DOI: https://doi.org/10.30970/fp.3(61).2026.289299300

УДК 338.24:004.9

ВПЛИВ ЦИФРОВІЗАЦІЇ НА ТРАНСФОРМАЦІЮ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

ОПЛАЧКО Ірина Олександрівна
кандидатка економічних наук, доцентка,
доцентка кафедри маркетингу
Національного університету водного господарства та природокористування
ORCID ID: https://orcid.org/0000-0003-0591-121X

ХОМИЧ Валентина Михайлівна
асистентка кафедри маркетингу
Національного університету водного господарства та природокористування
ORCID ID: https://orcid.org/0009-0005-2745-3370

Анотація. *У статті досліджено вплив цифровізації на трансформацію системи економічної безпеки держави. Оцінено ризики та переваги цифровізації на мікро-, мезо- і макрорівнях. Обґрунтовано чотириблокову систему індикаторів оцінки цифрової трансформації. Доведено зростання ролі кіберстійкості й цифровізації в умовах воєнного стану та запропоновано прикладні рекомендації для впровадження на рівні державного управління.*

Ключові слова: *економічна безпека держави, цифровізація, цифрова трансформація, індикатори безпеки, індикатори цифрової трансформації, цифрова стійкість*.

Постановка проблеми. В умовах стрімкої цифровізації економічних процесів виникає необхідність в адаптації систем державного управління до нових безпекових викликів. Масове впровадження технологій штучного інтелекту, хмарних обчислень, наскрізної автоматизації, аналітики великих даних тощо вплинуло на те, що важливими чинниками стійкості економічної системи держави стають швидкість обробки даних та резильєнтність цифрової інфраструктури. При цьому спостерігається певний розрив між високими темпами цифрової трансформації та вразливістю національних економічних систем, і застарілістю інституційних, нормативно-правових й інструментальних механізмів забезпечення економічної безпеки. Системними викликами забезпечення економічної безпеки держави також є залежність діяльності багатьох організацій у важливих секторах національної економіки від іноземних програмних продуктів, апаратного забезпечення та хмарних сервісів, що створює ризики блокування або «саботажу» економічної діяльності ззовні; все частіше виникають гібридні кіберзагрози (в тому числі кібератаки на систему електронних платежів, реєстри власності чи логістичні хаби тощо); розвиток «децентралізованих фінансів», віртуальних активів і алгоритмічних торгових платформ ускладнює державний контроль за рухом капіталу, створює нові канали для ухилення від оподаткування та виведення фінансових ресурсів. В умовах геополітичної турбулентності та воєнного стану цифрова інфраструктура стає однією з головних цілей для пошкодження та знищення. Втрата доступу до державних

CC BY

реєстрів, збої у функціонуванні систем банківського розрахунку або компрометація критичних даних здатні завдати значної шкоди реальному сектору економіки за короткий проміжок часу.

Таким чином, виникає потреба у переоцінці архітектури економічної безпеки держави: відхід від концепції «статичного захисту та реагування на наслідки» до концепції «цифрової адаптивності, резильєнтності та проактивного управління ризиками», що, в свою чергу, потребує розробки нових концептуальних підходів, індикаторів оцінки та конкретних практичних механізмів мінімізації цифрових ризиків.

Аналіз останніх досліджень і публікацій. Дослідженню окремих аспектів забезпечення економічної безпеки держави та оцінюванню впливу цифрових трансформацій присвячено значну кількість наукових праць. Так, критичну оцінку існуючому механізму розрахунку рівня економічної безпеки та обґрунтування необхідності його адаптації до викликів воєнного стану й цифровізації дала К. В. Єфремова [1]. Вплив цифровізації бізнесу на формування індикаторів національної безпеки проаналізовано у працях Д. Бедера та Ю. Цаль-Цалко [4]. Оцінку регіональних аспектів цифровізації, ризиків кіберзлочинності й витоку даних для безпеки суб'єктів господарювання висвітлено у дослідженнях А. В. Фаїзова, С. І. Мацюри та М. О. Мікуліної [5]. Специфіку трансформації економічних відносин під впливом новітніх технологій (штучного інтелекту, електронної комерції та блокчейну) досліджено у роботі А. Зіміної та О. Кавуна [6].

