

УДК 339.97:004.056.5(4-6ЄС)

DOI: <https://doi.org/10.32782/easterneurope.51-1>

ТРАНСФОРМАЦІЯ КІБЕРЗАГРОЗ ТА ЇЇ ВПЛИВ НА ЕКОНОМІЧНУ БЕЗПЕКУ ЄВРОПЕЙСЬКОГО СОЮЗУ

CYBER THREAT TRANSFORMATION AND ITS IMPACT ON EU ECONOMIC SECURITY¹

Бочарова Ю.Г.

доктор економічних наук, професор,
професор кафедри технологій в ресторанному господарстві,
готельно-ресторанної справи та менеджменту,
Криворізький національний університет
ORCID: <https://orcid.org/0000-0002-4829-8948>

Чернега О.Б.

доктор економічних наук, професор,
професор кафедри технологій в ресторанному господарстві,
готельно-ресторанної справи та менеджменту,
Криворізький національний університет
ORCID: <https://orcid.org/0000-0002-8504-6299>

Кожухова Т. В.

доктор економічних наук, професор,
професор кафедри технологій в ресторанному господарстві,
готельно-ресторанної справи та менеджменту,
Криворізький національний університет
ORCID: <https://orcid.org/0000-0001-6758-9890>

Bocharova Yuliia, Chernega Oksana, Kozhukhova Tetiana
Kryvyi Rih National University

У статті обґрунтовано нагальну необхідність системного переосмислення ландшафту цифрових загроз та їхнього комплексного деструктивного впливу на економічну безпеку Європейського Союзу. Актуальність дослідження зумовлена глибокою цифровізацією критичних секторів економіки ЄС, що перетворює кіберпростір у провідний вимір геополітичного та економічного протистояння. Систематизовано еволюцію оцінок безпекового середовища за звітами ENISA, простежено зміну векторів атак від локальних суб'єктів до цілісних цифрових екосистем. Концептуалізовано поетапне поширення економічних втрат у формі трьох поколінь наслідків: від прямих збитків окремих організацій до системної дестабілізації єдиного ринку та технологічного суверенітету ЄС. Охарактеризовано дворівневу регуляторну відповідь Євросоюзу щодо розбудови його кіберстійкості.

Ключові слова: кібербезпека, кіберзагрози, трансформація, економічна безпека, Європейський Союз, кіберстійкість.

In the article the urgent need for a comprehensive assessment of the evolving digital threat landscape and its systemic impact on the economic security and overall stability of the European Union is examined against the backdrop of rapid economic digitization. The widespread adoption of artificial intelligence, cloud solutions, and interconnected software components across critical infrastructure, governance systems, and commercial entities has radically reshaped the paradigm of modern security vulnerabilities. Under these conditions, cybersecurity is no longer a localized operational concern for individual information technology departments; rather, it has transformed

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project: 101127413 – EVSDESCI – ERASMUS-JMO-2023-HEI-TCH-RSCH



© Бочарова Ю.Г., Чернега О.Б., Кожухова Т. В., 2026

Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

into a core determinant of macroeconomic stability, state sovereignty, and market integrity within the European Union. The discussion focuses on analyzing long-term analytical tracking records from the European Union Agency for Cybersecurity to illustrate the structural migration of attack vectors, targets, and perpetrator motivations. Particular emphasis is placed on tracing the transition from isolated, financially motivated incidents directed at specific companies toward complex, cross-border campaigns aimed at compromising public administrative networks, strategic energy supply chains, and digital services. Furthermore, a conceptual perspective is provided regarding the cumulative escalation of financial and operational damages, demonstrating how primary data breaches and organizational disruptions propagate into macro-level market instabilities that challenge the European Union's technological independence. Additionally, the work explores the European Union's proactive regulatory transformation from reactive risk containment toward strategic cyber resilience. The analysis details the sequential implementation of comprehensive European legislative frameworks designed to enforce unified security benchmarks, enhance executive accountability, establish operational emergency response mechanisms, and institute mandatory technical standards for digital products distributed across the internal market.

Keywords: cybersecurity, cyber threats, transformation, economic security, European Union, cyber resilience.

