

V. Tokar,
Doctor of Economic Sciences, Professor, Professor of the Department of Software Engineering and Cybersecurity, State University of Trade and Economics
ORCID ID: <https://orcid.org/0000-0002-1879-5855>
V. Tiapanov,
PhD in Economics, Associate Professor, Vice-President of the Charitable Organization "Foundation Promoting Social and Economic Development of Kyiv Region"
ORCID ID: <https://orcid.org/0000-0003-1907-5654>
K. Savchuk,
PhD in Economics, Doctoral candidate, European University
ORCID ID: <https://orcid.org/0009-0008-8169-2470>

DOI: 10.32702/2306-6814.2024.11.37

THE SYSTEM FOR ENSURING STATE FINANCIAL SECURITY IN THE INFORMATION SOCIETY

В. В. Токар,
д. е. н., професор, професор кафедри інженерії програмного забезпечення та кібербезпеки,
Державний торговельно-економічний університет
В. В. Тіпанов,
к. е. н., доцент, віце-президент, благодійна організація "Фонд сприяння соціально-економічному розвитку Київщини"
К. Д. Савчук,
к. е. н., докторант, Європейський університет

СИСТЕМА ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ ДЕРЖАВИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

The aim of this article is to introduce a thorough framework aimed at ensuring the state financial security within the modern information-driven society. This study contributes to the existing body of theory by presenting a holistic and integrative approach to state financial security in the digital age. Unlike previous studies that often focus on isolated facets of financial security, this article offers a comprehensive framework encompassing regulatory, technological, and strategic measures. The novelty of this approach lies in its multidisciplinary perspective and its applicability to various financial contexts, rendering it a valuable resource for scholars and practitioners in the financial security domain.

The findings of the study underscore the indispensable elements required to ensure state financial security within an information-driven society. These elements encompass a robust regulatory framework, efficient financial supervisory bodies, comprehensive cybersecurity infrastructure, and sophisticated risk management strategies. Additionally, the study emphasizes the significance of financial intelligence units, regulations pertaining to financial technology (FinTech), public awareness initiatives, international collaboration, economic monitoring systems, and emergency response protocols. Collectively, these components establish a resilient financial system capable of confronting contemporary challenges.

The practical implications of this research are substantial for policymakers, regulatory authorities, and financial institutions. By adopting the proposed framework, these stakeholders can significantly enhance their ability to safeguard financial systems against an array of digital threats. This not only ensures adherence to regulatory norms but also upholds consumer trust, which is paramount in maintaining the integrity of financial markets. Furthermore, the research findings offer valuable insights for crafting effective public awareness campaigns. They also highlight the importance of fostering international cooperation to address global financial security issues, emphasizing a unified approach to combating threats in an increasingly interconnected world.

Метою статті є представлення концепції, спрямованої на забезпечення фінансової безпеки держави в сучасному інформаційному суспільстві. Це дослідження робить внесок у теорію, представляючи цілісний інтегративний підхід до фінансової безпеки держави в цифрову епоху. На відміну від попередніх досліджень, які часто зосереджуються на ізольованих аспектах фінансової безпеки, ця стаття пропонує комплексну концепцію, що охоплює регуляторні, технологічні та стратегічні заходи. Новизна цього підходу полягає в його міждисциплінарній перспективі та застосовності до різних фінансових контекстів, що робить його цінним ресурсом для науковців і практиків у сфері фінансової безпеки.

Результати дослідження підкреслюють невід'ємні елементи, необхідні для забезпечення фінансової безпеки держави в інформаційному суспільстві. Ці елементи охоплюють надійну нормативно-правову базу, ефективні органи фінансового нагляду, всеосяжну інфраструктуру кібербезпеки та продумані стратегії управління ризиками. Крім того, у дослідженні підкреслюється важливість функціонування підрозділів фінансової розвідки, розробки нормативно-правових актів, що стосуються фінансових технологій (FinTech), реалізації ініціатив з інформування громадськості, міжнародного співробітництва, систем економічного моніторингу та протоколів реагування на надзвичайні ситуації. Разом ці компоненти створюють стійку фінансову систему, здатну протистояти сучасним викликам.

