**JEL Classification**: G21, G32, D81 **DOI**: https://doi.org/10.31521/modecon.V47(2024)-1

**Ahafonov Andrii,** PhD Student at the Faculty of Management, Mykolayiv National Agrarian University, Mykolayiv, Ukraine

**ORCID ID:** 0009-0004-7480-0163

**e-mail:** 8_andreyag_8@ukr.net

## Innovative Tools for Security-Oriented Management of Commercial Banks in Ukraine

***Abstract. Introduction****. In the context of globalization and rapid technological development, security of commercial banks in Ukraine has become one of the most critical elements for their successful operation. Innovative tools for security-oriented management are essential to effectively address new challenges, such as cyber threats, financial fraud, and risks associated with market instability.*

***Purpose.*** *The purpose of this article is to substantiate the theoretical and methodological foundations and practical approaches to the implementation of innovative tools for security-oriented management in commercial banks operating in the Ukrainian market.*

***Results.*** *The analysis shows that Ukraine's modern financial market faces a high level of uncertainty and risk, which requires the implementation of innovative tools by commercial banks to ensure stability and security. The use of artificial intelligence, machine learning and big data analytics is crucial for the identification and prediction of risk factors. It is emphasized that innovative tools, such as early warning systems and blockchain technology, require adaptation to the specific conditions of the Ukrainian financial market and regulatory environment. These tools can increase the efficiency of risk management; however, their implementation must take into account the unique aspects of the local context.*

***Conclusions*** *Security-oriented management of commercial banks should be a focused and multifaceted process that includes not only technological solutions but also a methodical approach to risk assessment. An integral part of this management is the integration of preventive measures, the strengthening of internal control and audit, and the continuous improvement of security procedures to adapt to external threats and challenges. The results of the study can be valuable for Ukrainian banking institutions seeking to ensure the stability and reliability of their operations in the face of growing challenges and risks.*

***Keywords****: security-oriented management; security-oriented management practices; commercial bank management; commercial banks, financial management; risk management;, risk mitigation.*

**УДК** 658.15:005.334:336.71(477)

**Агафонов А. О.,** аспірант факультету менеджменту, Миколаївський національний аграрний університет, м. Миколаїв, Україна

## Інноваційні інструменти забезпечення безпекоорієнтованого управління комерційними банками України

***Анотація.*** *У сучасних умовах глобалізації та швидкого розвитку технологій безпека комерційних банків в Україні стає однією з найважливіших складових їхнього успішного функціонування. Інноваційні інструменти забезпечення безпекоорієнтованого управління стають необхідними для ефективного протистояння новим викликам, таким як кіберзагрози, фінансові шахрайства та ризики, пов'язані з нестабільністю ринку. Метою статті є обґрунтування теоретико-методичних засад та практичних підходів до впровадження інноваційних інструментів забезпечення безпекоорієнтованого управління комерційними банками в умовах українського ринку. Проаналізовано, що сучасний фінансовий ринок України стикається з високим рівнем невизначеності та ризику, що вимагає від комерційних банків впровадження інноваційних інструментів для забезпечення стабільності та безпеки. Використання технологій штучного інтелекту, машинного навчання та аналізу великих даних стає критично важливим для ідентифікації та прогнозування ризикових факторів. Наголошено, що інноваційні інструменти, такі як системи раннього попередження та блокчейн-технології, потребують адаптації до специфічних умов українського фінансового ринку і законодавства. Ці інструменти можуть підвищити ефективність управління ризиками, проте їхнє впровадження має враховувати особливості локального контексту. Зазначено, що безпекоорієнтоване управління комерційними банками має бути цілеспрямованим і багатогранним процесом, що включає не лише технологічні рішення, а й методичний підхід до оцінювання ризиків. Важливою складовою цього управління є інтеграція превентивних заходів, підвищення рівня внутрішнього контролю та аудиту, а також постійне вдосконалення безпекових процедур для адаптації до зовнішніх загроз і викликів.*

***Ключові слова****: безпекоорієнтоване управління; безпекоорієнтований менеджмент; управління комерційними банками; комерційні банки; фінансовий менеджмент; управління ризиками; ризик-менеджмент.*

***JEL Classification:*** *G21, G32, D81.*

[1]**Стаття надійшла до редакції**: 20.10.2024
**Received**: 20 October 2024

**Formulation of the problem.** Today's financial market in Ukraine is characterized by a high level of uncertainty and risk, which poses new challenges to commercial banks in ensuring the stability and security of their operations. In the face of economic and political changes, banking institutions need to adapt to complex conditions that require flexible approaches to risk management. A key objective is to implement innovative tools that enable rapid responses to potential threats while maintaining high levels of reliability and competitiveness in the marketplace.