Постановка проблеми. Стрімкий розвиток цифрової економіки, діджиталізація критичних секторів та масове впровадження технологій штучного інтелекту докорінно змінили ландшафт сучасних безпекових викликів. Кіберпростір остаточно втратив статус суто технологічного середовища, перетворившись на критичну арену геополітичного та економічного протистояння. Зростаюча залежність функціонування критичної інфраструктури, публічного сектору та бізнес-екосистем держав від цифрових рішень підвищує їхню вразливість до деструктивних кібервпливів. За таких умов забезпечення кібербезпеки перестає бути локальним технічним завданням окремих організацій, трансформується у системну передумову забезпечення економічної безпеки, суверенітету та стійкості ЄС.

Беручи до уваги все зазначене вище, цифрова інтеграція, що є головним драйвером економічного зростання ЄС, одночасно виступає каналом поширення масштабних системних ризиків.

Сучасні наукові підходи до оцінювання економічної безпеки переважно концентруються на прямих фінансових наслідках окремих кіберінцидентів, тоді як механізми трансформації локальних кібератак у системні макроекономічні ризики залишаються недостатньо концептуалізованими. Це створює розрив між стрімкою еволюцією цифрових загроз та науковим забезпеченням оцінювання їхнього впливу на економічну безпеку Європейського Союзу.

Аналіз результатів досліджень Агентства ЄС з кібербезпеки (ENISA) свідчить про структурні зміни ландшафту атак, їхніх цілей та суб'єктів реалізації: від ізольованих, фінансово мотивованих інцидентів проти окремих організацій до складних транскордонних кампаній, спрямованих на публічне управління, стратегічні енергетичні ланцюги та цифрові сервіси. Як результат, на сучасному етапі цифрової трансформації спостерігається кумулятивна ескалація фінансових та операційних збитків, коли первинні витоки даних та локальні збої дестабілізують

макроекономічні ринки та підривають технологічну незалежність Європейського Союзу.

Ситуація ускладнюється суперечністю між еволюцією кіберзагроз та необхідністю переходу від реактивного стримування ризиків до стратегічної кіберстійкості. Послідовна імплементація уніфікованих європейських нормативних вимог, підвищення відповідальності керівництва, створення механізмів оперативного реагування та введення обов'язкових технічних стандартів для цифрових продуктів потребують глибокого оцінювання їхнього реального впливу на економічну безпеку. Особливої актуальності ця проблема набуває в умовах поширення генеративного штучного інтелекту, розвитку хмарних сервісів, цифрових платформ та складних транскордонних ланцюгів постачання, що істотно підвищують взаємозалежність цифрових екосистем та масштаб потенційних економічних наслідків кібератак. За таких умов виникає необхідність переосмислення кіберзагроз не лише як технологічного, а й як макроекономічного чинника розвитку Європейського Союзу, що зумовлює нагальну наукову потребу в аналізі трансформаційних зсувів у ландшафті кіберзагроз та визначенні ефективності регуляторних інструментів ЄС у захисті його макроекономічної стабільності.

Аналіз останніх досліджень і публікацій. Особливості та етапи еволюції політики кібербезпеки ЄС у період від 90-х років XX століття до 2024 року ґрунтовно досліджені у праці Муханова Т.М., Легомінова С.В., Щавінський Ю.В., Якименко Ю. М., Нестеренко Г. П. [1]. Автори систематизували часову трансформацію регуляторного поля Євросоюзу та довели, що сучасна архітектура європейської кібербезпеки вибудовується навколо трьох стратегічних цілей: досягнення високого рівня кіберстійкості суб'єктів усіх рівнів (від інституцій ЄС до окремих організацій); забезпечення ефективного кіберстримування; а також активне просування безпечного, відкритого й стабільного глобального кіберпростору.

Дослідженню кіберзагрозам у системі забезпечення економічної безпеки держави та оцінці

стійкості її технологічної інфраструктури присвячено працю Пахненко О. М. та Божка М. О. [2]. Автори акцентують увагу на тому, що загрози у кіберпросторі перестають бути суто технічною проблемою, перетворюючись на ключовий чинник макроекономічної дестабілізації та виклик для національної безпеки.

