Technical sciences

UDC 004.6

Shevchuk Yurii

Master degree in Management of Information Security

Lviv Polytechnic National University,

Software engineer and Cybersecurity Expert, DataArt

ORCID: 0009-0008-3331-3886

CYBERSECURITY MANAGEMENT STRATEGY TO ENSURE THE PROTECTION OF PERSONAL AND CORPORATE DATA

Summary. *Cybersecurity encompasses a wide range of risks and measures that go beyond simply protecting personal data. Currently, businesses and individuals face serious threats in the form of sophisticated cyberattacks. In this regard, the development and application of cybersecurity in the field of information technology is a relevant and integral aspect in today's world, where information systems have become an important part of everyday life.*

The purpose of the article is to analyze cybersecurity management to ensure the protection of personal and corporate data.

Key words: *cybersecurity, personal and corporate data, cyberattacks, prevention.*

Cybersecurity is the process of protecting systems, networks and data from digital threats, and it goes far beyond simply safeguarding personal information. Effective cybersecurity plans must protect against a wide range of threats, including ransomware, phishing attacks, malware and complex persistent threats. These threats can compromise not only the confidentiality of individuals, but also the integrity of an organization, business continuity, and financial stability [5, p.6].

In the field of information technology, more and more companies and organizations are realizing the importance of cybersecurity and are paying a lot of attention to it. They create special departments and hire cybersecurity specialists to ensure reliable protection of information resources. In addition, the study of cybersecurity helps to develop new methods and technologies to protect against threats. Cybercriminals are constantly improving their methods, so it is important to stay ahead of the curve and adapt to new threats. Thus, the relevance of studying the development and application of cybersecurity in information technology is obvious. It helps to protect our digital lives and ensure the security of users, organizations, and nations [1].

The development and application of cybersecurity in the field of information technology is one of the most urgent tasks of modern development. Due to the increasing use of the Internet and digital technologies, cybersecurity threats are becoming more serious and widespread.

The protection of personal and corporate data is important to ensure the security of not only individuals and organizations, but also society as a whole. Figure 1 summarizes some measures that can help protect data.