Innovative tools for security-oriented management have been widely adopted in global banking practices, where technologies such as artificial intelligence, machine learning, and big data are used to assess and predict risk factors. However, for Ukrainian commercial banks, these tools are relatively new and require adaptation to the specifics of the national market and regulatory requirements. Such innovative approaches can significantly improve the effectiveness of security-oriented management and create opportunities to identify and mitigate potential threats more quickly and accurately.

**Analysis of recent research and publications.** The security-oriented management processes in Ukrainian commercial banks have become significantly more challenging in the context of martial law in Ukraine. Yan Li Chun and Ying Cao emphasized that most commercial banks are facing increased risks, management challenges and pressure on profitability as the financial crisis intensifies its impact on economic entities. The authors demonstrated that effective risk management is the key to the continuous and stable development of commercial banks. Based on the current status of risk management in commercial banks in China, the researchers examined the main aspects of risk management and proposed recommendations for improvement [8].

In their article [7], researchers Xiaodan Wan and Song Luo note that the rapid growth of financial innovation has intensified competition among commercial banks. The authors emphasize that while financial innovations provide commercial banks with competitive advantages, they must also take into account the increasing risks that these innovations entail. In order to maintain a stable market position, banking institutions must consider both the effectiveness of financial innovations and the potential risks. From a scientific point of view, it is important to conduct an in-depth analysis of the key risks and challenges for commercial banks and to propose practical recommendations for managing the risks associated with innovation.

A team of authors, Berisha Vlora, Morina Fisnik, Hetemi Alban and Zeqaj Blerta, demonstrated in their research that internal audit in commercial banks significantly reduces credit risk and contributes to the formation of an effective credit policy. The researchers argued that the size of a commercial bank influences specific audit characteristics, credit policy organization, and risk management [1].

Lin Jing and Han Lu emphasized that the k-nearest neighbors (kNN) algorithm is a classic clustering method; however, its effectiveness is limited when working with samples containing unstructured and fuzzy data because it relies on Euclidean distance, which is unsuitable for such data. These data are crucial for credit risk management in commercial banks, so they must be processed using a fuzzy clustering approach, specifically by calculating the fuzzy distance between each pair of samples based on the degree of membership in a lattice and forming a fuzzy distance matrix to replace the Euclidean distance in the kNN algorithm [3].

In his study, Zhao Yi focuses on analyzing the risks associated with mortgage lending in a specific commercial bank selected as a case study. Key risk indicators were identified, factors influencing the risk level were analyzed, and key risk management issues were systematized. The author constructed a linear regression model to assess the causes and characteristics of the bank's mortgage lending risks. It was demonstrated that an effective risk management system enabled the bank to reduce the annual percentage of non-performing mortgages. Thus, an effective risk management system is the basis for the prevention of risks in the mortgage lending sector of commercial banks [11].

Various aspects of security-oriented management in commercial banks worldwide have also been explored in studies by Yao Fengge, Wen Hongmei, Luan Jiaqi [9], Kuzmynchuk N., Zyma O., Shayturo O., Kutsenko T., Terovanesova O. [2], Yesuratnam G., Pushpa M. [10], among others.

The research and numerous publications on the implementation of innovative tools for security-oriented management in commercial banks confirm the relevance of the topic and its importance for mitigating new, unconventional threats.

**Formulation of research goals.** The purpose of the article is to substantiate the theoretical and methodological foundations and practical approaches to the implementation of innovative tools of security-oriented management in commercial banks in the context of the Ukrainian market.

**Outline of the main research material**. Security-oriented management of a commercial bank is a complex, multifaceted, goal-oriented process of maintaining and developing the security of a banking institution while ensuring its profitability, achieved through adaptation to changes and risks in the external and internal environment. This process involves decision-making at various levels aimed at minimizing risks, protecting assets and maintaining the trust of clients and partners, while ensuring the bank's resilience to economic and financial shocks.