Гібридизацію викликів у цифровому середовищі та їхній безпосередній вплив на економічний суверенітет ЄС проаналізовано у праці Фарранда Б., Каррапіко Х. та Турובהва А. [3]. Науковці акцентують увагу на тому, що загрози кіберпростору перейшли з суто технічної площини у вимір міжнародних відносин, трансформуючи кібербезпеку на ключову умову збереження економічного суверенітету Євросоюзу.

Систематизацію теоретико-методологічних підходів до економічної оцінки кіберризиків та їхнього впливу на суб'єктів цифрового середовища (компанії, користувачів, регуляторів) здійснено у фундаментальному огляді Абрарді Л., Коміно С. та Грасіні С. [4]. Автори узагальнили економічні та фінансові наслідки кібератак, а також систематизували регуляторні інструменти пом'якшення кіберризиків.

Глобальний вимір макроекономічного впливу цифрових загроз висвітлено у праці Бергари Е. Кобос під егідою Світового банку [5]. На основі емпіричного аналізу авторка доводить, що деструктивний ефект кібератак виходить далеко за межі локальних втрат окремих суб'єктів, спричиняючи каскадні збої у ланцюгах постачання, падіння інвестиційної активності та скорочення операційних грошових потоків. Водночас системне зниження рівня кіберінцидентів виступає прямим драйвером економічного зростання, здатним забезпечити приріст ВВП на душу населення до 1,5%, що підтверджує критичну роль інвестицій у кіберстійкість для макроекономічної стабільності.

Виділення невирішених раніше частин загальної проблеми. Визнаючи вагомий внесок зазначених науковців у концептуалізацію геополітичних, правових та загальноекономічних аспектів кібербезпеки, варто зазначити, що поза увагою дослідників досі залишається прикладна систематизація еволюції ландшафту цифрових загроз та їхнього безпосереднього впливу на економічну безпеку Євросоюзу. Зокрема, вимагає поглибленого аналізу трансформація векторів атак на основі офіційної аналітики ENISA у контексті формування сучасної європейської політики кіберстійкості.

Постановка завдання. Метою статті є дослідження особливостей трансформації сучасних кіберзагроз та визначення їх впливу на економічну безпеку ЄС на основі документів ENISA та сучасної політики ЄС у сфері забезпечення кіберстійкості.

Виклад основного матеріалу дослідження. Для ідентифікації ключових тенденцій

еволюції цифрових загроз та їхнього впливу на економічне середовище було проведено контент-аналіз та систематизацію щорічних аналітичних звітів Агентства Європейського Союзу з кібербезпеки (ENISA Threat Landscape) за 2020–2025 рр. [6–11], а також форсайт-дослідження розвитку загроз до 2030 року [12].

Систематизація накопичених масивів даних дозволила простежити зміну дослідницьких акцентів ENISA, трансформацію векторів атак та розширення кола потенційних об'єктів впливу. Крім того, проведена систематизація дозволила не лише простежити еволюцію окремих категорій кіберзагроз, а й визначити зміну пріоритетів у підходах Європейського Союзу до забезпечення економічної безпеки.

Аналіз звітів ENISA демонструє, що відбулося поступове зміщення акценту від реагування на окремі технічні інциденти до комплексного управління ризиками цифрової інфраструктури, стійкості критично важливих секторів економіки та підвищення рівня кіберстійкості держав-членів ЄС.

Такий підхід створює підґрунтя для оцінки взаємозв'язку між трансформацією кіберзагроз і змінами у політиці забезпечення економічної безпеки ЄС, оскільки саме характер загроз визначає напрями розвитку нормативно-правового регулювання, інституційних механізмів та інвестицій у цифрову стійкість.

Узагальнені результати порівняльного аналізу ключових параметрів ландшафту кіберзагроз наведено в таблиці 1.

Аналіз динаміки ключових загроз у звітах ENISA (2020–2025 рр., 2030 р.) дозволяє стверджувати, що протягом досліджуваного періоду:

1. Можна виділити 2 етапи прогресу ENISA у ідентифікації ландшафту кіберзагроз: 1 етап (2020 р.) – каталогізація основних кіберзагроз; 2 етап (2021–2025 рр.) – виявлення змін, трендів та детермінації кіберзагроз: 2021 р. – фіксація комерціалізації кіберзлочинності та розвитку шкідливого ПЗ; 2022 р. – геополітизація кіберпростору; 2023 р. – орієнтація на людський фактор та комплексні атаки; 2024–2025 рр. – інтеграція штучного інтелекту та системних кіберризиків.

