УДК 004.056.57

CYBERSECURITY

Radzimtsava Yu.V., student
Kniazhau Z.A., student
Scientific supervisor – Matusevich O.A., senior lecturer
English language department №1
Belarusian National University of Technology
Minsk, Republic of Belarus

In our time of innovative technologies, one of the main problems is the lack of security on the Internet. Cybersecurity is important not only for private users, but also for organizations. The amount of data on the network is increasing every day, making them vulnerable to cyber attacks. According to Cybersecurity Ventures, by 2025, damage from cyber attacks could reach $10.5 trillion annually. This forces users to protect their data, and cybercriminals, in turn, to create new ways to circumvent protection.

The main types at the moment are:

1) DDoS (Distributed Denial of Service): attacks that overload the server, making it unavailable. This is accomplished by flooding the target with many requests;

2) Phishing: attacks aimed at deceiving users in order to obtain their data, for example: emails, phone calls (vishing), fake websites, social networks (spear phishing);

3) Malware: programs that cause damage to computers and networks, for example: Trojans, botnets, spyware, Ransomware;

4) Cyber espionage and data breaches: attacks by organizations aimed at stealing confidential data;

5) Man-in-the-Middle (MitM) Attack: a MitM attack bypasses these protections by breaking a connection into two pieces. By creating a separate, encrypted connection with the client and the server, an attacker can read the data sent over the connection and modify it as desire before forwarding it on to its destination [1];

6) Malicious Apps: as employees increasingly use mobile devices to do their work and access sensitive company data, malicious mobile applications are increasingly dangerous. These applications can do any-

thing that desktop malware can, including stealing sensitive data, encrypting files with ransomware, and more [2].

Due to such dangers, precautions must be taken to ensure that your data is not stolen or your software is not corrupted. The information protection methods currently available are divided into two main categories:

I. Technical protection measures:

1) Data encryption: protects user data during transmission and storage;

2) Blockchain: prevention of data forgery;

3) Antiviruses: programs that detect malicious programs and eliminate them;

4) IDS/IPS systems: detect network intrusions and automatically block attacks;

5) Firewalls: filtering incoming and outgoing traffic.

II. Organizational protection measures:

1) Multi–factor authentication (MFA): the mandatory use of several login protection methods (password + SMS code + biometrics);

2) Data backup: regular creation of copies of data on external media and cloud servers.

As for Artificial Intelligence in cybersecurity, at the moment it has learned how to resist hackers well and improve the protection of user systems. Thanks to machine learning, it is able to anticipate hacker attacks and learn from them, which improves its ability to deal with threats from outside. Examples of cyber attacks:

1. Theft of S.T.A.L.K.E.R.

Hackers hacked the video game developer company GSC Game World. The criminals were able to gain access to 30 GB of information on the video game S.T.A.L.K.E.R. 2. The attackers demanded that the Russian voice acting be returned to the game, otherwise they threatened to publish the archive. GSC Game reported that an employee's PC was hacked [1].

2. The leakage of customer data from Ferrari.

In March 2023, cybercriminals hacked into the database of personal data of Ferrari customers. The motive was very simple – to get a ransom. The company sent out a newsletter to customers, in which it announced that it would not make a deal with hackers. The attackers gained access only to personal information that was not directly related to finances –

they could not find out the card numbers and which specific cars the customers bought [1].

3. The Leak Wolf attack.

A group of hackers calling themselves Leak Wolf stole the data of 40 Russian companies in a non-trivial way – without using malware.

They pretended to be employees of companies, received sensitive information and published it. Leak Wolf attacked more than 40 companies in this way. Experts believe that the group belongs to the hacktivists, as it does not make any demands, especially financial ones.

4. Cyber attack on Western Digital.

At the end of March 2023, cybercriminals hacked into the servers of Western Digital, a manufacturer of hard drives, solid-state and flash drives, as well as other storage devices, and then stole the company's data. The company had to turn off its cloud service for a while. Western Digital said that the criminals "gained access to a number of its internal systems".

5. Phishing attack on Reddit [3].

The attackers managed to deceive an employee of the company through a fake website disguised as one of the corporate ones. They stole his data and tokens for two-factor authorization. The attackers gained access to corporate systems, stole internal documents and source codes.

Computer crime poses a serious threat to economic security in the modern world. To combat cybercrime, it is necessary to apply an integrated approach, including technical, organizational and legal measures. Only through joint efforts can cyber threats be effectively countered and economic security ensured.

References

1. What is Cyber Security? // Check Point. – URL: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/ (date of access: 13.03.2025).

2. New Phishing Campaign Attacking Investors to Steal Login Credentials // Cyber Security News. – URL: https://cybersecuritynews.com/new-phishing-campaign-attacking-investors/ (date of access: 04.04.2025).

3. Types of Cybersecurity // SailPoint. – URL: https://www.sailpoint.com/identity-library/five-types-of-cybersecurity (date of access: 22.03.2025).