International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com || Volume 11 - Issue 01 || January 2025 || PP. 16-19

Ensuring Security in Cyberspace

Denys Malakhov,
CEO, expert in creating websites based on WordPress
DM LLC WEB STUDIO, Florida

Annotation: The article analyzes the specifics of ensuring security in cyberspace. The concept and essence of cyber threats and cyber attacks, statistics of the consequences of successful cyber attacks in Russia are considered. The main types of cyber threats and the goals of cybercriminals are given. The areas of ensuring the cybersecurity of the organization are identified, the possibility of using artificial intelligence and machine learning technologies is noted. The importance of a proactive position in cybersecurity issues is emphasized.
Keywords: cyberspace, cyber threats, cyber attacks, cybersecurity, cyber resilience.

The rapid development of technology has led to the formation of a new environment in which human life is carried out – cyberspace [1]. Cyberspace is represented by a complex of computer networks filled with digital content. It includes all the elements of social reality – social groups, processes, relationships, structure, dynamics, norms and values. Its specific features are the lack of centralization, symmetry and orderliness, a large and solid communication network, high mobility, cross-border, dynamic but chaotic interaction of all elements. A number of phenomena and effects that arise during the functioning of cyberspace pose a danger to humans and society.

The technological capabilities of cyberspace enhance accessibility, simplify interaction, and ensure anonymity. [2]. However, these conditions are favorable not only for ordinary users, but also for cybercriminals. As a result of the increasing use of information technology, cyber threats and cybercrimes are growing and spreading, which makes it important to study the means and methods of ensuring security in cyberspace.

The purpose of the work is to study the specifics of ensuring security in cyberspace. To achieve this goal, an analysis and synthesis of cybersecurity materials was carried out, and a system-structural approach was applied to the consideration of key aspects of the research problem.

Cyber threats are operational risks to information and technology assets that have consequences affecting the confidentiality, accessibility, and/or integrity of information or information systems. [3]. They can have different probability of realization and intensity. A cyberattack is an unauthorized action aimed at violating the security policy, causing damage or disrupting the operation of services or access to information of a cyber asset. [4]. Cyber attacks are carried out using cyber weapons, systems used to damage the structure or operation of other cyber systems.

In the United States, as in the world as a whole, the number of cyber attacks on the public sector, companies and individuals is increasing quarterly. According to Check Point estimates, in Q3 2024, the number of incidents has increased by 75% worldwide and by 56% in the United States compared to Q3 2023. [5]. The most common consequences of successful cyber attacks are shown in Figure 1.

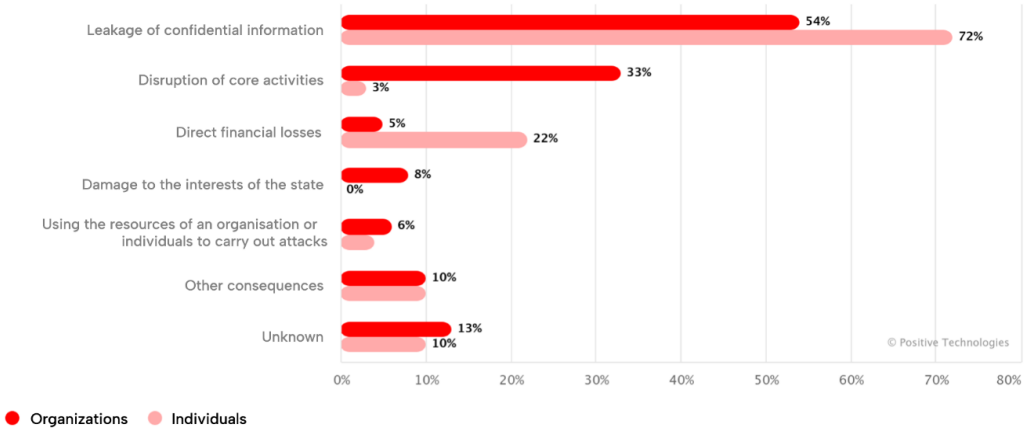

Fig. 1 – Consequences of successful cyber attacks
(leakage of confidential information, disruption of core activities, direct financial losses, damage to the interests of the state, using the resources of an organization or individuals to carry out attacks, other consequences, unknown // organizations, individuals)

The main types of cyber threats include [6, 7]:

1. Virus software. Software in which a file or program can be used to harm a user's device. The most common types of malicious software are shown in Figure 2.

