Маріупольський університет

ОСОБЛИВОСТІ ІНТЕГРАЦІЇ КРАЇН У СВІТОВИЙ ЕКОНОМІЧНИЙ ТА ПОЛІТИКО-ПРАВОВИЙ ПРОСТІР

Матеріали XII Міжнародної науково-практичної конференції

12 грудня 2025 року

Київ 2025

УДК 339.922 (063)

Особливості інтеграції країн у світовий економічний та політико-правовий простір: Матеріали XII Міжнародної науково-практичної конференції, 12 грудня 2025 р. / За заг. ред. к.е.н., доцента Марени Т.В. — Київ: МДУ, 2025. — 118 с.

Конференція присвячена проблемам активізації процесу інтеграції країн у світовий економічний та політико-правовий простір. В роботі конференції приймають участь науковці, викладачі, фахівці-практики, здобувачі вищої освіти.

***Основні напрями роботи конференції*:**

- Безпекова складова соціально-економічного розвитку країн світу;
- Розвиток інтеграційних процесів в умовах військово-політичного конфлікту;
- Розвиток міжнародних фінансово-кредитних та валютних відносин в умовах глобалізації;
- Інноваційно-інвестиційна діяльність країн світу;
- Забезпечення конкурентоспроможності національних економік;
- Проблеми забезпечення сталого розвитку;
- Особливості повоєнного відновлення економіки України.

Організаційний комітет конференції ставить перед собою такі задачі:

1. Обмін практичними і теоретичними напрацюваннями учасників конференції у сфері вивчення особливостей інтеграції країн у систему світогосподарських зв'язків;

2. Розробка напрямів розвитку міжнародних економічних відносин країн світу.

СЕКЦІЯ
БЕЗПЕКОВА СКЛАДОВА СОЦІАЛЬНО-ЕКОНОМІЧНОГО РОЗВИТКУ КРАЇН СВІТУ

КЮРДЖИЄВ А.С.,
здобувач вищої освіти третього (освітньо-наукового) рівня
ОНП «Економіка»,
Маріупольський державний університет
ТОЛПЕЖНІКОВ Р.О.,
доктор економічних наук, доцент,
професор кафедри економіки та міжнародних економічних відносин,
Маріупольський державний університет

ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ

Цифрова трансформація сучасної економіки суттєво змінює характер взаємодії між суб'єктами господарювання, державними інституціями та міжнародними ринками. Вона формує нові передумови розвитку, стимулює підвищення ефективності бізнес-процесів, однак одночасно створює значний спектр викликів економічній безпеці. Серед ключових ризиків, що виникають у цифровому середовищі, варто виділити кіберзагрози, технічні збої, порушення цілісності даних, залежність від цифрових платформ, інформаційні витоки та збільшення нестабільності ринкових процесів.

Теоретичні аспекти забезпечення економічної безпеки в умовах цифровізації вимагають ґрунтовного аналізу структурних змін у світовій економіці та їх вплив на економіку України. Важливим є розширення наукового підходу до визначення економічної безпеки за рахунок інтеграції понять цифрової стійкості, кібергігієни, інформаційної надійності та технологічної незалежності. Економічна безпека визначається сьогодні не лише як здатність протистояти фінансовим чи політичним впливам, але й як можливість ефективно управляти цифровими ризиками, формувати інноваційні механізми захисту та забезпечувати безперервність економічних процесів використовуючи інструменти прогнозування на основі штучного інтелекту.

Практичні засади включають розробку та впровадження інтегрованих моделей управління ризиками. Одним із найбільш ефективних підходів є модель «проактивні дії + реактивні заходи», у якій враховується як прямі витрати на запобігання загрозам, так і потенційні економічні втрати від їхньої реалізації. Формально модель можна описати наступним рівнянням:

$$Vr = f(c;l),$$

де Vr – вартість ризику, c– витрати на проактивні заходи, l – можливі втрати від настання ризику.

У практичній площині держави/підприємства повинні реалізувати багаторівневі системи кіберзахисту, впроваджувати цифрові протоколи безпеки, здійснювати постійний моніторинг інформаційних потоків, проводити аудит цифрових активів та забезпечувати навчання персоналу. Важливою передумовою зниження ризиків є взаємодія з міжнародними структурами, які формують глобальні стандарти інформаційної та економічної безпеки.

