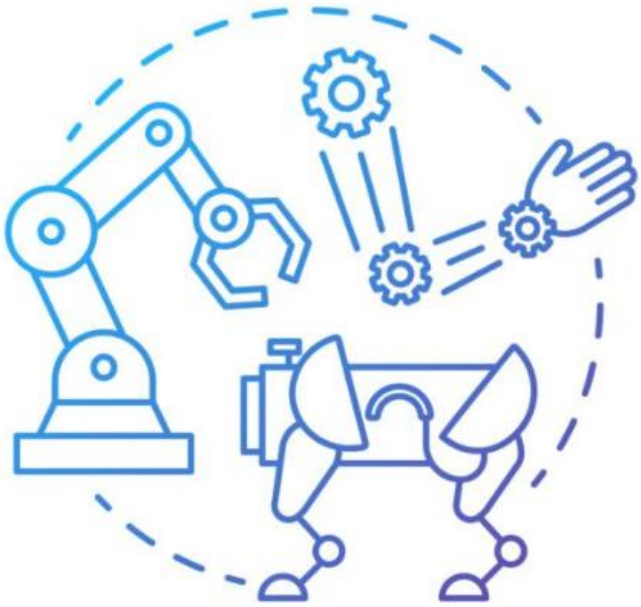
Міністерство освіти і науки України
Харківський національний університет радіоелектроніки
кафедра комп'ютерно-інтегрованих технологій, автоматизації, робототехніки та безпекової інженерії (КІТАРБІ)



МАТЕРІАЛИ

III Всеукраїнської конференції
«Комп'ютерно-інтегрованих технологій, автоматизації та робототехніки»
(Computer-integrated technologies, automation and robotics)
CITAR`26
14-15 травня 2026

[електронне видання]

Харків 2026

УДК: 005:004.896:62-65:338.3

Комп’ютерно-інтегрованих технологій, автоматизації та робототехніки 2026: матеріали III -ої Всеукраїнської конференції, Харків, 14-15 травня 2026.: тези доповідей / [редкол. І.Ш. Невлюдов (відповідальний редактор)].-Харків: [електронний друк], 2026. – 97 с.

У збірник включені тези доповідей, які присвячені сучасним автоматизованим технологіям Industry 4.0 та їх впровадження; інформаційні управляючі системи технологічного призначення; математичні методи в системах автоматизації; розробка та програмування в робототехніці; штучний інтелект та машинне навчання в автоматизації; інтеграція технологій у виробництві та промисловості; сенсорні технології та взаємодія людини з роботами в Industry 5.0; ефективність використання роботизованих систем у виробництві; етика та правові аспекти в робототехніці; Інтернет речей та Інтегровані системи в комп’ютерно-інтегрованих технологіях, автоматизації та робототехніки; технологічні виклики та інновації у світі робототехніки.

Computer-integrated technologies, automation and robotics 2026: Proceedings of III st All-Ukrainian Conference, Kharkiv, May 14-15, 2026: Thesises of Reports / [Ed. I.Sh. Nevlyudov (chief editor).] .- Kharkiv .: [electronic version], 2026. - 97 p.

The collection includes abstracts devoted to modern automated technologies of Industry 4.0 and their implementation; information control systems for technological purposes; mathematical methods in automation systems; development and programming in robotics; artificial intelligence and machine learning in automation; integration of technologies in production and industry; sensor technologies and human interaction with robots in Industry 5.0; efficiency of using robotic systems in production; ethics and legal aspects in robotics; Internet of Things.

ЗМІСТ

ANALYSIS OF POTENTIAL CYBER THREATS TO NETWORK SECURITY

R.V. Marunich, S.V. Sotnik
Kharkiv National University of Radio Electronics
Ukraine, 61166, Kharkiv, Nauky av., 14
E-mail: rostyslav.marunich@nure.ua

Abstract: The thesis provides an extensive analysis of contemporary cyber threats to network security in the context of global digitalization and society's growing dependence on information and communication technologies. It examines the main types of attacks on network infrastructure, their technical characteristics, and possible consequences for corporate and government information systems. A set of modern network protection methods is analyzed, including cryptographic mechanisms, monitoring systems, network segmentation, and intelligent anomaly analysis. The need to implement a multi-level cyber resilience system is justified.

Keywords: network security, cyber threats, information systems, DDoS attacks, phishing.

