DOI: https://doi.org/10.32782/ecovis/2026-2-17
УДК 330.341.1:004.056:338.24

Фісуненко Надія Олександрівна
кандидат економічних наук,
в.о. завідувача кафедри девелопменту нерухомості,
фінансів, обліку та маркетингу,
Український державний університет науки і технологій
ORCID: https://orcid.org/0000-0003-3985-7813

МІЖНАРОДНІ АНТИКРИЗОВІ СИСТЕМИ ЗАХИСТУ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ: ПОРІВНЯЛЬНИЙ АНАЛІЗ

У статті досліджено міжнародні антикризові системи захисту економіки в умовах цифровізації та здійснено їх порівняльний аналіз. Метою статті є виявлення спільних і відмінних рис інституційних, регуляторних та організаційних механізмів, за допомогою яких міжнародні актори забезпечують економічну стійкість до цифрових ризиків. Автором узагальнено підходи OECD, IMF, CPMI-IOSCO, ENISA та World Economic Forum, виокремлено ключові моделі антикризового реагування та обґрунтовано їх значення для формування сучасної політики захисту національної економіки в умовах цифрової трансформації. Наукова новизна полягає у систематизації міжнародних антикризових систем за критеріями об'єкта захисту, інструментів реагування, механізмів координації та параметрів цифрової стійкості. Практичне значення результатів пов'язане з можливістю їх використання для адаптації кращих міжнародних практик до українських умов.

Ключові слова: міжнародні антикризові системи, цифрова трансформація економіки, захист національної економіки, цифрова стійкість, стратегія, ризики, порівняльний аналіз.

Nadiia Fisunenko
Candidate of Economic Sciences,
Head of the Department of Real Estate Development, Finance,
Accounting, and Marketing,
Ukrainian State University of Science and Technology

INTERNATIONAL ANTI-CRISIS SYSTEMS FOR PROTECTING THE NATIONAL ECONOMY IN THE CONDITIONS OF DIGITAL TRANSFORMATION: A COMPARATIVE ANALYSIS

The article examines international anti-crisis systems for protecting the economy under digitalisation and proposes a comparative framework for their assessment. The study aims to identify common and distinctive features of institutional, regulatory and organisational mechanisms used to strengthen economic resilience against cyber incidents, digital infrastructure failures, supply-chain disruptions and technology-driven shocks. The analysis covers approaches developed by the OECD, the International Monetary Fund, the BIS CPMI-IOSCO framework, ENISA and the World Economic Forum. It shows that contemporary anti-crisis systems increasingly combine preventive governance, continuous monitoring, scenario-based stress testing, cross-border information sharing, incident reporting, recovery planning and resilience-oriented regulation rather than relying only on post-crisis response. Digitalisation changes the architecture of economic protection by deepening interdependence between financial systems, digital platforms, data flows, critical infrastructure and transnational service providers. Therefore, anti-crisis systems should be assessed not only by their response capacity, but also by their ability to anticipate vulnerabilities, ensure continuity of critical services and coordinate recovery across sectors and jurisdictions. The scientific contribution lies in a comparative classification of international anti-crisis systems by the object of protection, dominant digital risk, policy instruments, recovery logic and level of institutional coordination. Three analytical models are distinguished: a governance-based model of digital risk management, a financially focused model of cyber resilience for market infrastructures, and an ecosystem model addressing supply chains, cross-sector dependencies and strategic adaptability. The practical value of the findings lies in their applicability to national economic protection strategies, policy coordination, crisis-management frameworks, digital resilience indicators and the adaptation of international practices to Ukraine's recovery and long-term structural transformation.

Keywords: international anti-crisis systems, digital transformation of the economy, protection of the national economy, digital resilience, strategy, risks, comparative analysis.

Постановка проблеми. Поглиблення процесів цифровізації суттєво трансформувало змінило не лише умови сучасного економічного розвитку, а й структуру та механізми виникнення кризових ризиків.

Поширення цифрових платформи, хмарних технологій і фінансово-технологічних рішень, активація транскордонного обміну даними та використання програмних продуктів зовнішніх постачальників посилили взаємозалежність економічних систем. За таких умов навіть окреме порушення роботи цифрової інфраструктури чи кібератака здатні поширитися на пов'язані сфери та спричинити масштабні економічні наслідки.

