ECONOMIC SECURITY OF THE STATE

УДК 330.342.3:004.056
JEL O33, H56, L86
DOI: 10.26906/EiR.2025.2(97).3857

КІБЕРЗАГРОЗИ ЯК ВИКЛИК ЕКОНОМІЧНІЙ БЕЗПЕЦІ: ПОТЕНЦІАЛ ТЕХНОЛОГІЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Пахненко Олена Михайлівна*, кандидат економічних наук, доцент,
доцент кафедри фінансових технологій і підприємництва
Сумський державний університет
Божко Микола Олександрович, аспірант**
Сумський державний університет

**ORCID 0000-0002-4703-4078*
***ORCID 0009-0007-6813-9067*

Стаття отримана редакцією 23.04.2025
The article was received by editorial board on 23.04.2025

Вступ. В умовах цифрової трансформації економічні системи стають дедалі більш залежними від стабільної роботи інформаційно-комунікаційних технологій, що, у свою чергу, підвищує їхню вразливість до кібератак та створює додаткові ризики для макроекономічної стабільності. Кіберінциденти останніх років (зокрема, NotPetya у 2017 році, кібератаки на SolarWinds, Colonial Pipeline, Kaseya у 2020–2021 рр., кібератаки на енергетичну систему, мобільного оператора Київстар, «Укрзалізницю», спроби виведення з ладу державних сервісів та банківських платформ в Україні в період повномасштабної війни) яскраво демонструють, що кіберзагрози здатні не лише паралізувати діяльність окремих компаній чи галузей, а й становити системну загрозу національній безпеці.

У цифровій економіці кіберзагрози вже не є суто технічними інцидентами, а мають розглядатися як системний ризик для економічної безпеки держави. Відтак, кібербезпека стає невід'ємною складовою економічної безпеки. Це знаходить своє відображення у стратегіях національної безпеки більшості країн світу, а також міжнародних рекомендаційних та регулятивних документах, таких як Рамкова стратегія ЄС з кібербезпеки, керівні принципи ENISA та рекомендації МВФ щодо кіберстійкості фінансового сектору.

Особливу роль у протидії кіберзагрозам відіграє розвинена технологічна інфраструктура: захищені дата-центри, національні CERT-платформи, інструменти моніторингу, а також рішення на основі штучного інтелекту, що дозволяють оперативно виявляти та нейтралізовувати загрози в режимі реального часу. У зв'язку зі зростанням масштабності та частоти кібератак, аналіз потенціалу технологічної інфраструктури держави набуває особливої актуальності як з точки зору зміцнення її кіберстійкості, так і в контексті довгострокового забезпечення економічної безпеки.

Огляд останніх джерел досліджень і публікацій. Проблематика цифрової трансформації, кіберзагроз та економічної безпеки активно досліджується як українськими, так і зарубіжними науковцями. У роботах Стендер С., Фротер О., Снітко Ю. [1], Чайкіної А., Маслій О. та Черв'як А. [2] розглянуто стратегічні та організаційні підходи до забезпечення кіберзахисту в умовах цифровізації. Жукова Ю., Василенко В., Юрченко О. [3], а також Череп А. та ін. [4] акцентують увагу на цифрових векторах як чинниках національної безпеки. Зв'язок цифрової економіки й кібербезпеки досліджується також у роботах Бензарь А., Пєстової О. [5], Кіндзерського Ю. [6], Пічкурової З. [7] та інших. Наукові праці Березівського Я. [8], Колодинського С., Дракохруст Т. та Башинської М. [9] звертаються до теми технологічної інфраструктури, однак переважно в контексті конкурентоспроможності або економічного зростання.