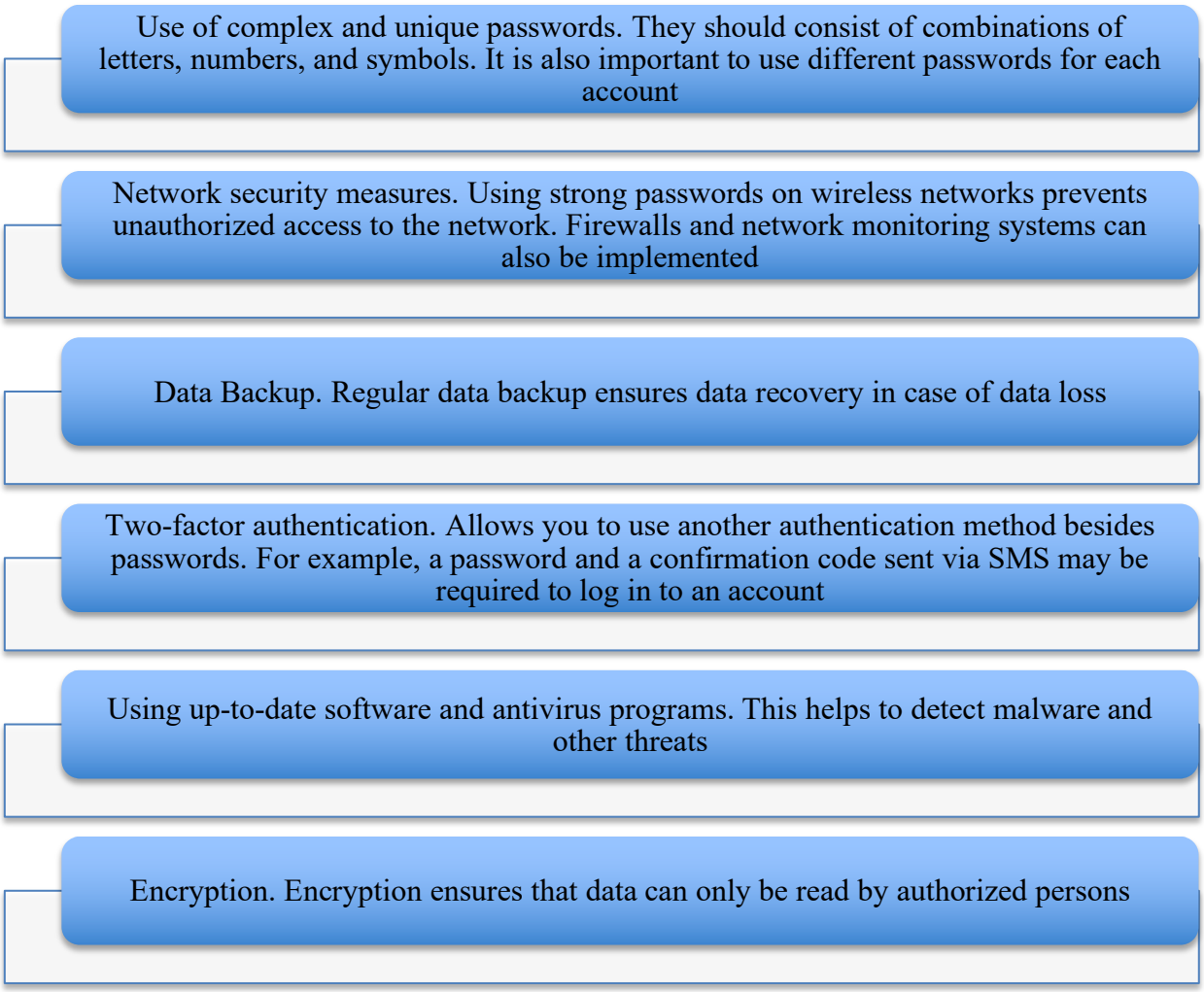

Fig. 1. Some measures to help protect data [3, p. 223]

Source: developed by author

Trust and stability in IT systems largely depend on robust information security measures. Training staff and implementing security awareness initiatives play a vital role in maintaining digital safety. As information and communication technologies continue to evolve, protecting computer networks from cybercriminal activities, unauthorized access, and various security breaches has become a fundamental priority. The field of cybersecurity focuses on establishing comprehensive defense mechanisms to safeguard digital infrastructure and sensitive data across different platforms and services.

With the growing sophistication of cyber threats, organizations must prioritize comprehensive security measures. Employee education initiatives,

coupled with detailed risk assessment procedures and strong IT security frameworks, form the cornerstone of modern cybersecurity strategy, particularly since human mistakes remain the primary vulnerability in most security breaches [9].

There is no foolproof way for any company to avoid a cyberattack, but there are a number of cybersecurity best practices that can help mitigate risk. Figure 2 summarizes some of the best practices for detecting and preventing cyberattacks.

