African Journal of Applied Research
Vol. 10, No. 1 (2024), pp. 431-441
http://www.ajaronline.com
http://doi.org/10.26437/ajar.30.06.2024.26

DIGITAL INNOVATIONS AND THEIR RAMIFICATIONS FOR FINANCIAL AND STATE SECURITY

Krysovatyy, A.[1], Desyatnyuk, O.[2], and Ptashchenko, O.[3]
[1]*Department of Finance, West Ukrainian National University, Ternopil, Ukraine.*
[2]*Administration, West Ukrainian National University, Ternopil, Ukraine.*
[3]*Department of Entrepreneurship and Trade, West Ukrainian National University, Ternopil, Ukraine.*
[1]*head_ac@wunu.edu.ua*
[2]*o.desyatnyuk@wunu.edu.ua*
[3]*ptashchenko@wunu.edu.ua*

ABSTRACT

Purpose: In the current era of rapid digitalisation across all spheres of public life, the issue of financial and national security takes on a new dimension. Digital technologies bring about significant changes in the security domain, accelerating and streamlining many processes. However, digitalisation also presents new challenges and threats. Therefore, studying and enhancing financial and national security strategies is necessary. The research aims to analyse the specifics of implementing digital technologies in financial and national security.

Design/Methodology/Approach: The study is theoretical. Theoretically, the ascent methods are applied from the abstract to the concrete, axiomatic, analysis, synthesis, logical-semantic, systems-analytical methods, scientific abstraction, and formalisation. The study is limited by the difficulty of empirically verifying theoretical conclusions.

Findings: Blockchain technology provides high transparency, accessibility, and accountability in financial operations. Challenges and risks related to the research process have been identified, including cybercrime and the need for updated regulatory and legal frameworks.

Research Limitation/Implications: The article examines the potential of modern digital technologies in optimising financial and national security strategies and the challenges and achievements of the digitalisation of security sector transformation. The study is limited by the lack of access to official, reliable data and the difficulty of implementing an empirical verification of theoretical conclusions.

Social Implication: The research demonstrates that security resilience in a globally integrated environment depends on the level of digital innovation implemented for risk management.

Practical Implication: The research findings have practical value for transforming contemporary financial and national security systems and shaping relevant government sector development programs.

Originality/ Value: The text outlines priority digitalisation solutions for risk prediction and mitigation. The study examines digital technologies that facilitate real-time automation of the risk management process.

Keywords: *Artificial intelligence. blockchain. cybersecurity. digital innovations. financial risks.*

INTRODUCTION

In the current globally integrated environment, information technologies are being implemented significantly, and a gradual transition to the digital economy of Industry 4.0 is taking place.

ISSN: 2408-7920

Digitalisation creates new opportunities for optimising financial and national security. However, it also brings new threats and challenges, as the open nature of information systems increases vulnerability to cyber-attacks and menacing influences.

Ensure national and financial security is a top priority in the context of Russia's military aggression and market instability. Digital technologies can serve as tools to ensure resilience and endurance against unforeseen circumstances. The integration of advanced information and communication technologies has demonstrated practical effectiveness. However, the impact of digitalisation is complex. It requires deep analysis and periodic optimisation of management practices and strategic approaches to ensure stability and reliability in a dynamic socio-economic environment.

Digital technologies concerning national and financial security are a topic of active research among Ukrainian and foreign scholars. Some contemporary works aim to define the role and significance of information technologies in the national and financial security system (Chalapko, 2021; Shostak & Suriak, 2023) and the correlation between national security and public administration (Zahurska-Antoniuk, 2020).

Ukrainian scholars primarily approach the concept of digitisation in national and financial security policy from a perspective of complexity (Popova & Khromov, 2021; Krysovatyy et al., 2024). However, some authors examine digital optimisation from the perspective of specific functional directions (Kukin, 2020).

According to Kostenko (2020), the full potential of digital technologies in ensuring national and financial security can only be realised through harmonising critical socio-economic and political factors. Recent scientific achievements include publications by Hidayat et al.. (2024), which present the concept of digital optimisation of security process management using artificial intelligence, cloud services, and blockchain technology.