Зарубіжні дослідження також активно розглядають різні аспекти взаємодії кібербезпеки й цифрової трансформації. Так, низка публікацій (Джунея А. (Juneja A.) та ін. [10], Лесмана Д. (Lesmana D.) та ін. [11], Валакієн А. (Valackiene A.) та Одеджаї Р. (Odejayi R.) [12]) присвячена впливу кіберзагроз на розвиток цифрової економіки та управління кіберризиками. Чень Х. (Chen X.) зі співавторами [13] здійснили порівняльну оцінку кіберпотенціалу провідних країн. Кремер Ф. (Cremer F.) та ін. [14] акцентують на проблемах доступності даних для аналізу кіберризиків. Окрему увагу приділено взаємодії інноваційних технологій і безпеки: Альдасоро І. (Aldasoro I.) та ін. [15] аналізують виклики, пов'язані з впровадженням штучного інтелекту у фінансовій сфері, а Сафітра М. (Safitra M.), Лубіс М. (Lubis M.), Фахрурроджа Х. (Fakhrurroja H.) [16] пропонують концептуальну рамку для майбутньої системи кіберзахисту.

Попри зростання кількості наукових публікацій, потенціал технологічної інфраструктури як складової протидії кіберзагрозам залишається недостатньо дослідженим, особливо в контексті формування економічної безпеки.

Постановка завдання. Метою статті є аналіз впливу кіберзагроз на економічну безпеку та дослідження потенціалу технологічної інфраструктури України як інструменту протидії сучасним кіберризикам.

Основний матеріал і результати. Механізм впливу кіберзагроз на економічну безпеку є багатоаспектним і може виявлятися у вигляді як прямих фінансових втрат (крадіжка коштів, витрати на відновлення IT-інфраструктури, збитки через зупинку операційних процесів), так і непрямих економічних наслідків (падіння довіри до цифрових платформ, зниження інвестиційної привабливості, зростання витрат на страхування та аудит тощо). Вразливість критичної інфраструктури – енергетичної, транспортної та комунікаційної – здатна спричинити масштабні економічні збої та призвести до регіональних криз.

Для узагальненої оцінки рівня готовності держав до кіберзагроз використовуються інтегральні індекси, зокрема Глобальний індекс кібербезпеки (Global Cybersecurity Index, GCI), Національний індекс кібербезпеки (National Cyber Security Index, NCSI), Індекс цифрової економіки та суспільства (Digital Economy and Society Index, DESI). Глобальний індекс кібербезпеки GCI, що розроблений Міжнародним союзом електрозв'язку (ITU), оцінює рівень кібербезпеки в країнах за п'ятьма ключовими напрямками: правові заходи, технічні заходи, організаційні заходи, розвиток потенціалу та міжнародна співпраця. У зв'язку зі змінами в методології розрахунку, порівняльний аналіз значень індексу є релевантним лише для двох останніх досліджень – 2020 та 2024 років (табл. 1).

Таблиця 1

Глобальний індекс кібербезпеки (GCI) України та країн європейського регіону

Складові GCI	Максимум	Україна		Європейський регіон (середнє для 45 країн)	
		2020 р.	2024 р.	2020 р.	2024 р.
Глобальний індекс кібербезпеки (GCI), у т.ч.:	100	65,93	83,93	82,53	87,87
Правові заходи	20	17,46	19,42	18,06	19,44
Технічні заходи	20	11,60	17,35	16,23	16,77
Організаційні заходи	20	13,06	15,97	15,33	17,70
Розвиток потенціалу	20	10,94	14,60	15,93	16,26
Міжнародна співпраця	20	12,87	16,58	16,98	17,70

Джерело: складено авторами на основі [17], [18]

Станом на 2024 рік значення Глобального індексу кібербезпеки (GCI) для України зросло на 27 % порівняно з показником 2020 року. За цей період Україна скоротила розрив із середніми значеннями для європейського регіону за всіма складовими індексу, а за компонентом «Технічні заходи» навіть перевищила середньоєвропейський рівень. Цей компонент GCI відображає впровадження країною технічної інфраструктури для забезпечення кібербезпеки, зокрема наявність національного CERT, впровадження технічних стандартів, механізмів сертифікації та моніторингу інцидентів у режимі реального часу.

Водночас, незважаючи на загальну позитивну динаміку, Україна зі значенням індексу 83,93 все ще залишається у групі країн, що перебувають на етапі становлення системи кібербезпеки (Tier 3).