According to Prytys V., the goal of security-oriented management is to create conditions for the company's

operations in which preventive measures throughout the entire management system have a positive impact on the company's security level and support the management in the successful implementation of the overall development strategy. At the same time, management must clearly understand the operational characteristics of the enterprise and consider the influence of the external environment, which is largely negative and requires detailed attention through key concepts - danger, threat and risk [15].

The conditions for ensuring security-oriented management of commercial banks will be analyzed and divided into two parts according to their dependence on the management decisions of the management of the commercial bank (Fig. 1).

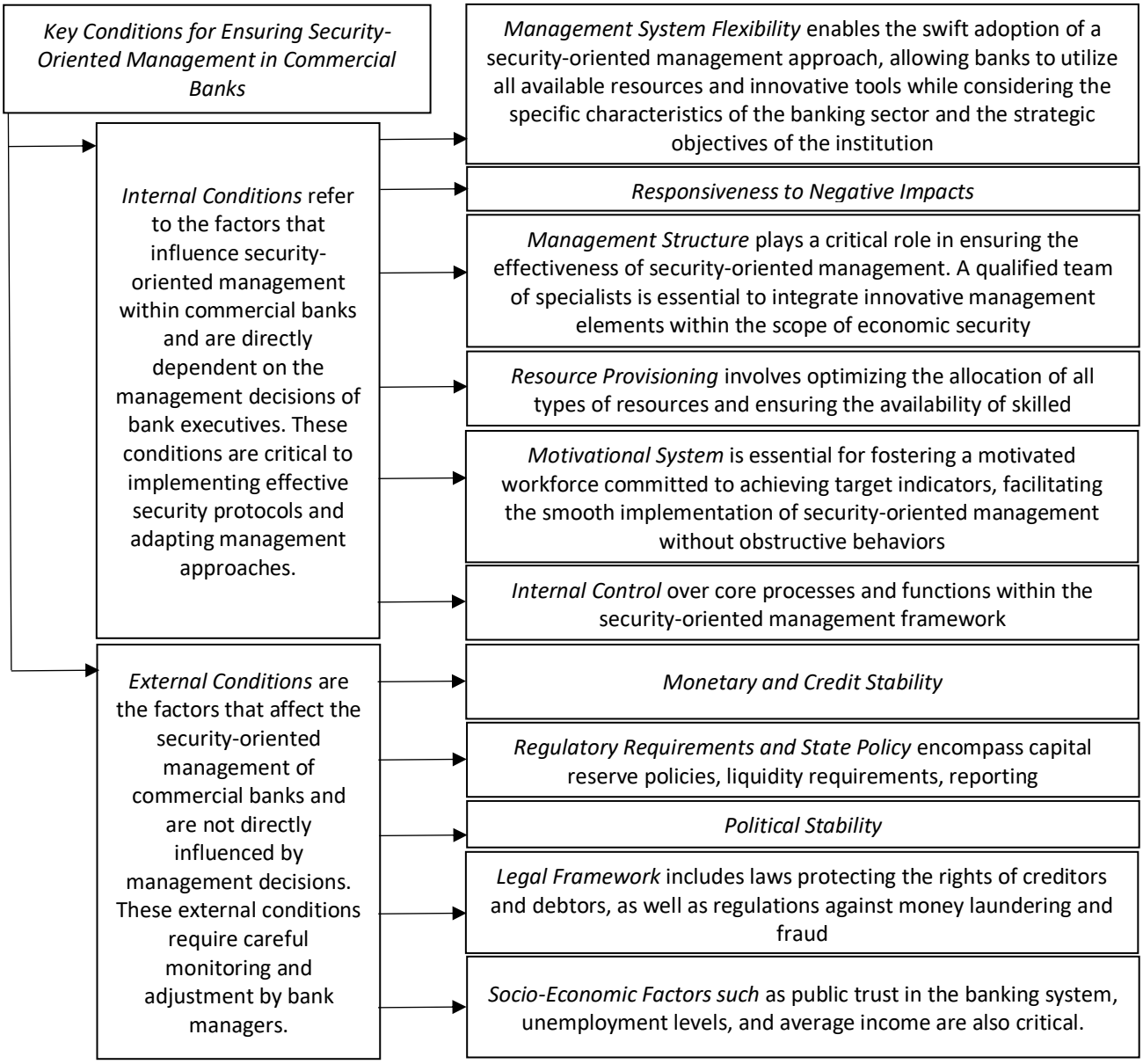


Figure 1 – **Key Conditions for Ensuring Security-Oriented Management in Commercial Banks**