Вагомий внесок у обґрунтування концепції трансформації системи економічної безпеки країни під впливом цифровізації та розробку відповідних індикаторів зробили І. Гнатенко та Д. Хорошко [7]. Міжнародно-правовий вимір регулювання кібербезпеки критичної інфраструктури зафіксовано у Директиві Європейського Парламенту та Ради (ЄС) 2022/2555 (NIS2) [8], а європейські засади цифрової стійкості й відновлюваності систем узагальнено у аналітичних матеріалах [9]. На національному рівні функціональні складові економічної безпеки зафіксовано у Стратегії економічної безпеки України до 2025 року [2], а орієнтири розвитку цифрової інфраструктури та електронних послуг визначено у Національній економічній стратегії на період до 2030 року [3].

Кількісну оцінку вагових коефіцієнтів цифровізації в системі фінансово-економічної безпеки держави в умовах воєнного стану представлено у дослідженнях І. Школьник, С. Фролова, В. Орлова, В. Даценка та Є. Козьменка [10].

Попри вагомі наукові здобутки, системне поєднання зазначених напрямів у чотириблокову систему індикаторів оцінки цифрової трансформації економічної безпеки держави та розробка прикладних рекомендацій для органів державного управління в умовах воєнного стану потребують подальшого поглибленого опрацювання.

Метою статті є дослідження індикаторів впливу цифровізації на трансформацію системи економічної безпеки держави.

Виклад основних результатів дослідження. У традиційній науковій парадигмі та нормативній базі економічна безпека держави розглядається як багатофакторна система, що охоплює п'ять базових функціональних складових, зокрема, макроекономічну безпеку, фінансову безпеку, інвестиційно-інноваційну безпеку та виробничу безпеку, зовнішньоекономічну безпеку [2]. Під впливом сучасних процесів цифровізації виникає потреба перегляду цієї класичної структури, оскільки цифрові технології трансформують кожен із наведених елементів – від фінансового сектору до виробничої та макроекономічної безпеки. Оновлення підходів пов'язане й із

CC BY

глобальними процесами. Стрімкий розвиток цифрової економіки створює як виклики, так і нові можливості для України [3]. Стійкість економіки сьогодні залежить від створення зручних цифрових умов для бізнесу, залучення інвестицій та розвитку сучасних цифрових послуг.

Безпека держави складається зі стійкості кожного окремого підприємства та кожного регіону. Коли підприємства впроваджують цифрові технології в управлінні, це позитивно впливає на загальний стан безпеки держави [4]. Однак рівень цифровізації в різних областях України є неоднаковим. Найвищі індекси цифрової трансформації мають регіони з розвиненою інфраструктурою, тоді як низькі показники вказують на необхідність підтримки інновацій у менш розвинених областях [5]. Такий нерівномірний розвиток створює ризики: області з низьким рівнем цифровізації є більш вразливими до кризових процесів. Крім цього, цифровізація створює нові загрози. Практичні дослідження показують, що кіберзлочинність та порушення конфіденційності мають найбільший вплив на бізнес, призводячи до фінансових втрат і зупинки підприємств [5]. Стрімке поширення штучного інтелекту, електронної торгівлі та блокчейну з одного боку прискорює робочі процеси [6], а з іншого – породжує шахрайство з розрахунками та електронне шпигунство.

Для системного розуміння впливу цифровізації доцільно виокремити ключові переваги та ризики на мікро-, мезо- та макрорівнях (табл. 1).

