Міністерство освіти і науки України

Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

Навчально-науковий інститут фінансів, економіки,
управління та права
Кафедра фінансів, банківського бізнесу та оподаткування

ЕКОНОМІЧНА БЕЗПЕКА: ДЕРЖАВА, РЕГІОН, ПІДПРИЄМСТВО

Матеріали IX Міжнародної
науково-практичної конференції

15 травня 2025 р.

Полтава
2025

5. Шмигаль: Україна отримала перші 3 млрд євро від ЄС за рахунок заморожених активів Росії URL https://www.radiosvoboda.org/a/news-ukraina-3-mlrd-euro-es-aktyvy-rosii/33271034.html

6. Перший транш кредиту у розмірі 752 млн фунтів стерлінгів надіслано Україні на військову техніку URL https://www.gov.uk/government/news/first-752-million-tranche-of-loan-sentto-ukraine-for-military-equipment

7. У 2025 році ЄС надасть Україні 35 млрд євро фінансової допомоги URL https://sud.ua/uk/news/ukraine/321409-v-2025-godu-es-predostavit-ukraine-35-mlrd-evro-finansovoy-pomoschi

UDC 658.012.32

Dmytrenko Alla,
D.Sc. (Economics), associate professor,
Associate Professor of Finance, Banking and Taxation
Dorokhova Tetyana,
master's student
National University "Yuri Kondratyuk Poltava Polytechnic"

CYBERSECURITY AS A KEY ELEMENT OF THE STATE'S ECONOMIC SECURITY

Cybersecurity, as a component of economic security, plays a crucial role in ensuring the stability and resilience of the state. In the context of globalization and constant changes in information technology, protecting critical infrastructure and information systems is becoming a priority for governments. Cyberattacks have a significant impact on the economy of a country. According to research, losses from cyberattacks in the world are growing annually [3]. In addition, a study of the impact of cyberattacks on the economy shows their multifaceted nature. Direct financial losses

include the theft of funds, disruptions in payment systems, the cost of restoring damaged systems and paying insurance claims.

In addition, attacks on financial institutions can destabilize financial markets. Indirect losses are manifested in the form of disruption of production processes, logistics chains, loss of business reputation, outflow of customers and investments [1]. For example, an attack on the banking system can lead to massive losses of customers, reduced investment and economic activity. The consumer sector also suffers losses when companies lose access to customer data and cannot fulfil their obligations. Cyber-attacks on critical infrastructure, such as energy networks, transport systems and financial institutions, can lead to large-scale economic crises and threaten national security. An analysis of modern cyber threats shows that they are becoming more complex and targeted [2].

Therefore, to counter cybersecurity threats, the state must develop comprehensive strategies. The main components of such strategies include development and implementation of legislative acts regulating activities in the field of cybersecurity. This also includes the protection of personal data, liability for cyberattacks and response mechanisms; investing in the education and training of cybersecurity professionals. It is also important to ensure that software is regularly updated; developing cyber-attack response plans, including the creation of rapid response teams that can respond quickly to threats and restore systems [4]. The growing number and sophistication of cyberattacks pose a significant threat to economic stability, causing direct and indirect financial losses, disrupting critical infrastructure, and undermining confidence in the digital economy. Effective counteraction to these threats requires a comprehensive approach, including improved legislation, awareness raising, and the creation of a national cybersecurity system, the introduction of modern security technologies, active international cooperation and support for the domestic cybersecurity industry. Successful implementation of

these strategies will not only reduce risks but also increase trust in digital technologies, which in turn will contribute to economic growth and stability of the state.

References

1. Cybersecurity: problems and solutions. Scientific Bulletin of Khmelnytskyi National University. 2020. С. 23-28.

2. Lysiak OI. Economic security of the state in the conditions of its formation. Economic analysis. 2021. С. 11-13.

3. Threats and challenges in the field of cybersecurity: the role of artificial intelligence. Bulletin of the National Academy of the Security Service of Ukraine. 2022. С. 9-14.

4. Onyshchenko S., Yanko A., Hlushko A., Maslii O., Cherviak A. Cybersecurity and improvement of the information security system. *Journal of the Balkan Tribological Association*. 2023. 29(5). pp. 818–835.

УДК 005

Орєхова Альвіна Іванівна,
завідувач кафедри менеджменту імені професора
Л.І. Михайлової, д.е.н., професор
Сумський національний аграрний університет

ОСОБЛИВОСТІ АНТИКРИЗОВОГО МЕНЕДЖМЕНТУ ПІДПРИЄМСТВ В УМОВАХ НЕВИЗНАЧЕНОСТІ

Сучасне бізнес-середовище характеризується зростаючою динамікою та непередбачуваністю. Геополітичні потрясіння, економічні коливання, технологічні прориви, пандемії та інші форс-мажорні обставини створюють високий рівень невизначеності, що значно підвищує ризики виникнення кризових ситуацій на підприємствах. Традиційні підходи до антикризового менеджменту, розроблені для більш стабільних умов, часто виявляються недостатньо ефективними в умовах глибокої та тривалої невизначеності.