**УДК** 004.946.5.056(043.2)

# КІБЕРБЕЗПЕКА У ЦИФРОВОМУ СУСПІЛЬСТВІ: НОВІ ЗАГРОЗИ ТА СТРАТЕГІЇ ЗАХИСТУ

**Ніколь Міщинська**

*Державний університет «Київський авіаційний інститут», Київ*

*Науковий керівник – Тетяна Холявкіна, к.т.н., доц.*

Ключові слова: кіберзагрози, цифрова безпека, криптографія, атаки, протидія.

Розвиток цифрових технологій ускладнює кіберзагрози, що вимагає вдосконалення методів захисту інформаційного простору. Зростання атак APT (Advanced Persistent Threats) демонструє використання кіберпростору для політичного протистояння, а атаки на критичну інфраструктуру стали засобом гібридної війни [1].

**Вступ.** Сучасні загрози включають не лише DDoS та фішинг, а й складніші методи компрометації, зокрема маніпуляції нейромережами та використання квантових алгоритмів для зламу криптографії [2]. Постквантова криптографія ставить нові вимоги до безпеки даних, оскільки традиційні алгоритми (RSA, ECC) можуть втратити стійкість [3].

**Матеріали та методи.**

Дослідження ґрунтується на контент-аналізі нормативних документів (ISO/IEC 27001, NIST SP 800-53), аналітичних звітів та випадків атак APT, DDoS, експлуатації вразливостей. Розглянуто концепції Zero Trust, машинного навчання у виявленні загроз, DevSecOps, а також стратегії кіберзахисту ЄС, США та України.

**Результати.** Аналіз основних векторів атак показує, що значна частина інцидентів пов’язана з людським фактором: інсайдерськими загрозами, соціальною інженерією та низьким рівнем цифрової гігієни [4]. Для зниження кіберризиків необхідний багаторівневий підхід, що включає Zero Trust-архітектуру, AI-аналіз поведінкових аномалій у трафіку та дотримання міжнародних стандартів кібербезпеки (ISO/IEC 27001, NIST SP 800-53) [5].

Особливу увагу слід приділити безпеці хмарних сервісів, адже уразливості в ланцюгах постачання ПЗ (наприклад, атака Sunburst у 2020 році) залишаються однією з головних загроз [7]. Використання Secure by Design і DevSecOps дозволяє мінімізувати ці ризики через автоматизований контроль безпеки [8].

Протидія кібератакам на державному рівні вимагає міжнародної координації, проте ефективність таких ініціатив, як Будапештська конвенція та NIS2, обмежується відмінностями у законодавстві [9]. Враховуючи автоматизацію атак та зростання загроз, кібербезпека має стати фундаментальним елементом цифрової інфраструктури, що потребує безперервної модернізації [10].

**Висновок.** Аналіз сучасних кіберзагроз показав зростання складності атак та необхідність впровадження багаторівневих стратегій захисту, таких як Zero Trust, DevSecOps та постквантова криптографія. Ефективна кібербезпека потребує безперервного моніторингу, адаптації до нових загроз та міжнародної координації.

**Список використаних джерел:**

1. Mindscope.biz.ua. (n.d.). Кібербезпека в епоху цифрової трансформації: Виклики та перспективи. Retrieved March 11, 2025, from https://mindscope.biz.ua/kiberbezpeka-v-epohu-czyfrovoyi-transformacziyi-vyklyky-ta-perspektyvy/ (date of access: 14.03.2025).

2. ResearchGate. (n.d.). Кібербезпека в цифровому навчальному середовищі. Retrieved March 11, 2025, from https://www.researchgate.net/publication/332716122_KIBERBEZPEKA_V_CIFROVOMU_NAVCALNOMU_SEREDOVISI (date of access: 14.03.2025).

3. Рада національної безпеки і оборони України. (2021). Проєкт Стратегії кібербезпеки України (2021–2025 роки). Retrieved March 11, 2025, from https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (date of access: 12.03.2025).

4. Програма розвитку ООН в Україні. (n.d.). Кращі практики управління кібербезпекою. Retrieved March 11, 2025, from https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_04.pdf (date of access: 14.03.2025).

5. Капітон, А. М., & Прокудін, А. Ю. (n.d.). Кібербезпека в епоху цифрової трансформації. Житомирський державний технологічний університет. Retrieved March 11, 2025, from https://conf.ztu.edu.ua/wp-content/uploads/2024/01/72.pdf (date of access: 13.03.2025).

6. Вісник Хмельницького національного університету. (n.d.). Сучасні підходи до дослідження кібербезпеки та кібергігієни. Retrieved March 11, 2025, from https://journals.khnu.km.ua/vestnik/wp-content/uploads/2023/07/vknu-ts-2023-n3321-210-213.pdf (date of access: 12.03.2025).

7. Запорізький національний університет. (n.d.). Кібербезпека та інформаційна безпека. Retrieved March 11, 2025, from https://moodle.znu.edu.ua/pluginfile.php/1275463/mod_resource/content/1/01_2_%D0%9F%D1%80%D0%B5%D0%B7%D0%B5%D0%BD%D1%82%D0%B0%D1%86%D1%96%D1%8F_%D0%B4%D0%BE_%D1%82%D0%B5%D0%BC%D0%B8_1.pdf (date of access: 14.03.2025).

8. Coordynata.com.ua. (n.d.). Сучасні тенденції правового регулювання кібербезпеки та інтелектуальна власність. Retrieved March 11, 2025, from https://coordynata.com.ua/sucasni-tendencii-pravovogo-reguluvanna-kiberbezpeki-ta-intelektualna-vlasnist (date of access: 13.03.2025).

9. Стендер, С. В., Фротер, О. С., & Снітко, Ю. М. (2023). Цифрова інтеграція та кіберзахист економіки України: правові аспекти та інноваційні стратегії. Академічні візії, (26). Retrieved March 11, 2025, from https://academy-vision.org/index.php/av/article/download/799/725/733 (date of access: 12.03.2025).

10. Academia.edu. (n.d.). Кібербезпека та кібергігієна: нова ера цифрових технологій. Retrieved March 11, 2025, from https://www.academia.edu/98205745/ (date of access: 14.03.2025).