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

7. Дахнова О.Є., Гнідь М.В. Прогнозування рівня бюджетної безпеки України. *Інфраструктура ринку*. 2019. № 31. С. 620-624.

8. Varnaliy Z., Pugach A. Forming the Priority Guidelines for Providing the State Economic Security. *Economics and region*. 2015. № 5 (54). С. 3–9. URL: http://nbuv.gov.ua/UJRN/econrig_2015_5_3

9. Glushko, A. D., Pantas, V. V., Babenko, S. R. (2022). Information policy in the system of financial security of the state. *Efficient economy*, 2. DOI: https://doi.org/10.32702/2307-2105-2022.2.95

УДК 330.341.1:004.056.5

Дубляк Вікторія Сергіївна,
студентка
Науковий керівник: Буряк Альона Анатоліївна,
кандидат економічних наук, доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ЦИФРОВІ РИЗИКИ В УМОВАХ ВОЄННОГО СТАНУ: ВИКЛИКИ ТА АДАПТИВНІ МЕХАНІЗМИ ЗМІЦНЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

Реалії повномасштабної війни в Україні зумовили суттєві трансформації в усіх сферах суспільного життя, зокрема в системі економічної безпеки. Одним із найбільш уразливих напрямів стала цифрова сфера, яка в умовах збройної агресії перетворилася на поле активного протиборства. Кібератаки, інформаційно-психологічні операції, деструкція цифрової інфраструктури – усе це стало частиною гібридної війни, що прямо впливає на функціонування економіки.

В умовах воєнного стану цифрові ризики не лише зростають за масштабом і частотою, а й набувають нових форм, зокрема – атак на енергетичні системи, логістику, банківську інфраструктуру, системи електронного врядування. Розуміння природи цих загроз та розробка адаптивних механізмів реагування є необхідними для підтримання стійкості економіки й захисту критичних функцій держави [1].

У період повномасштабного вторгнення рф цифрові ризики в Україні можна класифікувати за кількома групами [3]:

Кібератаки на критичну інфраструктуру. Ураження енергосистем, залізничної логістики, банківських систем тощо. Найбільш небезпечні – деструктивні атаки знищення даних. Інформаційно-психологічні операції. Масоване поширення фейків, дезінформації, використання бот-мереж для маніпуляцій громадською думкою, атак на репутацію стратегічних підприємств.

Загрози у хмарних середовищах. Більшість українських компаній і держструктур використовують хмарні сервіси, які потенційно можуть бути вразливими при відсутності багаторівневої аутентифікації, шифрування та аудиту доступу.

Злам державних реєстрів та платформ. Попри стійкість систем «Дія», ризик втрати даних або їх компрометації зберігається.

Цифрові загрози мають багатовимірний вплив на економічну безпеку. Серед найбільш вагомих наслідків [5]:

1. Фінансові збитки – втрати бізнесу від простоїв, витрати на відновлення систем, репутаційні ризики.

2. Зниження довіри до цифрових сервісів. Атаки на державні платформи або банківські системи підривають довіру до електронного управління та можуть гальмувати цифровізацію.

3. Ризик втрати стратегічної інформації, зокрема компрометація комунікацій в оборонно-промисловому секторі або у сфері закупівель веде до реальних воєнних втрат.

4. Порушення функціонування ланцюгів постачання, зокрема кібератаки на логістичні сервіси впливають на постачання продовольства, медикаментів, техніки.

Розглядаючи адаптивні механізми реагування та мінімізації ризиків, варто зазначити, що Україна, маючи багаторічний досвід гібридного протистояння, розробила низку механізмів для реагування на цифрові загрози [6]:

1. Координація з приватним сектором. Платформи на зразок Cyber Rapid Response Teams, підтримка українських IT-волонтерів (наприклад, IT Army of Ukraine) є прикладом ефективної самоорганізації.

2. Розбудова кіберсил. Створено кіберкомандування ЗСУ, кіберпідрозділи СБУ та Національної поліції, які здійснюють активне відстеження, блокування та контратаку на ворожі ресурси.

3. Міжнародна підтримка. Країни ЄС і НАТО надають Україні аналітичну та технічну підтримку в кіберзахисті. Також Україна долучилася до Європейської програми кіберстійкості.

4. Законодавча база. Прийнято Закон України «Про основні засади забезпечення кібербезпеки», активізовано впровадження національної стратегії кібербезпеки, а також адаптовано нові регуляторні документи у сфері критичної інфраструктури.

Підвищення цифрової стійкості є одним із ключових інструментів забезпечення економічної безпеки. Йдеться не лише про кіберзахист, а про цілісну систему управління ризиками, яка передбачає [7]:

– інтеграцію систем резервного копіювання та планів безперервності бізнесу;

– аудит кіберризиків у великих корпораціях та державному секторі;

– застосування систем моніторингу загроз на базі штучного інтелекту;

– підготовку кіберрезерву, зокрема фахівців, здатних швидко реагувати на інциденти.

Крім того, необхідно вбудовувати цифрову безпеку в економічне планування: при розробці держпрограм враховувати ризики з боку інформаційного середовища, аналізувати потенційні загрози для інвестиційного клімату, застосовувати економетричні моделі оцінки збитків від кіберінцидентів. Цифрові ризики в умовах війни стали ключовим фактором впливу на економічну стабільність держави. Знищення або злам цифрової інфраструктури здатні призвести до фінансових, репутаційних, логістичних втрат, а отже – до загального ослаблення національної економіки.

Україна демонструє високу адаптивність у реагуванні на кіберзагрози, однак у перспективі необхідно створити сталу систему цифрової безпеки, що базується на принципах кіберстійкості, міжсекторальної співпраці, дотримання прав людини та інтеграції до міжнародних цифрових стандартів. В умовах воєнного часу цифрова безпека стає одним із базових компонентів національного економічного захисту. Її зміцнення – не лише вимога сьогодення, а й запорука економічного відновлення у повоєнний період.

Література

1. 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.

2. Онищенко С.В., Маслій О.А. Ризики та загрози в умовах цифровізації: безпековий аспект. II International 223 Scientific Conference Development of Socio-Economic Systems in a Global Competitive Environment: Conference Proceedings, May 24th, 2019. Le Mans, France. P.54-56.

3. 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.

4. Krasnobayev, V., Yanko, A., Hlushko, A., Kruk, O., Kruk, O., Gakh, V. (2023). Cyberspace protection system based on the data comparison method. Economic and cyber security. Kharkiv: PC TECHNOLOGY CENTER, 3–29. https://doi.org/10.15587/ 978-617-7319-98-5.ch1

5. 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.

6. 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.

7. 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.

8. Onyshchenko S., Zhyvylo Ye., Hlushko A., Bilko S. Cyber risk management technology to strengthen the information security of the national economy. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2024, No 5. C. 136-142.