Таблиця 1

Аналіз впливу цифровізації за рівнями економічної системи

Рівень економіки	Ключові позитивні ефекти	Основні ризики та загрози
Мікрорівень	Оптимізація операційних та трансакційних витрат, автоматизація бізнес-процесів через впровадження ERP/CRM-систем, розширення ринків збуту за рахунок електронної комерції, підвищення продуктивності праці та гнучкості операцій.	Ризики витоку комерційної таємниці та персональних даних, прямі збитки від не надійного програмного забезпечення та фішингу, критична залежність від стабільності електропостачання та безперебійності каналів зв'язку. Головний ризик – підприємства стають мішенню для хакерів, можуть втратити фінансові резурси через збої в програмах або витік комерційної таємниці.
Мезорівень	Розвиток регіональних IT-кластерів, цифровізація місцевих публічних послуг, підвищення прозорості регіональних закупівель і використання бюджетних коштів, прискорення соціально-економічного розвитку громад.	Ризик поглиблення «цифровізаційного розриву» між великими містами-мільйонниками та сільськими чи прифронтовими громадами, нерівномірний доступ до швидкісного широкосмугового інтернету, відтік кваліфікованих кадрів із периферійних регіонів.
Макрорівень	Детінізація економічних відносин завдяки поширенню безготівкових розрахунків, підвищення ефективності адміністрування податкових і митних платежів, автоматизація державних функцій та ліквідація корупційних схем (системи «Дія», «Prozorro», e-Customs), зростання частки IT-сектору у ВВП та експорті.	Ризики втрати цифрового суверенітету через технологічну залежність від іноземного обладнання й критичного програмного забезпечення, можливість дестабілізації державних фінансів та критичної інфраструктури внаслідок ворожих кібератак.

Джерело: розроблено авторами

CC BY

Для того, щоб держава могла якісно контролювати стан економічної безпеки, потрібна впорядкована система індикаторів, яка відображає як технічний стан систем, так і їхній вплив на економіку. Дослідження підтверджують, що цифровізація сприяє підвищенню прозорості процесів та зниженню рівня корупції [7].

Важливою для приведення української системи кіберзахисту та стійкості критичної інфраструктури до європейських стандартів у процесі інтеграції до ЄС є імплементація Директиви Європейського Парламенту та Ради (ЄС) 2022/2555 (далі - Директива NIS2) [8]. Директива NIS2 вимагає від країн суворого контролю кібербезпеки не лише в державному секторі, а й у стратегічних галузях економіки: енергетиці, транспорті, банківській справі, охороні здоров'я та цифровій інфраструктурі [8].

Таким чином, цифровізація має бути не просто технологічною, а й забезпечувати здатність швидко відновлювати роботу системи після будь-якого збою чи ворожої атаки [9]. Для України це означає необхідність постійного моніторингу трьох чинників:

1. Рівень захисту ланцюгів постачання.
2. Швидкість відновлення даних у разі виведення з ладу серверів.
3. Рівень цифрової грамотності громадян, оскільки людський фактор залишається головною вразливістю у кібербезпеці.

Для узагальненої оцінки рівня готовності держав до кіберзагроз використовуються інтегральні індекси, зокрема Глобальний індекс кібербезпеки (Global Cybersecurity Index, GCI), Національний індекс кібербезпеки (National Cyber Security Index, NCSI), Індекс цифрової економіки та суспільства (Digital Economy and Society Index, DESI). Глобальний індекс кібербезпеки GCI, що розроблений Міжнародним союзом електрозв'язку (ITU), оцінює рівень кібербезпеки в країнах за п'ятьма ключовими напрямками: правові заходи, технічні заходи, організаційні заходи, розвиток потенціалу та міжнародна співпраця (рис. 1).

У період між 2020 та 2024 роками Україна продемонструвала помірний прогрес у сфері кібербезпекової зрілості (значення Глобального індексу кібербезпеки (GCI) для України зросло на 27 % порівняно з показником 2020 року). Показник у 83,93 бали зі 100 відображає системні зусилля зі зміцнення правових і технічних основ в умовах війни та цифровізації, в тому числі розширення країною технічної інфраструктури для забезпечення кібербезпеки, зокрема наявність національного CERT, впровадження технічних стандартів, механізмів сертифікації та моніторингу інцидентів у режимі реального часу. При цьому у Глобальному індексі кібербезпеки (Global Cybersecurity Index, GCI) 2024 року Україна віднесена до групи країн «Establishing» (третій рівень). Зокрема, в межах організаційної складової Україна демонструє найнижчі результати за показником наявності системи метрик кібербезпеки. Незважаючи на наявність національної стратегії кібербезпеки та визначення відповідальних державних органів, недостатньо формалізовані кількісні та якісні індикатори для оцінки ефективності заходів з кібербезпеки, а також механізми їх регулярного моніторингу.