Особливу увагу слід приділити оцінюванню економічних збитків, що можуть виникнути в результаті реалізації цифрових загроз. За даними OECD, глобальні втрати від кіберзлочинності щорічно зростають на 15–20%, що демонструє необхідність адаптації державної політики у сфері економічної безпеки. Держави, інтегруючись у світовий

економічний простір, повинні гармонізувати власні стандарти безпеки із міжнародними нормами, враховувати особливості цифрового ринку та забезпечувати захист критичної інфраструктури.

Запровадження комплексних цифрових стратегій та моделей захисту дозволяє зміцнити економічну стійкість країн та підвищити їхню конкурентоспроможність на глобальному рівні.

Оцінки вартості кіберзлочинності демонструють значну варіативність — від десятків мільярдів до трильйона доларів чи більше. Це пов'язано з відсутністю даних і різними методологіями. Існує моделювання, запозичене з економічно-історичних досліджень, де дані зазвичай неповні або переривчасті, щоб змоделювати вартість кіберзлочинності. За оцінками CSIS, глобальна вартість кіберзлочинності могла становити до 608 мільярдів доларів у 2017 році, що дорівнювало 0,8% глобального ВВП .

Таблиця 1

Регіональні втрати через кіберзлочинність 2017

Регіон (Світовий Банк)	Регіональне ВВП (USD,триліони)	Втрати від кіберзлочинності (USD,млрд)	Втрати від кіберзлочинності у % ВВП
Північна Америка	20,2	140-175	0,69-0,87
Європа та центральна Азія	20,3	160-180	0,79-0,89
Східна Азія та Тихоокеанський регіон	22,5	120-200	0,53-0,89
Південна Азія	2,9	7-15	0,24-0,52
Південна Америка	5,3	15-30	0,28 – 0,57
Південна Африка	1,5	1-3	0,07-0,20
MENA	3,1	2-5	0,06 -0,16
СВІТ	75,8	445-608	0,59-0,80

Цифровізація економіки відкриває нові можливості для держав та бізнесу, але одночасно породжує значні ризики — від втрат даних та кіберзлочинності до порушень роботи критичної інфраструктури.

Як вже було зазначено за оцінками OECD, глобальні втрати від кіберзлочинності щорічно зростають на 15–20%, що демонструє необхідність адаптації політики у сфері економічної безпеки (OECD, 2025). Уже 2020 року задокументовані прямі збитки від кіберінцидентів становили близько 28 млрд дол. США, а в 2025 р бизько 55 млрд дол. США.

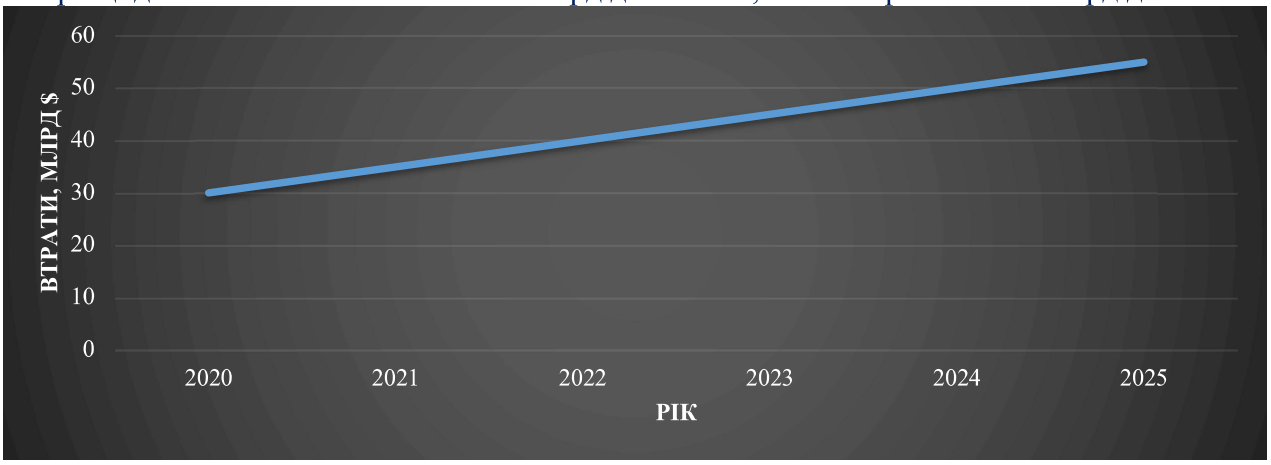

Рис.1. Динаміка економічних втрат від кіберзлочинності, 2020-2025 рр.