Практичні висновки цього дослідження мають важливе значення для політиків, регуляторних органів та фінансових установ. Прийнявши запропоновану концепцію, ці зацікавлені сторони можуть значно підвищити свою здатність захищати фінансові системи від різноманітних цифрових загроз. Це не лише забезпечить дотримання регуляторних норм, а й підтримає довіру споживачів, яка є першочерговою для збереження цілісності фінансових ринків. Крім того, результати дослідження містять цінні ідеї для розробки ефективних кампаній з інформування громадськості. У статті також підкреслено важливість посилення міжнародного співробітництва для вирішення питань глобальної фінансової безпеки, наголошено на необхідності дотримання єдиного підходу до боротьби із загрозами у все більш взаємопов'язаному світі.

Key words: economic security, financial security, financial threats, information society, information technology.

Ключові слова: економічна безпека, фінансова безпека, фінансові загрози, інформаційне суспільство, інформаційні технології.

GENERAL STATEMENT OF THE PROBLEM AND ITS CONNECTION WITH IMPORTANT SCIENTIFIC OR PRACTICAL TASKS

In today's digital era, the connection between financial stability and the information society is profound, with technological advancements presenting both opportunities and challenges. The reliance on information technology has transformed traditional security methods in financial matters. The shift to digital finance has introduced new risks such as cyber-attacks and digital fraud, endangering stability and trust. Protecting financial security now requires a multifaceted approach

including regulatory, technological, and strategic measures.

This article proposes a comprehensive framework to enhance financial security in an information-driven age, outlining key components necessary for resilience. It identifies threats to stability and offers precise solutions, emphasizing the need for a unified strategy. Regulatory frameworks are crucial, providing legal boundaries, ensuring compliance, and promoting transparency. Regulatory bodies play a vital role in enforcing these rules, overseeing financial entities, and managing crises to protect consumers and maintain stability.

ANALYSIS OF RECENT STUDIES AND PUBLICATIONS

A substantial body of literature explores state financial security, addressing various facets and challenges in today's world. Buha, Bychin, and Ozerna delve into the definition and structure of financial security, emphasizing its critical role in economic stability. They examine administrative and legal relations, identify threats, and discuss financial market issues, focusing particularly on Ukraine. Their analysis highlights financial security's dynamic nature, essential for socio-economic development and stability, and underscores the need for effective state risk management mechanisms to prevent crises and foster economic growth [1, p. 71—72]. However, they note the limited discussion on regulatory frameworks to tackle emerging threats in the information society.

Demianyshyn, Lobodina, Kostetskyi, and Demianyshyn highlight strategic directions for digital transformation in public finance management, such as centralizing IT management and implementing electronic services to ensure transparency and prevent human interference. Information technology serves dual purposes: achieving strategic goals and facilitating digital development in public finance management [2, p. 68]. However, they do not mention the involvement of stakeholders like cybersecurity experts and government agencies, nor do they address the importance of ongoing monitoring and evaluation mechanisms to assess digital transformation initiatives' effectiveness.

Tkachuk identifies shadow economic activities and money laundering as significant threats to Ukraine's economic and financial systems. His proposed framework for economic security includes balanced actions to maintain stability and resilience, addressing threats like the shadow economy, organized crime, corruption, and capital flight. He emphasizes civil society institutions' role in combating these threats [3, p. 17]. However, Tkachuk's article does not explore regulatory frameworks necessary for safeguarding financial transactions and data in the information society, and it lacks concrete solutions or recommendations for mitigating these risks.

Kuzminska addresses security challenges in Ukraine, such as inflation, economic shadowing, and illegal income legitimization. Her article defines economic and financial security and emphasizes the need for conducive conditions for sustainable development and system stability. Analyzing financial security across various levels optimizes decision-making support and identifies threats to national financial interests [4, p. 190]. While regulatory acts are mentioned, their specific impact on financial security in the information society is not explored.