Several contemporary scholars examine specific issues of digitising financial and investment mechanisms as the basis for financial security (Desyatnyuk et al., 2024; Xu & Zhang, 2024). A significant contribution to the general methodology of digitising the national security sphere has been made by several scientists in the modern domestic scientific community (Parkhomenko-Kutsevil, 2020; Klochko & Semenets-Orlova, 2022).

The research is relevant because systematic strategies must be developed for digitising the security policy sphere in national and financial concepts. Although the published works hold value, many issues must be solved. Strategies for the digital transformation of financial and national security require more detailed conceptualisation from theoretical and practical perspectives, with the involvement of leading global experts.

This study explores the role of digital technologies in ensuring national and financial security in a dynamic context of the conceptual priorities of the management paradigm in the current crisis.

LITERATURE REVIEW

Scholars focusing on implementing digital technologies into financial and national security amidst uncertainty and crisis phenomena lay the theoretical and methodological basis for the researched issues. Scientific professional journals contain numerous publications on the researched topic. Ukrainian scientists have analysed the fundamentals of digitising the national security sphere (Prymush, 2022), explained the conceptual principles of financial security strategy involving the potential of digitisation (Pantielieieva, 2020), and defined the optimal functionality of digital tools in the system of state management of national security (Krysovatyy et al., 2021). The above scholars have considered the impact of the international situation on shaping national security, responding to a set of threats and means of countering them. The researchers have established that, within the general context, one of the priority tasks of the legal mechanism of public administration of national security is to establish effective institutional interaction involving innovative digital technologies.

Contemporary foreign scholars have identified the digital toolkit for control and monitoring as the foundation for ensuring national security (Degli Esposti et al., 2021). Budiasih (2024) has also formulated the main conceptual principles of digitising financial operations. Anwary (2022) emphasises the need to actively implement digitisation tools in the security sector. Scientists emphasise that digital transformation leads to the emergence of new threats. One of the main threats is cyberattacks, which can target critical infrastructure, government systems, or economic structures. Attackers can use a variety of techniques, including phishing, attacks on Internet-connected devices, and the use of malware. In the context of digital transformation, national security, these authors argue, is becoming a continuous challenge requiring improvement and innovative solutions in cybersecurity. Applying modern methods and technologies of cyber defence is critical for ensuring the sustainability of the state under the constant development of digital technologies.

Scholarly research has identified several findings that justify the effective implementation of digital technologies to address contemporary challenges to Ukraine's national security (Szczepaniuk et al., 2020). Digital transformation enables big data and analytics to predict potential crises, identify patterns and trends that may indicate danger or potential crises, and respond quickly. For instance, social media monitoring systems can detect signals of potential crises and react rapidly. Crisis management is also carried out through digital platforms and systems. They allow for responding to crises in real-time, allocating resources and organising assistance in emergencies. This can range from sending automatic alerts to citizens to arranging rescue operations and managing logistics. However, some foreign scholars have highlighted the challenges in implementing specific elements of digital optimisation in current circumstances (El-Muhammady, 2021). Several contemporary researchers (Cangiano et al., 2019; Javed & Faizan, 2024) have made a significant scholarly contribution to addressing financial security issues in the context of intensive digitisation.

MATERIALS AND METHODS

The study is theoretical. At the theoretical level, the following methods were used: descent from the abstract to the concrete, axiomatic, analysis, synthesis, logical-semantic, systems-analytical methods, scientific abstraction, and formalisation. The study is characterised by the complexity of implementing an empirical verification of theoretical conclusions. The logical-semantic method was utilised to deepen the conceptual-categorical apparatus. In contrast, the analytics made it possible to investigate the normative-legal framework of the digital optimisation process of national and financial security. The method of ascending from the abstract to the concrete helped formulate theoretical definitions, specify the conceptual apparatus, identify basic concepts and categories, and draw conclusions from the research. Formalisation was employed to structure the principles, functions, tasks, and priorities of implementing digital technologies in national and financial security. The research is limited by the difficulty of implementing an empirical test of theoretical conclusions and the lack of unrestricted access to official, reliable data.

RESULTS

Current challenges for financial and national security.

In the age of rapid digitalisation, implementing innovations in national and financial security presents both opportunities and challenges. A strategic approach to automating processes is required to enhance operational efficiency, proactively manage risks, and ensure financial stability. Digital technologies now offer functionality beyond traditional threat monitoring and mitigation methods. The tools outlined implement a comprehensive security system, enabling prompt responses to new challenges and timely anticipation, strategically adapting to the environment's dynamics.