У цих умовах захист національної економіки в умовах цифрової трансформації вже не зводиться до дотримання фінансової стабільності. Його важливими складовими стають стійкість цифрової інфораскструктури, узгодженість стратегічних дій регуляторних органів, готовність до оперативного реагування та відновлення, а також налагоджений міжнародний обмін інформацією про цифрові загрози.

Актуальність теми зумовлена тим, що міжнародні антикризові системи, сформовані під впливом цифровізації, уже перестали бути допоміжним елементом політики безпеки. Вони перетворилися на невід'ємну складову економічного управління, оскільки саме через них забезпечуються безперервність критичних сервісів, зниження системних ризиків, координація дій між державними та приватними інституціями, а також відновлення після цифрових інцидентів.

Для України ця проблематика має особливе значення з огляду на поєднання завдань цифрової модернізації, воєнних викликів та потреби у формуванні довгострокової стратегії захисту національної економіки.

Аналіз останніх досліджень і публікацій. Проблематика цифрових ризиків і стійкості економічних систем активно розробляється як міжнародними організаціями, так і науковцями. У звіті «Організації економічного співробітництва та розвитку» [7, с. 10–16; 9, с. 6–7] визначено, що цифрова безпека розглядається в економічному та соціальному вимірі, а цифрові ризики пропонується інтегрувати у процеси прийняття рішень на всіх рівнях управління.

В своїх дослідження науковці R. Barbosa, B. Chen, O. Khadarina, T. Okuda, R. Rangachary, E. Shao, F. Suntheim, T. Tsuruga [3, с. 80–82] розглядають «кіберризики» вже як чинник макрофінансової нестабільності, наголошуючи, що тяжкі цифрові інциденти здатні викликати втрату довіри, порушення надання критичних послуг та масштабні ефекти поширення через фінансові й технологічні зв'язки.

Відповідно до розробленого міжнародного методичного документу підготовленого Комітетом з платежів та ринкової інфраструктури Банку міжнародних розрахунків та Радою Міжнародної організації комісій з цінних паперів [1, с. 1–3; 2, с. 7–8], акцент зроблено на кіберстійкості фінансової ринкової інфраструктури, включно з управлінням, тестуванням, раннім виявленням, інформаційним обміном, реагуванням і відновленням.

Європейський напрям представлений, зокрема, напрацюваннями ENISA [5, с. 3–4, 25], де аналізуються ризики цифрових ланцюгів постачання та підкреслюється, що сучасні атаки все частіше націлені не на кінцеву організацію, а на постачальника, що збільшує масштаби потенційного економічного впливу.

World Economic Forum [11, с. 3–4] у своєму глобальному огляді кібербезпеки фіксує посилення кібернерівності, що розвиваються та має прямі наслідки для нерівномірності антикризової спроможності.

Наукові дослідження A. Craig, S. Shackelford і J. Hiller [4, с. 721–724] обґрунтовують значення проактивного регуляторного підходу до кібербезпеки, який має поєднувати приватні інструменти управління ризиком і державну координацію.

D. Fowler та співавтори [6, с. 183–187] розглядають стійкість цифрово насичених виробничих систем як багаторівневе явище, що охоплює як виробничу ефективність, так і ширші суспільні наслідки.

R. Osman і S. El-Gendy [10, с. 846–852], використовуючи модель CGE, показують, що штучно індуковані кібератаки можуть спричиняти істотні втрати ВВП, порушення торгівлі та ланцюгів постачання.

Разом із тим у наявних дослідженнях бракує цілісного порівняльного аналізу міжнародних антикризових систем саме як систем захисту економіки в умовах цифровізації. Частина джерел концентрується на кібербезпеці як такій, частина – на фінансовій інфраструктурі, частина – на цифровій трансформації бізнесу чи держави. Натомість недостатньо розкритими залишаються питання зіставлення різних міжнародних моделей за їхнім об'єктом захисту, інструментами реагування, логікою координації та практичним значенням для формування національної антикризової політики.