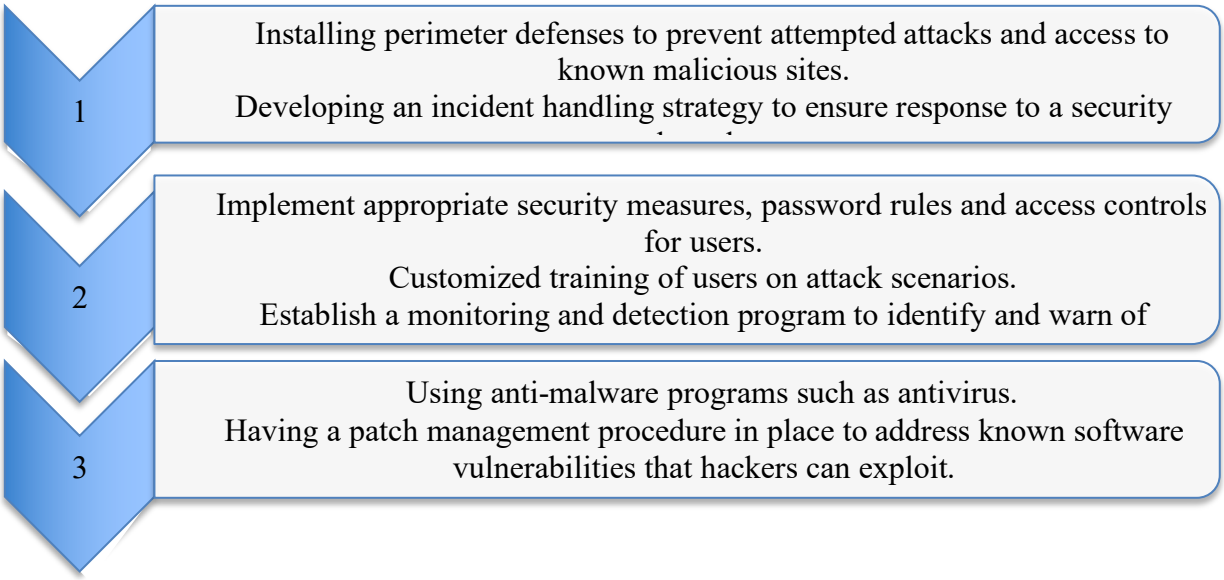

Fig. 2. Best practices for detecting and preventing cyberattacks [11]

Source: developed by author

Modern cybersecurity solutions include a wide range of tools, from antivirus software to password management systems. These technologies provide comprehensive protection, including data encryption, penetration testing and web vulnerability scanning.

Utilizing advanced defenses such as firewalls and incident response systems, cybersecurity software creates a strong barrier against various types of cyberattacks. Malware, ransomware, spyware and phishing attacks are just some of the threats that enterprise networks, mobile applications and software platforms are protected against. In critical situations, these tools also ensure disaster recovery and continuity of network infrastructure.

Modern companies actively employ various cloud platforms since relying on a single provider often proves insufficient for their diverse requirements. This multi-cloud approach is particularly common among organizations deploying containerized applications across different cloud service providers' infrastructures.

A crucial element in protecting these digital environments is specialized security software. Through encryption protocols and user authentication mechanisms, this technology safeguards critical systems from various threats. The protective features extend to defending against malicious programs that could compromise processing efficiency, breach confidential files, or inflict severe damage to computing infrastructure. Additionally, the software serves as a shield for confidential user credentials, including financial records, payment information, and personal identification numbers, preventing unauthorized access and malware infiltration.

Cloud migration presents both opportunities and challenges for modern enterprises. While organizations can leverage numerous advantages from cloud adoption, they must also navigate complex security landscapes that extend beyond conventional cybersecurity measures. Whether deploying applications across hybrid environments, private infrastructure, or public platforms, protecting various cloud components demands specialized knowledge. Security professionals need comprehensive expertise in safeguarding diverse elements like serverless architectures, container orchestration systems including Kubernetes, virtual machines, and other cloud-native workloads. This heightened security awareness becomes crucial as traditional protection methods alone prove insufficient for addressing cloud-specific vulnerabilities.

While on-premises IT systems provide increased security and control over data, they are costly to implement and require significant hardware purchases and maintenance, limiting scalability. However, cloud-based solutions, whether

public, private or hybrid, share many of the same security mechanisms as traditional approaches, but have unique security features.

Cloud adoption offers businesses unprecedented agility and operational efficiency. Without waiting for physical infrastructure deployment or hardware delivery, organizations can instantly leverage new services and resources. The cloud's on-demand nature enables companies to implement robust security measures that adapt to emerging threats while efficiently managing their data. This transformation brings remarkable advantages in terms of cost optimization and scalability. The flexibility and speed of cloud computing make it an attractive solution for organizations looking to modernize their infrastructure and streamline operations.

Software, networks, services and devices interact with the cloud through APIs that function as portals between systems. Cloud service providers control access mechanisms that regulate the flow of information. Sharing cloud infrastructure poses additional security threats because data is stored remotely and organizations' devices and servers must constantly access cloud servers. In this regard, securing the cloud environment involves not only securing the cloud itself, but also all components connected to it.

The main components of a cloud security strategy are characterized in Figure 3.