The analytical processing of large volumes of information is used better to understand the interdependence of risks and causal factors. Digital optimisation of the security system automates routine processes, enhancing the quality of financial risk management. Modern digital technologies provide comprehensive risk identification and assessment tools, enabling the accumulation and reflection of potential threats in various areas (Chalapko, 2021; Shostak & Suriak, 2023). Furthermore, these technologies enable the analysis of potential scenarios by modelling different environmental conditions to assess their impact. Such assessments comprehensively understand potential vulnerabilities and help adjust risk minimisation strategies.

The potential of digitalisation to achieve the required financial and national security level.

The modern digital technologies inherent in Industry 4.0 are expressed through robotics, cyber systems, the Internet of Things, artificial intelligence, cloud solutions, unmanned technologies, identification tools, paperless solutions and blockchain. (Popova & Khromov, 2021; Krysovatyy et al., 2024). However, it is essential to note that this list is not exhaustive and is constantly expanding. Digital technologies are generally valued for efficiently processing and analysing large amounts of data (El-Muhammady, 2021).

Cybersecurity becomes increasingly crucial as our reliance on digital technologies grows and we store more data on digital platforms. Digital technologies currently provide reliable solutions, such as encryption, intrusion detection, and threat identification systems based on artificial intelligence. These technologies effectively protect confidential information, strengthen defences against cyber threats, and prevent data breaches (Cangiano et al., 2019; Javed & Faizan, 2024). Using digital technologies targeted towards security can minimise the risk of financial losses caused by cyber-attacks and ensure the integrity of financial systems.

By automating traditional risk management processes, these technologies reduce the risks associated with human factors. When operating in real-time mode, they ensure efficient and prompt risk management actions (Desyatnyuk et al., 2024; Xu & Zhang, 2024).

Cloud computing has revolutionised accessibility and interaction in risk management. Cloud solutions simplify exchanging informative data for real-time risk assessment without being limited by spatial determinants. The potential of cloud computing facilitates seamless cooperation among individual elements of the security system and optimises risk awareness levels. Cloud platforms offer scalable data storage and emergency data recovery, reducing the risk of permanent data loss caused by crisis events and environmental factors.

Blockchain technology provides high transparency, accessibility, and accountability in financial operations. Blockchain technology is particularly relevant in areas where compliance and origin are paramount (Hidayat et al., 2024). Its implementation can strengthen trust among stakeholders and minimise financial fraud.

In the field of national security management, preventive measures and a system for responding to threats and challenges are necessary due to the risks of espionage through advanced technological capabilities, such as location tracking programs and the accumulation of personal data. Cybersecurity is primarily concerned with this, as it is positioned as a prerequisite for national security today. As cyberattacks increase in frequency and diversity, the state governance system must utilise advanced technological capabilities to safeguard critical infrastructure and information from cyber threats. The ethical balance between human rights and ensuring national security is critical (Degli Esposti et al., 2021).

In the process of security monitoring activities, innovative technologies are considered beneficial. For example, modern satellite systems allow for real-time observation, enabling effective and prompt responses to threats to national security (Parkhomenko-Kutsevil, 2020; Klochko & Semenets-Orlova, 2022). Mobile applications, chats, and specialised platforms provide unrestricted access to information regarding government and state institutions, stimulating public oversight and identifying current issues. Therefore, digital optimisation in the context of national security involves leveraging the possibilities of digitisation and cutting-edge technologies to significantly enhance the system of preventive protection (Figure 1).