Найвразливішими напрямами залишаються «Організаційні заходи» та «Розвиток потенціалу». Зокрема, в межах організаційної складової Україна демонструє найнижчі результати за показником наявності системи метрик кібербезпеки. Незважаючи на наявність національної стратегії кібербезпеки та визначення відповідальних державних органів, відсутні формалізовані кількісні та якісні індикатори для оцінки ефективності заходів з кібербезпеки, а також механізми їх регулярного моніторингу.

Щодо напряму розвитку потенціалу, Україна досягла певного прогресу у сфері підготовки фахівців з кібербезпеки. Однак, кількість освітніх програм та академічних навчальних планів залишається недостатньою. Найгірша ситуація спостерігається у сфері державного стимулювання: відсутні або не функціонують у повній мірі механізми підтримки розвитку людського капіталу в галузі кібербезпеки.

Подібні висновки можна зробити і на основі аналізу динаміки Національного індексу кібербезпеки (NCSI) для України (рис. 1). Протягом останніх років Україна демонструє стабільне зростання NCSI, досягнувши рівня 80,83 зі 100 у 2024 році і посівши 21-ше місце у глобальному рейтингу.

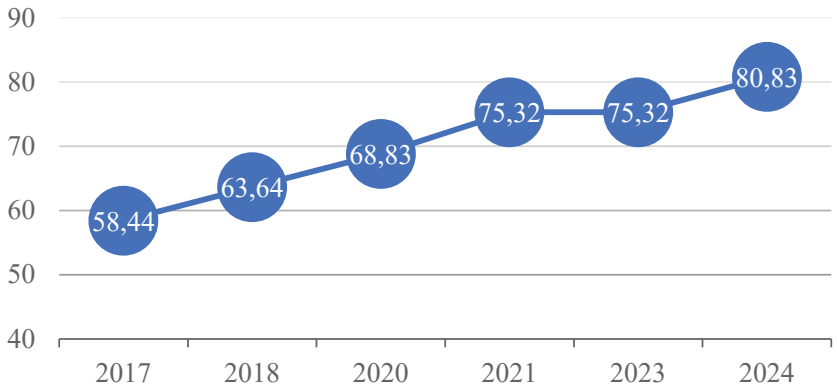

Рис. 1. Динаміка значень індексу NCSI для України

Джерело: сформовано авторами на основі [19]

Україна має повне виконання критеріїв за кількома стратегічними та оперативними напрямами, зокрема: кібербезпекова політика, науково-дослідні розробки, захист персональних даних, протидія кіберзлочинності та військова кібероборона. Водночас аналіз складових NCSI дозволяє виокремити низку вразливих аспектів у національній системі кібербезпеки України, зокрема:

– управління кіберкризами (56 %) – відсутні або недостатньо розвинені національний план реагування, регулярні навчання та операційна підтримка у кризових ситуаціях;

– освіта та професійний розвиток (60 %) – хоч і сформовані базові елементи кіберосвіти, вищі рівні підготовки залишаються недостатньо розвиненими (низькі бали за бакалаврські та магістерські програми, асоціації фахівців);

– реагування на кіберінциденти (64 %) – не всі компоненти реагування реалізовані в повному обсязі, зокрема, інструменти звітності та міжнародна координація;

– міжнародний внесок у кібербезпеку (67 %) – обмежена участь у кібердипломатії, відсутність внеску в розвиток потенціалу інших країн.

Аналіз індексів GCI та NCSI демонструє помітне зростання інституційної спроможності України у сфері кібербезпеки, особливо в напрямах технічного забезпечення, розробки стратегій та окремих компонентів реагування. Водночас наявні слабкі сторони, виявлені в обох індексах, зумовлюють потребу у глибшому розгляді одного з ключових елементів кіберзахисту – технологічної інфраструктури.

У науковій літературі технологічна інфраструктура визначається як сукупність технічних, мережевих, обчислювальних та організаційних елементів, що забезпечують функціонування, розвиток і безпеку цифрового середовища держави. Вона включає телекомунікаційні мережі, центри обробки даних (дата-центри), хмарні сервіси, інструменти кіберзахисту, системи електронного урядування та інституційні структури, відповідальні за управління цифровими ризиками. Такий підхід, зокрема, підтримується у звітах міжнародних організацій, зокрема ENISA та OECD, де підкреслюється системна роль технологічної інфраструктури в досягненні кіберстійкості держав.

