Секція 7
ЄВРОІНТЕГРАЦІЯ Й ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ

INFORMATION SECURITY OF UKRAINE: STATE AND PROSPECTS OF DEVELOPMENT

Kotsur S.O., applicant for educational degree «master's»
Supervisor – Candidate of Economic Sciences, Associate Professor **Y.M. Kotko**
State Biotechnology University

The state policy in the field of information security and critical infrastructure protection requires special flexibility and adaptability to meet the changing requirements of today. In the context of a full-scale war, the number of cyberattacks and threats against government agencies, defense industries, IT networks, etc. has increased significantly.

According to the State Service for Special Communications, in 2023 the number of cyberattacks increased by 16% and reached 2,543 incidents compared to 2022. According to some estimates by experts from the National Security and Defense Council's Information Security and Cybersecurity Service, Ukraine has managed to gain an advantage in countering cyberattacks and information aggression. However, the enemy is constantly maneuvering and improving, so the most important issue today is to identify weaknesses and their reliable cyber defense [1, p. 85; 87-89].

Accordingly, every country in the world, and Ukraine is no exception, must comply with current trends in the digital space and cybersecurity, in particular:

- large-scale disinformation (the use of generative artificial intelligence models to create more realistic and complex fakes with audio and visual phishing tools to obtain confidential user data or damage an individual network);
- political cyberattacks by other states (the use of malware and cloud technologies that affect the management of large organizations in critical infrastructure and partnerships in sensitive industries);
- multi-vector DDoS attacks (the use of several different protocols simultaneously increases the effectiveness of cyberattacks and complicates the possibility of their detection and leakage of credentials to compromise digital logins);

- phishing cyberattacks (unethical use of artificial intelligence will allow the creation of phishing emails with intelligence in real-time according to various scenarios or the creation of keyloggers for fraudulent actions);

- high-risk APIs (AI programs and applications are a powerful tool for improving and analyzing information, but they can lead to unexpected risks - identifying weaknesses in the cyber resilience of government agencies/enterprises) [2, pp. 53; 55-57].

Information security for Ukraine is essential for the functioning of our economy and society, the smooth operation of critical infrastructure, educational institutions, data and communication privacy, and national defense.

Accordingly, it is necessary to introduce ways of its development, including: implementing international standards and best practices in the field of cybersecurity (GDPR, PSTI, RED); establishing active cooperation between various institutions, enterprises or institutes to ensure the security of cyberspace; introducing significant changes in the higher education system (acquiring a specific range of knowledge and skills required in the modern labor market; acquiring social and communication skills; self-development and self-improvement); development and implementation of state programs/grants (educational project "re/start in cyber"; program "Cyber Defenders" - provides comprehensive training in cyber defense and cyber defense); increased investment in the development of modern technologies and security practices, etc. After all, all these areas have gained even greater relevance today, as they are aimed at countering modern approaches to cyberattacks, minimizing their risks and forming the concept of cyber resilience of the state.

Information sources:

1. Hrosul V., Galoyan D., Mkrtchyan T., Volosov A., Balamut H., Kolesnyk A. Assessment of digital maturity, the transformation of business models in the context of digital transformation. *Reice-Revista Electronica de Investigacion en Ciencias Economicas.* - 2023. - Vol. 11, Issue 21. - P. 81-105. - DOI 10.5377/reice.v11i21.16546.

2. Kameneva I.P., Artemchuk V.O. Problema informatyvnosti ta vyznachennia informatyvnykh struktur dlia pidtrymky pryiniattia rishen v haluzi ekolohichnoi bezpeky. *Elektronne modeliuvannia*. 2022. Vol. 44. No. 3. S. 50–64. https://doi.org/10.15407/emodel.44.03.050

3. Kavun S., Levkina R., Kotko Ya., Levkin D., Levkin A. Information Security in Project Management for the Financial and Budgetary Capacity of the National Economy. *CEUR Workshop Proceedings: Cybersecurity Providing in Information and Telecommunication Systems* II, CPITS-II 2023, Kyiv, October 26, 2023. - Kyiv, 2023. - Vol. 3550. - P. 246-254.