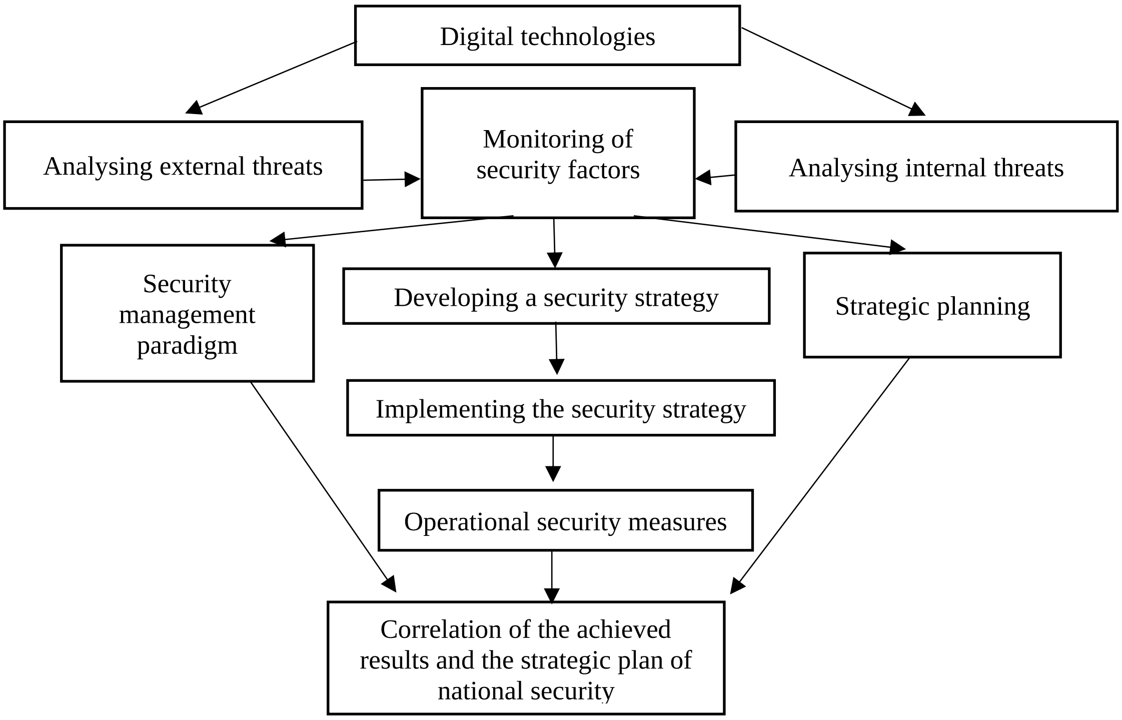
Digital technologies
Analysing external threats
Monitoring of security factors
Analysing internal threats
Security management paradigm
Developing a security strategy
Strategic planning
Implementing the security strategy
Operational security measures
Correlation of the achieved results and the strategic plan of national security

Figure 1: Algorithm of digital national security optimisation process
Source: author

Upon analysing Figure 1, it is essential to note that monitoring and operational neutralising external and internal threats and dangers are critical in national security. Modern digital technologies create optimal conditions for real-time monitoring and reporting, allowing for the quick identification of potential risks and prompt responses to them. Visualisation tools and information panels clearly understand key risk indicators, enabling timely decision-making to mitigate new threats. This real-time approach optimises risk minimisation strategies, allowing vulnerabilities to be addressed before they transform into significant security issues.

Ukraine's 2025 economic security strategy involves using modern financial regulation tools to achieve security objectives effectively. These tools include FINTEX, which stands for financial technologies. The definition emphasises the use of modern digital instruments in financial circulation. One example is cryptocurrency, a digital currency that operates autonomously without involvement in the central payment system. It has led to the development of numerous startups, investment platforms, exchanges, and exchangers. FINTEX tools are closely associated with the widespread adoption of mobile devices, the emergence of alternative electronic and digital payment methods, and new national and international payment systems. Additionally, artificial intelligence technologies are being utilised by implementing robotic personal advisors, chatbots, biometrics, and digital client identification in financial services (Cangiano et al., 2019; Javed & Faizan, 2024).

Innovative digital solutions to prevent risks related to financial and national security.

To effectively implement financial security, it is crucial to update the organisational and legal framework of the industry, amend existing financial legislation, and use modern digital technologies to control and hold accountable for financial fraud. Digital technologies can give enterprises greater confidence in strategic economic planning, financial support, and protection against risks, which significantly ensures financial security. However, the era of digitalisation of the economy has brought about critical digital threats such as corporate data theft, hacking attacks, industrial espionage, and insufficient provision of digital technologies and competent personnel (Budiasih, 2024).

Effective information management is required to prevent threats to national security. The information resource security system encompasses several basic concepts, including the formation, processing, and transmission of information related to financial and national security processes. It also involves ensuring technological independence in critical areas of informatisation, such as supporting innovation in the defence sector (Cangiano et al., 2019; Javed & Faizan, 2024).

