Міністерство освіти і науки України

Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

Навчально-науковий інститут фінансів, економіки,
управління та права
Кафедра фінансів, банківського бізнесу та оподаткування

ЕКОНОМІЧНА БЕЗПЕКА: ДЕРЖАВА, РЕГІОН, ПІДПРИЄМСТВО

Матеріали IX Міжнародної
науково-практичної конференції

15 травня 2025 р.

Полтава
2025

УДК 330.342.146:004.056.5

Сидоренко Каріна Олександрівна,
студентка
Науковий керівник: Буряк Альона Анатоліївна,
кандидат економічних наук, доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ФОРМУВАННЯ КІБЕРСТІЙКОСТІ ЕКОНОМІКИ В УМОВАХ ІНФОРМАЦІЙНИХ ЗАГРОЗ

У сучасному світі, де цифрові технології стали основою функціонування усіх сфер економіки, питання кібербезпеки набуло статусу стратегічного пріоритету. Зростаюча цифровізація створює нові можливості, але водночас – численні ризики, пов'язані з інформаційними атаками, витоками даних та технологічними маніпуляціями [1]. У контексті війни, гібридних загроз та глобальної конкуренції, забезпечення стійкості економіки до кіберризиків виступає фундаментом економічної безпеки держави. Визначення, оцінка та нейтралізація таких загроз вимагають міждисциплінарного підходу – від ІТ та права до економіки й стратегічного управління.

Кіберстійкість – це здатність економічної системи протистояти, адаптуватися та швидко відновлюватися після кіберінцидентів [2]. Йдеться не лише про технічну захищеність окремих об'єктів, а про системний підхід, який охоплює [4]:

– державне регулювання та стратегічне планування;

– розвиток кіберкультури у бізнесі та суспільстві;

– інтеграцію безпекових вимог у цифрову трансформацію;

– забезпечення резервних сценаріїв функціонування ключових секторів економіки в умовах кібератак.

Формування кіберстійкості вимагає не реактивних, а проактивних підходів, де безпека закладається у процеси ще на етапі їх проєктування за принципом «security by design». Ключові загрози для економіки в цифровому середовищі [6]:

– атаки на об'єкти критичної інфраструктури (енергетика, зв'язок, транспорт);

– компрометація фінансових систем через фішинг, зловмисне ПЗ;

– економічні шкідливі кампанії (інформаційна дестабілізація, паніка на ринках);

– промислове шпигунство та витік технологічної інформації;

– атаки з вимогою викупу та подальшим блокуванням операційних процесів.

Під впливом цифрових загроз економіка зазнає не тільки прямого збитку, а й втрати конкурентних переваг, інвестиційної привабливості, технологічної автономності. Особливо небезпечними є скоординовані атаки, які поєднують технічні засоби з інформаційно-психологічним впливом, що підриває довіру до економічних та політичних інститутів.

Розглядаючи міжнародний досвід кіберстійкості, варто зазначити, що розвинені держави впроваджують національні стратегії кібербезпеки з фокусом на економічну стійкість, зокрема:

– США: модель «національного цифрового щита», що поєднує державні і приватні ініціативи;

– ЄС: директива NIS2, яка розширює зобов'язання щодо кіберзахисту на ключові сектори економіки;

– Ізраїль: інституціоналізована система кіберкомандування в економічному секторі;

– Сінгапур: національний центр кібербезпеки із повноваженнями для реагування на економічні загрози.

Усі ці країни активно залучають наукову спільноту, громадські організації та приватний сектор до формування політик кіберстійкості.

Для забезпечення належного рівня кіберстійкості в Україні варто [7]:

– законодавчо закріпити вимоги до безпеки критичної інфраструктури;

– створити публічну карту кіберінцидентів, що відображатиме їх вплив на економіку;

– стимулювати інвестиції в цифрову безпеку на рівні підприємств;

– підтримувати освітні та просвітницькі ініціативи з кіберграмотності;

– запровадити обов'язкові аудити інформаційної безпеки для стратегічних підприємств;

– розвивати партнерства між державою, бізнесом та IT-сектором.

Особливу увагу слід приділити секторам, що є найбільш уразливими: енергетиці, фінансам, логістиці, телекомунікаціям. Важливо також адаптувати міжнародні стандарти (ISO/IEC 27001, NIST) до українського законодавчого поля та специфіки загроз.