Таблиця 2

Основні цифрові ризики та їхній вплив

Тип ризику	Прояв	Потенційні наслідки
Кіберзагрози	Зовнішні атаки, фішинг	Відмова систем, фінансові збитки
Інформаційні витоки	Компрометація даних	Репутаційні та юридичні наслідки
Збої інфраструктури	Відмова серверів	Порушення бізнес-процесів

У результаті дослідження теоретичних і практичних засад забезпечення економічної безпеки в умовах цифрової трансформації встановлено, що цифровізація одночасно стимулює інноваційний розвиток економіки та створює критично важливий спектр ризиків, які потребують системного управління. Сучасна економіка функціонує в умовах високої цифрової залежності, що формує нову модель економічної безпеки, зосереджену на цифровій стійкості, захисті інформаційних активів та здатності ефективно управляти технологічними загрозами.

Аналіз дозволив ідентифікувати основні типи ризиків, притаманні цифровому середовищу. Зокрема, кіберзагрози, що проявляються у формі зовнішніх атак або фішингових кампаній, можуть призводити до відмови інформаційних систем і значних фінансових втрат. Інформаційні витоки та компрометація даних загрожують репутаційними та юридичними наслідками, які негативно впливають на довіру до суб'єктів господарювання. Збої інфраструктури, пов'язані з відмовами серверів або порушенням критичних цифрових сервісів, здатні паралізувати бізнес-процеси та спричинити тривалі економічні втрати. Врахування цих ризиків є ключовим компонентом сучасних моделей економічної безпеки.

Глобальна динаміка кіберзбитків, що, за оцінками OECD, зростає на 15–20% щорічно, підтверджує об'єктивну необхідність адаптації державної політики та управлінських стратегій до реалій цифрової економіки. Значне збільшення обсягів збитків — від 28 млрд дол. США у 2020 році до прогнозованих близько 55 млрд дол. США у 2025 році — свідчить про загострення проблеми та потребу у впровадженні багаторівневих систем кіберзахисту, міжнародної координації та гармонізації стандартів цифрової безпеки.

Практичні засади забезпечення економічної безпеки полягають у застосуванні інтегрованих моделей управління ризиками, які поєднують проактивні заходи запобігання загрозам та реактивні інструменти мінімізації збитків після їх настання. Особливого значення набувають впровадження цифрових протоколів безпеки, регулярний аудит інформаційних ресурсів, системний моніторинг кіберінцидентів, підвищення цифрових компетентностей персоналу, а також стратегічне планування на основі сучасних аналітичних та прогностичних інструментів.

Отже, забезпечення економічної безпеки в умовах цифрової трансформації вимагає цілісного, науково обґрунтованого та стратегічного підходу, що враховує різнорівневі цифрові ризики, їхні потенційні наслідки та глобальні тенденції розвитку кіберпростору. Реалізація таких підходів сприятиме зміцненню стійкості економічних систем, підвищенню конкурентоспроможності держави та формуванню безпечного цифрового середовища для бізнесу та суспільства.

Список використаних джерел:

1. Zveryakov M. Economic Security in the Digital Economy. Kyiv, 2020.
2. Center for Strategic and International Studies (CSIS), McAfee. Economic Impact of Cybercrime — No Slowing Down. Washington, D.C., 2018
3. OECD (2025). Economic Security in a Changing World
4. Schwab K. The Fourth Industrial Revolution. World Economic Forum.