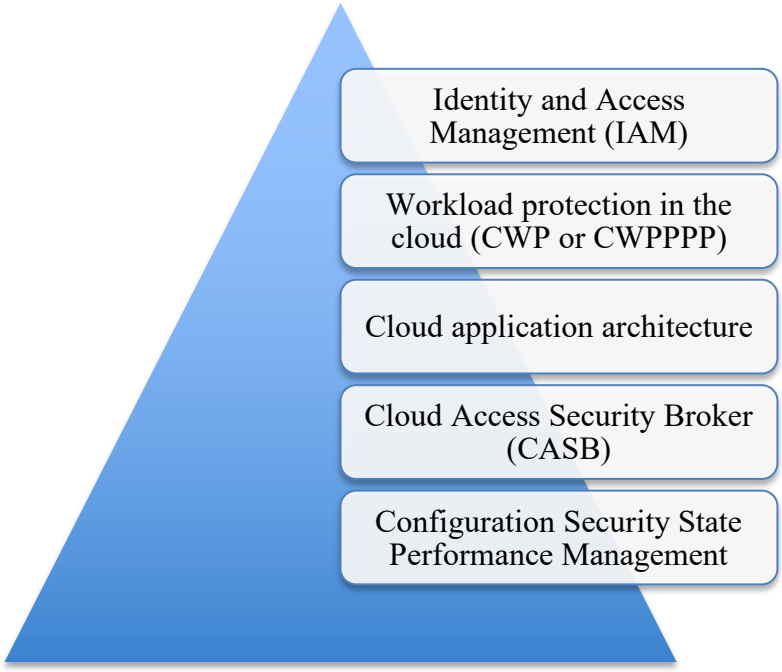

Fig. 3. Main components of cloud security strategy [2]

Source: developed by author

Organizations utilize IAM tools that implement security policies and manage identity data, while offering features like single sign-on. These solutions operate on the fundamental concept of least privilege access control. Though these systems help streamline access management, their security aspects sometimes fall short of expectations. The core principle ensures that employees receive minimal necessary permissions to perform their duties, with access granted only when required. By tracking user activities and enforcing strict policies, IAM platforms aim to maintain secure resource allocation, despite not always being primarily security-focused in their design.

Protecting cloud-based operations presents unique challenges due to their mobility across various providers and platforms. Security threats such as malware, zero-day vulnerabilities, and ransomware pose significant risks to cloud workloads, similar to how they affect high-performance professional desktop computers. The dynamic nature of cloud environments, where workloads frequently migrate between different hosts and vendors, necessitates a

collaborative security approach. CWPP technology offers essential protection for these moving workloads, particularly since both Windows and Linux-based systems face potential security breaches if left unprotected. The successful implementation of cloud security measures depends heavily on shared responsibility among all stakeholders involved in the process.

When developing software for cloud environments, it is critical to pay special attention to data protection. Companies need to carefully evaluate all aspects of security before implementing cloud services. In particular, the use of managed databases requires a thorough understanding of data protection mechanisms.

Creating a secure architecture for cloud applications involves many elements: implementing proven secure programming techniques, implementing strong authentication and authorization systems, and using cryptographic protocols to protect data in both transmission and storage.

Cloud security demands a fundamental shift in developer mindset. Unlike conventional development where security often takes a backseat, cloud-based applications require security considerations from day one. Organizations frequently take responsibility for validating the security of their cloud solutions, as data protection typically remains their duty rather than the provider's. To enhance cloud service security oversight, CASB technology serves as a specialized monitoring and control mechanism that organizations can implement.

Security policy enforcement and DLP rule implementation are managed through CASB servers that function as intermediary checkpoints between providers of cloud services and their users [4].

CASBs can also provide real-time activity monitoring so that security professionals can see which users are accessing cloud services and when. They are an important part of a cloud security strategy because they help ensure that only authorized users can access sensitive data, which helps prevent data leakage.

Organizations should consider using CASBs if they use cloud services to store or process sensitive data or if they must comply with data privacy regulations such as the EU's General Data Protection Regulation (GDPR).

CSPM solutions are designed to automate the identification and mitigation of risks in cloud infrastructures, making them easier to protect. Through continuous cloud risk monitoring, CSPM helps organizations prevent, identify, respond to, and predict risks in accordance with centralized governance, security, and compliance policies.

CSPM is especially important for Internet-accessible resources, as attackers are increasingly automating the search for vulnerabilities in cloud infrastructure. Because cybercriminals can easily access customer lists and intellectual property, security failures often make headline news.

If cloud storage services containing sensitive corporate information are misconfigured, it can lead to the inadvertent disclosure of that data to unauthorized parties. Fortunately, the Center for Internet Security (CIS) publishes guidelines for securely configuring cloud resources so that organizations can compare their level of security against best practices at any time.

Cloud services give organizations a clear view of activity on their network, allowing them to quickly identify potential threats. With thousands of accounts spread across multiple clouds, it's important to ensure that your cloud infrastructure is properly secured.

Cloud service providers typically provide a variety of tools to help users accomplish these tasks. For example, activity monitoring helps organizations identify malicious behavior and block it before damage is done. Many vendors also offer threat intelligence services that provide users with information on the latest threats and recommendations on how to protect against them.