Srapilov, Sabitova, and Li advocate for enhancing Kazakhstan's domestic information policy, proposing a strategic document for nationwide implementation to cover societal development aspects and leverage digital technologies. They emphasize the need for protocols for information exchange among state entities during crises [5, p. 32]. However, the article lacks evidence to support claims of legislative deficiencies, weakening its credibility.

Hlushko, Pantas, and Babenko propose a comprehensive system to enhance Ukraine's information policy for

financial security, highlighting the importance of developing a national information infrastructure to protect national interests [6]. However, their study lacks specifics on implementing these measures and their funding, which are crucial for practical steps to enhance financial security.

Dankiewicz, Balawejder, Chudy-Laskowska, and Britchenko stress the importance of state financial security for economic growth and stability. Their study, focused on Poland, identifies indicators for assessing state financial security and develops an econometric model linking them to banking sector stability [7, p. 89—90]. While they conclude positively about Poland's banking stability, the study's limited scope and narrow data set restrict its generalizability to other countries.

Kostyshyn examines the foundational concepts of financial security, addressing ambiguities in definitions within Ukraine's financial sector. He proposes a model consisting of interrelated subsystems influenced by environmental factors [8, p. 130]. Despite outlining conceptual approaches, Kostyshyn does not discuss specific indicators relevant to assessing financial security within the information society.

Rushchyshyn, Medynska, Nikonenko, Kostak, and Ivanova justify regulatory support in shaping financial security, highlighting legal backing and oversight mechanisms. They suggest a comprehensive mechanism to bolster financial security, including legal, structural, organizational, and resource-related measures [9, p. 239]. However, their recommendations lack clarity on specific actions, and their research methods are not thoroughly explained.

Blikhar, Mykhalitska, Vereskliia, Komarnytska, and Koziar advocate for a distinct economic policy for Ukraine, focusing on real economic growth and reducing debt dependency. They emphasize robust legal frameworks to safeguard financial security amidst external and internal crises [10, p. 435]. However, they tend to oversimplify Ukraine's financial challenges and lack a forward-looking approach to anticipate future issues.

Andriyiv reviews challenges in transitioning to a digital economy, such as digital inequality and cyber threats. He underscores the importance of monitoring these challenges to mitigate potential threats to economic security [11, p. 13]. However, he lacks specific policy recommendations or strategies to address these issues, essential for guiding decision-makers.

Korobtsova explores financial security during martial law, emphasizing the importance of funding sources for production and state regulation in banking and entrepreneurship [12, p. 144—145]. While she suggests measures like state regulation, Korobtsova does not offer a comprehensive strategy for adapting financial security systems to the information society's challenges.

Kasianenko, Antoniuk, Myronova, and Lyulov examine financialization's impact on Ukraine's financial security, highlighting the stock market's role and internal economic challenges [13, p. 97]. They suggest continuous monitoring of financial gaps but fall short in providing concrete policy recommendations.

Poltorak, Potryvaieva, Kuzoma, Volosiuk, and Bobrovska propose a doctrinal framework for managing state

Table 1. Elements of the system for ensuring state financial security in the information society