АНАЛІЗ МОЖЛИВИХ КІБЕРЗАГРОЗ МЕРЕЖЕВОЇ БЕЗПЕКИ

Р. В. Маруніч, С. В. Сотник
Харківський національний університет радіоелектроніки
Україна, 61166, Харків, пр. Науки 14
E-mail: rostyslav.marunich@nure.ua

***Анотація*:** Тези надають розширений аналіз сучасних кіберзагроз мережевої безпеки в умовах глобальної цифровізації та зростання залежності суспільства від інформаційно-комунікаційних технологій. Досліджено основні види атак на мережеву інфраструктуру, їх технічні особливості та можливі наслідки для корпоративних і державних інформаційних систем. Проаналізовано комплекс сучасних методів захисту мереж, включаючи криптографічні механізми, системи моніторингу, сегментацію мереж та інтелектуальний аналіз аномалій. Обґрунтовано необхідність впровадження багаторівневої системи забезпечення кіберстійкості.

***Ключові слова*:** мережева безпека, кіберзагрози, інформаційні системи, DDoS-атаки, фішинг.

The current stage of information society development is characterized by the deep integration of network technologies into all spheres of human activity [1-5]. Almost every organization uses corporate networks, cloud services, remote access systems, and mobile platforms [6-10]. Concurrently, Internet of Things technologies are evolving, increasing the number of devices connected to the network [11-16].

Along with the expansion of the digital space, the level of cyber threats is also growing. Malicious actors use modern attack automation tools, artificial intelligence, and sophisticated methods of concealing their activities. As a result, cyberspace becomes an environment where a constant confrontation occurs between means of protection and methods of intrusion.

Network security breaches can have critical consequences: from personal data leaks and financial losses to a complete shutdown of an enterprise's operations or strategic facilities. In the context of modern challenges, the issue of ensuring cyber resilience is gaining strategic importance for the state and businesses.

MATERIALS AND RESEARCH RESULTS. Among the most common threats to network security are DDoS attacks (Fig. 1). They are implemented by sending a large number of requests to a server from various devices that are part of a botnet. As a result of the overload, the server becomes

unavailable to legitimate users. Such attacks can be used as a tool for financial blackmail or as an element of information warfare.

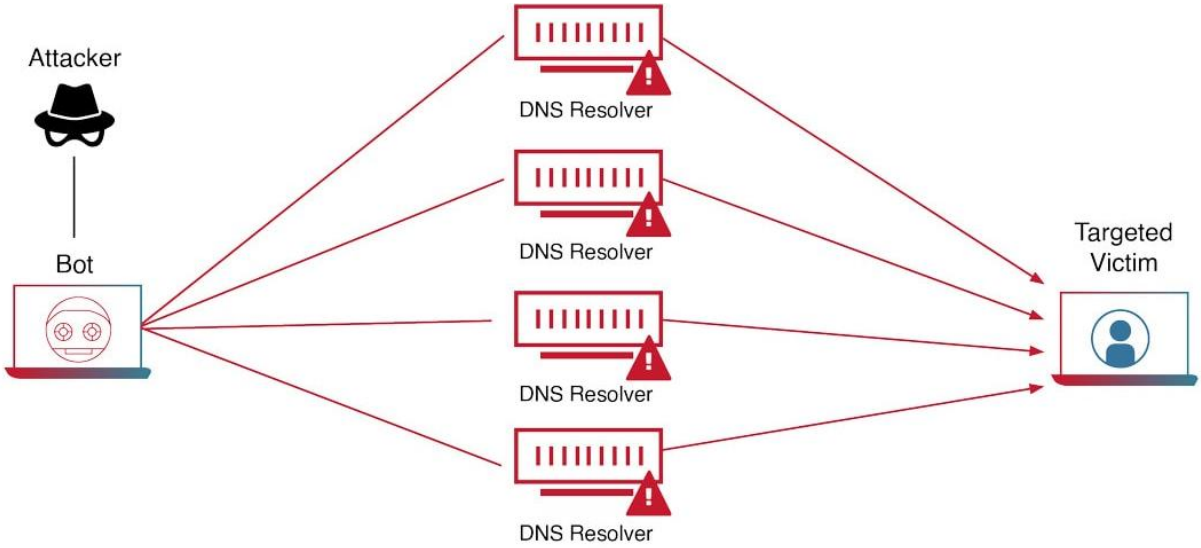


Figure 1 – Generalized diagram of a DDoS attack

The figure 1 depicts a DNS Amplification attack (DDoS), where an attacker, through a bot, uses multiple DNS resolvers to repeatedly amplify and redirect a large volume of traffic to the target victim.