On 23 February 2023, Ukraine ratified the agreement on the country's participation in the EU's Digital Europe programme, which provides innovative opportunities for developing a digital society (Krysovatyy et al., 2024). In summary, using digital technologies to improve financial and national security requires ensuring progressive conditions for advancing state and societal institutions and reliable protection against internal or external threats. It involves a coordinated effort between authorities, businesses, and society.

The development of digital financial technologies has the potential to enhance financial security by ensuring transaction security, effective control, and minimising opportunities for corruption. Digital technologies are potent drivers of transparency in the financial system, particularly at the state level. Regulatory and supervisory technologies are crucial for increasing transparency in currency regulation, preventing capital flight and money laundering disguised as foreign investments, and limiting the shadow financial market sector. To achieve this, financial security regulatory frameworks should be based on risk monitoring and assessment. The concept will help maintain data confidentiality and cybersecurity, which are crucial to state financial security.

It is recommended that modern digital technologies be implemented actively. Their application creates optimal conditions for successful transformative processes in the security sphere. Digital technologies can streamline the execution process of practical governmental activities such as strategic planning, monitoring, controlling, and evaluating decisions made regarding national and financial security. Artificial intelligence tools are envisaged to form the basis for qualitative dynamics in national and financial security policies.

DISCUSSION

The analysis of current scientific trends suggests that active involvement of digital technologies effectively ensures national and financial security. Individual researchers (Bonavolontà & D'Angelo, 2021) highlight the potential of digital tools to enhance the interaction between society and the state in ensuring national security. According to Mandel and Irwin (2021), the synergy between traditional and innovative digital methods can mitigate the imbalance in the security sphere at regional and sectoral levels.

Some modern publications consider the possibility of digitising a significant portion of management processes in the security sphere (Biden, 2021). Scholars Esberg and Mikulaschek (2021) argue that the primary objective of the digital transformation process in financial and national security is accumulating, protecting, and optimising information arrays. J. Esberg and C. Mikulaschek highlight the negative aspects of digital optimisation of national security, including vulnerability to viruses and cyberattacks, ethical issues, and dependence on modern technology.

Babuta et al. (2020) question the appropriateness of involving artificial intelligence in national security policy implementation. Meanwhile, Robinson et al. (2021) emphasise the principles of moderation and phased implementation of artificial intelligence tools in the researched sphere. They highlight the prerequisites for effective security policy, including an appropriate resource base and society’s readiness for dynamic changes.

In today’s unstable reality, security policy’s scope has significantly expanded. This has been demonstrated by implementing innovative technological solutions and opportunities for digital optimisation in the research sphere. According to Mincewicz (2020), modern scholars emphasise that the state’s implementation of functions to protect national interests in the digital era involves government intervention in society.

Most contemporary scholars consider prioritising national interests, ensuring law and order, and maintaining a safe financial and economic environment as the foundation of national and financial security. Digital technologies are considered practical tools for optimising existing approaches and introducing new ones to ensure the appropriate financial and national security level.

CONCLUSION

The research has argued that digital technologies are crucial in implementing national and financial security. The analysis of the main directions of digital transformation of security policy has shown that using digital technologies in the security sphere aims to automate defensive operations. Challenges and risks related to the research process have been identified, including cybercrime and the need for updated regulatory and legal frameworks.

The paper has explored digital technologies’ potential to achieve the necessary financial and national security levels. It outlines a range of priority digitisation solutions for risk forecasting and prevention, including artificial intelligence. The feasibility and prospects of implementing innovative electronic systems and the opportunities provided by modern tools and technologies for optimising the security system have been analysed.

The research results have demonstrated that digital technologies can speed up the processing of large volumes of information and improve the quality of decisions. Additionally, their application positively impacts the effectiveness of government activities, reduces potential losses and risks, and ensures the efficiency of protection systems.

In considering directions for further scientific research on the investigated topic, it is vital to analyse the potential of digital technologies in guaranteeing national stability and protecting citizens' rights. Particular attention should be given to preserving the confidentiality of digital information, minimising threats in the digital space, developing scientific and personnel potential, and enhancing investment opportunities. The proposed approach aims to improve the country's national and financial security. It is expected to work in synergy with other efforts towards this goal.

