Kateryna Pugachevska
Candidate of Economic Sciences, Docent,
Associate Professor at the Department of Management,
Economic Processes Management and Tourism
Mukachevo State University

Пугачевська К.Й.
кандидат економічних наук, доцент,
доцент кафедри менеджменту,
управління економічними процесами та туризму
Мукачівського державного університету

DOI: https://doi.org/10.30525/978-9934-26-501-3-47

INFORMATION SECURITY MANAGEMENT OF THE ENTERPRISE: MODERN APPROACHES AND CHALLENGES

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА: СУЧАСНІ ПІДХОДИ ТА ВИКЛИКИ

In the age of digital technologies, the protection of sensitive information has become a vital concern for organizations across industries. One of the most effective ways to safeguard an organization's digital assets is through the implementation of an information security management system. This problematic is especially relevant for domestic enterprises, because Ukraine is in the first positions in the rank of countries exposed to cyber attacks by other states. It is worth mentioning as well that the most massive cyberattacks that have taken place in recent years: on February 15-16, 2022 the most powerful cyberattack targeted state websites, the Diya portal and online services of state banks, including Privatbank and Oschadbank; December 12, 2023 – a cyber attack on Kyivstar left 24,4 million subscribers without mobile signals and internet for days, and the company lost 10% of its annual turnover; January 25, 2024 – a cyber attack on the "Parkovy" data center, whose clients are state-owned companies, as a result, the services of "Naftogaz", "Ukrposhta", "Ukrzaliznytsia" and "Shlyah" border crossing system partially did not work.

An information security management system (ISMS) offers several significant benefits to organizations: risk management, compliance, customer trust, cost savings, competitive advantages. By following best practices and aligning with established frameworks, enterprises can effectively implement and maintain an ISMS that not only helps mitigate threats but also provides a competitive advantage in the market by enabling opportunities [1].

Since modern information security systems as fairly complex organizational and technical systems function in conditions of uncertainty of external and internal information environment, the management of such systems should be based only on the results of the system analysis. The implementation of the system approach includes a complex of interrelated measures with the use of special technical and organizational means, normative legal acts. The system approach allows to define the provision of information security as a complex type of activity that imposes special requirements on its structural characteristics.

In a study conducted by Microsoft at the end of 2023 [2] millions of attacks of various types on its own customers were analyzed and the three most common reasons for hacking IT systems were identified: weak identity control; inefficiency of operational security processes, which not only creates conditions for a cyber attack, but causes a long recovery as well; lack of an effective data protection strategy. At the same time, according to

Microsoft experts, the structure of the cybercriminal economy may include: a RaaS operator (organizations that develop and support tools for the operation of ransomware, in particular, developers who create payloads for malicious software, and payment web portals for communication with victims); RaaS program (or syndicate) (operator-affiliate agreement); affiliates (small groups of people who are associated with one or more RaaS programs and whose role is to hack organizations and deploy RaaS program payloads on victims' IT systems); access brokers (intermediaries who sell access to the network to other cybercriminals or gain access themselves through virus campaigns or exploitation of weak points); organizations and individuals (organizations that have weak cybersecurity practices).

Throughout 2023 the number of EMEA DDoS attack events climbed to almost 2500, more than three times as high as those experienced in the Asia Pacific and Japan and Latin America combined. The complexity and severity of DDoS attacks have been transformed by geopolitical motives, which is why there's been an increase in hacktivism and nation-state-sponsored attacks alike.

According to Akamai research [3], hackers most often use DNS attacks – hacking through the domain name spoofing network. Also, despite the return to L3 and L4 attacks (attacks at the level of the infrastructure), the attacks of the 7th level have also affected many spheres – intelligent attacks that are aimed at finding weak points in the infrastructure. In Europe, the Middle East and Africa, the most DDoS attacks of the 3rd and 4th levels occur in the field of financial services, and the attacks of the 7th level – in the field of e-commerce.

In Ukraine 2543 cyber incidents were recorded in 2023, which is 15,9% more than in 2022. According to the government computer emergency response team CERT-UA, 347 cyber attacks were recorded against the government and government organizations, 276 – for local authorities, 175 – for organizations in the security and defense sector, 127 – commercial organizations. The energy sector was attacked 92 times, the telecom sector 81 times, educational institutions 38 times [4].

These trends in Ukraine and the world once again prove the need to strengthen information protection, to constantly update software in accordance with the development of technologies. Thus, information security is one of the key components of global security. In the process of globalization, in the context of information society, the role of information security will continue to grow.

References:

1. The Role and Implementation of an Information Security Management System in Modern Enterprises. Available at: https://ctrl-disrupt.nl/en/-insights-news/the-role-and-implementation-of-an-information-security-management-system-in-modern-enterprises (accessed October 19, 2024).

2. Microsoft Digital Defense Report 2023. Available at: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023 (accessed October 20, 2024).

3. State of Internet Reports. Available at: https://www.akamai.com/security-research/the-state-of-the-internet (accessed October 19, 2024).

4. State Service of Special Communications and Information Protection of Ukraine. Available at: https://cip.gov.ua/en/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti (accessed October 19, 2024).