In December 2025, Poland experienced a coordinated cyberattack on its energy sector, which affected over 30 distributed generation facilities, including wind and solar power plants, as well as a large combined heat and power plant supplying heat to nearly half a million consumers [17, 18]. The attackers, identified as a group linked to Sandworm, exploited vulnerabilities in firewalls and the absence of multi-factor authentication to penetrate the networks. The attack was hybrid in nature, simultaneously impacting IT systems with the DynoWiper data wiper malware and OT (operational technology) systems by corrupting the firmware of RTU controllers, resulting in a loss of communication and the inability to remotely control generation [18, 19]. Although a large-scale blackout was avoided due to the lack of a coordinated attack on all facilities simultaneously, the incident demonstrated the vulnerability of distributed energy systems and the risk of cascading failures, which could have led to frequency destabilization across the country's entire power grid.

Equally pressing is the problem of the spread of malicious software. Viruses, Trojan programs, and ransomware infiltrate systems through email, infected files, or by exploiting software vulnerabilities. Ransomware encrypts critical data and blocks access to it until a ransom is paid. Such incidents can lead to significant financial losses and prolonged enterprise downtime.

Phishing and social engineering remain among the most effective tools for attackers. Attacks of this type aim to manipulate user behavior to obtain confidential information. Fake websites or electronic messages mimic the official services of banks or government institutions. As a result, users voluntarily divulge their credentials, creating opportunities for unauthorized system access.

Man-in-the-Middle attacks involve intercepting or altering data during transmission between two parties. They are often carried out on unsecured Wi-Fi networks or where proper traffic encryption is lacking. In such cases, the attacker gains the ability to control the information exchange, which can lead to the theft of confidential data.

A significant threat also comes from the exploitation of vulnerabilities in network equipment and software. Failure to install updates promptly, the use of outdated protocols, or a lack of network segmentation creates additional risks of infiltration into an organization's internal infrastructure.

Cyber threats can cause complex consequences of a technical, financial, and reputational nature. Data breaches lead to a loss of trust from customers and partners. Financial losses can arise both from the direct theft of funds and from the shutdown of business operations. For critical infrastructure facilities, cyber incidents can have even more serious consequences, including disrupting the functioning of energy systems, transportation networks, or telecommunications. In the modern context, cyberspace is viewed as one of the vectors of hybrid influence on a state's economic and political stability.

An effective protection system must be based on a multi-layered approach. At the first level, technical means are applied, including firewalls, intrusion detection and prevention systems, cryptographic data protection protocols, and multi-factor authentication. A multi-level model for ensuring network security is shown in Fig. 2.

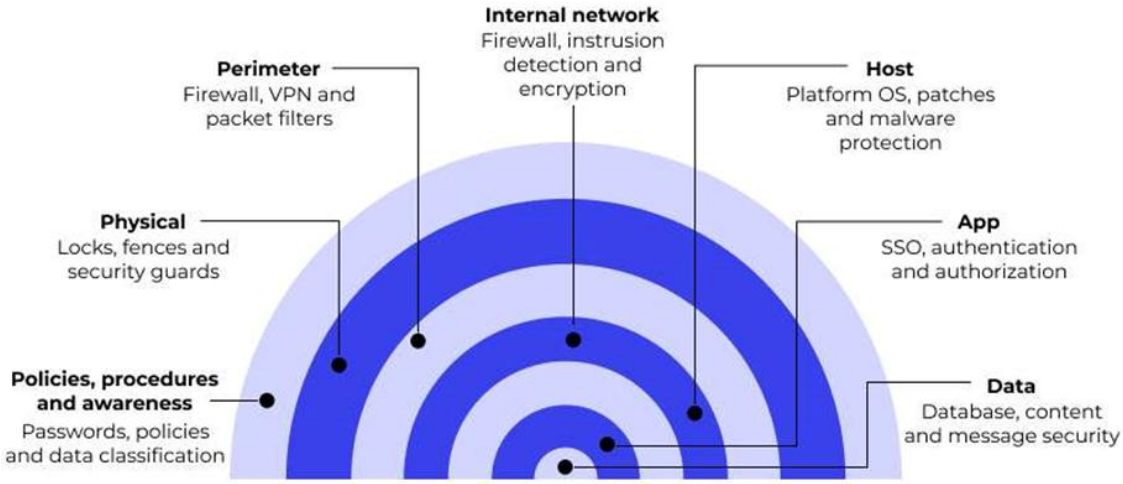


Figure 2 – Multilevel network security model

At the second level, continuous network traffic monitoring and anomaly analysis play an important role. The use of artificial intelligence technologies allows for the automatic detection of atypical behavior in the network and a prompt response to potential threats.

Figure 2 illustrates a multi-layered network security model, demonstrating that reliable protection of an information system is achieved not through a single solution, but by implementing a comprehensive set of measures at all levels – from physical security of facilities and perimeter security to access control at the application level and data integrity, including organizational policy.

