**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 X Міжнародної
науково-практичної конференції

13 травня 2026 р.

Полтава
2026

**УДК 336.32**

***Березка Богдан Тарасович,***
*студент*
*Науковий керівник: Худолій Юлія Сергіївна,*
*кандидат економічних наук, доцент*
*Національний університет «Полтавська політехніка імені Юрія Кондратюка»*

# ЕКОНОМІЧНА БЕЗПЕКА ДЕРЖАВИ В УМОВАХ ЦИФРОВІЗАЦІЇ: ЗАГРОЗИ ТА МЕХАНІЗМИ ПРОТИДІЇ

Цифрова трансформація економіки формує якісно новий вимір загроз економічній безпеці держави, які не мають аналогів у докризових концепціях. Кириленко С. В. зазначає наступне: «В умовах цифрової економіки система економічної безпеки держави набуває нових рис: загрози стають транскордонними, невидимими та асиметричними, що принципово змінює підходи до їхньої ідентифікації та нейтралізації» [3, с. 41]. Традиційні моделі забезпечення економічної безпеки, побудовані навколо захисту фізичних активів, виробничого та фінансового потенціалу, виявляються недостатніми в умовах, коли критично важливі функції держави – від бюджетного управління до регулювання ринків – реалізуються через цифрові платформи і є вразливими до кібератак, технологічної залежності та маніпуляцій з даними.

Маслій О. А. та співавтори у монографії, присвяченій детермінантам економічної безпеки держави в парадигмі цифрового розвитку, обґрунтовують наступну тезу: «цифровізація є одночасно чинником зміцнення і джерелом нових загроз економічній безпеці: вона підвищує ефективність державного управління, але водночас розширює поверхню атаки для деструктивних зовнішніх і внутрішніх суб'єктів» [2, с. 47]. Автори пропонують розглядати економічну безпеку в цифровому середовищі через призму трьох взаємопов'язаних підсистем: *цифрової стійкості* (здатність протистояти кібератакам і збоям цифрової інфраструктури), *цифрового суверенітету* (незалежність від іноземних технологічних платформ і збереження контролю над стратегічними даними) та *цифрової довіри* (достовірність економічної інформації в публічному просторі та надійність цифрових фінансових сервісів).

Біличенко М. М. у своєму дослідженні зазначає, що еконцептуальна модель оцінки економічної безпеки підприємства в умовах цифрової трансформації має інтегрувати традиційні фінансово-економічні індикатори з показниками цифрової захищеності, технологічної незалежності та інформаційної прозорості [1]. Перенесення цього підходу на рівень держави означає необхідність формування багаторівневої системи індикаторів економічної безпеки, де цифровий вимір є самостійним і рівнозначним структурним компонентом поряд із традиційними складовими – фінансовою, виробничою, інвестиційною, соціальною та енергетичною безпекою.

На основі узагальнення результатів досліджень вищезазначених авторів щодо розуміння цифрових загроз економічній безпеці держави у таблиці 1 розглянуто елементи протидії, що відповідають основним класам таких загроз [1–3]. Виокремлення загроз та відповідних механізмів протидії дозволяє виділити три рівні моделі економічної безпеки держави в цифровому середовищі. Перший – превентивний, включає систему моніторингу цифрових загроз у режимі реального часу, розвідку загроз та регуляторне нормування вимог до кіберзахисту суб’єктів критичної інфраструктури. Другий – реагування: містить протоколи швидкого реагування на інциденти, механізми відновлення цифрових сервісів, санкційні та правові інструменти відповіді на кібератаки.

Таблиця 1

Цифрові загрози економічній безпеці держави та елементи протидії

| Клас цифрових загроз | Прояв у сфері економічної безпеки держави | Елемент протидії |
|---|---|---|
| Кіберзлочинність та кібератаки на критичну інфраструктуру | Дестабілізація фінансової системи, енергетики, логістики; прямі економічні збитки та підрив довіри до цифрових сервісів держави | Національна система кіберзахисту (CERT-UA); обов'язковий аудит кіберстійкості об'єктів критичної інфраструктури; страхування кіберризиків |
| Цифровий шпіонаж та витік стратегічних даних | Несанкціонований доступ до державної економічної статистики, планів відновлення, бюджетних даних; передача стратегічної інформації ворожим суб'єктам | Класифікація відкритих даних за рівнем стратегічної чутливості; шифрування державних інформаційних ресурсів; контроль доступу за моделлю Zero Trust |
| Маніпуляції з цифровими фінансовими ринками та криптовалютами | Дестабілізація валютного курсу, відтік капіталу через криптоканали, фінансування тіньових схем та санкційний арбітраж | Регуляторний нагляд за цифровими активами (VASP); реалізація вимог FATF щодо крипторинку; моніторинг транскордонних потоків капіталу |
| Технологічна залежність та цифровий суверенітет | Вразливість від іноземних IT-платформ, хмарних сервісів і програмного забезпечення; ризик відключення від критичних цифрових сервісів | Державна програма цифрового імпортозаміщення; розвиток вітчизняної IT-індустрії; локалізація критичних державних даних на національних серверах |
| Дезінформація та маніпуляції з економічними даними | Викривлення економічних очікувань, підрив інвестиційної привабливості, дестабілізація ринків через фейкові економічні новини | Системи верифікації офіційних економічних даних; моніторинг медіапростору на предмет економічної дезінформації; цифрова медіаграмотність |

*Джерело: складено авторами на основі [1–3]*

Третій – стратегічний: передбачає розбудову цифрового суверенітету через розвиток вітчизняної IT-галузі, локалізацію критичних даних та формування кваліфікованого кадрового резерву у сфері кіберзахисту. Кириленко С. В. наголошує, що лише системна реалізація усіх трьох рівнів захисту здатна забезпечити стійку економічну безпеку держави в умовах цифровізації [3, с. 45].

Отже, економічна безпека держави в цифровому середовищі є багаторівневим феноменом, що охоплює кіберзахист критичної інфраструктури, збереження цифрового суверенітету, регулювання цифрових фінансових ринків та протидію економічній дезінформації. Розглянуті напрямки протидії загрозам базуються на поєднанні превентивних, реагувальних та стратегічних механізмів.

**Література**

1. Біличенко М. М. Концептуальна модель оцінки економічної безпеки підприємства в умовах цифрової трансформації. *Здобутки економіки: перспективи та інновації*. 2025. № 18. https://doi.org/10.5281/zenodo.15540326.

2. Маслій О. А., Кудінова А. О., Буряк А. А., Янко А. С., Білько С. С. *Детермінанти економічної безпеки держави в парадигмі цифрового розвитку*: монографія. Івано-Франківськ: НАІР, 2025. 324 с.

3. Кириленко С. В. Система економічної безпеки в умовах цифрової економіки. *Journal of Strategic Economic Research*. 2024. № 1. С. 40–47.

4. Onyshchenko, S., Matkovskyi, A., Puhach, A. Analysis of threats to economic security of Ukraine in conditions of innovative economic development. *Economic Annals-XXI*. 2014. № 1-2(2). С. 8–11. URL: http://nbuv.gov.ua/UJRN/ecchado_2014_1-2(2)__3.