Element	Description	Functions
Regulatory framework	A set of laws, regulations, and guidelines established to govern financial activities and ensure compliance within the financial system.	Defines legal boundaries, ensures compliance, mitigates risks, and promotes transparency and accountability.
Financial supervisory authorities	Governmental or independent bodies responsible for overseeing financial institutions and markets to maintain stability and protect consumers.	Monitor financial entities, enforce regulations, conduct audits, and manage crises.
Cybersecurity infrastructure	Systems, policies, and measures designed to protect financial data and systems from cyber threats and attacks.	Prevents, detects, and responds to cyber threats, ensuring data integrity and confidentiality.
Risk management strategies	Comprehensive plans and processes to identify, assess, and mitigate financial risks.	Identifies potential risks, implements control measures, and ensures continuity of financial operations.
Financial intelligence units (FIUs)	Agencies dedicated to collecting, analyzing, and disseminating financial information to combat money laundering and terrorist financing.	Detects and prevents illicit financial activities, shares intelligence with other agencies, and supports investigations.
Financial technology (FinTech) regulations	Guidelines and rules specific to the development and use of financial technologies.	Promotes innovation while ensuring security, consumer protection, and financial stability.
Public awareness programs	Initiatives aimed at educating the public about financial security, risks, and responsible financial behavior.	Enhances public understanding, encourages prudent financial practices, and reduces susceptibility to fraud.
International cCooperation	Collaboration with international organizations and other countries to enhance global financial security.	Facilitates information sharing, aligns regulations, and coordinates responses to transnational financial threats.
Economic monitoring systems	Tools and processes for continuous monitoring of economic indicators and financial market activities.	Provides real-time data, identifies emerging threats, and supports decision-making processes.
Emergency response mechanisms	Established protocols and resources to manage and mitigate financial crises or disruptions.	Ensures rapid response, stabilizes financial systems, and restores public confidence in times of crisis.

Source: elaborated by authors.

financial security, structured into five levels. Their model integrates mission, priorities, and technological innovation [14, p. 32—33]. However, they overlook cybersecurity risks and lack specific adaptive strategies for the information society.

Hlushko and Maslii discuss the influence of information policy on state financial security amid information warfare, proposing strategic information policy directions to enhance financial security [15, p. 44—45]. However, they do not compare Ukraine's policy with other countries or address potential challenges in implementation.

Zakharkina, Chukhno, and Veremiiienko emphasize public finance transparency's role in state financial security, stating that transparency fosters trust and effective public debt regulation [16, p. 129]. However, they lack concrete policy recommendations and do not consider the perspectives of different stakeholders essential for effective implementation.

Despite providing essential insights into various aspects of state financial security, there is a need for a deeper exploration of ensuring state financial security in the information society, especially in defining system elements and highlighting threats.

FORMULATION OF THE OBJECTIVES OF THE ARTICLE (TASK STATEMENT)

The article aims to establish a robust framework to protect a state's financial security in the modern information-centric world. It outlines essential components for building a resilient financial system capable of addressing current challenges, identifying key threats, and proposing measures to mitigate risks, emphasizing the importance of a comprehensive strategy.

SUMMARY OF THE MAIN RESEARCH MATERIAL

Table 1 highlights the diverse elements required to ensure state financial security in an information society. Each element plays a vital role in creating a robust, resilient, and secure financial system capable of withstanding the challenges of the modern world.

The regulatory framework serves as the foundation of a state's financial security, comprising laws, regulations, and guidelines governing financial activities to ensure compliance and transparency. Financial supervisory authorities oversee institutions and markets, maintaining stability and consumer protection through enforcement, audits, and crisis management.

Table 2. Key threats to state financial security in the information society and mitigation measures

