

## Секція 4

# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

## ADAPTIVE SECURITY FRAMEWORKS FOR SAFEGUARDING CBDCS USING ARTIFICIAL INTELLIGENCE

**Koldovskiy A.**, PhD in Economics, Senior lecturer  
*Department of International Management and Marketing, WSB Merito University  
Global Talent International*

The integration of Artificial intelligence (AI) within the security framework of Central bank digital currencies (CBDCs) revealed promising advancements. AI-driven algorithms exhibited a high level of adaptability in detecting and mitigating evolving cyber threats. Through the analysis of historical data, these algorithms showcased an ability to predict potential vulnerabilities and proactively fortify the security measures.

While there's a growing body of research surrounding AI in cybersecurity and financial systems, the specific focus on adaptive security frameworks for CBDCs is relatively nascent. The existing literature tends to cover broader aspects of AI in financial security and cybersecurity, with limited direct emphasis on CBDCs.

Studies by Meshal and Haitham (2020) and AL-Dosari, Fetais, Kucukvar, (2022) have highlighted the growing importance of AI in fortifying cybersecurity within financial systems. They emphasize AI's role in predicting, detecting, and responding to potential cyber threats, showcasing its potential for CBDC security. Research by Taser and Bozyiğit (2022) demonstrates the efficacy of machine learning models in financial fraud detection. This study explores the application of unsupervised and supervised learning algorithms in identifying anomalies and patterns, aligning with the need for adaptive threat prediction in CBDCs. Recent works by Biswas et al. (2020) and Doerr, Gambacorta and Serena (2021) showcase the potential integration of AI in central bank operations. While not directly focused on CBDCs, they lay the groundwork for AI's adoption within financial institutions, indicating the viability of AI-enhanced security measures in the context of CBDCs.

The implementation of AI-based threat detection mechanisms exhibited a notable enhancement in the identification of irregular activities within CBDC transactions. The self-learning capabilities of AI systems showcased a capacity to evolve alongside emerging threats, constantly refining their ability to detect and prevent potential risks.

The adaptive nature of AI-infused security frameworks allowed for real-time response to detected threats. The systems autonomously adjusted security protocols and responded to anomalies, significantly reducing the response time to security breaches within the CBDC ecosystem.

The integration of AI led to increased resilience in the face of sophisticated cyber-attacks. By differentiating normal transaction patterns from potentially malicious activities, false positives in threat detection reduced, enhancing overall system efficiency while maintaining robust security. The utilization of adaptive security frameworks employing AI within CBDC ecosystems presents a significant stride towards fortifying their security. The results underscore the efficacy of AI in proactively identifying, addressing, and adapting to cyber threats in real-time, marking a fundamental shift in the approach to safeguarding CBDCs.

AI-powered security frameworks exhibit a remarkable potential to anticipate and counteract vulnerabilities, thereby offering a dynamic defense mechanism crucial in the realm of digital currency security. The adaptability and self-learning nature of AI contribute significantly to the resilience and responsiveness required in safeguarding CBDCs against evolving threats.

The recommendations poised for fortifying Central Bank Digital Currencies through adaptive security measures using AI encompass a multi-faceted approach. Continued AI Integration and Research stands as a pivotal directive, urging sustained efforts in research and development that spotlight the integration of AI within CBDC security frameworks. This initiative calls for the continual refinement and expansion of AI algorithms specifically tailored to combat emerging threats, ensuring a proactive response to evolving cybersecurity challenges.

Collaborative Initiatives mark an essential stride, advocating for the convergence of expertise among central banks, cybersecurity specialists, and AI developers. This collaborative front seeks to harmonize knowledge and resources, nurturing the development of adaptive security measures meticulously crafted for the unique landscape of CBDCs.

Regulatory Adaptation emerges as a vital consideration, calling for the flexible adjustment of regulatory frameworks. These adaptations are crucial to accommodate the dynamic nature of AI-integrated security systems, ensuring compliance and ethical application within the intricate ecosystem of Central Bank Digital Currencies.

Investment in AI Education is heralded as an imperative step, underscoring the need to foster educational programs and training initiatives. Equipping professionals with the essential skills to adeptly manage AI-powered security systems within the CBDC landscape is fundamental to fortifying the robustness of these digital currencies.

Continuous Evaluation and Improvement serves as the cornerstone, advocating for the perpetual assessment and enhancement of AI-infused security measures. This directive necessitates regular audits, stress tests, and ongoing evaluation to swiftly identify vulnerabilities, thereby reinforcing the defenses in place and aligning with the ever-evolving threat landscape.

In summary, the integration of Artificial Intelligence within adaptive security frameworks marks a paradigm shift in fortifying the security landscape of Central Bank Digital Currencies. This innovative amalgamation offers a multifaceted and robust defense mechanism, laying a resilient foundation to counter the surging tide of emerging cyber threats.

The strategic fusion of AI technologies with adaptive security frameworks presents an avant-garde approach, empowering the defenses surrounding CBDCs with a

dynamic and agile response capability. This synergy harnesses the cognitive prowess of AI algorithms, enabling a proactive stance against potential vulnerabilities, threats, and malicious activities within the intricate network of digital transactions.

Moreover, the integration of AI engenders an environment of continuous vigilance and responsiveness. The AI-powered systems not only detect and neutralize threats but also evolve and adapt in real-time, marking a significant departure from conventional reactive security measures. This real-time adaptability forms a formidable shield, dynamically adjusting security protocols and responses in tandem with the evolving threat landscape.

Conclusively, this innovative fusion of AI within adaptive security frameworks heralds a new era in the protection of Central Bank Digital Currencies, instilling a sense of confidence in the reliability and resilience of these financial assets. It promises a proactive, agile, and ever-evolving defense system, essential in safeguarding the integrity and stability of the evolving digital financial ecosystem.

#### **Information sources:**

1. AL-Dosari, K., Fetais, N., Kucukvar, M. (2022). Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges, Cybernetics and Systems, URL: <https://www.tandfonline.com/doi/full/10.1080/01969722.2022>.
2. Biswas, S., Carson, B., Chung, V., Singh, S., Thomas, R. (2020). AI-bank of the future: Can banks meet the AI challenge? Global Banking & Securities. URL: <https://www.mckinsey.com/~media/McKinsey/Industries/Financial.pdf>.
3. Doerr, S., Gambacorta, L., Serena, J.M. (2021). Big Data and Machine Learning in Central Banking. BIS Working Papers. URL: <https://www.bis.org/publ/work930.htm>.
4. Meshal, A. Haitham, N. (2020). Artificial Intelligence in Financial Industry. URL: <https://ssrn.com/abstract=3578238> or <http://dx.doi.org/10.2139/ssrn.3578238>.
5. Taser P. Bozyiğit F. (2022). Machine Learning Applications for Fraud Detection in Finance Sector. The Impact of Artificial Intelligence on Governance, Economics and Finance, Volume 2 (pp.121-146). URL: <https://www.researchgate.net/publication>.

## **DIGITALIZATION AND INTERNET ADVERTISING IN BUSINESS ACTIVITIES: PERFORMANCE INDICATORS**

**Levkina R.V.**, Dr. ec. sc., prof.  
*Odesa Polytechnic National University*  
**Levkin A.V.**, PhD., associate prof.  
*State Biotechnological University*

The digital transformation of entrepreneurship and society as a whole requires new approaches to the organization of business and the introduction of information technologies in all spheres of life. Under such conditions, access to necessary information resources is significantly simplified and information about goods (services) is distributed accordingly. The majority of potential buyers get information about products on the Internet. Their share is constantly increasing.