The protection of sensitive corporate data and IT systems heavily relies on encryption technologies. When information travels through networks or is stored, cryptographic methods ensure its security by making it inaccessible without

specific decryption keys. This fundamental security approach has proven itself over centuries as an essential defensive tool.

By transforming readable data into scrambled code, cryptography prevents unauthorized individuals from accessing sensitive information, even if they manage to intercept it. This security measure has become indispensable in modern computer networking, where companies must safeguard their digital assets. The beauty of cryptographic systems lies in their ability to render data incomprehensible to anyone lacking the proper decryption credentials, while still allowing authorized users seamless access.

Different organizations require unique cryptographic solutions based on their individual management demands and security frameworks. To achieve optimal encryption protection tailored to your particular requirements, collaborating with an MSSP (managed security service provider) represents the most effective approach [10].

In general, there are two types of cryptography commonly used in the cybersecurity field, shown in Figure 4.

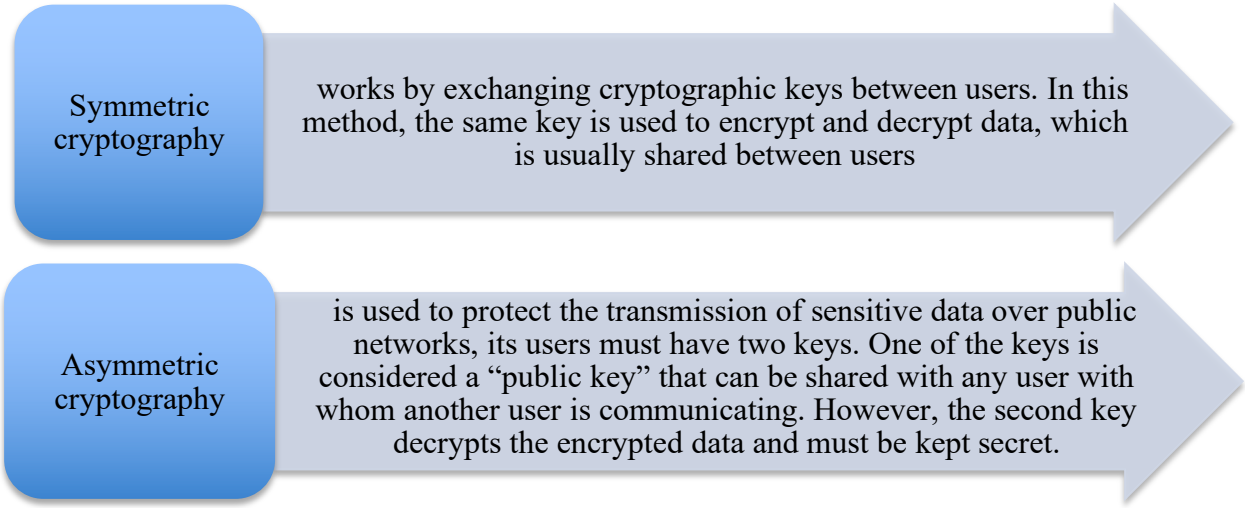

Fig. 4. Types of cryptography [10]

Source: developed by author

In practice, as with the basic types, there are two main approaches or methods of cryptography that work together to protect data:

- data encryption is the process of using an algorithm to convert binary data from one form to another, accessible only with a specific key. To make encryption work, an algorithm converts plaintext into a hard-to-decipher form (also called ciphertext) that can only be converted back to plaintext using a cryptographic key. The development of sophisticated encryption algorithms will help increase the security of data transmission and minimize the risk of data compromise;

- decryption - is the reverse process of encryption. Using a cryptographic key corresponding to an encryption algorithm, a user can decrypt sensitive data stored or transmitted over a network.

Depending on the complexity and reliability of the algorithms used, both encryption and decryption in cryptography can help optimize security and protect sensitive data [8, p.395].

Some of the common applications of cryptography are as follows:

1.Encryption of BYOD devices. Regulations (BYOD) allow employees to use their personal phones and computers at work or for on premises and possibly for work tasks. But BYOD devices are at high risk of security threats if they are used on unsecured public networks.