2. Основними загрозами кібербезпеки виступають програми-вимагачі, шкідливе ПЗ, фішинг та соціальна інженерія, DDoS-атаки, компрометація даних.

3. Відбулася не стільки поява принципово нових типів атак, скільки зміна їх складності, масштабу, мети та об'єкту впливу. Якщо у 2020 р. основними об'єктами атак були окремі організації, самі атаки носили здебільшого локальний характер, реалізовувалися за допомогою шкідливого програмного забезпечення, мотивувалися бажанням кіберзлочинців отримати фінансовий результат – прибуток, то у 2025 році основними об'єктами атак стали екосистеми та публічний сектор. Атаки набули транскордонного та системного

Таблиця 1

Трансформація ключових загроз у звітах ENISA Threat Landscape

Рік	Основний акцент ENISA	Основні об'єкти атаки	Основні загрози кібербезпеці
2020	15 основних категорій загроз розвитку цифрового середовища	Окремі організації	Шкідливе ПЗ; веб-атаки; фішинг; атаки на веб-додатки; спам; DDoS-атаки; викрадення облікових даних; витік (компрометація) даних; внутрішні загрози; витік інформації; програми-вимагачі; кібершпигунство; криптоджекінг; фізична втрата, пошкодження або викрадення обладнання; ботнети.
2021	Комерціалізація кіберзлочинності, програми-вимагачі	Бізнес, ланцюги постачання	Програми-вимагачі; шкідливе ПЗ; криптоджекінг; загрози електронної пошти (фішинг, спам); загрози для даних (витік та компрометація); загрози доступності та цілісності (DDoS-атаки); дезінформація; атаки на ланцюги постачання.
2022	Кібербезпека в умовах геополітичної турбулентності та війни в Україні	Критична інфраструктура, громадяни	Програми-вимагачі; шкідливе ПЗ; соціальна інженерія та фішинг; викрадення та витік даних; DDoS-атаки; загрози доступності (фізичні та логічні збої); іноземні інформаційні маніпуляції та дезінформація; атаки на ланцюги постачання.
2023	Розвиток складних схем кіберзлочинності, соціальна інженерія		Програми-вимагачі; DDoS-атаки; загрози для даних (витік та компрометація); соціальна інженерія та фішинг; шкідливе ПЗ; атаки на ланцюги постачання; іноземні інформаційні маніпуляції та дезінформація; експлуатація вразливостей «нульового дня».
2024	Консолідація основних категорій загроз та посилення уваги до критичної інфраструктури	Цифрові екосистеми ЄС	DoS / DDoS / RDoS-атаки; програми-вимагачі; загрози для даних (витік та компрометація); загрози соціальної інженерії; шкідливе ПЗ; атаки на ланцюги постачання; веб-загрози (атаки на веб-ресурси та додатки); іноземні інформаційні маніпуляції та дезінформація; експлуатація вразливостей «нульового дня».
2025	Зростання складності комплексних атак та підвищення ризиків для цифрової інфраструктури		Фішинг; експлуатація вразливостей ПЗ; ботнети; шкідливі додатки; внутрішні загрози
До 2030	Тренди трансформації цифрових загроз до 2030 р., рівень захисту старих систем, вплив кліматичного фактору на кібербезпеку		Компрометація ланцюгів постачання через програмні залежності; дефіцит кваліфікованих кадрів; людський фактор та експлуатація застарілих систем у кіберфізичних екосистемах; експлуатація неоновленого та застарілого ПЗ у перевантаженому міжсекторальному технологічному середовищі; зростання цифрово-стежкового авторитаризму та втрата приватності; транскордонні провайдери ІКТ-послуг як єдина точка відмови; удосконалені кампанії дезінформації та інформаційних операцій; зростання складних гібридних загроз; зловживання штучним інтелектом; фізичний вплив природних та екологічних катастроф на критичну цифрову інфраструктуру

Джерело: сформовано авторами на основі контент-аналізу джерел [6–12]

характеру, а їхньою метою все частіше ставала не лише економічна вигода, а й здобуття геополітичного впливу, дестабілізація та саботаж. При цьому суб'єктний склад агресорів розширився до поєднання кіберзлочинних угруповань із державними акторами, які активно імплементують у свої інструменти технології штучного інтелекту та витончену соціальну інженерію.

