MODERN DIGITAL TOOLS OF CYBERSECURITY IN THE SYSTEM OF ANTI-CRISIS MANAGEMENT OF ENTERPRISES

Oleksandr Pravdyvets
https://orcid.org/0000-0001-5242-9683
Ph.D. (Military Sciences), Associate Professor
Department of Financial and Economic Security Management,
Research and Training Institute of Security Management, "KROK" University, Kyiv

The modern globalized world is actively developing in a new paradigm of the information society, a world where global cyberspace plays a significant role in our lives, improving cybersecurity is an essential component of ensuring information security, economic development and national security. Economic conditions and changes in the global technological landscape force Ukrainian enterprises to introduce modern digital tools to ensure their cybersecurity, while, as noted in, the recent innovative development of economic security systems of modern Ukrainian enterprises is characterized by the active use of digital technologies. Therefore, the protection of enterprises' digital infrastructure is a key element of their overall economic security system, as cyber threats can have catastrophic consequences for financial stability, reputation, and business competitiveness. In confirmation of this, Roger Spitz, President of the Institute for the Future noted that the importance of cybersecurity at the moment should be at the level of national security. In the modern global information society, the growing importance of cyberspace in both personal and professional life underscores the need for enhanced cybersecurity. As economic conditions and technological advancements evolve rapidly, Ukrainian enterprises are compelled to implement modern digital tools to protect their digital infrastructure. The adoption of digital technologies is now a defining feature of the economic security systems of Ukrainian businesses. Given the potentially catastrophic consequences of cyber threats on financial stability, business reputation, and competitiveness, cybersecurity has become a strategic priority on par with national security. The study presents an overview of the main classes of digital cybersecurity tools, emphasizing their role in detecting, preventing, and responding to digital threats. Among the most critical are AI-based threat detection systems capable of identifying anomalous network activities and adapting to changing conditions through machine learning. In addition, data protection technologies such as encryption, access control, and backup and recovery systems are essential to ensure

the integrity and resilience of business operations. Another focus of the research is on multi-factor authentication and identity management tools that significantly enhance protection against unauthorized access and strengthen digital trust within corporate systems. Practical applications of such tools are explored across key sectors. In finance, for example, cybersecurity technologies help monitor and block suspicious transactions, while in energy, real-time monitoring systems help ensure the continuity and protection of infrastructure. The paper also emphasizes the necessity of a tailored approach to cybersecurity implementation. Effective integration of digital protection tools requires both technical solutions and organizational strategies, including the development of internal policies, staff training, and system audits. Recognizing the diversity of the cybersecurity market, the study assesses tools based on cost-effectiveness using two main criteria: price and quality. Three categories of cybersecurity products were identified:

1. High Quality, High Price: Suitable for large enterprises, with products like Palo Alto Networks, Cisco Secure IDS/IPS, and CrowdStrike Falcon offering scalable protection.

2. High Quality, Reasonable Price: Tools such as Microsoft Azure MFA, Duo Security, and Bitdefender GravityZone provide a good costfunctionality balance for medium-sized businesses.

3. Good Quality, Low Price: Symantec Encryption and Vormetric Data Security Platform serve the needs of small and medium enterprises with limited budgets.

The choice of cybersecurity products depends on the specific needs, scale, and risk exposure of each organization. The research concludes that the integration of digital cybersecurity solutions is not merely a technological upgrade, but a core component of enterprise resilience in the face of economic digitalization. Ongoing development, customization, and updating of these tools are essential to maintain operational continuity and defend against the ever-changing threat landscape in modern cyberspace. Thus, the use of modern digital cybersecurity tools is a prerequisite for maintaining anti-crisis resilience and security of enterprises in the context of digitalization of the economy. These tools provide effective solutions for detecting and preventing threats, as well as for protecting information resources from possible attacks. It is important that the integration and implementation of such tools into the crisis management system takes place taking into account the specifics of each enterprise's activities, and also requires constant development and updating, taking into account new challenges and threats in modern cyberspace.

Keywords

cybersecurity tools; digital economy; enterprise security; AI-based protection; identity management; information systems; cyber risk; digital resilience

References

1. Pravdyvets O.M., Kulakovskyi O.Yu. Modern cybersecurity paradigm. II International Conference "Cybersecurity: Intelligence, Protection and Counteraction..." VITI 23.04.2024. Kiev. P. 11. (Electronic resource – Access mode: https://cyberwarfare.viti.edu.ua/assets/files/Cyberwarfare_2024.pdf).
2. Pravdyvets, O., Litvin, N. Strategic directions of innovative development of the system of financial and economic security of the enterprise based on digital technologies. Financial and Credit Activity Problems of Theory and Practice, 6(59), pp. 273–282. (Electronic resource – Access mode: https://doi.org/10.55643/fcaptp.6.59.2024.4575).
3. Roger Spitz, Lidia Zuin - The Definitive Guide to Thriving on Disruption: Volume I - Ref2raming and Navigating Disruption 2022.
4. Korotchenko L.A., Degtyar O.A., Analysis of Methods of Cyber Warfare and Cyber Operations Used by the World's Leading Countries and NATO Members. Science and Technology Today. Kyiv – 2024. – No. 7(35) 2024. – P. 776 – 788.
5. Cyber component of the Russian-Ukrainian war: lessons and assessments of the international community. (Electronic resource – Access mode:https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/kiberskladnyk-rosiysko-ukrayinskoyi-viyny-uroky-ta-otsinky).
6. Ekonomichna Pravda – Special Project "Defense of Ukraine": Cyberattacks on Ukrainian Business Continue: How to Protect Yourself. (Electronic resource – Access mode: https://epravda.com.ua/projects/zakhyst-krainy/2024/05/03/713224/)