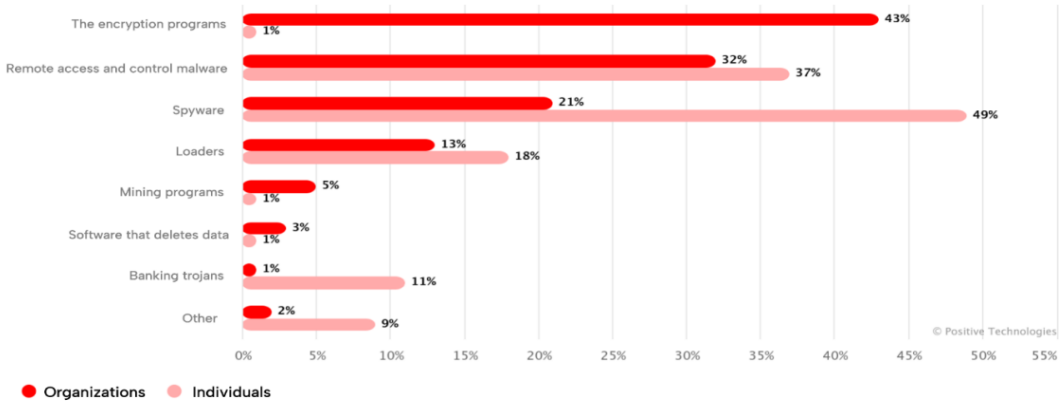

Fig. 2 – Statistics of successful attacks using different types of malware
(the encryption programs, remote access and control malware, spyware, loaders, mining programs, software that deletes data, banking trojans, other // organizations, individuals)

2. **Ransomware:** Software that allows an attacker to block the system files of the victim's device and demands payment for their decryption and unlocking.
3. **Social Engineering:** Attacks based on manipulation in the process of human interaction: The attacker tricks the user into violating security procedures in order to obtain confidential information.
4. **Phishing:** The attack is implemented in the form of mass mailing of fraudulent emails that look like messages from reliable or well-known sources. The purpose of phishing messages is to steal confidential data.
5. **Distributed denial-of-service attacks (DDoS):** When implemented, several attacking systems disrupt the traffic of the target system, such as a server, website, or other network resource. By flooding the target with messages, connection requests, or packets, DDoS attacks can slow down the system or cause it to crash, preventing legitimate traffic from using it.
6. **Advanced persistent threats (APT):** This is a targeted attack when an attacker penetrates the network and remains unnoticed for a long time, stealing data.
7. **Man-in-the-middle attacks (MitM):** These attacks are interception attacks in which an attacker intercepts and relays messages between two parties who believe they are communicating with each other.
8. **SQL injection:** A method that allows an attacker to gain access to a web application's database by injecting a string of malicious SQL code into a database query. SQL injection provides access to confidential data and allows attackers to execute harmful SQL statements.

The main goals of cybercriminals are shown at Figure 3.

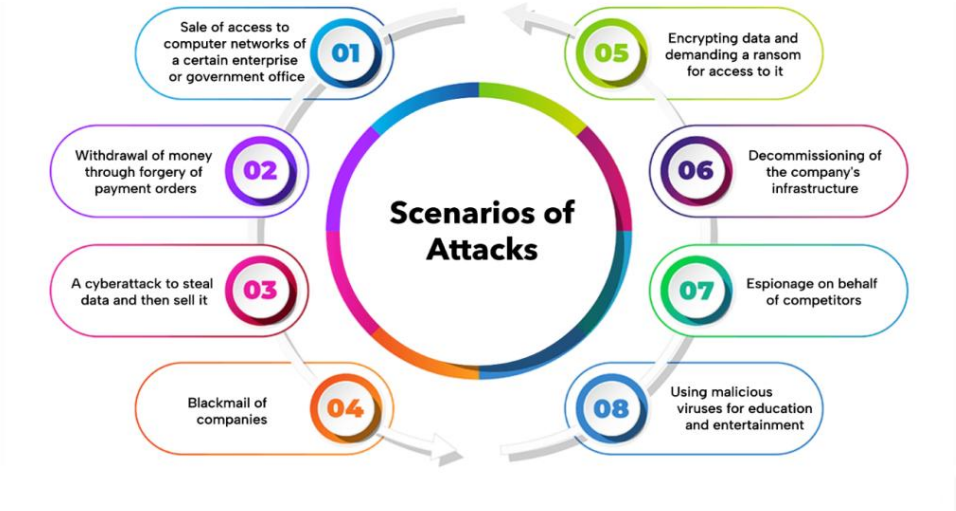

Fig. 3 – Scenarios of Cybercriminal Attacks

(Scenarios of Attacks – 01 Sale of access to computer networks of a certain enterprise or government office – 02 Withdrawal of money through forgery of payment orders – 03 A cyberattack to steal data and then sell it – 04 Blackmail of companies – 05 Encrypting data and demanding a ransom for access to it – 06 Decommissioning of the company's infrastructure – 07 Espionage on behalf of competitors – 08 Using malicious viruses for education and entertainment)

Ensuring cybersecurity is a complex task that includes the following areas: [8]:

1. **Network Security:** It is designed to detect and block network attacks. Includes data and access management tools: DLP (Data Loss Prevention), IAM (Identity and Access Management), NAC (Network Access Control) и NGFW (Next-Generation Firewall). Multilevel technologies for preventing network threats include IPS (Intrusion Prevention System), NGAV (Next-Generation Antivirus), Sandboxing and CDR (Content Disarm and Reconstruction). Network analytics, threat detection, and SOAR (Security Orchestration, Automation and Response) automated technologies are also important.
2. **Cloud Security:** Includes solutions, management tools, policies, and services that help protect the organization's cloud deployment from attacks.
3. **Endpoint Security:** Enables protection of end-user devices through data and network security management tools, advanced threat prevention, and technologies that support cybercrime investigations.
4. **Mobile Security:** Prevents attacks carried out through mobile devices that have access to corporate data, and protects operating systems and devices from rooting and hacking.
5. **Internet of Things Security:** Protects connected devices by detecting, classifying, and automatically segmenting them to manage network activity and using IPS as a virtual patch to prevent exploits against vulnerable devices.
6. **Web Apps Security:** Prevents attacks on web applications, including bot attacks, and stops any malicious interactions with applications and APIs.
7. **Zero Trust:** Traditional security models focus on the perimeter, erecting walls around an organization's valuable cyber assets. However, this approach has several issues, such as the potential for internal threats and the rapid erosion of the network perimeter. In the context of cloud solution implementation and remote work, a zero-trust approach becomes more relevant, utilizing a more granular security strategy that protects individual resources through a combination of micro-segmentation, monitoring, and role-based access control.

Artificial intelligence and machine learning technologies can be used to detect threats, identify network vulnerabilities, and reduce IT department workload. [9]. These technologies also make it possible to automate many cybersecurity-related tasks, such as intrusion detection, malware analysis, and vulnerability assessment.

Cybersecurity is not an isolated IT problem, but a critical business function that affects every aspect of a company's operations. [10]. To effectively counter cyber attacks, organizations need to take a proactive rather than a reactive position: not wait for an incident to occur in order to assess the value of a sustainable

cybersecurity position, but invest in continuous training and security system development, taking into account emerging threats and adapting their strategies accordingly. A proactive approach implies not only understanding the technical aspects of cyber threats, but also assessing their potential impact on business.

Currently, absolute protection against all cyber threats is impossible, which is why the most promising approach to ensuring cybersecurity is a business-oriented model aimed at protecting the company's key cyber assets and preventing unacceptable incidents. [11] Within this framework, companies with a mature information base implement effective cybersecurity based on real concerns and business needs.

Thus, in the context of global digital transformation, the resilience of states and companies depends on cyber resilience. There is an increasing demand in the market for measurable cybersecurity that aims to achieve a guaranteed outcome in the form of preventing cyberattacks with unacceptable consequences. To address issues in the field of cybersecurity, the concept of effective security can be used, which involves building an information protection system that can be qualitatively and quantitatively measured, ensures the safety of the company's cyber assets, and prevents the occurrence of unacceptable events.

Reference List

[1]. Gavrilova U.V., Subocheva O.N., Krasulina K.R., Social security in cyberspace: specifics and technologies of violation. // Social'no-gumanitarnye znaniya. – 2023 - #12 p.195-199

[2]. Ivanova E.S., Evdokimova A.N. Cybersecurity is at the heart of ensuring country's national security. // Zhurnal prikladnykh issledovanij – 2022 – v.7, #11 p.559-563. DOI: 10.47576/2712-7516_2022_11_7_559

[3]. Cremer F., Sheehan B., Fortmann M., Kia A.N., Mullins M., Murphy F., Materne S. Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Pap Risk Insur Issues Pract*, 2022, vol. 47, no. 3, pp. 698-736. DOI: 10.1057/s41288-022-00266-6

[4]. Yuchong L., Qinghui L. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 2021, vol. 7, pp. 8176-8186. DOI: 10.1016/j.egyr.2021.08.126

[5]. A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide // Check Point. – 2024. – URL: https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/ (date of request: 10.01.2025).

[6]. Shea S., Gillis A.S. *Cybersecurity* (2024). TechTarget. Available at: https://www.techtarget.com/searchsecurity/definition/cybersecurity (accessed 10.08.2024).

[7]. Ahmetov R.D., Timergalin A.R., Knyazev O.A. Study of cybersecurity issues and methods of its provision. // Mirovaya nauka – 2021 - #7 (52) p.108-113.

[8]. *What is Cyber Security?* Check Point. Available at: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/ (accessed 10.08.2024).

[9]. Wasyihun S.A., Yirga Y.M., Abebe A.D. Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2024, vol. 2, 100031. DOI: 10.1016/j.csa.2023.100031

[10]. *Key strategies for building cyber resilience in 2024* (2024). World Economic Forum. Available at: https://www.weforum.org/agenda/2024/04/cybersecurity-key-strategies-cyber-resilience-2024/ (accessed 10.08.2024).

[11]. Martynyuk M.S. Organizational and managerial mechanisms for ensuring cybersecurity of Russian companies. // Finansovye rynki i banki – 2023 - #6. p.5-9.