В Україні технологічна інфраструктура останніми роками зазнала значного оновлення і розширення. За даними міжнародних дослідницьких платформ, на початок 2024 року в Україні функціонують понад п'ятдесят повноцінних дата-центрів, що надають хмарні та обчислювальні послуги приватному і державному секторам. До основних вузлів обміну інтернет-трафіком належать понад два десятки IXP (Internet Exchange Points), включаючи найбільші – UA-IX і DTEL-IX, які забезпечують високу пропускну здатність і резервування маршрутів [20].

Значним елементом телекомунікаційної інфраструктури є розгалужена система мобільного зв'язку: за останні роки оператори мобільного зв'язку розширили покриття мережі четвертого покоління (4G) до понад 95 % населення. Паралельно здійснюється модернізація оптоволоконних мереж, які активно впроваджуються не лише в міських, але й у сільських громадах, зокрема для підключення медичних і освітніх закладів. Проте впровадження технології п'ятого покоління (5G) в Україні поки що залишається на етапі пілотних проєктів і технічної підготовки.

У структурі національного захисту цифрового простору важливу роль відіграє наявність інституційних механізмів реагування на кіберзагрози. Центром реагування на комп'ютерні надзвичайні події є CERT-UA, який координує дії державного сектору щодо протидії інцидентам, забезпечуючи постійний моніторинг цифрового простору, оповіщення та інформаційний обмін. Поряд з ним функціонують профільні CERT-команди у системах Національного банку України, Міністерства оборони, Державної служби спеціального зв'язку та захисту інформації, а також у низці приватних структур [21]. Ці органи забезпечують оперативне реагування на кібератаки, що в умовах триваючої гібридної війни є критично важливим.

Важливо зазначити, що технологічна інфраструктура також підтримує роботу стратегічних цифрових державних платформ, таких як «Дія», «Прозорро», Єдиний державний реєстр, цифрові послуги електронної ідентифікації (BankID, MobileID, ID.gov.ua), які забезпечують доступ громадян і бізнесу до адміністративних функцій, а також є об'єктами підвищеного ризику з погляду кіберзахисту.

Попри значний поступ у розбудові цифрової інфраструктури, зокрема в частині розширення доступу до якісного зв'язку та підвищення спроможності дата-центрів, залишаються актуальними чимало викликів. До них належать обмежене впровадження високошвидкісних мобільних технологій, залежність від іноземного обладнання, недостатній рівень енергетичної автономності інфраструктурних об'єктів та потреба у масштабуванні резервних потужностей. Крім того, з початком повномасштабної війни вся критична інфраструктура України зазнає постійних ворожих кібератак. Одним із наймасштабніших інцидентів була кібератака на «Київстар» у грудні 2023 року, яка призвела до порушення зв'язку, збоїв в роботі екстрених служб і серйозних економічних втрат.

Незважаючи на складні обставини, технологічна інфраструктура України демонструє значний адаптаційний потенціал до нових типів загроз. На це вказують кілька ключових факторів. Перш за все, це наявність розвиненої інституційної структури реагування. Функціонування національного CERT-UA, а також низки відомчих команд реагування на інциденти забезпечує координацію дій у державному секторі, що особливо важливо з огляду на збільшення кількості цільових атак на державні цифрові платформи, реєстри та критичну інфраструктуру.

Не менш важливу роль відіграє розвиток IT-сектору, який зберігає високий рівень спроможності, незважаючи на виклики повномасштабної війни. Україна має одну з найпотужніших IT-галузей у центрально-східній Європі, із тисячами компаній, які розробляють продукти у сфері кіберзахисту, хмарних рішень та штучного інтелекту.

Важливим аспектом є забезпечення децентралізації та гнучкості у побудові цифрових платформ. Це сприяє зниженню ризиків повного виведення з ладу систем у разі масованих кібератак. Проєкт «Дія» є показовим прикладом швидкого впровадження сучасних підходів до створення стійких і масштабованих цифрових сервісів.