4. Найбільш уразливими до кіберзагроз були фінансовий сектор; енергетика; транспорт;

охорона здоров'я; цифрові послуги; державне управління.

5. Мала місце зміна акцентів ENISA пов'язана не тільки із розвитком технологій (розвиток технології штучного інтелекту, хмарних технологій тощо), а й із глобальними подіями та трендами, зокрема цифровізацією економіки; геополітичною нестабільністю; кліматичними змінами, як наслідок, простежується перехід від окремих технічних атак до комплексних багатовекторних кампаній,

що передбачають атаки на ланцюги постачання, поєднання технологічних та психологічних методів, активне використання інформаційних маніпуляцій, атаки на критичну інфраструктуру.

Таким чином, проведений аналіз засвідчив, що еволюція кіберзагроз характеризується не стільки появою принципово нових типів атак, скільки істотним ускладненням їх архітектури. Сучасні кібератаки набувають ознак багаторівневих кампаній, що поєднують технічні, інформаційно-психологічні, організаційні та економічні інструменти впливу. Саме така інтеграція різних механізмів деструктивного впливу формує якісно новий рівень ризиків, за якого економічні наслідки виникають не лише через безпосереднє порушення функціонування інформаційних систем, а й через втрату довіри до цифрового середовища, скорочення інвестиційної активності, зростання витрат на кіберзахист та порушення міжнародних виробничих ланцюгів.

Кіберзагрози дедалі більше впливають на економічну безпеку. Так, процес трансформації деструктивного впливу кібератак від локальних операційних збитків окремих організацій до макроекономічного масштабу чітко підтверджується емпіричними даними міжнародних аналітичних досліджень. Зокрема, за оцінками звіту Howden Group, оціночні сукупні економічні втрати від кібератак упродовж 2020–2025 рр. лише для чотирьох найбільших економік Європи (Німеччини, Франції, Італії та Іспанії) склали 307 млрд євро [13]. При цьому майже двом третинам цих збитків (близько 204 млрд євро) можна було б запобігти за умови дотримання базової кібергігієни та належного рівня кіберстрахування. Наведене підтверджує, що деструктивний потенціал цифрових загроз створює системні ризики для фінансової стабільності та економічної стійкості ЄС.

Таким чином, сучасні атаки спрямовані вже не лише на інформаційні системи, а на безперервність діяльності підприємств, функціонування критичної інфраструктури, цифрові послуги та державне управління, ланцюги постачання.

Контент-аналіз звітів ENISA дозволив виділити три покоління економічних наслідків кіберзагроз:

I покоління – втрата інформації (даних), прямі фінансові збитки;

II покоління – фінансові втрати підприємств (зростання операційних витрат), порушення роботи організацій;

III покоління – дестабілізація критичної інфраструктури та економіки держав, що обумовлюють ризики економічної стійкості, конкурентоспроможності та функціонування внутрішнього ринку ЄС.

Запропонована класифікація трьох поколінь економічних наслідків відображає поступовий перехід від локального рівня впливу до системних макроекономічних ефектів. Якщо наслідки

першого покоління характеризуються безпосередніми фінансовими втратами окремих суб'єктів господарювання, а другого – формуванням додаткових операційних витрат і порушенням бізнес-процесів, то наслідки третього покоління виходять за межі окремих організацій та охоплюють функціонування критичної інфраструктури, стійкість внутрішнього ринку, інвестиційну привабливість, конкурентоспроможність і технологічний суверенітет Європейського Союзу. Саме на цьому рівні кіберзагрози набувають ознак системного чинника економічної безпеки.

Таким чином, на сучасному етапі розвитку об'єктом захисту є економічна стійкість, безперервність господарської діяльності, критична інфраструктура, функціонування єдиного цифрового ринку, технологічний суверенітет ЄС, а отже кібербезпека трансформується з технічної складової інформаційної безпеки у ключовий елемент забезпечення економічної безпеки ЄС.

