

# Cybersecurity Threats and Countermeasures

Vinnytsia National Technical University

## *Анотація*

Дана стаття демонструє основні складові кібербезпеки, підкреслюючи необхідність структурованого методу захисту сфери даних через стрімке зростання цифрового беззаконня.

**Ключові слова:** технології, кібербезпека, атаки, захист, компанії.

## **Abstract**

This article demonstrates the main components of cybersecurity, emphasizing the need for a structured method of protecting the data sphere due to the rapid growth of digital lawlessness.

**Keywords:** technology, cybersecurity, attacks, protection, companies.

Technology is now a very important part of our lives. Many aspects of our lives, such as business, education and personal communication, have changed significantly thanks to them. The ability to use technology makes our lives much easier, as it provides quick access to resources and increases productivity. However, in addition to the advantages, there are also disadvantages of such rapid development of technologies, and these are: cyber threats. In 2024, the number of cyber attacks on Ukraine increased by 69.8%, reaching 4315 incidents, compared to 2023, when 2541 cyber incidents were recorded. Attackers actively used messengers, social networks and all possible options to deceive users.[1]

The most difficult cyber threat to eliminate is malware, which is a general term for various types of viruses, worms, ransomware, spyware, and Trojans. Malware is defined as any code that can be used to steal data, bypass access control, or damage or compromise a system. For example, the WannaCry ransomware attack in 2017 affected more than 200,000 machines in 150 countries and caused billions of dollars in damage. [2] Many businesses have been paralyzed by ransomware, which holds a victim's data hostage until a ransom is paid. Phishing attacks remain one of the most popular methods of stealing data without the owner's permission. These attacks use fake emails, text messages, or websites that look like they're real to trick people into entering their credit card numbers, passwords, or other sensitive information.

Systematic phishing attacks began on the America Online (AOL) network in 1995. In order to steal legitimate credentials, attackers contacted victims via AOL Instant Messenger (AIM), posing as AOL employees checking user passwords. [3]

Another common type of cyber attack is Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks. These attacks are aimed at overloading servers or network resources, making them unavailable to users. The most powerful DDoS attack in history happened in 2023 and became one of the significant events in the history of cyber security. The attack was aimed at one of the large online stores using the Google Cloud CDN platform, with the aim of causing financial losses and disabling the site. [4]

Another cybersecurity threat is insider threats, where employees with access to a company's network abuse their authority to steal information or interfere with normal business operations. Insider threats, whether intentional or unintentional, can be difficult to identify and counter.

Organizations must implement a multi-layered security strategy to avoid ever-changing cyberthreats. Implementing strong authentication mechanisms, such as multi-factor authentication (MFA), is an important step in preventing others from accessing your information, as fraudsters require an additional authentication step to access your accounts, and MFA significantly reduces the likelihood of compromised accounts.

Regular software updates and troubleshooting are essential to preventing cyberattacks. Cybercriminals often gain access to systems by exploiting known vulnerabilities in outdated software. These risks can be mitigated by ensuring that updates are provided on schedule.

Cybersecurity training programs help employees become more aware of and defend against many kinds of threats. Training, including phishing simulations, helps identify fraud attempts on the employee's system and how to prevent those system breaches. Reducing the risk of successful cyberattacks can be done by making people more aware of potential threats.

To improve defenses, companies should modernize network security and device security to meet the challenges of cyberattacks. Malicious activity can be detected and blocked in real time using firewalls, intrusion detection systems (IDS), and endpoint detection and response (EDR) technologies. In addition, the Zero Trust approach boosts security by mandating persistent authentication of users and devices before any resource access, thereby drastically lowering unauthorized intrusion risks.[5] Another important method of protecting confidential information is data encryption, which prevents unauthorized access even if the data has been intercepted by attackers. End-to-end encryption (E2EE) is widely used in modern communication applications, such as WhatsApp, which provides a high level of confidentiality, since only the sender and recipient can decrypt the message. Thus, even in the event of interception, unauthorized users will not be able to access the content of the correspondence.

One of the major challenges in the modern world is cybersecurity, as the scale and complexity of cyberattacks grow day by day. Protection of information systems should be ensured through a multi-layered approach, comprising technical, organizational, and legislative measures. This includes the deployment of state-of-the-art tools in cybersecurity such as firewalls, intrusion detection systems, various encryption technologies, and "zero trust" models that go a long way in securing against unauthorized access and compromise of information. Also significant is the human aspect, which most cybersecurity experts fail to address. Most cyberattackers usually prey on unintentional user negligence around maintaining security. Thus, staff training and raising cyber literacy should be among the top priority measures for any organization. An appropriate incident response strategy can reduce the impact of an attack and enable system recovery in a timely fashion. A comprehensive combination of modern technologies, user education and compliance with international standards allows you to effectively counteract cyber threats, ensuring the stability of the digital space.

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ/REFERENCES

1. Institute of Mass Information. In 2024, the number of cyberattacks on Ukraine increased by 70%. Available at: <https://imi.org.ua/news/u-2024-rotsi-kilkist-kiberatak-na-ukrayinu-zroslo-na-70-i65931>
2. ITDEU. The 10 biggest cyberattacks in history. Available at: [https://itedu.center.ua/blog/top/10-najbilshix-kiberatak-v-istori%D1%97/?srsltid=AfmBOor7\\_fra17kM-A1kUWaIDeFm-DAy0BTSQg\\_wfynwZ043OCxY9oA](https://itedu.center.ua/blog/top/10-najbilshix-kiberatak-v-istori%D1%97/?srsltid=AfmBOor7_fra17kM-A1kUWaIDeFm-DAy0BTSQg_wfynwZ043OCxY9oA)
3. ESET. Phishing - what is it and what is the purpose of phishing. Available at: <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/fishing/>
4. FoxmindEd. The largest DDoS attacks in the history of cybersecurity. Available at: <https://foxminded.ua/naibilshi-ddos-ataky/>
5. Microsoft. Modern security architecture based on the zero-trust model. Available at: <https://www.microsoft.com/uk-ua/security/business/zero-trust>

**Бусигіна Вероніка Павлівна** – студентка групи 1 ПКТ-24б, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м. Вінниця. E-mail: [veronikabysygina@gmail.com](mailto:veronikabysygina@gmail.com)

**Науковий керівник:** Крютченко Олена Олександрівна, викладач англійської мови, кафедра іноземних мов, Вінницький національний технічний університет. E-mail: [olena.kriut@gmail.com](mailto:olena.kriut@gmail.com)

**Busygina Veronica** – a student of Faculty of Intelligent Information Technologies and Automation, 1 PKT-24b group, Vinnytsia National Technical University, Vinnytsia. E-mail: [veronikabysygina@gmail.com](mailto:veronikabysygina@gmail.com)

**Scientific supervisor** Kriutchenko Olena Oleksandrivna – a teacher of English, a Department of the Foreign Languages, Vinnytsia National Technical University. E-mail: [olena.kriut@gmail.com](mailto:olena.kriut@gmail.com)