Threat	Description	Measures
Cyber-attacks on financial institutions	Cyber-attacks such as hacking, malware, and ransomware targeting financial institutions can lead to significant financial losses and disrupt economic stability.	Implement robust cybersecurity protocols, conduct regular security audits, train staff on security practices, and establish rapid incident response teams.
Data breaches	Unauthorized access to sensitive financial data can result in identity theft, fraud, and loss of consumer trust.	Use advanced encryption methods, enforce strict access controls, regularly update security systems, and perform vulnerability assessments.
Digital fraud and scams	Increasing digital transactions have led to a rise in fraud and scams, including phishing, identity theft, and online payment fraud.	Enhance public awareness campaigns, deploy advanced fraud detection systems, collaborate with financial institutions for real-time monitoring, and strengthen legal frameworks against digital fraud.
Systemic risks from FinTech	Rapid development and integration of FinTech can introduce systemic risks due to insufficient regulation and oversight.	Develop comprehensive FinTech regulations, establish dedicated oversight bodies, encourage best practices in technology deployment, and ensure compliance with financial stability standards.
Dependence on digital infrastructure	Heavy reliance on digital infrastructure makes the financial system vulnerable to technical failures, cyber-attacks, and natural disasters.	Diversify infrastructure, implement redundant systems, conduct regular stress tests, and create robust disaster recovery plans.
Privacy concerns	Increased data collection and usage in financial services can lead to privacy violations and misuse of personal information.	Enforce stringent data protection regulations, promote transparency in data usage, offer consumer control over personal data, and ensure compliance with privacy standards.
Cryptocurrencies and unregulated digital assets	The rise of cryptocurrencies and other digital assets poses challenges to financial regulation and can facilitate illegal activities.	Implement clear regulatory frameworks for digital assets, monitor cryptocurrency transactions, and collaborate internationally to enforce regulations and combat illicit activities.
Information warfare and disinformation	The spread of false information and disinformation campaigns can destabilize financial markets and erode public confidence.	Establish mechanisms for rapid detection and counteraction of disinformation, enhance media literacy, and collaborate with tech companies to address the spread of false information.
Technological unemployment	Automation and digitalization can lead to job losses in traditional financial sectors, affecting economic stability.	Promote reskilling and upskilling programs, support job creation in emerging sectors, and implement social safety nets for affected workers.
Global financial interconnectedness	High levels of global interconnectedness increase the vulnerability to external shocks and contagion from financial crises in other countries.	Strengthen international cooperation, establish contingency plans for global financial shocks, and enhance monitoring of international financial developments.

Source: elaborated by authors.

In the digital age, cybersecurity infrastructure is vital for safeguarding financial data and systems from cyber threats. Risk management strategies identify, assess, and mitigate financial risks, ensuring operational continuity. Financial Intelligence Units combat money laundering and terrorist financing, sharing intelligence to maintain system integrity. FinTech regulations guide technology development while ensuring security and stability.

Public awareness programs educate about financial security and responsible behavior. International cooperation enhances global financial security through collaboration and information sharing. Economic monitoring systems provide real-time data for threat identification and decision-making. Emergency response

mechanisms manage crises, stabilizing systems and restoring public confidence swiftly.

Table 2 outlines ten critical threats that modern financial systems face within the context of an increasingly digital and interconnected world. This comprehensive analysis not only identifies these threats but also provides measures to tackle or minimize their consequences, ensuring a robust framework for maintaining state financial security.

Cyber-attacks, including hacking and malware, pose significant risks to financial institutions, causing financial losses and operational disruptions. Robust cybersecurity measures, regular audits, staff training, and rapid incident response teams are crucial defenses. Unauthorized access to sensitive financial data can lead to identity theft and fraud. Preventive measures include encryption, access

controls, security updates, and vulnerability assessments. Digital transactions have increased fraud, such as phishing and online payment scams. Mitigation involves awareness campaigns, fraud detection systems, real-time monitoring, and legal framework strengthening. FinTech's growth requires comprehensive regulations, oversight bodies, technology best practices, and adherence to stability standards. Dependence on digital infrastructure necessitates diversification, redundancy, stress tests, and disaster recovery planning.

Data usage in finance raises privacy and legal concerns. Stringent data protection, transparency, user control, and privacy compliance are vital. Cryptocurrencies raise regulatory challenges, requiring clear frameworks, transaction monitoring, and international cooperation against illegal activities. False information can destabilize markets. Detecting and countering disinformation, media literacy promotion, and collaboration with tech firms are crucial. Digitalization may disrupt traditional finance jobs. Reskilling, upskilling, job creation, and social safety nets ease transitions and maintain stability. Global interconnectedness heightens vulnerability to financial shocks. Enhanced cooperation, contingency plans, and international monitoring mitigate risks.

CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH IN THIS AREA

The study emphasizes a holistic approach to state financial security, integrating regulatory, technological, and collaborative strategies. Regulations establish boundaries and ensure transparency, enforced by oversight bodies to protect against misconduct. Cybersecurity is vital in the digital era, securing data and consumer trust. Risk management strategies identify and mitigate financial risks, ensuring operational continuity. Financial intelligence units combat illegal activities, while FinTech regulations ensure safe innovation integration. Public education enhances awareness of financial risks. International cooperation is crucial for global financial security, enabling effective regulation alignment. Real-time monitoring and emergency response mechanisms anticipate and manage threats during crises. Future research should focus on advancing cybersecurity, regulating FinTech, addressing digital transformation's employment impact, and strengthening global financial connections to mitigate shocks.

Acknowledgements. The study was carried out as part of the grant "EU ECONOMIC SECURITY" (project number: 101083446, project acronym: EUECOSEC, call: ERASMUS-JMO-2022-HEI-TCH-RSCH, topic: ERASMUS-JMO-2022-CHAIR) supported by the European Education and Culture Executive Agency.

Literature:

1. Buha, H., Bychin, S., Ozerna, I. (2023). The definition and structure of financial security. *Baltic Journal of Economic Studies*, vol. 9 (2), pp. 65—72. URL: <https://doi.org/10.30525/2256-0742/2023-9-2-65-72> (date of access: 10.04.2024).
2. Дем'янишин, В. Г., Лободіна, З. М., Костецький, В. В., Дем'янишин В. В. (2023). Напрями розвитку інформаційних технологій в управлінні публічними фінансами, державними фінансовими ресурсами та фінансовою безпекою суб'єктів господарювання державного секто-

ру. *Інноваційна економіка*, № 1, с. 58—70. URL: <https://doi.org/10.37332/2309-1533.2023.1.9> (date of access: 10.04.2024).

3. Ткачук, І. (2023). Інститути громадянського суспільства в системі забезпечення фінансової безпеки держави. *Economic Synergy*, Вип. 1 (7), с. 8—19. URL: <https://doi.org/10.53920/ES-2023-1-1> (date of access: 10.04.2024).

4. Кузьмінська, О. (2022). Сутність фінансової безпеки як об'єкта аналізу. *Світ фінансів*, Вип. 4 (73), с. 184—192. URL: <https://doi.org/10.35774/sf2022.04.184> (date of access: 10.04.2024).

5. Srapilov, S. M., Sabitova, A., Li, S. O. (2022). On the role of the information policy of the state in the information society. *Journal of Actual Problems of Jurisprudence*, vol. 103, No. 3, pp. 25—33. URL: <https://doi.org/10.26577/JAPJ.2022.v103.i3.03> (date of access: 10.04.2024).

6. Глушко, А. Д., Пантась, В. В., Бабенко, С. Р. (2022). Інформаційна політика в системі забезпечення фінансової безпеки держави. *Ефективна економіка*, № 2, URL: <https://doi.org/10.32702/2307-2105-2022.2.95> (date of access: 02.05.2024).

7. Dankiewicz, R., Balawejder, B., Chudy-Laskowska, K., Britchenko, I. (2022). Impact factors and structural analysis of the state's financial security. *Journal of International Studies*, vol. 15 (4), pp. 80—92. URL: <https://doi.org/10.14254/2071-8330.2022/15-4/5> (date of access: 02.05.2024).

8. Костишин, Ю. С. (2020). Концептуальні засади формування системи фінансової безпеки держави. *Економіка, управління та адміністрування*, Вип. 1 (91), с. 123—132. URL: [https://doi.org/10.26642/ema-2020-1\(91\)-123-132](https://doi.org/10.26642/ema-2020-1(91)-123-132) (date of access: 02.05.2024).

9. Rushchysyn, N., Medynska, T., Nikonenko, U., Kostak, Z., Ivanova, R. (2021). Regulatory and legal component in ensuring state's financial security. *Business: Theory and Practice*, vol. 22 (2), pp 232—240. URL: <https://doi.org/10.3846/btp.2021.13580> (date of access: 02.05.2024).