In addition to technical measures, it is necessary to implement organizational protection mechanisms, including regular staff training, security audits, and the development of incident response plans. The human factor remains one of the key risks, so improving the level of cyber hygiene among users is an important element of the overall security strategy.

CONCLUSIONS. As a result of the analysis, it has been established that modern network infrastructures operate under conditions of constantly increasing complexity of cyber threats. The most common are DDoS attacks, the spread of malicious software, phishing, and the exploitation of network equipment vulnerabilities. Ensuring an adequate level of network security is only possible through a comprehensive combination of technical, organizational, and analytical measures. A promising direction for development is the implementation of intelligent systems for automated attack detection and increasing the level of cyber resilience of network systems. Further research

should be directed towards the development of adaptive protection mechanisms capable of responding to new types of cyber threats in real-time and ensuring the stable functioning of the information infrastructure in the face of modern challenges.

REFERENCES:

1. Fesenko, A., & et al. (2026). Comparative Analysis of Programming Languages for Developing System User Interfaces. All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations” (ICSTRO-2026) February 12-13, 2026. – pp. 119-123
2. Nevliudov, I. S., & et al. (2025). Design of the structure and motion control system of a stationary robot manipulator for construction work. Нові технології в будівництві. – №47. – pp. 37-45
3. Sotnik, S. (2025). A Modular System for Gear Calculations: A Comprehensive Computational Approach. DESIGN, CONSTRUCTION, MAINTENANCE. – vol. 5. – pp. 273-289
4. Fesenko, A., & et al. (2026). Selection of Communication Interfaces for a Microclimate Monitoring System. All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations” (ICSTRO-2026) February 12-13, 2026. – pp. 72-76
5. Sotnik, S. V. (2025). Support systems for robotics: principles, algorithms and development prospects. Journal of natural sciences and technologies. – 4(2). – pp. 419-430
6. Taran, A., & et al. (2026). Impact of 5G/6G Networks on the Development of IOT, Robotics, and Autonomous Systems. Low Latest and Mass Connection of Devices. All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations” (ICSTRO-2026) February 12-13, 2026. – pp. 114-118
7. Taran, A., & et al. (2026). Low-Code/No-Code Web Platforms: Opportunities and Limitations. A. All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations” (ICSTRO-2026) February 12-13, 2026. – pp. 96-100
8. Taran, A., & et al. (2026). WEB3 and Decentralized Applications. A Practical Look at Blockchain Development. All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations” (ICSTRO-2026) February 12-13, 2026. – pp. 81-85
9. Taran, A., & et al. (2026). AI as a Developer Tool: Github Copilot and Other Artificial Intelligence Assistants. All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations” (ICSTRO-2026) February 12-13, 2026. – pp. 67-71
10. Dvoinikova, I., & et al. (2026). Analysis of the Effectiveness and Cybersecurity Risks of the Github Copilot Tool. All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations” (ICSTRO-2026) February 12-13, 2026. – pp. 34-38
11. Sotnik, S. (2024). Integration of IoT into security systems: opportunities and risks. International Journal of Academic Engineering Research (IJAER). – Vol. 8, Issue 11. – pp. 56-61
12. Mandrykov, K., & et al. (2026). Comparative Analysis of Industrial Data Transmission Protocols (IIOT) in Automation Systems. All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations” (ICSTRO-2026) February 12-13, 2026. – pp. 49-53
13. Marunich, R.V., & et al. (2025). Modern IoT technologies for creating automated access systems. Sustainable smart cities and communities: business and innovation solutions 2025: Proceedings of I st I International Conference, Kharkiv, April 21, 2025: Thesises of Reports. – pp. 38-39

14. Khalimonov, Y., Sezonova, I., & et al. (2024). Approaches to ensuring proper working conditions using sensor technologies IoT // International Conference «DIGITAL INNOVATION & SUSTAINABLE DEVELOPMENT 2024» - pp. 24-25

15. Polikanov, K. A., & et al. (2025). Overview of modern technologies for residential automation. «Computer-integrated technologies, automation and robotics» CITAR-2025. – pp. 85-89

16. Achkan, M. S., & et al. (2025). Integration of cloud technologies into modern SCADA systems: prospects and challenges. «Computer-integrated technologies, automation and robotics» CITAR-2025. – pp. 26-29

17. Explained: OT Cyber Attack on Poland. [Електронний ресурс]. – Режим доступу: https://www.omicroncybersecurity.com/en/resources/explained-ot-cyber-attack-on-poland

18. Energy Sector Incident Report - 29 December 2025. [Електронний ресурс]. – Режим доступу: https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/