5. McAfee. Global Cybercrime Report 2023.

ЛУБІНЕЦЬ Д.В.,
здобувач вищої освіти другого (магістерського) рівня
ОП «Міжнародний бізнес»,
Маріупольський державний університет

МІЖНАРОДНА МІГРАЦІЯ ЯК ЧИННИК ЕКОНОМІЧНОЇ БЕЗПЕКИ КРАЇН: ГЛОБАЛЬНІ ТЕНДЕНЦІЇ ТА УКРАЇНСЬКИЙ КОНТЕКСТ

В умовах поглиблення глобалізаційних процесів та посилення транснаціональної мобільності населення міжнародна міграція перетворюється на один із ключових факторів соціально-економічного розвитку та економічної безпеки держав. Міграційні потоки істотно впливають на ринок праці, демографічну структуру, формування людського капіталу, фіскальну стійкість і макроекономічну рівновагу країн. Для України актуальність проблеми управління міжнародними міграційними процесами суттєво зросла в умовах повномасштабної війни, масового вимушеного переміщення населення, зростання зовнішньої міграції та ризиків довгострокової втрати трудового й інтелектуального потенціалу.

За даними Департаменту з економічних і соціальних питань Організації Об'єднаних Націй, чисельність міжнародних мігрантів у світі зросла з 153 млн осіб у 1990 році до 304 млн осіб у 2024 році, тобто майже вдвічі за три десятиліття (UN DESA, 2024). Частка міжнародних мігрантів у загальній чисельності населення світу становить близько 3,7 %, що свідчить про поступове зростання глобальної мобільності населення. Водночас динаміка міжнародної міграції є нерівномірною та відображає глибокі диспропорції соціально-економічного розвитку між регіонами світу (рис.1).

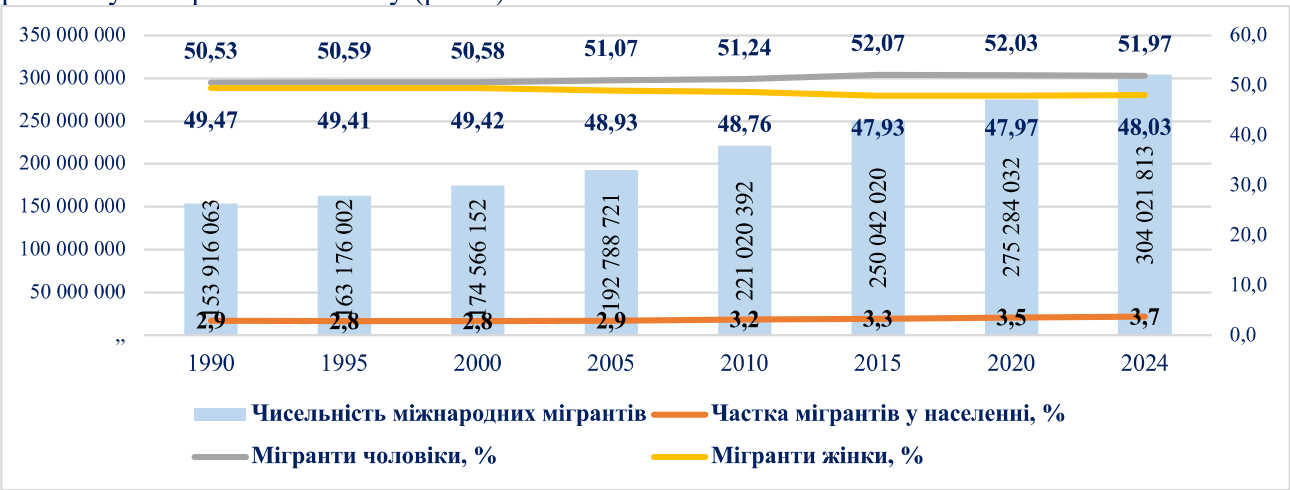

Рис.1. Чисельність міжнародних мігрантів, 1990-2024 рр.

Переважна частина міжнародних мігрантів обирає країни з високим рівнем доходу як основні напрями переміщення, зокрема Сполучені Штати Америки, Канаду та держави Європи, що зумовлено вищим рівнем економічної та соціальної стабільності. Водночас значну роль у сучасних міграційних потоках відіграють країни Перської затоки — основні експортери нафти, які активно залучають мігрантів, насамперед з країн Азії, у межах програм тимчасової трудової міграції.

Особливе значення у структурі сучасних міграційних процесів має трудова міграція, яка є домінуючою формою міжнародної мобільності населення. Економічні мотиви залишаються ключовими рушіями трудової міграції, оскільки мігранти орієнтуються на країни з вищим рівнем оплати праці, кращими умовами зайнятості та ширшими можливостями професійного розвитку. За даними OECD, у країнах-членах організації частка іноземних