10. Бліхар, М., Михаліцька, Н., Верескля, М., Комарницька, І., Козяр, Г. (2021). Фінансова безпека держави: міжнародний досвід дослідження інституціонально-правових причин кризових явищ в економіці. *Financial and Credit Activity Problems of Theory and Practice*, Вип. 2 (37), с. 426—437. URL: <https://doi.org/10.18371/fcaptr.v2i37.230333> (date of access: 02.05.2024).

11. Андріїв, Н. М. (2022). Виклики для економічної безпеки держави в умовах формування цифрової економіки. *Інфраструктура ринку*, Вип. 64, с. 10—15. URL: <https://doi.org/10.32843/infrastruct64-2> (date of access: 02.05.2024).

12. Коробцова, Д. В. (2022). Правове забезпечення фінансової безпеки держави в умовах воєнного стану. *Аналітично-порівняльне правознавство*, № 2, с. 141—146. URL: <https://doi.org/10.24144/2788-6018.2022.02.27> (date of access: 02.05.2024).

13. Касьяненко, В. О., Антонюк, Н. А., Миронова, А. М., Люльов, О. В. (2019). Індикатори фінансової безпеки держави в умовах світової глобалізації. *Вісник СумДУ. Серія "Економіка"*, № 4, с. 87—92. URL: <https://doi.org/10.21272/1817-9215.2019.4-11> (date of access: 02.05.2024).

14. Poltorak, A., Potryvaieva, N., Kuzoma, V., Volosiuk, Y., Bobrovska, N. (2021). Development of doctrinal model for state's financial security management and forecasting its level. *Eastern-European Journal of Enterprise Technologies*, vol. 5 (13), pp. 26—33. URL: <https://doi.org/10.15587/1729-4061.2021.243056> (date of access: 02.05.2024).

15. Глушко, А. Д., Маслій, О. А. (2022). Вплив інформаційної політики на рівень фінансової безпеки України. *Науковий вісник Херсонського державного університету*, Вип. 46, с. 39—46. URL: <https://doi.org/10.32999/ksu2307-8030/2022-46-6> (date of access: 02.05.2024).

16. Захаркіна, Л. С., Чухно, Р. Ю., Веремієнко, Є. В. (2021). Транспарентність публічних фінансів як фактор забезпечення фінансової безпеки держави. *Вісник СумДУ. Серія "Економіка"*, № 4, с. 122—130. URL: <https://doi.org/10.21272/1817-9215.2021.4-15> (date of access: 02.05.2024).

References:

1. Buha, H., Bychin, S. and Ozerna, I. (2023), "The definition and structure of financial security", *Baltic Journal of Economic Studies*, vol. 9 (2), pp. 65—72. DOI: <https://doi.org/10.30525/2256-0742/2023-9-2-65-72>.

2. Demianyshyn, V. H., Lobodina, Z. M., Kostetskyi, V. V. and Demianyshyn, V. V. (2023), "Directions for the development of information technologies in the management of public finances, state financial resources and financial security of public sector entities", *Innovative Economy*, vol. 2, pp. 58—70. DOI: <https://doi.org/10.37332/2309-1533.2023.1.9>.

3. Tkachuk, I. (2023), "Institutions of civil society in system of providing state financial security", *Economic Synergy*, vol. 1 (7), pp. 8—19. DOI: <https://doi.org/10.53920/ES-2023-1-1>.

4. Kuzminska, O. (2022), "The essence of financial security as an object of analysis", *World of Finance*, vol. 4 (73), pp. 184—192. DOI: <https://doi.org/10.35774/sf2022.04.184>.

5. Srapilov, S. M., Sabitova, A. and Li, S. O. (2022), "On the role of the information policy of the state in the information society", *Journal of Actual Problems of Jurisprudence*, vol. 103, No. 3, pp. 25—33. DOI: <https://doi.org/10.26577/JAPJ.2022.v103.i3.03>.