2.To guard against unauthorized access, organizations must prioritize email security through robust encryption protocols, particularly when handling confidential information. Secure key management and end-to-end encryption solutions play a vital role in preventing cybercriminals from intercepting and exploiting sensitive email content.

3.Additionally, the growing trend of personal device usage in the workplace demands enhanced security measures. When staff members are allowed to use their own devices either on-site or for remote work, implementing strong encryption protocols becomes crucial. This is especially critical since personal devices accessing or storing company data significantly increase the organization's vulnerability to potential data breaches.

4.Database encryption is critical to minimize risks when storing information both on-premises and in the cloud. This is especially true when dealing with sensitive information about customers, employees, and company intellectual property.

5.Encryption also plays a key role in securing various types of corporate data. First of all, it concerns financial documents of the organization and its business partners, as well as personal data of employees that require special protection.

In today's world of data protection, HTTPS protocol plays a key role in securing websites, guaranteeing the confidentiality and authenticity of online transactions. TDE transparent encryption technology is widely used to protect databases and is particularly effective when working with SQL systems. These encryption methods are critical to safeguarding sensitive information, including customer and vendor data [8, p.397].

HTTPS encryption also helps to protect against attacks such as DNS spoofing, where cyber criminals try to redirect users to insecure websites to steal their sensitive information. HTTPS encryption is also widely used in customer-oriented industries such as retail, where customers can immediately identify an insecure website by the presence of "https" in the URL.

Reference

1. Alahmari A., Duncan B. (2020) Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. Paper presented at the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020, 15-19 June 2020, Dublin, Ireland). https://doi.org/10.1109/CyberSA49311.2020.9139638

2. AlDaajeh S., Saleous H., Alrabaee S., Barka E., Breitinger F., Choo K.K.R. (2022) The Role of National Cybersecurity Strategies on the Improvement

of Cybersecurity Education. Computers and Security, 119, 102754. https://doi.org/10.1016/j.cose.2022.102754

3. Carayannis E.G., Grigoroudis E., Rehman S.S., Samarakoon N. (2021) Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience. IEEE Transactions on Engineering Management, 68(1), 223–234. https://doi.org/10.1109/TEM.2019.2909909

4. Firoozjaei M.D., Mahmoudyar N., Baseri Y., Ghorbani A.A. (2022) An Evaluation Framework for Industrial Control System Cyber Incidents. International Journal of Critical Infrastructure Protection, 36(C), 100487. https://doi.org/10.1016/j.ijcip.2021.100487

5. Furnell S., Bishop M. (2020) Addressing Cyber Security Skills: The Spectrum, Not the Silo. Computer Fraud and Security, 2020(2), 6–11. https://doi.org/10.1016/S1361-3723(20)30017-8.

6. Jiang L., Jayatilaka A., Nasim M., Grobler M., Zahedi M., Ali Babar M. (2022) Systematic Literature Review on Cyber Situational Awareness Visualizations. IEEE Access, 10, 575–577. https://doi.org/10.1109/access.2022.3178195.

7. Li Y., Liu Q. (2021) A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments. Energy Reports, 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126.

8. Marcantoni M., Jayawardhana B., Perez Chaher M., Bunte K. (2022) Secure Formation Control via Edge Computing Enabled by Fully Homomorphic Encryption and Mixed Uniform-Logarithmic Quantization. IEEE Control Systems Letters, 7, 395–400. https://doi. org/10.1109/LCSYS.2022.3188944.

9. Michalec O., Milyaeva S., Rashid A. (2022) When the Future Meets the Past: Can Safety and Cyber Security Coexist in Modern Critical Infrastructures? Big Data & Society, 9(1), 205395172211083. https://doi.org/10.1177/20539517221108369.

10. Morgan P.L., Collins E.I.M., Spiliotopoulos T., Greeno D.J., Jones D.M. (2022) Reducing Risk to Security and Privacy in the Selection of Trigger-Action Rules: Implicit vs. Explicit Priming for Domestic Smart Devices. International Journal of Human – Computer Studies, 168, 102902. https://doi.org/10.1016/j.ijhcs.2022.102902.

11. Rajan R., Rana N.P., Parameswar N., Dhir S., Sushil S., Dwivedi Y.K. (2021) Developing a Modified Total Interpretive Structural Model (M-TISM) for Organizational Strategic Cybersecurity Management. Technological Forecasting and Social Change, 170, 120872. https:// doi.org/10.1016/j.techfore.2021.120872.