*Source: adapted by the author for the study based on [15]*

Based on the research of Halhash M.R., it is essential for commercial banks operating under conditions of instability to establish a management system that not only withstands adverse external influences, but also remains flexible and adaptable to changes in the external environment [14]. Developing a security-oriented management strategy allows banks to respond quickly to external risks from market fluctuations, social, economic, or political threats. This approach supports efficient bank operations even under challenging circumstances, ensuring not only stability but also successful adaptation to new challenges. As a result, security-oriented management becomes an integral part of a commercial bank's strategy, enhancing its competitiveness and ability

to achieve its financial goals. Another important aspect, as noted in [4] and [5], is the methodological approach to assessing the security status in the midst of instability and uncertainty.

As Havlovska N., Krymchak O., Podhala V. aptly point out, the primary components of security-oriented management include: preventive measures, crisis response, promotion of security culture, threat and risk management, and continuous improvement [13].

In addition, the authors emphasize that the classic tools of security-oriented management include: security information systems - both hardware and software for protecting the organization's information resources; event monitoring systems - real-time tracking and analysis of security-related events; security audits - independent assessments of the effectiveness of security measures; employee training to enhance security skills; and a defined organizational structure - establishing a dedicated security department with clearly assigned responsibilities [13].

The main approaches to ensure the safety oriented management of commercial banks in Ukraine include

1. Integration of risk analysis technologies - use of artificial intelligence, machine learning and big data tools to identify and predict risks. These technologies enable banks to assess and analyze large amounts of data in real time, identify potential threats, and adjust risk management strategies accordingly.

2. Development and implementation of early warning systems - Establishing monitoring systems that detect signs of danger at an early stage. This enables banks to respond to risks in a timely manner, implement preventive measures, and reduce the negative impact on financial indicators.

3. Strengthening Internal Control and Audit Levels - Improving internal audit and control procedures to monitor compliance with security standards, reduce the risk of operational disruptions and fraud, and ensure that banking activities comply with regulatory standards and internal policies.

4. Cybersecurity and Data Protection - Developing effective cybersecurity strategies and measures to protect customer and confidential data, including regularly updating security protocols, implementing multi-factor authentication, and encrypting data.

5. Adapting Business Models to Regulatory Requirements - Flexibly adapting management models in response to changes in the Ukrainian regulatory framework and international standards. This ensures compliance with new regulatory requirements, reduces legal risks, and enhances banks' overall resilience.

These approaches enable Ukrainian commercial banks to effectively manage risks, increase the level of security in their operations, and strengthen their market position.

Innovative tools to ensure security-oriented management are becoming essential in Ukraine's financial sector, especially given the growing global challenges in cybersecurity, risk management, and regulatory compliance. As commercial banks actively adopt new technologies to mitigate risks and strengthen controls, the implementation of innovative approaches should be based on leading international practices.

The first category of innovative tools includes artificial intelligence and machine learning technologies for risk assessment and prediction. These technologies enable the creation of predictive models capable of analyzing vast amounts of data to identify patterns and potential threats that might not be detected by traditional methods. Well-known algorithms such as gradient boosting and deep neural networks are being used to improve risk management in banks around the world, particularly in the U.S. and U.K. banking systems. In commercial banking, AI can also be used for rapid borrower analysis and credit risk assessment, reducing application processing time and minimizing default risk.

Blockchain technologies are also emerging as innovative tools for ensuring transaction transparency and fraud prevention in banking institutions. Blockchain offers banks the ability to ensure a high level of transparency and security for transactions and financial records. The decentralized block system that stores transaction data makes it immutable, increasing protection against external interference.

Blockchain creates a transparent system for recording transactions, increasing data trustworthiness and preventing tampering. Security departments in some U.S. banks are using blockchain to monitor transactions in real time to detect potential fraudulent activity. Benefits include increased transparency and protection from unauthorized access, but drawbacks include high implementation costs and significant resource requirements for data storage.

