
Audit and revision	Real-time transaction monitoring to detect fraud or unusual behavior.	Continuous auditing tools, anomaly detection, AI-audits

Source: compiled based on [1—2; 4; 6].

Artificial intelligence, combined with RPA and intelligent systems, enables the automatic verification of documents, contracts, and invoices for compliance with standard templates and regulations; detection of duplicates, arithmetic errors, and violations of payment or reporting terms; real-time auditing of transactions; and the generation of alerts upon identifying potential violations or anomalies.

For example, companies are actively implementing RPA to automatically collect and verify invoices, billing statements, and reports. Robotic processes independently extract information from various systems, cross-check data, verify the consistency of amounts, dates, and counterparties, and ensure the presence of all required signatures. In case of discrepancies or errors, notifications are automatically generated and sent to the responsible employees.

Based on the presented provisions, it is evident that despite the high cost of implementing artificial intelligence technologies in the enterprise's economic security system, their use creates fundamentally new opportunities for risk management, specifically in terms of: real-time threat response; minimizing errors and impact of subjective decisions; resource savings (through cost optimization in auditing, analysis, and control); improved forecast accuracy.

CONCLUSIONS

The analysis has shown that the integration of artificial intelligence technologies into the enterprise's economic security system is a promising direction for enhancing risk management effectiveness in a dynamic and unstable external environment. Despite the significant initial costs associated with implementing such technological solutions, their practical application enables the achievement of a qualitatively new level of economic resilience and rapid threat response. The main advantages of implementing AI in the economic security system of an enterprise include: real-time response to risks and threats, which minimizes the impact of negative events; reduction of human errors and subjectivity, enhancing the objectivity and soundness of management decisions; cost optimization for auditing, monitoring, and data analysis through the automation of control and diagnostic procedures; improved accuracy in forecasting risky situations and potential threats, enabling the enterprise to act proactively and reduce uncertainty in the business environment.

The results of the study demonstrate that artificial intelligence enables the integration of disparate information flows, allowing for the creation of a comprehensive picture of an enterprise's security status, enhances organizational adaptability to changes in the external environment, and facilitates the development of a proactive risk management system.

Thus, AI is no longer merely a technological tool but is transforming into a strategic resource that enhances a company's competitiveness, strengthens its economic security, and creates the conditions for sustainable development in a highly competitive digital environment.

The prospects for further research lie in an in-depth analysis of the effectiveness of artificial intelligence

applications across various areas of enterprise economic security.

Література:

1. Ковтуненко Ю. В. Умови забезпечення економічно безпечного інноваційного розвитку підприємств промислового сектору. Економічний дискурс. Міжнародний науковий журнал. 2017. № 3. 2017. С. 138—146.
2. Колесніков А.П., Карапетян О.М. Штучний інтелект: переваги та загрози використання. Ефективна економіка. 2023. № 8. DOI: <http://doi.org/10.32702/2307-2105.2023.8.9>
3. Новаківський І.І., Рачинська Г.В. Застосування штучного інтелекту для управління інноваційними процесами у ланцюгах вартості. Вісник НУ "Львівська політехніка". 2011. № 720. С. 303—309.
4. Станіна О. Роль штучного інтелекту в забезпеченні економічної безпеки держави. Науковий вісник Дніпровського державного університету внутрішніх справ, 2024. № 1. С. 337—342.
5. Халіна О., Шмагалю В. Вплив застосування технологій штучного інтелекту на діяльність суб'єктів економічної безпеки підприємств машинобудування. Економіка та суспільство, 2024. № 62. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/3938> (дата звернення: 15.02.25).
6. Чайковська І., Ткач Т., Чайковський М. Роль сучасних інформаційних систем та технологій у забезпеченні економічної безпеки підприємства в умовах digital-економіки. Herald of Khmelnytskyi National University. Economic Sciences, 2024. № 330 (3), pp. 424—430.

References:

1. Kovtunenکو, Yu.V. (2017), "Conditions for ensuring economically safe innovative development of enterprises in the industrial sector", Ekonomichnyy diskurs. Mizhnarodnyy naukovyy zhurnal, vol. 3, pp. 138—146.
2. Kolesnikov, A.P. and Karapetyan, O.M. (2023), "Artificial intelligence: benefits and threats of use", Efektyvna ekonomika, vol. 8. DOI: <http://doi.org/10.32702/2307-2105.2023.8.9>
3. Novakivskyi, I.I. and Rachynska, G.V. (2011), "Application of artificial intelligence to manage innovation processes in value chains", Visnyk NU "L'vivs'ka politekhnika", vol. 720, pp. 303—309.
4. Stanina, O. (2024), "The role of artificial intelligence in ensuring the economic security of the state", Naukovyy visnyk Dniprovskoho derzhavnoho universytetu vnutrishnikh sprav, vol. 1, pp. 337—342.
5. Khalina, O. and Shmagalo, V. (2024), "The impact of the use of artificial intelligence technologies on the activities of economic security entities of mechanical engineering enterprises", Ekonomika ta suspil'stvo, vol. 62. Available at: <https://economyandsociety.in.ua/index.php/journal/article/view/3938> (accessed 15.02.25).
6. Chaykovska I., Tkach T. and Chaykovsky M. (2024), "The role of modern information systems and technologies in ensuring the economic security of an enterprise in the digital economy", Herald of Khmelnytskyi National University. Economic Sciences, vol. 330 (3), pp. 424—430.

Стаття надійшла до редакції 23.05.2025 р.