Водночас трансформація кіберзагроз змінює не лише характер функціонування інформаційних систем, а й механізми забезпечення економічної безпеки Європейського Союзу. Якщо раніше економічні втрати від кібератак переважно концентрувалися на рівні окремих суб'єктів господарювання, то сучасні комплексні атаки поширюють свій вплив на міжгалузеві виробничі зв'язки, транскордонні ланцюги створення вартості, фінансові ринки та функціонування єдиного внутрішнього ринку ЄС. Таким чином, кіберпростір поступово перетворюється на один із ключових факторів забезпечення конкурентоспроможності, технологічної автономії та економічної стійкості Європейського Союзу.

Трансформація кіберзагроз, тренд цифрового розвитку економіки та суспільства в ЄС супроводжується розвитком нормативної бази ЄС в цій сфері.

Перехід від реактивного реагування до стратегічного забезпечення кіберстійкості (Cyber Resilience) знайшов своє відображення у прийнятті та імплементації ключових регуляторних актів ЄС нового покоління, що сформували дві послідовні законодавчі хвилі.

Перша хвиля (2022 р.) охопила оновлену Директиву про мережеву та інформаційну безпеку (NIS2) [14], яка суттєво розширила коло суб'єктів критичної інфраструктури та посилила персональну відповідальність керівництва за кіберризики (2023 р.), а також Регламент про цифрову оперативну стійкість (DORA) [15], що встановив жорсткі вимоги для фінансового сектору (застосовується з січня 2025 р.).

Друга хвиля (жовтень–грудень 2024 р.) представлена Законом про кіберстійкість (Cyber Resilience Act) [16], який уперше запровадив обов'язкові стандарти безпеки для програмного забезпечення та продуктів із цифровими елементами на ринку Євросоюзу (2024 р., з повним застосуванням вимог від грудня 2027 р.),

а також Законом про кіберсолідарність (Cyber Solidarity Act) [17], ухваленим у 2024 р. Останній спрямований на посилення оперативних спроможностей ЄС через створення Європейської системи кібералертів (European Cyber Alert System), Механізму реагування на надзвичайні кіберситуації (Cyber Emergency Mechanism) та формування Резерву кібербезпеки ЄС (EU Cybersecurity Reserve) для оперативної взаємодопомоги під час масштабних атак.

Аналіз еволюції нормативно-правового регулювання свідчить, що сучасна політика Європейського Союзу спрямована не лише на підвищення рівня кіберзахисту окремих суб'єктів, а й на формування єдиного економічного простору, що базується на високому рівні цифрової довіри. Запровадження уніфікованих вимог до кіберстійкості створює однакові конкурентні умови для функціонування бізнесу, знижує трансакційні витрати цифрової взаємодії та підвищує стійкість внутрішнього ринку до зовнішніх шоків.

Висновки. У результаті проведеного дослідження: Доведено еволюційну трансформацію ландшафту кіберзагроз від локальних технічних атак до системних геоекономічних викликів. На основі контент-аналізу аналітичних звітів Агентства ЄС з кібербезпеки (ENISA Threat Landscape за 2020–2025 рр. та форсайту до 2030 р.) виділено два ключові етапи розвитку оцінки загроз:

- перший етап (2020 р.) – первинна каталогізація базових типів кіберзагроз;
- другий етап (2021–2025 рр.) – ідентифікація трендів та детермінації загроз: комерціалізація кіберзлочинності, геополітизація кіберпростору, орієнтація на людський фактор та інтеграція штучного інтелекту у складні багатовекторні атаки. Зсув об'єктів впливу від окремих організацій до цілісних цифрових екосистем, ланцюгів постачання та публічного сектору засвідчив, що сучасною метою атакуючих є не лише миттєва фінансова вигода, а й дестабілізація критичної інфраструктури, саботаж та здобуття геополітичного впливу.