Early warning and predictive analytics systems use predictive models to monitor key indicators and risk factors to provide early warning of potential threats. Some banks use predictive analytics systems to identify customer default risk. Monitoring data confirms the effectiveness of these systems in significantly reducing non-performing loans by proactively identifying problem assets.

Early warning systems, particularly time series analysis, help predict risks and threats. Successful implementation of such systems has been observed in German banks, where big data-driven analytics platforms are used for real-time risk assessment. Benefits include timely warnings and rapid response to threats, while drawbacks include high implementation costs.

As cyber threats become one of the most serious challenges for banks, cloud-based cybersecurity platforms are essential for data protection. Cloud platforms enable banks to implement layered access controls, update security protocols in real time, and respond effectively to threats. With cloud solutions, banks can reduce the risk of data leakage by 30%, which

is especially important in light of increasing information security requirements.

International examples of successful deployments of cloud-based cybersecurity platforms to protect customer data show a reduction in the risk of data leakage and increased customer confidence in the security of banking operations.

Cloud technologies offer commercial banks the flexibility to rapidly scale their security systems. In the UK, for example, many banks are using cloud platforms for remote monitoring of cyber threats. Benefits include increased mobility and flexibility, but risks include reliance on third-party vendors and potential data security issues.

Integrating regulatory technology (RegTech) for compliance purposes automates processes related to regulatory compliance, making compliance management much easier. By leveraging monitoring and reporting technologies, commercial banks can reduce operational costs associated with compliance and minimize the risk of fines.

Some banking institutions are using RegTech to automate compliance checks, improving both compliance efficiency and adherence. RegTech, which includes the automation of data collection and processing, facilitates compliance with financial regulations and standards. Banks in the European Union are actively using RegTech to ensure compliance with EU regulatory requirements, helping to significantly reduce operational costs, although such technologies require regular updates and adaptations to regulatory changes.

Biometric technologies, such as facial and fingerprint recognition, enhance customer privacy and reduce the risk of fraud.

Implementing innovative tools for security-oriented management is a priority for commercial banks in Ukraine. The experience of leading global banks confirms the effectiveness of tools such as artificial intelligence, blockchain, predictive analytics systems, cloud-based cybersecurity platforms, RegTech, and biometric authentication. The use of these technologies increases the efficiency of risk management and regulatory compliance, and significantly improves the protection of customer data.

**Conclusions.** In the process of substantiating the theoretical and methodological foundations and practical approaches to the implementation of innovative tools for the security-oriented management of commercial banks in the Ukrainian market, the following conclusions were drawn

1. The analysis showed that the current financial market of Ukraine is faced with a high level of uncertainty and risk, which requires the implementation of innovative tools by commercial banks to ensure stability and security. The use of artificial intelligence, machine learning and big data analytics has become crucial for the identification and prediction of risk factors.

2. It was emphasized that innovative tools, such as early warning systems and blockchain technologies, require adaptation to the specific conditions of the Ukrainian financial market and legislation. While these tools can increase the efficiency of risk management, their implementation must take into account the unique aspects of the local context.

3. Security-oriented management for commercial banks should be a focused and multifaceted process that includes not only technological solutions, but also a methodological approach to risk assessment. An essential component of this management is the integration of preventive measures, strengthened internal control and audit, and continuous improvement of security procedures to adapt to external threats and challenges.

The results of the research can be valuable for Ukrainian banking institutions that want to ensure the stability and reliability of their activities in the face of increasing challenges and risks.