Мета статті. Метою статті є здійснення порівняльного аналізу міжнародних антикризових систем захисту національної економіки в умовах цифрової трансформації, виявлення їхніх спільних і відмінних рис, а також обґрунтування можливостей використання відповідного міжнародного досвіду у формуванні сучасної стратегії захисту національної економіки.

Виклад основного матеріалу дослідження. У сучасних умовах антикризова система захисту економіки не може розглядатися лише як сукупність реактивних заходів, спрямованих на подолання наслідків уже реалізованої кризи. Цифровізація змінює цю логіку: антикризові системи дедалі більшою

мірою ґрунтуються на попередженні, безперервному моніторингу, ранньому виявленні загроз, інформаційному обміні, сценарному тестуванні та швидкому відновленні критичних сервісів. Саме тому міжнародні моделі доцільно порівнювати не лише за набором інституцій, а й за їх здатністю забезпечувати економічну безперервність, керованість системних ризиків та адаптивність у цифровому середовищі.

На основі аналізу верифікованих міжнародних джерел доцільно виокремити щонайменше п'ять основних міжнародних підходів. Перший з них представлено у звіті «Організації економічного співробітництва та розвитку» (OECD). Його особливість полягає в тому, що цифрова безпека трактується не як вузько технічне питання, а як складова економічного процвітання і суспільної довіри. У рекомендаціях OECD наголошується на включенні цифрового ризику до процесів прийняття управлінських рішень, розробці планів підготовленості й безперервності, а також на необхідності створення національних стратегій, які стимулюють кооперацію між усіма зацікавленими сторонами [7, с. 12–16].

Отже, модель OECD можна охарактеризувати як систему управління цифровим ризиком на основі економічної доцільності, партнерства та міжсекторальної координації.

Другий підхід репрезентований A. N. Craig, S. J. Shackelford, J. S. Hiller, де цифрові ризики розглядаються крізь призму макрофінансової стабільності. Згідно з дослідженнями науковців, тяжкий кіберінцидент може поширюватися через втрату довіри, зупинку критичних послуг, технологічну взаємозалежність і спільних постачальників послуг, що створює загрозу вже не окремим компаніям, а фінансовій системі загалом [4, с. 4–5].

У зв'язку з цим необхідно підкреслити потребу в національних стратегіях кібербезпеки для фінансового сектору, посиленні нагляду, обов'язковому звітуванні про інциденти, розвитку кризових протоколів та відпрацюванні сценаріїв безперервності діяльності [3, с. 17–18].

Цю модель можна визначити як макрофінансову антикризову систему цифрової стійкості, в центрі якої перебувають запобігання системним шокам і захист довіри до фінансового ринку.

Третій напрям розроблений відповідно до міжнародного методичного документу підготовленого Комітетом з платежів та ринкової інфраструктури Банку міжнародних розрахунків та Радою Міжнародної організації комісій з цінних паперів демонструє, зосередженість на фінансовій ринковій інфраструктурі. До основних складових цієї системи належить організація управління, визначення ризиків, упровадження захисних заходів, своєчасне виявлення порушень, реагування на них і відновлення після інцендентів. Окреме значення мають регулярне тестування, постійний контроль ситуації та накопичення практичного досвіду [1, с. 1–3].

Важливим орієнтиром є відновлення критично важливих операцій не пізніше ніж дві години. Такий підхід свідчить, що система захисту національної економіки в умовах цифрової трансформації має забезпечити не лише протидію загрозам, а й безперервність роботи ключових фінансових і ринкових інститутів навіть за надзвичайно складних обставин.

Подальший моніторинг упровадження цих підходів показав, що високий рівень формального прийняття стандартів не гарантує фактичної готовності, якщо відсутні реалістичні плани відновлення, комплексне тестування та координація з учасниками екосистеми [2, с. 7–8].

Таким чином, модель CPMI-IOSCO є високоспеціалізованою міжнародною антикризовою системою для системно важливої фінансової інфраструктури.