Фактором зміцнення потенціалу також є активна міжнародна співпраця України у сфері кібербезпеки. Протягом останніх років держава поглиблює партнерство з Європейським Союзом, НАТО, країнами Балтії та США у напрямах кіберзахисту, цифрової стійкості та обміну оперативною інформацією. Участь у програмах на кшталт EU4Digital або CyberEast дозволяє не лише підвищити кваліфікацію фахівців, а й інтегрувати українську інфраструктуру у спільний європейський безпековий простір.

Висновки. Наявна технологічна інфраструктура України створює базові передумови для підвищення кіберстійкості держави. Її подальший розвиток у напрямі масштабування, автономізації, інтеграції

з міжнародними системами моніторингу, а також стимулювання інновацій у сфері кібербезпеки, є критично важливим для зменшення вразливості перед сучасними та перспективними кіберзагрозами. Втім, для повноцінної реалізації потенціалу технологічної інфраструктури необхідним залишається подолання низки стримуючих чинників, до яких належать обмежене впровадження технологій 5G, залежність від імпортного обладнання критичної IT-інфраструктури, недостатній рівень автоматизації у секторах поза урядовим доменом, а також брак системної підтримки розвитку вітчизняних розробників кіберзахисних рішень.

Виконано в рамках науково-дослідної теми «Кібербезпекові та цифрові трансформації економіки країни воєнного часу: боротьба із кіберзлочинами, корупцією та тіньовим сектором» (№ д/р 0124U000544), що фінансується за рахунок коштів державного бюджету.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Стендер С. В., Фротер О. С., Снітко Ю. М. Цифрова інтеграція та кіберзахист економіки України: правові аспекти та інноваційні стратегії. *Академічні візії.* 2023. № 26. URL: https://academy-vision.org/index.php/av/article/view/799 (дата звернення: 21.04.2025)

2. Чайкіна А., Маслій О., Черв'як А. Сучасні драйвери підвищення економічної безпеки країни в умовах цифрової трансформації. *Сталий розвиток економіки*. 2024. № 2 (49). С. 307–313. DOI: https://doi.org/10.32782/2308-1988/2024-49-49

3. Жукова Ю., Василенко В., Юрченко О. Стратегії забезпечення економічної безпеки країни в умовах глобальних викликів. *Herald of Khmelnytskyi National University. Economic Sciences.* 2024. № 328 (2). С. 401–409. DOI: https://doi.org/10.31891/2307-5740-2024-328-60

4. Череп А., Череп О., Гельман В., Лосєва Е. Європейські вектори цифровізації економіки задля забезпечення національної безпеки держави. *Молодий вчений*. 2023. № 11 (123). С. 163–167. DOI: https://doi.org/10.32839/2304-5809/2023-11-123-6

5. Бензарь А., Пєстова О. Проблеми та перспективи розвитку цифрової економіки в Україні. *Цифрова економіка та економічна безпека.* 2022. № 2 (02). С. 148–155. DOI: https://doi.org/10.32782/dees.2-25

6. Кіндзерський Ю. В. Кібербезпека та становлення цифрової економіки: проблеми взаємозв'язку. *Економічний вісник Дніпровської політехніки*. 2020. №3. С. 18–26. DOI: https://doi.org/10.33271/ebdut/71.018

7. Пічкурова З. Розвиток цифрової економіки України в умовах воєнного стану. *Економіка та суспільство*. 2023. № 58. DOI: https://doi.org/10.32782/2524-0072/2023-58-73

8. Березівський Я. П. Ідентифікація умов та чинників формування технологічної конкурентоспроможності національної економіки. *Вісник Львівського торговельно-економічного університету. Економічні науки.* 2021. № 64. С. 31–35. DOI: https://doi.org/10.36477/2522-1205-2021-64-05

9. Kolodynskyi S., Drakokhrust T., Bashynska M. The innovative infrastructure of economic development in the framework of international digital transformation. *Baltic Journal of Economic Studies.* 2018. Vol. 4 (4). P. 166–172. DOI: https://doi.org/10.30525/2256-0742/2018-4-4-166-172

10. Juneja A., Goswami S. S., Mondal S. Cyber Security and Digital Economy: Opportunities, Growth and Challenges. *Journal of Technology Innovations and Energy*. 2024. Vol. 3(2). P. 1–22. DOI: https://doi.org/10.56556/jtie.v3i2.907