CC BY

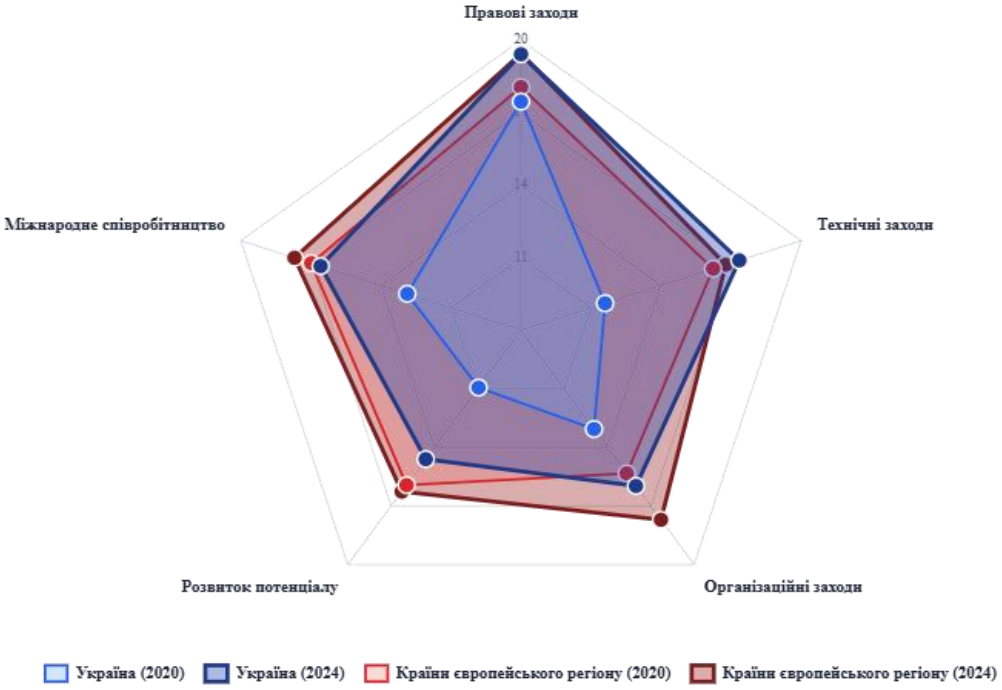


Рис. 1. Глобальний індекс кібербезпеки (GCI) України та країн європейського регіону за складовими у 2024 р.

Схожа тенденція простежується й при зміні значень Національного індексу кібербезпеки (NCSI) для України. Індекс оцінює готовність країн протидіяти кіберзагрозам і ефективно реагувати на інциденти, показує зрілість державних інституцій у сфері кібербезпеки, готовність захищати цифрові системи тощо.

За даними 2025 року, Україна має 88,33% виконання критеріїв NCSI і посідає 17-те місце серед 140 країн. Це свідчить про високий рівень готовності до протидії кіберзагрозам завдяки розвитку національної політики, створенню відповідних органів та стратегій. При цьому динаміка значень Національного індексу кібербезпеки (NCSI) для України демонструє стійке зростання (рис. 2).