Запропоновано концептуалізацію трьох поколінь економічних наслідків кіберзагроз. Встановлено, що вплив кібератак на економічне середовище пройшов шлях трансформації від мікро- до макрорівня:

I покоління – прямі фінансові збитки та компрометація/втрата даних на рівні окремих суб'єктів;

II покоління – опосередковані операційні втрати підприємств, зростання витрат на

відновлення бізнес-процесів та порушення функціонування організацій;

III покоління – системна дестабілізація критичної інфраструктури, створення ризиків для економічної стійкості, конкурентоспроможності, технологічного суверенітету та функціонування єдиного цифрового ринку ЄС.

Обґрунтовано, що за таких умов кібербезпека остаточно трансформувалася з суто технічної складової IT-інфраструктури у базовий елемент забезпечення економічної безпеки та стійкості держави, наднаціональних об'єднань.

Систематизовано регуляторні відповіді Європейського Союзу на нові виклики кіберстійкості. Обґрунтовано, що перехід ЄС від реактивного реагування до стратегічного розбудовування кіберстійкості (Cyber Resilience) реалізовано через дві послідовні законодавчі хвилі:

Перша хвиля (2022 р.) охопила Директиву NIS2 та Регламент DORA, які суттєво розширили периметр критичної інфраструктури, посилили персональну відповідальність керівництва та встановили жорсткі стандарти цифрової оперативності для фінансового сектору.

Друга хвиля (2024 р.) представлена Законом про кіберстійкість (Cyber Resilience Act – запровадження безпекових стандартів для ПЗ та продуктів із цифровими елементами) та Законом про кіберсолідарність (Cyber Solidarity Act – розбудова оперативних спроможностей через Європейську систему кібералертів, Механізм реагування на надзвичайні ситуації та Резерв кібербезпеки ЄС).

Отримані результати дають підстави розглядати кібербезпеку не як окремий напрям цифрової політики, а як структурний елемент системи економічної безпеки Європейського Союзу. Трансформація сучасних кіберзагроз свідчить про поступове зміщення центру уваги від захисту окремих інформаційних ресурсів до забезпечення стійкості економічних систем, критичної інфраструктури, цифрових ланцюгів створення вартості та технологічного суверенітету. Це визначає необхідність інтеграції кіберризиків у стратегічне планування економічної політики та систему оцінювання економічної безпеки держав і наднаціональних об'єднань.

Подальші наукові розвідки у даному напрямі будуть спрямовувати на розробку кількісних методико-прикладних підходів до оцінки збитків від кіберзагроз III покоління для економіки ЄС та України.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Мужанова Т. М., Легомінова С. В., Щавінський Ю. В., Якименко Ю. М., Нестеренко Г. П. Основні підходи й напрями розвитку політики кібербезпеки Європейського Союзу. *Кібербезпека: освіта, наука, техніка*. 2024. № 4 (24). С. 133–149. DOI: <https://doi.org/10.28925/2663-4023.2024.24.133149>
2. Пахненко О. М., Божко М. О. Кіберзагрози як виклик економічній безпеці: потенціал технологічної інфраструктури України. *Економіка і регіон*. 2025. № 2 (97). DOI: [https://doi.org/10.26906/EiR.2025.2\(97\).3857](https://doi.org/10.26906/EiR.2025.2(97).3857)

3. Farrand B., Carrapico H., Turobov A. The new geopolitics of EU cybersecurity: security, economy and sovereignty. *International Affairs*. 2024. Vol. 100, No. 6. P. 2379–2397. DOI: <https://doi.org/10.1093/ia/iaae231>
4. Abrardi L., Comino S., Grassini S. The economics of cyber risk: a survey of the literature. *Journal of Industrial and Business Economics*. 2026. Vol. 53. pp. 573–607. DOI: <https://doi.org/10.1007/s40812-025-00370-3>
5. Vergara Cobos E. Cybersecurity Economics for Emerging Markets. Washington, DC : World Bank, 2024. 156 p. URL: <https://openknowledge.worldbank.org/server/api/core/bitstreams/2bbe8bb7-dd68-4159-a808-e60403fb2fc6/content> (date of access: 28.07.2026). DOI: <https://doi.org/10.1596/978-1-4648-2120-2>.
6. ENISA (2026). ENISA Threat Landscape 2025. URL: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf.
7. ENISA (2024). ENISA Threat Landscape 2024. URL: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf.
8. ENISA (2023). ENISA Threat Landscape 2023. URL: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf>.
9. ENISA (2022). ENISA Threat Landscape 2022. URL: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202022.pdf>.
10. ENISA (2021). ENISA Threat Landscape 2021. URL: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202021.pdf>.
11. ENISA (2020). ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected. URL: <https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020>.
12. ENISA (2024). Foresight cybersecurity threats for 2030 – update. URL: https://www.enisa.europa.eu/sites/default/files/2024-11/Foresight%20Cybersecurity%20Threats%20for%202030-Update-fullreport_en_0.pdf.
13. Cyber Insurance Market Outlook 2025 / Howden Group Holdings. 2025. URL: <https://howdengroupholdings.com/reports/2025-cyber-report>.
14. NIS2 Directive: securing network and information systems. URL: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>.
15. Digital Operational Resilience Act (DORA). URL: https://eiopa.europa.eu/digital-operational-resilience-act-dora_en.
16. Cyber Resilience Act. URL: <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>.
17. Cyber Solidarity Act. URL: <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>.