REFERENCES

Anwary, I. (2022). The Role of Public Administration in combating cybercrime: An Analysis of the Legal Framework in Indonesia. *International Journal of Cyber Criminology, 16(2),* 216–227. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/135

Babuta, A., Oswald, M., & Janjeva, A. (2020). Artificial intelligence and UK national security: policy considerations. Technical Report. *RUSI, London.* https://nrl.northumbria.ac.uk/id/eprint/42963/

Biden, J. R. (2021). Interim national security strategic guidance. *The White House, 8.* https://apps.dtic.mil/sti/citations/AD1157244

Bielialov, T., Kalina, I., Goi, V., Kravchenko, O., & Shyshpanova, N. (2023). Global experience of digitalization of economic processes in the context of transformation. *Journal of Law and Sustainable Development*, 11(3).

Bonavolontà, V., & D'Angelo, M. (2021). Digital transition and public administration in Italy: the experience of the Italian National Social Security Institution− INPS. *Ubezpieczenia Społeczne. Teoria i praktyka, 4*, 87–101. https://yadda.icm.edu.pl/yadda/element/bwmeta1.element.ojs

Bondarenko, S., Bratko, A., Antonov, V., Kolisnichenko, R., Hubanov, O., & Mysyk, A. (2022). Improving the state system of strategic planning of national security in the context of informatization of society. *Journal of Information Technology Management*, 14, 1-24. https://doi.org/10.22059/jitm.2022.88861

Budiasih, Y. (2024). The Influence of Digital Technology on Financial Management. *Accounting Studies and Tax Journal (COUNT), 1(1),* 92-100. https://doi.org/10.62207/wb6d3c96

Cangiano, M., Gelb, A., & Goodwin-Groen, R. (2019). Public financial management and the digitalisation of payments. *Public financial management and the digitalisation of payments: Cangiano. Washington DC: Center for Global Development.* https://www.zbw.eu/econis-archiv/bitstream/11159/3501/1/public-financial-management-and-digitalization-payments.pdf

Chalapko, V. (2021). Information security: the problem of place and role in the national security system. *The Bulletin of Yaroslav Mudryi National Law University. Series: philosophy, philosophy of law, political science, sociology, 4(51).* https://doi.org/10.21564/2663-5704.51.242004

Degli Esposti, S., Ball, K., & Dibb, S. (2021). What's in it for us? Benevolence, national security, and digital surveillance. *Public Administration Review, 81(5),* 862–873. https://doi.org/10.1111/puar.13362

Desyatnyuk, O., Naumenko, M., Lytovchenko, I., & Beketov, O. (2024). Impact of Digitalization on International Financial Security in Conditions of Sustainable Development. *Problemy Ekorozwoju/Problems of Sustainable Development, 1,* 104-114. https://ph.pollub.pl/index.php/preko/article/view/5325/4341

El-Muhammady, A. (2021). Balancing national development, national security, and cybersecurity policy. *Routledge Companion to Global Cyber-Security Strategy*. https://books.google.com.ua/books?hl=uk&lr=&id=1uYLEAAAQBAJ&oi=fnd&pg=PT383&dq=national+security+and+public+management&ots=MnK44pWo5T&sig=t9r3199boMD15o9Kmhk0ohr9MVo&redir_esc=y#v=onepage&q=national%20security%20and%20public%20management&f=false

Esberg, J., & Mikulaschek, C. (2021). Digital Technologies, Peace and Security: Challenges and Opportunities for United Nations Peace Operations. *United Nations Peacekeeping, 7*. https://peacekeeping.un.org/sites/default/files/esberg_and_mikulaschek_-_conflict_peace_and_digital_technologies_-_v3_210825.pdf

Hidayat, M., Defitri, S. Y., & Hilman, H. (2024). The Impact of Artificial Intelligence (AI) on Financial Management. *Management Studies and Business Journal (Productivity), 1(1),* 123–129. https://doi.org/10.62207/s298rx18

Javed, U., & Faizan, A. (2024). Guardians of the Digital Realm: Navigating the Frontiers of Cybersecurity. *Integrated Journal of Science and Technology, 1(2)*. https://ijstindex.com/index.php/ijst/article/view/6

Klochko, O., & Semenets-Orlova, I. (2022). National security: the Ukrainian dimension. *Scientific works of the Interregional Academy of Personnel Management. Political science and public administration, 2(62),* 66–75. https://doi.org/10.32689/2523-4625-2022-2(62)-10

Kostenko, D. M. (2020). A conceptual model for forming a network architecture of Ukraine's public administration of national security. *Investments: practice and experience, 13–14,* 118–124. https://doi.org/10.32702/2306-6814.2020.13-14.118

Krysovatyi, A., Lipyanina-Goncharenko, H., Sachenko, S., & Desyatnyuk, O. (2021). Economic Crime Detection Using Support Vector Machine Classification. Modern Machine Learning Technologies and Data Science Workshop. *Proc. 3rd International Workshop (MoMLeT&DS 2021), I: Main Conference. Lviv-Shatsk, Ukraine,* 830-840.