Четвертий напрям представлений підходами ENISA та загальноєвропейською політикою в сфері кіберстійкості. матеріали агентства свідчать, що значна частина сучасних цифрових криз виникає не в межах окремої організації, а через ланцюги постачання [5, с. 3–4; 25].

Це зумовлює перехід від моделі «захисту окремої організації» до змішаної моделі мережевої стійкості, де критичним стає стратегічне управління взаємозалежностями. Для захисту національної економіки в умовах цифрової трансформації особливого значення набувають оцінювання надійності постачальників, безпека коду, аналіз критичних залежностей, контроль третіх сторін та вироблення механізмів спільного реагування.

Відповідно, європейський підхід можна розглядати як антикризову систему екосистемного типу, орієнтовану на складні цифрові ланцюги та транскордонні ризики.

П'ятий аналітичний напрям репрезентує World Economic Forum, який не є регулятором у вузькому розумінні, однак формує впливову міжнародну платформу стратегічного бачення.

У Global Cybersecurity Outlook 2025 зафіксовано, що 35% малих організацій вважають власну кіберстійкість недостатньою, тоді як між регіонами світу існують істотні відмінності у впевненості щодо спроможності відповідати на великі кіберінциденти [11, с. 3–4].

Це важливо для порівняльного аналізу, оскільки демонструє: навіть найкращі формальні системи не є універсально ефективними без належного людського капіталу, фінансування, гармонізації регулювання та зменшення цифрової нерівності.

Отже, підхід WEF доповнює інші моделі стратегічним баченням асиметрії антикризової готовності в умовах глобальної цифрової взаємозалежності.

Порівняльний аналіз дозволяє систематизувати міжнародні антикризові системи за кількома критеріями: об'єкт захисту, домінуючий тип ризику, основні інструменти, характер координації та логіка відновлення.

Для систематизації результатів дослідження узагальнимо ключові характеристики цих моделей у табл. 1.

Порівняльна оцінка свідчить, що між міжнародними антикризовими системами існують не лише відмінності, а й суттєві точки перетину. По-перше, всі вони визнають неможливість повного усунення цифрового ризику і, відповідно, роблять акцент на стійкості, безперервності та відновленні. По-друге, всі системи так чи інакше спираються на координацію між державою, регуляторами, бізнесом і провайдерами критичних сервісів. По-третє, для більшості моделей ключовими стають інструменти раннього виявлення, сценарного тестування, інформаційного обміну та планування безперервності [1, с. 2–3; 2, с. 7–8; 3, с. 17–18].

Разом із тим відмінності між моделями є принциповими. OECD концентрується на управлінні ризиком як частині економічної політики і наголошує на формуванні умов для взаємодії всіх стейкголдерів [7, с. 12–16].

IMF виходить з того, що цифровий інцидент може стати макрофінансовою подією, а тому потребує спеціальної регуляторної й кризової інфраструктури для фінансового сектору [3, с. 4–5; 17–18].

CPMI-IOSCO будують систему навколо системно важливих інфраструктур і задають чіткі орієнтири швидкості відновлення, тестування та відповідальності [1, с. 1–3; 2, с. 7–8].

ENISA переносить акцент на ланцюги постачання, демонструючи, що економічні кризи нового типу можуть починатися з вразливостей коду, програмних оновлень чи зовнішніх сервісів [5, с. 3–4; 25].

WEF, своєю чергою, висвітлює глобальний розрив у спроможностях реагування, що дозволяє розглядати цифрову нерівність як окремий чинник кризової вразливості [11, с. 3–4].

З огляду на це доцільно виділити три узагальнені моделі міжнародних антикризових систем захисту економіки в умовах цифровізації.

Перша – модель управління цифровим ризиком, що базується на поєднанні стратегічного регулювання, міжсекторальної кооперації, формування культури цифрової безпеки та інтеграції ризику в процеси прийняття рішень. Вона найповніше представлена в документах OECD і є фундаментальною для економік, які потребують системного, а не вузько галузевого реагування [7, с. 10–16].