11. Lesmana D., Afifuddin M., Adriyanto A. Challenges and Cybersecurity Threats in Digital Economic Transformation. *International Journal of Humanities Education and Social Sciences (IJHESS)*. 2023. Vol. 2 (6). DOI: https://doi.org/10.55227/ijhess.v2i6.515

12. Valackiene A., Odejayi R.O. The impact of cyber security management on the digital economy: multiple case study analysis. *Intellectual Economics*. 2024. Vol. 18 (2). P. 261–283. DOI: https://doi.org/10.13165/IE-24-18-2-02

13. Chen X., Wang T., Lin X., Hinde D., Yan Q., Zmire Z. The Potential of the Digital Economy: A Comparative Assessment of Key Countries' Cybersecurity. *International Journal of Education and Humanities.* 2023. Vol. 11 (1). P. 1–7. DOI: https://doi.org/10.54097/ijeh.v11i1.12740

14. Cremer F., Sheehan B., Fortmann M., Kia A. N., Mullins M., Murphy F., Materne S. Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance: Issues and Practice*. 2022. Vol. 47 (3). P. 698–736. DOI: https://doi.org/10.1057/s41288-022-00266-6

15. Aldasoro I., Doerr S., Gambacorta L., Notra S., Oliviero T., Whyte D. Generative Artificial Intelligence and Cyber Security in Central Banking. *Journal of Financial Regulation.* 2025. Vol. 11 (1). P. 119–128. DOI: https://doi.org/10.1093/jfr/fjae008

16. Safitra M. F., Lubis M., Fakhrurroja H. Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability (Switzerland)*. 2023. Vol. 15 (18). DOI: https://doi.org/10.3390/su151813369

17. Global Cybersecurity Index 2020: Measuring commitment to cybersecurity. International Telecommunication Union. Geneva, 2021. URL: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (дата звернення: 21.04.2025)

18. Global Cybersecurity Index 2024: 5th Edition. International Telecommunication Union. Geneva, 2021. URL: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024 (дата звернення: 21.04.2025).

19. National Cyber Security Index. e-Governance Academy Foundation, 2025. URL: https://ncsi.ega.ee/ncsi-index/ (дата звернення: 21.04.2025).
20. Country Reports: Ukraine. Internet Society Pulse. URL: https://pulse.internetsociety.org/en/reports/ua/ (дата звернення: 21.04.2025).
21. Про CERT-UA. Computer Emergency Response Team of Ukraine. URL: https://cert.gov.ua/about-us (дата звернення: 21.04.2025).

REFERENCES:

1. Stender S.V., Froter O.S., Snitko Yu.M. (2023). Tsyfrova intehratsiia ta kiberzakhyst ekonomiky Ukrainy: pravovi aspekty ta innovatsiini stratehii [Digital integration and cyber protection of the Ukrainian economy: legal aspects and innovative strategies]. *Academic Visions*, vol. 26. Available at: https://academy-vision.org/index.php/av/article/view/799 (accessed: April 21, 2025)
2. Chaykina A., Masliy O., Chervyak A. (2024). Suchasni drayvery pidvyshchennya ekonomichnoyi bezpeky krayiny v umovakh tsyfrovoyi transformatsiyi [Modern drivers of increasing the country's economic security in the context of digital transformation]. *Sustainable Development of Economy*, vol. 2(49), pp. 307–313. DOI: https://doi.org/10.32782/2308-1988/2024-49-49
3. Zhukova Y., Vasylenko V., Yurchenko O. (2024). Stratehii zabezpechennia ekonomichnoi bezpeky krainy v umovakh hlobalnykh vyklykiv [Strategies for ensuring economic security of the country under global challenges]. *Herald of Khmelnytskyi National University. Economic Sciences*, vol. 328 (2), pp. 401–409. DOI: https://doi.org/10.31891/2307-5740-2024-328-60
4. Cherep A., Cherep O., Helman V., Losieva E. (2023). Yevropeyski vektory tsyfrovizatsiyi ekonomiky zadlya zabezpechennya natsionalnoyi bezpeky derzhavy [European vectors of economic digitalization for ensuring the national security of the state]. *Young Scientist*, vol. 11 (123), pp. 163–167. DOI: https://doi.org/10.32839/2304-5809/2023-11-123-6
5. Benzar A., Piestova O. (2022). Problemy ta perspektyvy rozvytku tsyfrovoi ekonomiky v Ukraini [Problems and prospects of the development of the digital economy in Ukraine]. *Digital Economy and Economic Security*, vol. 2 (02), pp. 148–155. DOI: https://doi.org/10.32782/dees.2-25
6. Kindzerskyi Yu. V. (2020). Kiberbezpeka ta stanovlennia tsyfrovoi ekonomiky: problemy vzaiemozviazku [Cybersecurity and becoming of the digital economy: problems of interconnection]. *Economics Bulletin of Dnipro University of Technology*, vol. 3, pp. 18–26. DOI: https://doi.org/10.33271/ebdut/71.018
7. Pichkurova Z. (2023). Rozvytok tsyfrovoi ekonomiky Ukrainy v umovakh voiennoho stanu [Development of Ukraine's digital economy under martial law]. *Economy and Society*, vol. 58. DOI: https://doi.org/10.32782/2524-0072/2023-58-73
8. Berezivsky Ya. P. (2021). Identyfikatsiia umov ta chynnykiv formuvannia tekhnolohichnoi konkurentospromozhnosti natsionalnoi ekonomiky [Identification of conditions and factors of formation of technological competitiveness of the national economy]. *Herald of Lviv University of Trade and Economics. Economic Sciences,* vol. 64, pp. 31–35. DOI: https://doi.org/10.36477/2522-1205-2021-64-05
9. Kolodynskyi S., Drakokhrust T., Bashynska M. (2018). The innovative infrastructure of economic development in the framework of international digital transformation. *Baltic Journal of Economic Studies*, vol. 4 (4), pp. 166–172. DOI: https://doi.org/10.30525/2256-0742/2018-4-4-166-172
10. Juneja A., Goswami S. S., Mondal S. (2024). Cyber Security and Digital Economy: Opportunities, Growth and Challenges. *Journal of Technology Innovations and Energy*, vol. 3 (2), pp. 1–22. DOI: https://doi.org/10.56556/jtie.v3i2.907
11. Lesmana D., Afifuddin M., Adriyanto A. (2023). Challenges and Cybersecurity Threats in Digital Economic Transformation. *International Journal of Humanities Education and Social Sciences (IJHESS)*, vol. 2 (6). DOI: https://doi.org/10.55227/ijhess.v2i6.515
12. Valackiene A., Odejayi R.O. (2024). The impact of cyber security management on the digital economy: multiple case study analysis. *Intellectual Economics*, vol. 18 (2), pp. 261–283. DOI: https://doi.org/10.13165/IE-24-18-2-02
13. Chen X., Wang T., Lin X., Hinde D., Yan Q., Zmire Z. (2023). The Potential of the Digital Economy: A Comparative Assessment of Key Countries' Cybersecurity. *International Journal of Education and Humanities,* vol. 11 (1), pp. 1–7. DOI: https://doi.org/10.54097/ijeh.v11i1.12740
14. Cremer F., Sheehan B., Fortmann M., Kia A. N., Mullins M., Murphy F., Materne S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance: Issues and Practice,* vol. 47 (3), pp. 698–736. DOI: https://doi.org/10.1057/s41288-022-00266-6
15. Aldasoro I., Doerr S., Gambacorta L., Notra S., Oliviero T., Whyte D. (2025). Generative Artificial Intelligence and Cyber Security in Central Banking. *Journal of Financial Regulation,* vol. 11 (1), pp. 119–128. DOI: https://doi.org/10.1093/jfr/fjae008
16. Safitra M. F., Lubis M., Fakhrurroja H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability (Switzerland),* vol. 15 (18). DOI: https://doi.org/10.3390/su151813369
17. Global Cybersecurity Index 2020: Measuring commitment to cybersecurity. International Telecommunication Union. Geneva, 2021. Available at: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (accessed: April 21, 2025).
18. Global Cybersecurity Index 2024: 5th Edition. International Telecommunication Union. Geneva, 2021. Available at: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024 (accessed: April 21, 2025).