6. Hlushko, A., Pantas, V. and Babenko, S. (2022), "Information policy in the system of financial security of the state", *Efektivna ekonomika*, vol. 2. DOI: <https://doi.org/10.32702/2307-2105-2022.2.95>.

7. Dankiewicz, R., Balawejder, B., Chudy-Laskowska, K. and Britchenko, I. (2022), "Impact factors and structural analysis of the state's financial security", *Journal of International Studies*, vol. 15 (4), pp. 80—92. DOI: <https://doi.org/10.14254/2071-8330.2022/15-4/5>.

8. Kostyshyn, Yu. S. (2020), "Conceptual principles of formation of the state financial security system", *Economics, Management and Administration*, vol. 1 (91), pp. 123—132. DOI: [https://doi.org/10.26642/ema-2020-1\(91\)-123-132](https://doi.org/10.26642/ema-2020-1(91)-123-132).

9. Rushchysyn, N., Medynska, T., Nikonenko, U., Kostak, Z. and Ivanova, R. (2021), "Regulatory and legal component in ensuring state's financial security", *Business:*

Theory and Practice, vol. 22 (2), pp 232—240. DOI: <https://doi.org/10.3846/btp.2021.13580>.

10. Blikhar, M., Mykhalitska, N., Vereskliia, M., Komarnytska, I. and Koziar, G. (2021), "Financial security of the state: international experience in the study of institutional and legal causes of crisis phenomena in the economy", *Financial and Credit Activity Problems of Theory and Practice*, vol. 2 (37), pp. 426—437. DOI: <https://doi.org/10.18371/fcaptp.v2i37.230333>.

11. Andriyiv, N. M. (2022), "Challenges for economic security of the state in the conditions of forming the digital economy", *Market Infrastructure*, vol. 64, pp. 10—15. DOI: <https://doi.org/10.32843/infrastructure64-2>.

12. Korobtsova, D. V. (2022), "Legal provision of financial security of the state in martial law", *Analytical and Comparative Jurisprudence*, vol. 2, pp. 141—146. DOI: <https://doi.org/10.24144/2788-6018.2022.02.27>.

13. Kasianenko, V., Antoniuk, N., Myronova, A. and Lyulov, O. (2019), "State financial security indicators in the world of globalization", *Visnyk of Sumy State University*, vol. 4, pp. 87—92. DOI: <https://doi.org/10.21272/1817-9215.2019.4-11>.

14. Poltorak, A., Potryvaieva, N., Kuzoma, V., Volosiuk, Y. and Bobrovska, N. (2021), "Development of doctrinal model for state's financial security management and forecasting its level", *Eastern-European Journal of Enterprise Technologies*, vol. 5 (13), pp. 26—33. DOI: <https://doi.org/10.15587/1729-4061.2021.243056>.

15. Hlushko, A. and Maslii, O. (2022), "The influence of information policy on the level of financial security of Ukraine", *Scientific Bulletin of Kherson State University*, vol. 46, pp. 39—46. DOI: <https://doi.org/10.32999/ksu2307-8030/2022-46-6>.

16. Zakharkina, L. S., Chukhno, R. Yu. and Veremienko, Ye. V. (2021), "Public finances' transparency as a factor of ensuring the state's financial security", *Visnyk of Sumy State University*, vol. 4, pp. 122—130. <https://doi.org/10.21272/1817-9215.2021.4-15>.

Стаття надійшла до редакції 20.05.2024 р.

<https://nayka.com.ua>

Електронне фахове видання

Ефективна
ЕКОНОМІКА

Виходить 12 разів на рік

Журнал включено до переліку наукових фахових видань України з ЕКОНОМІЧНИХ НАУК (Категорія «Б»)
Спеціальності – 051, 071, 072, 073, 075, 076, 292

e-mail: economy_2008@ukr.net

viber: +38 050 3820663