Друга – модель кіберстійкості критичної фінансової інфраструктури, орієнтована на підтримку довіри, безперервності платежів, розрахунків і клірингу, а також на недопущення каскадного поширення шоків. Її найпослідовніше реалізують IMF та CPMI-IOSCO [1, с. 1–3; 3, с. 17–18]. Саме ця модель є найбільш жорсткою з позиції формалізації процедур відновлення та контролю.

Третя – екосистемна модель цифрової стійкості, у центрі якої перебувають складні зв'язки між організаціями, постачальниками, платформами, сервісами та цифровими ланцюгами створення вартості. Вона найбільш виразно проявляється в підходах ENISA, а також підтверджується сучасними дослідженнями щодо виробничої та торговельної стійкості в умовах цифрових атак [5, с. 25; 6, с. 183–187; 10, с. 846–852].

У межах цієї моделі захист економіки вже не може бути забезпечений лише на рівні окремого під-

Таблиця 1

Порівняльна характеристика міжнародних антикризових систем захисту економіки в умовах цифровізації

Система / інституція	Об'єкт захисту	Ключові інструменти	Антикризова логіка	Обмеження
OECD	Економіка, суспільна довіра, цифрове середовище	національні стратегії, управління ризиком, партнерства, безперервність	інтеграція цифрового ризику у процеси економічного управління	загальний рамковий характер, потреба у національній деталізації
IMF	Фінансовий сектор і макрофінансова стабільність	нагляд, звітування про інциденти, кризові протоколи, стрес-сценарії	запобігання системним фінансовим наслідкам цифрових інцидентів	фокус переважно на фінансовій сфері
CPMI-IOSCO	Фінансова ринкова інфраструктура	2hRTO, тестування, відновлення, ситуаційна обізнаність, координація	підтримка безперервності системно важливих платежів і розрахунків	висока спеціалізація і вузький секторний масштаб
ENISA / європейський контур	Ланцюги постачання, код, треті сторони, мережеві екосистеми	аналіз загроз, рекомендації для постачальників, безпека коду, перевірка контрагентів	зниження каскадних наслідків цифрових атак у взаємозалежних мережах	сильна залежність від рівня зрілості національних політик
WEF	Глобальна кіберстійкість організацій і країн	стратегічні оцінки, індикатори нерівності, ризикові опитування	виявлення асиметрій готовності та глобальних тенденцій	аналітичний, а не регуляторний характер

Джерело: сформовано автором на основі [1; 2; 3; 5; 7-9; 11]

приємства або навіть окремого сектора; він потребує координації по всьому ланцюгу взаємозалежностей.

Практичне значення порівняльного аналізу полягає в тому, що він дозволяє перейти від абстрактного розуміння цифрової безпеки до конкретних параметрів формування політики захисту економіки. По суті, міжнародний досвід свідчить, що ефективна антикризова система в умовах цифровізації має поєднувати щонайменше такі елементи

1) національну стратегію цифрової стійкості;

2) секторальні кризові протоколи, насамперед для фінансової інфраструктури; ;

3) обов'язкові механізми звітування про інциденти;

4) сценарне тестування і перевірку планів відновлення;

5) інструменти оцінювання цифрових ризиків і невизначеності;

6) розвинену систему міжвідомчої та міжнародної координації;

7) механізми управління ризиками третіх сторін і ланцюгів постачання.

Для України цей підхід має особливе значення, що підтверджується дослідженнями OECD щодо цифрової трансформації бізнесу в умовах війни.

У звіті OECD за 2024 рік зазначено, що цифрові інструменти не лише підвищують продуктивність, а й допомагають національній економіці підвищувати стійкість і відновлюваність у кризових умовах [8, с. 3–4; 30].

Водночас наголошується, що можливість цифровізації в Україні використовується ще не повністю. Тому підтримка цифрової трансформації національної економіки має поєднуватись з належною координацією державної політики, тобто формування якісної стратегії захисту, розвитком цифрових компетентностей.

У цьому контексті результати порівняльного аналізу дозволяють сформулювати низку орієнтирів для національної політики. По-перше, стратегія захисту національної економіки має включати цифровий компонент не як окремий технічний додаток, а як центральний елемент антикризового управління. По-друге, необхідно розвивати систему оцінювання цифрової стійкості, спираючись на міжнародні підходи до вимірювання невизначеності, інцидентності та готовності до відновлення [9, с. 32–33].

