DOI: https://doi.org/10.36059/978-966-397-478-1-61

ТЕХНОЛОГІЧНА БЕЗПЕКА ТА ЦИФРОВА ЕКОНОМІКА: ВИКЛИКИ ТА ПЕРСПЕКТИВИ В УМОВАХ ГЛОБАЛЬНОЇ НЕСТАБІЛЬНОСТІ

Сохацький Олександр Юрійович
доктор філософії, докторант,
Західноукраїнський національний університет
ORCID: https://orcid.org/000-0001-8735-866X

Технологічна безпека та цифрова економіка є фундаментальними складовими сучасного економічного розвитку, особливо в контексті національної безпеки та суверенітету держави. В умовах стрімкого розвитку інформаційних технологій та цифрових трансформацій виникають нові загрози, що можуть впливати на економічну незалежність, політичну стабільність та соціальну безпеку держави. Сучасні глобалізаційні процеси, поряд із розвитком цифрової економіки, формують нові виклики для України, що зумовлює необхідність розробки комплексної стратегії технологічної безпеки та адаптації до цифрових реалій.

Технологічна безпека визначається як здатність держави забезпечувати розвиток і функціонування стратегічно важливих галузей економіки за рахунок власного науково-технологічного потенціалу, а також ефективно захищати свої цифрові, промислові та інноваційні ресурси від зовнішніх загроз (Куліш та ін., 2023). В сучасних умовах особливе значення має розвиток власних дослідно-конструкторських та інноваційних можливостей, що сприяє мінімізації залежності від зовнішніх технологічних рішень. Серед ключових викликів для технологічної безпеки можна виділити кібератаки, економічний шантаж через технологічну залежність, недостатній рівень цифрової грамотності та критичну залежність від імпортних компонентів.

Цифрова економіка, яка базується на використанні передових технологій, таких як штучний інтелект, хмарні обчислення, блокчейн та Інтернет речей, визначає нові економічні парадигми та формує інноваційні бізнес-моделі. В Україні розвиток цифрової економіки є одним із пріоритетних напрямів державної політики, що підтверджується прийняттям законодавчих ініціатив у сфері цифровізації та впровадженням проекту «Дія» (Міністерство цифрової трансформації України, 2023). Однак, для забезпечення ефективного функціонування цифрової економіки необхідно створення безпечного та стійкого технологічного середовища.

Значним ризиком для цифрової економіки є інформаційна вразливість та ризики кібератак, які можуть призводити до масштабних фінансових

втрат та витоку конфіденційної інформації. Згідно з даними Міжнародного союзу електрозв'язку (ITU, 2023), Україна входить до групи країн з високим рівнем кіберзагроз через активні військові та економічні атаки на її цифрову інфраструктуру. Одним із основних напрямів забезпечення технологічної безпеки є розвиток власних кіберзахисних платформ, впровадження стандартів кібербезпеки, підготовка спеціалістів у сфері інформаційної безпеки та розширення міжнародного співробітництва у сфері кіберзахисту.

Окрім інформаційної безпеки, критичне значення має питання технологічного суверенітету та імпортозаміщення стратегічно важливих технологій. У 2022–2023 роках було зафіксовано понад 600 випадків порушення ланцюгів поставок внаслідок глобальної кризи напівпровідникового виробництва, що вплинуло на виробництво електронних компонентів у багатьох країнах, зокрема в Україні (OECD, 2023). У зв'язку з цим виникає необхідність розробки та впровадження державних програм з розвитку власного виробництва критичних технологій, таких як мікроелектроніка, робототехніка, квантові обчислення та штучний інтелект.

Не менш важливим аспектом розвитку цифрової економіки є питання правового регулювання та захисту персональних даних. В Україні у 2021 році було прийнято Закон «Про захист персональних даних», що відповідає стандартам ЄС (GDPR), однак практична імплементація залишається недостатньо ефективною (Державна служба спеціального зв'язку та захисту інформації України, 2023). Для досягнення необхідного рівня технологічної безпеки важливим є створення національної інфраструктури управління персональними даними, впровадження технологій шифрування та контроль використання інформаційних ресурсів у державному секторі.

Окрему увагу слід приділити впливу цифрової економіки на зайнятість та соціальну сферу. В умовах стрімкої автоматизації та цифровізації економічних процесів відбувається трансформація ринку праці, що вимагає переорієнтації робочої сили та підвищення рівня цифрової грамотності серед населення. Відповідно до дослідження Світового економічного форуму (WEF, 2023), до 2030 року близько 40% професій зазнають значних змін через автоматизацію, що потребує розвитку програм перекваліфікації та професійної адаптації кадрів.

Загалом, забезпечення технологічної безпеки та сталого розвитку цифрової економіки потребує комплексного підходу, що включає розвиток інноваційних технологій, захист цифрової інфраструктури, створення ефективної нормативно-правової бази та підготовку висококваліфікованих кадрів. У контексті глобальної цифрової трансформації Україна має унікальні можливості для реалізації стратегій технологічного розвитку, які дозволять зміцнити її економічний потенціал, посилити

конкурентоспроможність на міжнародній арені та забезпечити національну безпеку.

Розвиток цифрової економіки неможливий без належного рівня технологічної безпеки. Використання інноваційних технологій має супроводжуватися заходами з управління ризиками, захисту інформаційних ресурсів та зміцнення технологічного суверенітету держави. Враховуючи сучасні виклики, пов'язані з глобальною нестабільністю та зростаючими кіберзагрозами, Україні необхідно розробити стратегічний підхід до розвитку цифрової інфраструктури, що дозволить ефективно використовувати потенціал цифрової економіки та забезпечити довгострокову стійкість держави в технологічному вимірі.

Список використаних джерел:

1. Куліш О., Петренко В. Технологічна безпека в умовах цифрової економіки. *Науковий вісник економічних досліджень*. 2023. № 12(3). С. 45–62.
2. Міністерство цифрової трансформації України. Національна стратегія цифрового розвитку. Мінцифра України. Київ, 2023. URL: https://zakon.rada.gov.ua/go/1351-2024-р (дата звернення: 18.02.2025).
3. International Telecommunication Union. Global Cybersecurity Index 2023. ITU. 2023. URL https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx (дата звернення: 18.02.2025).
4. OECD. The Impact of Semiconductor Shortages on Global Supply Chains. Organisation for Economic Co-operation and Development. Paris, 2023. URL https://www.oecd.org/industry/impact-of-semiconductor-shortages-on-global-supply-chains.pdf (дата звернення: 18.02.2025).
5. World Economic Forum. The Future of Jobs Report 2023. WEF. 2023. URL: https://www.weforum.org/reports/the-future-of-jobs-report-2023
6. Державна служба спеціального зв'язку та захисту інформації України. Закон України «Про захист персональних даних». ДССЗЗІ України. 2023. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 18.02.2025).