REFERENCES:

1. Muzhanova T. M., Lehominova, S. V., Shchavinskyy, Yu. V., Yakymenko, Yu. M., & Nesterenko, H. P. (2024). Osnovni pidkhody y napriamy rozvytku polityky kiberbezpeky Yevropeiskoho Soiuzu [Key approaches and directions of cybersecurity policy development of the European Union]. *Kiberbezpeka: osvita, nauka, tekhnika – Cybersecurity: Education, Science, Technique*, no. 4(24), pp. 133–149. DOI: <https://doi.org/10.28925/2663-4023.2024.24.133149> [in Ukrainian].
2. Pakhnenko O. M., & Bozhko, M. O. (2025). Kiberzahrozy yak vyklyk ekonomichnii bezpetsi: potentsial tekhnolohichnoi infrastruktury Ukrainy [Cyber threats as a challenge to economic security: The potential of Ukraine's technological infrastructure]. *Ekonomika i rehion – Economy and Region*, no. 2(97). DOI: [https://doi.org/10.26906/EiR.2025.2\(97\).3857](https://doi.org/10.26906/EiR.2025.2(97).3857) [in Ukrainian].
3. Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: Security, economy and sovereignty. *International Affairs*, vol. 100, no.6, pp. 2379–2397. DOI: <https://doi.org/10.1093/ia/iaae231>.
4. Abrardi, L., Comino, S., & Grassini, S. (2026). The economics of cyber risk: A survey of the literature. *Journal of Industrial and Business Economics*, vol. 53, pp. 573–607. DOI: <https://doi.org/10.1007/s40812-025-00370-3>.
5. Vergara Cobos, E. (2024). Cybersecurity economics for emerging markets. World Bank. DOI: <https://doi.org/10.1596/978-1-4648-2120-2>.
6. ENISA. (2026). ENISA Threat Landscape 2025. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf.
7. ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf.
8. ENISA. (2023). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. Available at: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf>.
9. ENISA. (2022). ENISA Threat Landscape 2022. European Union Agency for Cybersecurity. Available at: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202022.pdf>.
10. ENISA. (2021). ENISA Threat Landscape 2021. European Union Agency for Cybersecurity. Available at: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202021.pdf>.
11. ENISA. (2020). ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected. European Union Agency for Cybersecurity. Available at: <https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020>.
12. ENISA. (2024). Foresight Cybersecurity Threats for 2030 – Update. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/sites/default/files/2024-11/Foresight%20Cybersecurity%20Threats%20for%202030-Update-fullreport_en_0.pdf.

13. Howden Group. (2025). Cyber Insurance Market Outlook 2025. Howden Group Holdings. Available at: <https://www.howdengroupholdings.com/reports/2025-cyber-report>.
14. European Commission. (2022). NIS2 Directive: Securing network and information systems. Available at: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>.
15. EIOPA. (2022). Digital Operational Resilience Act (DORA). European Insurance and Occupational Pensions Authority. Available at: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.
16. European Commission. (2024). Cyber Resilience Act. Available at: <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>.
17. European Commission. (2024). Cyber Solidarity Act. Available at: <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>.

Дата надходження статті: 20.07.2026
Дата прийняття статті до публікації: 15.08.2026
Дата публікації статті: 27.08.2026