По-третє, фінансова система, енергетика, державні цифрові сервіси та логістичні ланцюги повинні розглядатися як пріоритетні сфери для сценарного моделювання й кризового планування. По-четверте, важливим є поєднання державного регулювання з приватною відповідальністю, що відповідає логіці проактивної кіберполітики, описаної у працях A. Craig, S. Shackelford і J. Hiller [4, с. 721–724].

Отже, міжнародні антикризові системи захисту економіки в умовах цифровізації демонструють перехід від вузького реагування на інцидент до багаторівневої моделі стійкості, яка охоплює управління ризиком, регуляторні інструменти, інституційне навчання, підтримку критичної інфраструктури, контроль ланцюгів постачання та координацію відновлення. Саме така логіка має стати методологічною основою для формування сучасної стратегії захисту національної економіки.

Висновки. У статті здійснено порівняльний аналіз міжнародних антикризових систем захисту економіки в умовах цифровізації. Встановлено, що цифровізація змінює природу кризових процесів, посилюючи залежність економіки від даних, платформ, постачальників цифрових сервісів, фінансової ринкової інфраструктури та транскордонних мережевих взаємозв'язків. У результаті антикризові системи дедалі менше орієнтуються лише на ліквідацію наслідків і дедалі більше – на випереджальне управління ризиком, підтримку безперервності критичних функцій і прискорене відновлення.

Доведено, що міжнародний досвід дозволяє виокремити три узагальнені моделі антикризового захисту економіки: модель управління цифровим ризиком, модель кіберстійкості критичної фінансової інфраструктури та екосистемну модель цифрової стійкості. Перша акцентує інтеграцію цифрової безпеки в економічне управління, друга зосереджена на запобіганні системним макрофінансовим ефектам, третя – на захисті складних мережевих взаємозалежностей і ланцюгів постачання.

Обґрунтовано, що для формування ефективної стратегії захисту національної економіки доцільно поєднати в національній політиці кращі елементи всіх трьох моделей: стратегічне управління цифровим ризиком, обов'язкове кризове планування та тестування критичної інфраструктури, системне управління ризиками третіх сторін, розбудову механізмів міжвідомчої й міжнародної координації, а також розвиток індикаторів цифрової стійкості. Практичне значення отриманих результатів полягає у можливості їх використання для вдосконалення антикризової політики держави, розробки механізмів захисту критичних економічних секторів і адаптації міжнародних практик до потреб України в умовах цифрової трансформації.

СПИСОК ЛІТЕРАТУРИ

1. Bank for International Settlements and International Organization of Securities Commissions 2022. All rights reserved. Brief excerpts may be reproduced or translated provided the source is stated. CPMI-IOSCO. Level 3 assessment on *Financial Market Infrastructures' Cyber Resilience*. 2022. 50 p. URL: https://www.bis.org/cpmi/publ/d212.pdf (дата звернення: 19.07.2026).
2. Bank for International Settlements Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions. *Guidance on cyber resilience for financial market infrastructures*. Basel : BIS, 2016. 32 p. URL: https://www.bis.org/cpmi/publ/d146.pdf (дата звернення: 21.07.2026).