19. National Cyber Security Index. e-Governance Academy Foundation, 2025. Available at: https://ncsi.ega.ee/ncsi-index/ (accessed: April 21, 2025).
20. Country Reports: Ukraine. Internet Society Pulse. Available at: https://pulse.internetsociety.org/en/reports/ua/ (accessed: April 21, 2025).
21. Pro CERT-UA [About CERT-UA]. Computer Emergency Response Team of Ukraine. Available at: https://cert.gov.ua/about-us (accessed: April 21, 2025).

УДК 330.342.3:004.056
JEL O33, H56, L86

Пахненко Олена Михайлівна, кандидат економічних наук, доцент, доцент кафедри фінансових технологій і підприємництва, Сумський державний університет. **Божко Микола Олександрович,** аспірант, Сумський державний університет. **Кіберзагрози як виклик економічній безпеці: потенціал технологічної інфраструктури України.**

У статті досліджено вплив кіберзагроз на економічну безпеку в умовах цифрової трансформації. Проведено аналіз індексів кібербезпеки (GCI та NCSI), які дозволяють оцінити рівень національної спроможності до протидії кіберризикам. Увагу зосереджено на технологічній інфраструктурі як ключовому чиннику забезпечення кіберстійкості держави. Надано визначення поняття «технологічна інфраструктура» та охарактеризовано стан таких компонентів технологічної інфраструктури України, як телекомунікаційні мережі, центри обробки даних, хмарні сервіси, інституції кіберзахисту, точки обміну трафіком тощо. Окрему увагу приділено потенціалу технологічної інфраструктури в контексті адаптації до кіберзагроз і підтримки стійкості економіки. Обґрунтовано необхідність подальшої модернізації інфраструктурних потужностей, розвитку партнерств, посилення автоматизації захисних механізмів і підтримки вітчизняних інновацій у сфері кіберзахисту.

Ключові слова: економічна безпека, кіберзагрози, кібершахрайство, технологічні ресурси, технологічний потенціал, цифровізація, цифрова трансформація, загрози.

UDC 330.342.3:004.056
JEL O33, H56, L86

Olena Pakhnenko, PhD in Economics, Associate Professor, Associate Professor of the Department of Financial Technologies and Entrepreneurship, Sumy State University. **Mykola Bozhko,** Postgraduate Student, Sumy State University. **Cyber threats as a challenge to economic security: the potential of Ukraine's technological infrastructure.**

The article explores the growing impact of cyber threats on economic security amid the digital transformation of national economies and increasing reliance on information and communication technologies. This study emphasizes the importance of national technological infrastructure as a key enabler in strengthening cyber resilience and ensuring the stability of digital environments under conditions of hybrid threats. Using internationally recognized metrics such as the Global Cybersecurity Index (GCI) and the National Cyber Security Index (NCSI), the paper evaluates Ukraine's current institutional and infrastructural readiness to resist cyberattacks. It highlights key areas of progress, such as improvements in technical measures and public policy development, as well as persistent vulnerabilities in organizational coordination and capacity building. The article offers a clarified definition of technological infrastructure and presents a comprehensive overview of its key components, based on international frameworks and academic sources. These include telecommunication networks, data centres, cloud services, internet exchange points (IXPs), cybersecurity response institutions (e.g., CERT-UA), and core government digital platforms. The current state and development dynamics of these components in Ukraine are analysed in detail, with emphasis on their relevance for effective threat detection, real-time incident response, and business continuity support. Furthermore, the article examines the strategic potential of Ukraine's technological infrastructure to adapt to increasingly sophisticated and large-scale cyberattacks. Particular attention is given to the functional resilience of decentralized digital public services, the expansion of broadband infrastructure, and the operational readiness of national and sectoral CERT teams. The paper also identifies several critical constraints, including insufficient 5G deployment, reliance on imported equipment, lack of sovereign cloud capacity, and the need for systemic support for domestic cybersecurity innovations.

Key words: economic security, cyber threats, cyber fraud, technological resources, technological potential, digitalization, digital transformation, threats.