- explore innovative supervision models using sandboxes, big data, and cloud computing.

- enhance supervision capabilities across different digital currency application scenarios.

5. Mitigating operational risks and safeguarding data privacy:

- strengthen supervision and support for vulnerable areas to prevent financial risks.

- promote orderly competition, discourage fraud, and educate the public about digital currencies.

- prioritize data security and protect public interests and the credibility of the digital UAH.

- monitor financial asset price volatility and prevent potential risk transmission chains.

By implementing these policy recommendations, the digital UAH can be effectively harnessed to promote economic development while mitigating associated risks and safeguarding financial stability and privacy.

References:

1. Bordo，M.D. Levin，A.T. (2017). Central Bank Digital Currency and the Future of Monetary Policy. NBER Working. Paper 237.

2. Barrdear，J.，Kumhof，M. (2016). The Macroeconomics of Central Bank Issued Digital Currencies. Bank of England Staff Working Papers No. 605.

UDC 04.002:658.5

A. Levkin, Candidate of Technical Science, Assoc. Prof. (*SBTU, Kharkiv*)
Ya. Kotko, Candidate of Economic Sciences (*SBTU, Kharkiv*)

THE LATEST CYBERSECURITY TECHNOLOGIES IN THE CONTEXT OF DIGITAL TRANSFORMATION

Continuous development and implementation of the latest cybersecurity technologies to protect confidential information at the enterprise, minimize financial losses in commodity and monetary transactions, create an effective system and prevent cyberattacks, including phishing attacks, allows to improve the protection of the integrity of the processes of economic activity of enterprises.

In addition, most of the latest technologies should take into account, first of all, advances in artificial intelligence (monitoring of huge amounts of information, possible risks and potential threats to form accurate forecasts of business activities of enterprises); biometrics (use of algorithms to analyze user behavior and detect hacker actions); hybrid models; multi-factor cloud technologies (technologies for eliminating risks with network user authentication, encryption and access control to proprietary data) [1, S. 12–20].

As the volume of digital technologies introduced grows every year, participants in the information environment must update and ensure the protection of their data. To help business entities, government officials, and society in general effectively protect their confidential information, cybersecurity system developers need to implement modern programs to protect large amounts of information. Here are the most common information security programs: Eperi (provides full protection of information using encryption methodology); Acronis (provides full backup and restoration of individual elements from the entire system, selection of the main information complexes for constant protection, taking into account constant changes and automatic backups); Barracuda (protects data using cloud virtual machines, including information encryption); CybeReady (focuses on the human error factor that causes the leakage of confidential information, uses the latest methods to raise awareness of cybersecurity of information environments); Spectral (filters incorrect key configurations and scans the cybersecurity life cycle of software to detect information leakage) [2, S. 13–20; 3, Pp. 139–142].

Cybersecurity is of particular importance for all business entities in a full-scale war, as cyberattacks, key breaches, information leaks and phishing emails undermine the country's national economy and defense capabilities. Since the beginning of the war, Ukraine has seen 2,800 attacks against government agencies, businesses, and other participants in the information environment. According to Microsoft, in 2022, most cyberattacks in the world were directed against the United States and Ukraine (over 20%).

According to the authors of these studies, in order to combat cyberattacks on the country's information environment and infrastructure, it is necessary to introduce the latest technologies to minimize intrusions into the information environment and reduce data leakage. Some Ukrainian organizations use a set of cybersecurity programs, including Email Security (to prevent data loss, protect against malicious traffic), Network Access Control (to protect the information network from unknown intruders), Endpoint Security (to protect all infrastructure elements from system hacking and prevent virus infection of servers), etc.

Cybersecurity plays a crucial role in the regular protection of sensitive data information through various technologies and programs that provide backup and recovery of information in case of loss. This is achieved by encrypting, archiving and authenticating data and ensures full management and access to confidential information from anywhere in the country at any time.

References:

1. Letychevskyi O.O. Suchasni naukovi problemy kiberbezpeky. *Visnyk NAN Ukrainy*. 2023. № 2. S. 12–20. URL: https://doi.org/10.15407/visn2023.02.012

2. Onyshchenko S., & Hlushko A. Analitychnyi vymir kiberbezpeky Ukrainy v umovakh zrostannia vyklykiv ta zagroz. *Ekonomika i region*. 2022. Vol. 1. Issue. 84. S. 13–20. URL: https://doi.org/https://doi.org/10.26906/EiR.2022.1(84).2540.

3. Levkin A., Levkina R., Petrenko A., & Chaliy I. Economic Security as a Result of Modern Biotechnology Implementation. *Problems of Infocommunications Science and Technology (PIC S&T'2019): 2019 IEEE International Scientific-Practical Conference (Kyiv 8-11 October 2019).* Kyiv, 2019. Pp. 139–142.

UDC 04.002.658.5

D. Levkin, Candidate of Engineering Science, Assoc. Prof. (*SBTU, Kharkiv*)
O. Zhernovnykova, Dr of Pedagogical Science, Prof. *(H.S. Skovoroda KNPU, Kharkiv)*
Ya. Kotko, Candidate of Economic Sciences (*SBTU, Kharkiv*)

MODERN MATHEMATICAL METHODS IN THE CYBER SECURITY SYSTEM

A modern cyber security system ensures data processing and storage, confidentiality, availability and integrity of information. Various relationships between data types and methods of combating possible cyber attacks are based on known mathematical models and algorithms from computational methods for their implementation. Mathematical methods and computational methods are the basis of confidential information protection systems, detection and prevention systems of potential cyber threats. To increase the effectiveness of cyber protection of the data environment, it is necessary, if possible, to develop new mathematical models and methods of their implementation, as well as to modernize already existing mathematical models and computational methods that will take into account the specific features of the simulated systems [1, S. 6–13]. This, in turn, will complicate the type of boundary value problems, systems