3. Barbosa R., Chen B., Khadarina O., Okuda T., Rangachary R., Shao E., Suntheim F., Tsuruga T. Cyber Risk: A Growing Concern for Macrofinancial Stability. Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks. Washington, DC : International Monetary Fund, 2024. Chapter 3. P. 77–102. URL: https://www.imf.org/-/media/files/publications/gfsr/2024/april/english/ch3.pdf (дата звернення: 01.07.2026).
4. Craig A. N., Shackelford S. J., Hiller J. S. Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis. *American Business Law Journal*. 2015. Vol. 52, Iss. 4. P. 721–787. DOI: https://doi.org/10.1111/ablj.12055.
5. European Union Agency for Cybersecurity. Threat Landscape for Supply Chain Attacks. Athens : ENISA, 2021. 57 p. URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Supply%20Chain%20Attacks.pdf (дата звернення: 11.07.2026).
6. Fowler D. S., Epiphaniou G., Higgins M. D., Maple C. Aspects of resilience for smart manufacturing systems. *Strategic Change*. 2023. Vol. 32, Iss. 6. P. 183–193. DOI: https://doi.org/10.1002/jsc.2555.
7. OECD. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. Paris : OECD Publishing, 2015. 72 p. DOI: https://doi.org/10.1787/9789264245471-en.
8. OECD. Enhancing Resilience by Boosting Digital Business Transformation in Ukraine. Paris : OECD Publishing, 2024. 111 p. DOI: https://doi.org/10.1787/4b13b0bb-en.
9. OECD. New Perspectives on Measuring Cybersecurity. OECD Digital Economy Papers. 2024. No. 366. Paris : OECD Publishing. 59 p. DOI: https://doi.org/10.1787/b1e31997-en.
10. Osman R., El-Gendy S. Interconnected and resilient: A CGE analysis of AI-driven cyberattacks in global trade. *Risk Analysis*. 2025. Vol. 45. P. 846–862. DOI: https://doi.org/10.1111/risa.14321.
11. World Economic Forum. Global Cybersecurity Outlook 2025. Geneva : *World Economic Forum*. 2025. 49 p. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (дата звернення: 21.06.2026).

REFERENCES

1. Bank for International Settlements and International Organization of Securities Commissions (2022) Level 3 assessment on Financial Market Infrastructures' Cyber Resilience. Basel: Bank for International Settlements, 50 p. Available at: https://www.bis.org/cpmi/publ/d212.pdf (accessed July 19, 2026).
2. Bank for International Settlements Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions (2016) Guidance on cyber resilience for financial market infrastructures. Basel: Bank for International Settlements, 32 p. Available at: https://www.bis.org/cpmi/publ/d146.pdf (accessed July 21, 2026).
3. Barbosa R., Chen B., Khadarina O., Okuda T., Rangachary R., Shao E., Suntheim F., Tsuruga T. (2024) Cyber Risk: A Growing Concern for Macrofinancial Stability. In: Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks. Washington, DC: International Monetary Fund, Chapter 3, pp. 77–102. Available at: https://www.imf.org/-/media/files/publications/gfsr/2024/april/english/ch3.pdf (accessed July 1, 2026).
4. Craig A. N., Shackelford S. J., Hiller J. S. (2015) Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis. *American Business Law Journal*, vol. 52, no. 4, pp. 721–787. DOI: https://doi.org/10.1111/ablj.12055.
5. European Union Agency for Cybersecurity (2021) Threat Landscape for Supply Chain Attacks. Athens: European Union Agency for Cybersecurity, 57 p. Available at: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Supply%20Chain%20Attacks.pdf (accessed July 11, 2026).
6. Fowler D. S., Epiphaniou G., Higgins M. D., Maple C. (2023) Aspects of resilience for smart manufacturing systems. *Strategic Change*, vol. 32, no. 6, pp. 183–193. DOI: https://doi.org/10.1002/jsc.2555.
7. OECD (2015) Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. Paris: OECD, 72 p. DOI: https://doi.org/10.1787/9789264245471-en.
8. OECD (2024) Enhancing Resilience by Boosting Digital Business Transformation in Ukraine. Paris: OECD, 111 p. DOI: https://doi.org/10.1787/4b13b0bb-en.
9. OECD (2024) New Perspectives on Measuring Cybersecurity. OECD Digital *Economy Papers*, no. 366. Paris: OECD, 59 p. DOI: https://doi.org/10.1787/b1e31997-en.
10. Osman R., El-Gendy S. (2025) Interconnected and resilient: A CGE analysis of AI-driven cyberattacks in global trade. *Risk Analysis*, vol. 45, pp. 846–862. DOI: https://doi.org/10.1111/risa.14321.
11. World Economic Forum (2025) Global Cybersecurity Outlook 2025. Geneva: *World Economic Forum*, 49 p. Available at: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (accessed June 21, 2026).

Дата надходження статті: 13.07.2026
Дата прийняття статті до публікації: 14.08.2026
Дата публікації статті: 28.08.2026