Krysovatyy, A., Ptashchenko, O., Kurtsev, O., & Arutyunyan, O. (2024). The Concept of Inclusive Economy as a Component of Sustainable Development. *Problems of Sustainable Development, 1,* 164-172. https://ph.pollub.pl/index.php/preko/article/view/5755/4346

Kukin, I. V. (2020). A comprehensive mechanism for the public management of personal information security in the field of national security and its border sector. *Public Management and Customs Administration, 4(27),* 134-139 http://biblio.umsf.dp.ua/jspui/handle/123456789/4250

Mandel, D., & Irwin, D. (2021). Uncertainty, Intelligence, and National Security Decision-making. *International Journal of Intelligence and CounterIntelligence, 34(3),* 558–582. https://doi.org/10.1080/08850607.2020.1809056

Mincewicz, W. (2020). Blockchain technology and national security-the ability to implement a blockchain in the area of national security. *De Securitate et Defensione. O Bezpieczeństwie i Obronności, 6(2)*, 114-129. https://doi.org/10.34739/dsd.2020.02.08

Pantielieieva, N. M. (2020). Financial security in the digital economy: expectations and reality. *Financial Space, 38(2)*. https://doi.org/10.18371/fp.2(38).2020.209289

Parkhomenko-Kutsevil, O. I. (2020). Information transparency of the public administration system as a basis for ensuring national security. *Scientific Bulletin: Public Administration, 3(5)*, 195–203. https://doi.org/10.32689/2618-0065-2020-3(5)-195-203

Popova, L. M., & Khromov, A. V. (2021). Informatisation of society: main trends and threats to national security. *Modern problems of legal, economic, and social development of the state.* https://dspace.univd.edu.ua/server/api/core/bitstreams/eeefd0b3-6100-4d79-87b2-5aba66bf2775/content#page=77

Prymush, R. B. (2022). Directions for increasing the effectiveness of public administration in national security. *Economics, management and administration, 2(100),* 44–48. https://doi.org/10.26642/ema-2022-2(100)-44-48

Robinson, N., Hardy, A., & Ertan, A. (2021). Estonia: A Curious and Cautious Approach to Artificial Intelligence and National Security. *Routledge Companion to Artificial Intelligence and National Security Policy*. https://doi.org/10.2139/ssrn.4105328

Shevchenko, I., Lysak, O., Zalievska-Shyshak, A., Mazur, I., Korotun, M., & Nestor, V. (2023). Digital economy in a global context: World experience. *International Journal of Professional Business Review, 8(4)*. https://doi.org/10.26668/businessreview/2023.v8i4.1551

Shostak, L.V., & Suriak, A.V. (2023). Peculiarities of ensuring the security of an enterprise in the context of digital transformation of the economy. *Scientific view: economics and management, 3 (83),* 140-145. http://biblio.umsf.dp.ua/jspui/handle/123456789/6330

Sytnyk, H. P., Zubchyk, O. A., & Orel, M. H. (2022). Conceptual understanding of the peculiarities of managing innovation-driven development of the state in the current conditions. *Science and Innovation*, 18(2), 3-15. https://doi.org/10.15407/scine18.02.003

Szczepaniuk, E.K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Assessment of information security in public administration. *Computers and Security, 90*. https://doi.org/10.1016/j.cose.2019.101709

Xu, X., & Zhang, H. (2024). Analysis of enterprise financial management under the background of digital transformation. *SHS Web of Conferences, 181*. https://doi.org/10.1051/shsconf/202418102030

Zahurska-Antoniuk, V. (2020). National security and public administration. *Galician Economic Bulletin, 66(5),* 187–193. https://doi.org/10.33108/galicianvisnyk_tntu2020.05.187