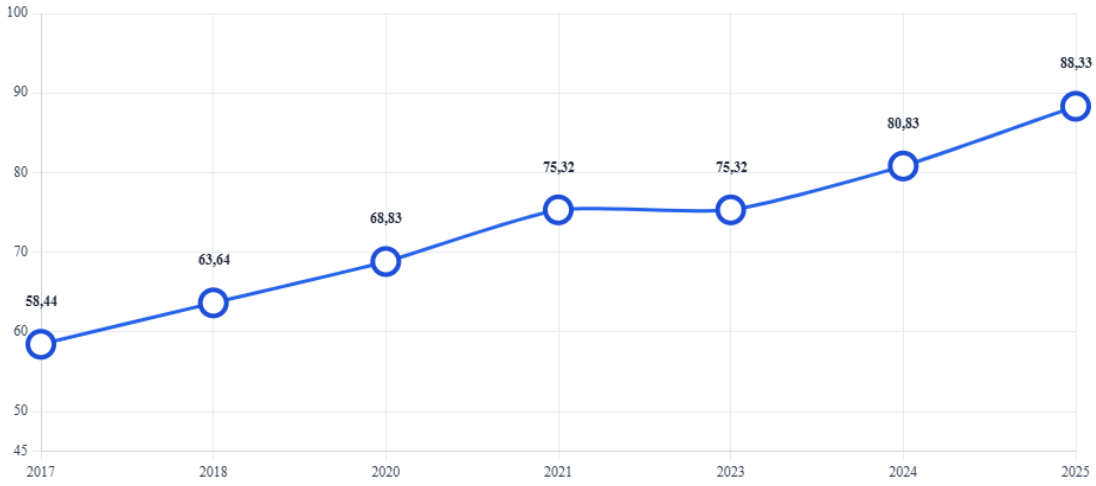


Рис. 2. Динаміка значень Національного індексу кібербезпеки (NCSI) для України (2017-2025 рр.)

CC BY

Стрімка цифровізація перетворила цифрові технології на ключовий драйвер економічного зростання, але водночас зробила економічну безпеку України прямо залежною від рівня її кіберстійкості. Порівняльний аналіз профілю України за індексами GCI та NCSI виявляє виразний дихотомічний розрив між високою системно-силовою підготовкою та прогалинами у процесному й кадровому забезпеченні.

Аналіз міжнародної практики свідчить, що оцінювання цифрової економіки вже давно виходить за межі визначення кількості електронних послуг. Незважаючи на різну методологію розрахунку міжнародних індексів, усі вони оцінюють однакові фундаментальні характеристики цифрової економіки: рівень кіберзахисту, цифрової інфраструктури, людського капіталу та інституційної готовності.

Попри високу аналітичну цінність міжнародних індексів, вони слугують переважно для міждержавного моніторингу і не завжди дають змогу оперативно оцінити поточний стан стійкості національної економіки в умовах динамічних загроз. У зв'язку з цим постає завдання адаптації міжнародного досвіду у вітчизняну систему моніторингу. На основі систематизації та адаптації наукових праць І. Гнатенко та Д. Хорошка [7], ключові напрями вимірювання цифровізації було сформовано у вигляді чіткої системи індикаторів оцінки цифрової трансформації економічної безпеки (табл. 2).

Таблиця 2

Система індикаторів оцінки цифрової трансформації економічної безпеки

Напрям	Індикатор	Сутність та опис індикатора
1. Технологічна захищеність та кібербезпека	Рівень кібербезпеки	Показує, наскільки надійно захищені державні реєстри, банківська система, енергетика та інші важливі об'єкти від кібератак.
	Обсяг інвестицій у цифрову безпеку	Відображає, скільки (яку частку) коштів держава та бізнес витрачають на закупівлю сучасних захисних програм і обладнання.
	Місце країни у світових рейтингах цифрової безпеки	Дає змогу порівняти рівень захищеності України з іншими державами світу.
2. Автоматизація та оперативність державного контролю	Швидкість реагування на загрози	Показує, скільки часу минає від появи проблеми в економіці до ухвалення конкретного рішення.
	Рівень автоматизації аналізу	Визначає частку аналітичних процедур, які виконуються комп'ютерними програмами без упередженого людського втручання.
	Ефективність цифрових систем безпеки	Оцінює, наскільки успішно державні електронні платформи виявляють елементи тіньової економіки тощо.
3. Розвиток державних послуг та підготовка фахівців	Рівень цифрової інтеграції в державне управління	Показує, яка частина державних, податкових та митних послуг переведена в електронний формат.
	Цифрова грамотність працівників	Вимірює вміння державних службовців і працівників підприємств безпечно та ефективно працювати з цифровими технологіями.
	Якість співпраці держави, бізнесу	Оцінює відкритість державних даних, прозорість ухвалення рішень та наявність

CC BY

	та громадян	зручного електронного зв'язку.
4. Загальна економічна та фінансова стійкість	Показник економічної стабільності	Відображає загальний рівень стійкості економіки під впливом цифровізації.
	Загальна ефективність цифрових змін	Підсумковий показник, який демонструє користь від упровадження всіх цифрових рішень у системі безпеки.