**References:**

1. Berisha, V., Morina, F., Hetemi, A., Zeqaj, B. (2023). The Role of Internal Audit in Credit Risk Management in Commercial Banks. Economic Alternatives, 29(1), 115-130. DOI: https://doi.org/10.37075/EA.2023.1.06.
2. Kuzmynchuk, N., Zyma, O., Shayturo, O., Kutsenko, T., Terovanesova, O. (2021). Security-Oriented Bankruptcy Management as a Basis for Ensuring the Enterprises Competitiveness: Information and Analytical Tool and Counteracting Crime (Legal Aspect). 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology, PIC S and T 2021 – Proceedings (Kharkiv, 5 October 2021 - 7 October 2021). pp. 453-457. DOI: https://doi.org/10.1109/PICST54195.2021.9772179.
3. Lin, J., Han, L. (2021). Lattice clustering and its application in credit risk management of commercial banks. Procedia Computer Science, 183, 145-151. DOI: https://doi.org/10.1016/j.procs.2021.02.043.
4. Poltorak, A., Khrystenko, O., Sukhorukova, A., Moroz, T., Sharin, O. (2022). Development of an integrated approach to assessing the impact of innovative development on the level of financial security of households. Eastern-European Journal of Enterprise Technologies, 1/13(115),103-112. DOI: https://doi.org/10.15587/1729-4061.2022.253062.
5. Poltorak, A., Volosyuk, Yu., Tyshchenko, S., Khrystenko O., Ribachuk V. (2023). Development of directions for improving the monitoring of the state economic security under conditions of global instability. Eastern-European Journal of Enterprise Technologies, 2(13-122), 17–27. DOI: 10.15587/1729-4061.2022.253062.
6. Sirenko, N., Atamanyuk, I., Volosyuk, Yu., Poltorak, A., Melnyk, O., Fenenko, P. (2020). Paradigm changes that strengthen the financial security of the state through FINTECH development. 11th International IEEE Conference Dependable Systems, Services and Technologies, DESSERT2020. DOI: https://doi.org/10.1109/DESSERT50317.2020.9125026.

7. Xiaodan, W., Song, L. (2023). Research on risk management of commercial Banks under financial innovation based on fixed effects model. ACM International Conference Proceeding Series. 8th International Conference on Intelligent Information Processing, ICIIP 2023 (Bucharest, 21 November 2023 - 22 November 2023). pp. 223 - 227. DOI: https://doi.org/10.1145/3635175.3635215.
8. Yan, L. Ch., Ying, C. (2010). Discussion on risk management of commercial bank. Proceedings - 2010 2nd IEEE International Conference on Information and Financial Engineering, ICIFE 2010 (17 September 2010 - 19 September 2010). pp. 770-773. DOI: https://doi.org/10.1109/ICIFE.2010.5609470.
9. Yao, F., Wen, H., Luan, J. (2013). CVaR measurement and operational risk management in commercial banks according to the peak value method of extreme value theory. Mathematical and Computer Modelling, 58(1-2), 15-27. DOI: https://doi.org/10.1016/j.mcm.2012.07.013.
10. Yesuratnam, G., Pushpa, M. (2010). Congestion management for security oriented power system operation using generation rescheduling. 2010 IEEE 11th International Conference on Probabilistic Methods Applied to Power Systems, PMAPS 2010 (14 June 2010 - 17 June 2010). pp. 287-292. DOI: https://doi.org/10.1109/PMAPS.2010.5528719.
11. Zhao, Yi. (2024). A Study on Risk Management of Commercial Banks' Home Mortgage Loans Based on Risk Management Framework. Applied Mathematics and Nonlinear Sciences, 9(1), 20230226. DOI: https://doi.org/10.2478/amns.2023.2.00226.
12. Bashynska, I. O. (2019). Risk tolerance as a criterion of safety-oriented management of an industrial enterprise. Biznes Inform, 11, 330–336. DOI: https://doi.org/10.32983/2222-4459-2019-11-330-336.
13. Havlovska, N., Krymchak, O., Podhala, V. (2024). Formation of priorities of security-oriented management of enterprises in conditions of turbulence of the external environment. Modeling the development of the economic systems, 1, 275–281. DOI: https://doi.org/10.31891/mdes/2024-11-41.
14. Halhash, M. R. (2024). Problems of formation of safety-oriented management in organizations. Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia, 4(284), 5-14. DOI: https://doi.org/10.33216/1998-7927-2024-284-4-5-14.
15. Prytys, V. I. (2020). Conditions for the implementation of security-oriented management of enterprises, taking into account existing threats. Biznes Inform, 3, 453-459. DOI: https://doi.org/10.32983/2222-4459-2020-3-453-459.
16. Ministry of Economic Development and Trade of Ukraine (2015). On the approval of Methodological recommendations regarding the comprehensive assessment of the volume of non-productive outflow (export) of financial resources outside of Ukraine (Order No. 286 of 03/24/2015). https://zakon.rada.gov.ua/rada/show/v0286731-15#Text [in Ukrainian].