

WHY IS CYBERSECURITY BECOMING MORE POPULAR?

Vinnitsia National Technical University

Анотація

Дана тема розкриває причини збільшення популярності професії кібербезпеки, що стає все більш актуальною у світі цифрових технологій.

Ключові слова: кібербезпека, дані, технології, інформація, атаки, кіберзлочинці, технічні виклики, втрати.

Abstract

This topic reveals the reasons for the increasing popularity of the cybersecurity profession, which is becoming increasingly relevant in the world of digital technologies.

Keywords: cybersecurity, data, technology, information, attacks, cybercriminals, technical challenges, losses.

Cybersecurity is becoming increasingly important in today's digital world. Every year the amount of data processed increases, and with it the number of cyber threats. Nowadays, every aspect of life – from banking transactions to personal data on social networks – becomes a potential target for attackers. In this regard, the issue of ensuring the security of information technologies has become extremely relevant for every organization, governments, as well as for ordinary users. Therefore, let's consider the main reasons for the growth of cybersecurity.

The first reason for the growing popularity of cybersecurity is the increasing adoption of cloud technologies in organizations. Cloud adoption is the process of moving an organization's data, applications, and IT resources from traditional on-premises infrastructure to cloud services. Today, over 94% of enterprises have already migrated to the cloud and started working remotely [1]. The transition to cloud technologies opens up new opportunities for businesses, such as flexibility, scalability, and resource availability. However, with these advantages come new threats, in particular, storing and processing sensitive information in the cloud becomes a potential target for cybercriminals.

Another major reason for the growing popularity of cybersecurity is the need to protect company and customer data. Any leak or malicious interference with confidential information, especially financial and medical data, can have serious consequences for both the company and its customers [2]. If this data falls into the hands of attackers, the consequences can include financial losses, reputational damage, or even legal sanctions. Attackers can manipulate or delete data, which has not only material but also moral consequences for the victims. Companies that store customer data provided to them for processing, such as medical reports, addresses, credit card numbers, etc., are particularly vulnerable. Both company personnel and external users can have access to this data, which adds to the problem of access control. Timely detection and blocking of unauthorized actions helps prevent serious leaks and protect privacy.

In addition, as user data protection increases, new methods of hacking applications are emerging. According to Gartner, global IT spending is expected to grow by 8% in 2024, reaching \$5.1 trillion, with 80% of IT leaders increasing their cybersecurity budgets [3]. This shows that the demand for more effective cybersecurity solutions continues to grow, as companies are forced to invest in protecting their systems from increasingly sophisticated attacks. Attackers are not stopping there and are using the latest technologies to find vulnerabilities in companies' software and infrastructure. Cybercriminals are using artificial intelligence and machine learning to automate attacks, which significantly increases their effectiveness. Attacks are becoming

increasingly sophisticated, and many of them occur without obvious signs to users, making them difficult to detect and respond to.

Of course, the reasons for the growing popularity of cybersecurity can be continued, but the main ones are mentioned above. These factors emphasize that cybersecurity has become not only a technical necessity, but also an important strategic element for business success. Given the constant technological changes, it can be expected that the demand for innovative solutions in the field of cybersecurity will only grow.

Thus, the growing popularity of cybersecurity is the result of numerous factors, including the spread of cloud technologies, increasing risks to data protection, and the constant improvement of attack methods by attackers. Organizations are forced to constantly adapt their security strategies, taking into account new challenges arising from technological progress. Cybercriminals use increasingly sophisticated and automated attack methods, which requires companies to constantly invest in protecting their information systems. Data security is becoming one of the top priorities for businesses, as the leakage of sensitive information can lead to serious economic and reputational losses.

REFERENCES

1. 5 Reasons Why Cybersecurity Is Important Now More Than Ever. URL: <https://www.edoxi.com/studyhub-detail/why-cybersecurity-is-important-now> (date of application 15.01.2026)
2. Cyber security: More important than ever. URL: <https://www.etsglobal.org/dz/en/blog/news/importance-of-learning-english> (date of application 15.01.2026)
3. 10 Cyber Security Trends for 2025. URL: <https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-trends/> (date of application 15.01.2026)

Маркевич Мар'яна Михайлівна – студентка групи 1БКС-23б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: 7mariaanaa@gmail.com

Дерун Віталіна Гарольдівна – старший викладач кафедри іноземних мов, Вінницький національний технічний університет, м. Вінниця, e-mail: vitalinaderun@gmail.com

Markevych Mariana Mykhailivna – student of group 1BKS-23b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: 7mariaanaa@gmail.com

Derun Vitalina Garoldivna – Senior Lecturer of the Foreign Languages Department, Vinnytsia National Technical University, Vinnytsia, e-mail: vitalinaderun@gmail.com