Джерело: сформовано за даними [3; 7]

Запропонована система індикаторів побудована за принципом комплексного охоплення ключових напрямів цифрової трансформації, що безпосередньо або опосередковано впливають на рівень економічної безпеки держави. Її структуровано у чотири взаємопов'язані блоки, кожен з яких характеризує окремий аспект цифрової зрілості економічної системи та водночас доповнює інші складові.

Перший блок «Технологічна захищеність та кібербезпека» характеризує базові умови функціонування цифрової економіки. Саме рівень розвитку цифрової інфраструктури, кібербезпеки, захисту інформаційних ресурсів та доступності цифрових технологій визначає спроможність держави забезпечувати безпечне функціонування інших цифрових процесів. За відсутності належного рівня технологічної захищеності навіть високий рівень цифровізації не гарантує підвищення економічної безпеки, оскільки зростає вразливість до кібератак, втрати даних та порушення роботи критичної інфраструктури.

Другий блок «Автоматизація та оперативність державного контролю» відображає рівень використання цифрових технологій у процесах державного управління, моніторингу та контролю економічної діяльності. Автоматизовані інформаційні системи дозволяють скоротити часові витрати на обробку інформації, мінімізувати вплив людського фактора, оперативно виявляти відхилення від нормативних показників та забезпечувати своєчасне реагування на потенційні ризики. Саме цей блок виступає своєрідною сполучною ланкою між технологічною базою цифрової економіки та практичним використанням цифрових рішень у системі державного управління.

Третій блок «Розвиток державних послуг та підготовка фахівців» характеризує рівень практичного впровадження цифрових технологій у взаємодії держави, бізнесу та громадян. Розвиток електронного урядування, цифрових адміністративних послуг, електронного документообігу та цифрових платформ сприяє підвищенню прозорості державного управління, скороченню адміністративних витрат і зниженню корупційних ризиків. Водночас саме цей блок найбільшою мірою демонструє реальний рівень використання результатів цифрової трансформації в економічній діяльності.

Четвертий блок «Загальна економічна та фінансова стійкість» є інтегруючим, оскільки відображає кінцеві результати впливу цифровізації на розвиток економічної системи. На відміну від попередніх блоків, що характеризують окремі процеси цифрової трансформації, показники економічної стійкості демонструють її практичний ефект у вигляді підвищення конкурентоспроможності економіки, інвестиційної привабливості, фінансової стабільності та здатності держави ефективно протидіяти внутрішнім і зовнішнім загрозам.

Для отримання загальної картини ці показники доцільно зводити у єдиний інтегральний індекс економічної безпеки за допомогою методу стандартизації даних та застосування вагових коефіцієнтів.

CC BY

Важливу роль у загальній системі відіграють індикатори фінансової системи. Цифровізація банківської системи та платіжних інструментів гарантує безперебійне функціонування розрахунків під час надзвичайних станів або воєнних дій [10].

З огляду на це, доцільним є впровадження запропонованих індикаторів у державний механізм прийняття рішень. На базі проведеного аналізу сформовано такі рекомендації щодо удосконалення системи оцінювання та забезпечення економічної безпеки України з урахуванням впливу складових цифровізації:

- оновлення офіційних Методичних рекомендацій щодо розрахунку рівня економічної безпеки України шляхом включення до них окремого блока цифрової стійкості. Врахування вагового коефіцієнта цифровізації у загальній оцінці дозволить державі офіційно вимірювати та фіксувати внесок цифровізації у макроекономічну стабільність;

- розробка на базі Міністерства цифрової трансформації, Міністерства економіки та довкілля та Національного банку України єдиної автоматизованої панелі індикаторів. Це дозволить профільним органам здійснювати безперервний аналіз швидкості реагування на загрози, рівня автоматизації аналізу і завчасно нейтралізувати фінансові та кіберризики до настання системних збитків;

- забезпечення гнучкості системи моніторингу шляхом оперативного коригування ваги індикаторів у кризові періоди. Зокрема, в умовах воєнного стану обов'язковому обліку підлягають такі специфічні показники, як частка хмарного дублювання державних реєстрів за кордоном, стійкість платіжної інфраструктури та рівень забезпечення критичної інфраструктури автономним зв'язком;

- врахування показників обсягу інвестицій у цифрову безпеку, динаміки цифрової грамотності у списку метрик при розробці Стратегії економічної безпеки України. Їх систематичний моніторинг дозволить превентивно оцінювати готовність держави до майбутніх викликів.

