***Денис ТКАЧУК***
*PhD, старший викладач Карпатського національного університету імені Василя Стефаника*

# КІБЕРБЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ

Сучасний етап розвитку світової економіки характеризується стрімким поширенням цифрових технологій, які здійснюють безпосередній вплив на трансформацію системи національної безпеки. За таких умов кіберпростір стає повноцінним середовищем функціонування економіки, в рамках якої формуються нові ризики, що пов'язані із цифровими загрозами, кіберзлочинністю та вразливістю інформаційних систем. Це обумовлює необхідність розгляду кібербезпеки як однієї із ключових складових національної економічної безпеки.

Впровадження інформаційно-комунікаційних технологій в державне управління, фінансову систему та критичну інфраструктуру створює передумови для підвищення ефективності економіки, проте формує залежність від стабільного функціонування цифрового середовища. Забезпечення ефективної системи кібербезпеки набуває первинного значення в умовах зростання кіберзагроз і активізації гібридних форм протистояння між державами. Кіберзлочинність перетворюється на комплексне явище, яке здатне здійснювати вплив на фінансову стабільність держави, функціонування інституцій публічної влади, критичну інфраструктуру тощо [1, с.82-86].

Важливою характеристикою сучасних кіберризиків є їх багаторівневий та накопичувальний характер. Поряд із відкритими атаками існують латентні загрози, які поступово накопичуються та можуть підсилювати негативні наслідки в майбутньому. Такий ефект здатний викликати каскадні порушення в економічній системі, що призводить до зниження загальної стійкості держави. У цьому контексті кібербезпека набуває стратегічного значення як інструмент запобігання системним кризам [1, с.87].

Також кіберзагрози мають значний вплив на фінансовий сектор. Кібератаки у банківській сфері спричиняють значні економічні втрати, підривають довіру до фінансових інститутів та провокують макроекономічну нестабільність. У свою чергу, розвиток фінансових технологій і цифрових платформ підвищує вразливість економічних систем, оскільки складність їх архітектури та високий рівень автоматизації створюють додаткові точки ризику.

У сучасних умовах цифровізації кібербезпека тісно пов'язана з питанням захисту конфіденційної інформації. Витік комерційної або персональної інформації може призвести до суттєвих економічних втрат, зниження

конкурентоспроможності підприємств та підриву економічної безпеки держави в цілому. Це підтверджує необхідність формування комплексної системи інформаційної безпеки, яка забезпечуватиме цілісність, достовірність і захищеність даних [2].

На рівні державної політики ключовим напрямом забезпечення кібербезпеки є формування системного підходу до управління цифровими ризиками. Досвід розвинених країн свідчить, що ефективна модель кібербезпеки базується на поєднанні державного регулювання, розвитку технологічної інфраструктури та міжсекторальної взаємодії. Важливу роль відіграє стратегічна координація між державними органами та приватним сектором, а також інтеграція у міжнародні системи кібербезпеки. Велике значення має також впровадження інституційних механізмів цифрової безпеки, зокрема створення центрів кібероперацій, використання систем моніторингу та раннього виявлення загроз, а також формування кіберрезерву фахівців. Підвищення цифрової грамотності населення та працівників державного сектору розглядається є важливим елементом забезпечення кіберстійкості держави [3, с. 143-144; 4, с.81-83 ].

На мікроекономічному рівні ефективність кібербезпеки залежить від впровадження превентивних заходів. До таких заходів належать контроль доступу до інформаційних ресурсів, управління вразливостями, резервне копіювання даних, запобігання витоку інформації та постійне навчання персоналу. Поєднання технічних та організаційних інструментів дозволяє зменшити ймовірність кіберінцидентів та обмежити їх економічні наслідки [5, с.222-223].

Отже, кібербезпека є невід'ємною складовою національної економічної безпеки в умовах цифровізації. Вона являє собою широкий спектр операцій у цифровому середовищі, який охоплює захист інформації, інфраструктури, формування інституційних механізмів управління ризиками тощо. Зростання ролі цифрових технологій в економіці зумовлює необхідність переходу від реактивних до превентивних моделей кіберполітики, спрямованих на раннє виявлення та нейтралізацію загроз.

## Список використаних джерел:

*1. Тютюник І.В., Михайлюк О.С., Пасько Д.В. Національна безпека в цифрову епоху: структурний аналіз кіберризиків та організованої кіберзлочинності. Економіка. Менеджмент. Бізнес. 2025. №4. С.81-89.*

*2. Волинець В.В. Конфіденційність комерційної інформації як складова економічної безпеки України. Український політико-правовий дискурс. 2025. №12.*

*3. Стельмах А. Сучасні аспекти розвитку цифровізації у системі національної безпеки: закордонний досвід. Публічне управління: концепції, парадигма, розвиток, удосконалення. 2025. Вип.12. С.141-147.*

*4. Пилипенко О. ІТ-сектор як фактор економічної стійкості та відновлення національної економіки України. Вчені записки Університету «КРОК». 2026. №1(81). С.78-87.*

*5. Миронченко Д.В. Механізми попередження кіберзагроз для забезпечення економічної безпеки країни. Актуальні проблеми економіки. 2025. № 12(294). С.219-226.*