Наукова спільнота має відігравати провідну роль у розробці інструментів оцінки кіберризиків, створенні моделей економічної стійкості до інформаційних впливів, просуванні інновацій у сфері цифрової безпеки. Доцільно формувати міжвідомчі дослідницькі консорціуми, які б інтегрували знання в галузі IT, права, економіки, соціології для комплексної оцінки кіберзагроз. Важливо також залучити українські стартапи до розробки інноваційних рішень, таких як системи виявлення аномалій, блокчейн-сервіси захисту даних, автономні кіберпатрулі тощо.

Формування кіберстійкої економіки – це не лише питання технічної безпеки, а комплексне завдання, яке

охоплює управлінські, освітні, правові та технологічні аспекти. У сучасних умовах саме здатність швидко реагувати на кіберзагрози та адаптуватися до нових форм інформаційного впливу визначає рівень економічної безпеки держави. Для України, яка перебуває під постійним тиском гібридної війни, розвиток кіберстійкості є умовою збереження суверенітету та економічної стабільності. Необхідно забезпечити сталу координацію між усіма учасниками інформаційного простору – державою, бізнесом, громадянським суспільством і наукою – для побудови безпекоорієнтованої цифрової економіки.

Література

1. Buriak A., Masliy O. Strategic foundations of security-oriented international space: economic, informational and ecological dimensions. Економіка і регіон. 2024. №1 (92). С. 281–287. DOI: https://doi.org/10.26906/EiR.2024.1(92).3341.

2. Буряк А.А., Кудряшова Д.О., Сторожук Л.М. Стратегія розвитку digital-економіки в Україні: національна візія та виклики глобалізації. Система управління відходами в циркулярній економіці: фінансові, соціальні, екологічні та енергетичні детермінанти : монографія. Суми : Сумський державний університет, 2023. С. 239–248.

3. Пугач О. Моделювання загроз системі економічної безпеки національної економіки з позицій їх своєчасного виявлення та передбачення. *Економіка і регіон*. 2015. № 3 (52). С. 103–109.

4. Buryak, A.A., Makhovka, V.M., & Storozhuk, L.M. (2023). Strategy and mechanisms for implementing the digital economy in the EU and Ukraine as a condition for overcoming the crisis. Economy and Region, 2(89), 53-59. DOI: https://doi.org/10.26906/eip.v0i2(89).2934.

5. Onyshchenko, S., Maslii, O., Hlushko, A. (2025). Digital and Economic Security of the State Under Global Threats. In: Dovgyi, S., Siemens, E., Globa, L., Kopiika, O., Stryzhak, O. (eds)

Applied Innovations in Information and Communication Technology. ICAIIT 2024. Lecture Notes in Networks and Systems, vol 1338. Springer, Cham. https://doi.org/10.1007/978-3-031-89296-7_29

6. Buriak A., Levchenko I. The role of international organizations in the formation of a security-oriented information environment and the implementation of strategies for ensuring the economic and ecological security of Ukraine. Current problems of sustainable development. 2024. No 1. Vol. 1. P. 7–12.

7. Masliy O.A., Buriak A.A. (2023) Transformation of threats for the economic security and security of the infor-mation environment of Ukraine in the conditions of a full-scale war. State and regions. Series: Economics and Business, no. 3(129), pp. 28–32.

УДК 336

Кудінова Аліна Олександрівна,
кандидат економічних наук, доцент
Черевань Кіра Сергіївна,
студентка
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ВИКОРИСТАННЯ ШІ ПРИ ЗАБЕЗПЕЧЕННІ БЕЗПЕКООРІЄНТОВАНОГО ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ПІДПРИЄМСТВА[5]

Практика менеджменту показує, що роль штучного інтелекту (ШІ) в безпекових стратегіях підприємства постійно підвищується, оскільки він стає центральним інструментом у створенні динамічних та стійких інформаційних середовищ,

[5] Тези підготовлено в межах виконання НДР молодих учених «Формування безпекоорієнтованого інформаційного середовища для підвищення економічної безпеки України у воєнний та повоєнний періоди», державний реєстраційний номер 0124U000615