Висновки. Таким чином, цифровізація є важливим чинником трансформації системи економічної безпеки держави, що забезпечує перехід від «статичного захисту» до проактивної цифрової резильєнтності та адаптивності. На основі діагностики викликів на мікро-, мезо- та макрорівнях і з урахуванням європейського досвіду обґрунтовано чотириблокову систему індикаторів оцінки цифрової трансформації економічної безпеки – від базової кібербезпеки та автоматизації контролю до розвитку послуг і забезпечення економічної та фінансової стійкості, що утворюють єдиний причинно-наслідковий ланцюг. Практичне впровадження запропонованої системи індикаторів та прикладних рекомендацій забезпечить якісний перехід від суб'єктивної та запізнілої оцінки загроз до ситуаційного моніторингу в режимі реального часу. Створення автоматизованої панелі індикаторів суттєво прискорить ухвалення управлінських рішень і мінімізує людський фактор, а гармонізація вітчизняної нормативної бази із європейськими стандартами дозволить підвищити рівень кіберстійкості критичної інфраструктури.

Список використаної літератури

1. Єфремова К. В. Новітні вимоги до розрахунку рівня економічної безпеки України під впливом цифровізації. *Економічна безпека: міжнародний і національний рівень* : зб. наук. пр. за матеріалами ІІ-ї науково-практичної конференції, 21 квітня 2023 року. Харків: НДІ ПЗІР НАПрН України, 2023. С. 25-30. URL: https://openarchive.nure.ua/server/api/core/bitstreams/0b84abe6-3cea-4774-ac1d-fef62087fab3/content.

2. Про Стратегію економічної безпеки України на період до 2025 року : Указ Президента України від 11.08.2021 р. № 347/2021. URL: https://zakon.rada.gov.ua/laws/show/347/2021#Text.

3. Про затвердження Національної економічної стратегії на період до 2030 року : Постанова Кабінету Міністрів України від 03.03.2021 р. № 179. URL: https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#n25.

4. Бедер Д., Цаль-Цалко Ю. Формування економічних індикаторів національної безпеки в умовах цифровізації бізнесу та змін в економіці. *Society and Security.* 2024. № 1(2). С. 3-13. URL: https://doi.org/10.26642/sas-2024-1(2)-3-13.

5. Фаїзов А. В., Мацюра С. І., Мікуліна М. О. Вплив цифровізації на стратегії забезпечення економічної безпеки бізнесу в Україні. *Здобутки економіки: перспективи та інновації*. 2025. №17. URL: https://doi.org/10.5281/zenodo.15333050.

6. Зіміна А., Кавун О. Вплив цифровізації на трансформацію економічних відносин. *Економіка та суспільство*. 2025. №75. URL: https://doi.org/10.32782/2524-0072/2025-75-17.

7. Гнатенко І., Хорошко Д. Трансформація системи економічної безпеки країни в контексті цифровізації. *Актуальні проблеми економіки*. 2025. №3 (25). С. 195–207. URL: https://eco-science.net/wp-content/uploads/2025/03/3.25._topic_Iryna-Hnatenko-Dmytro-Khoroshko-195-207.pdf.

8. Директива Європейського Парламенту та Ради (ЄС) 2022/2555 про заходи для забезпечення високого спільного рівня кібербезпеки в усій Співдружності (Директива NIS2) від 14 грудня 2022 р. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text.

9. Digital resilience and system recovery frameworks in the European Union. *Publications Office of the EU*. URL: https://op.europa.eu/en/publication-detail/-/publication/468a892a-5097-11eb-b59f-01aa75ed71a1/.

10. Inna Shkolnyk, Serhiy Frolov, Volodymyr Orlov, Viktoriia Datsenko and Yevhenii Kozmenko. The impact of financial digitalization on ensuring the economic security of a country at war: New measurement vectors. *Investment Management and Financial Innovations*. 2022. №*19* (3). P. 119-138. URL: http://dx.doi.org/10.21511/imfi.19(3).2022.11.

Дата надходження статті: 24.08.2026
Дата прийняття статті: 15.09.2026
Дата публікації статті: 30.09.2026