

УДК 351.86:004.056.53

DOI: <https://doi.org/10.31470/2786-6246-2026-17-240-251>

Чумакова Ганна, кандидат наук з державного управління (PhD), доцент кафедри публічного управління та адміністрування Одеського національного технологічного університету

Chumakova Hanna, Candidate of Sciences in Public administration (PhD), associate professor of the Department of public management and administration at Odesa National University of Technology

ORCID ID: <https://orcid.org/0000-0003-4134-8209>

Пасічник Віталій, асистент кафедри публічного управління та адміністрування Одеського національного технологічного університету

Pasichniuk Vitaliy, assistant professor of Department of Public Management and Administration at Odesa National University of Technology

ORCID ID: <https://orcid.org/0009-0006-2625-7594>

Караган Максим, здобувач другого рівня вищої освіти кафедри публічного управління та адміністрування Одеського національного технологічного університету

Karahan Maxym, student of Department of public management and administration at Odesa National University of Technology

ORCID ID: <https://orcid.org/0009-0009-9677-7853>

ГАРМОНІЗАЦІЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ З ВИМОГАМИ ТА СТАНДАРТАМИ ЄВРОПЕЙСЬКОГО СОЮЗУ

HARMONIZATION OF UKRAINE'S NATIONAL CYBER RESILIENCE SYSTEM FOR CRITICAL INFRASTRUCTURE WITH EUROPEAN UNION REQUIREMENTS AND STANDARDS

Анотація. Стаття присвячена дослідженню теоретико-методологічних та прикладних засад гармонізації національної системи кіберстійкості критичної інфраструктури України з правом Європейського Союзу. Обґрунтовано, що кіберстійкість критичної інфраструктури є не суто технічною, а комплексною управлінською проблемою, розв'язання якої передбачає узгоджений розвиток правового, інституційного, кадрового, фінансового та технологічного механізмів публічного управління, а не обмежується транспозицією окремих правових норм.

На основі аналізу динаміки кіберінцидентів та стану формування Реєстру об'єктів критичної інфраструктури продемонстровано, що масштаб і складність кіберзагроз зростають випереджальними темпами порівняно з інституційною та кадровою спроможністю системи публічного управління їм протидіяти. Розкрито зміст вимог директив Європейського Союзу NIS2 й CER та здійснено порівняльний аналіз темпів їх транспозиції в державах-членах, що дало підстави розглядати гармонізацію як тривалий і нерівномірний процес, притаманний навіть країнам із розвиненою інституційною спроможністю.

*Corresponding author



Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (<https://creativecommons.org/licenses/by/4.0/>)

ISSN 2786-6246 (print)
ISSN 2786-9091 (online)

Досліджено національні правові та інституційні механізми гармонізації, зокрема законодавче забезпечення функціонування єдиної системи реагування на кіберінциденти, розвиток кадрового потенціалу сфери кіберзахисту та вдосконалення методичного забезпечення оцінювання стану кіберзахисту суб'єктів критичної інфраструктури. Особливу увагу приділено людському чиннику кіберстійкості – еволюції соціальної інженерії як вектора кібератак, що доповнює технічні виміри захисту критичної інфраструктури.

Запропоновано авторську модель гармонізації національної системи кіберстійкості критичної інфраструктури, що інтегрує правовий, інституційний, кадровий, фінансовий і технологічний механізми в межах циклічного управлінського процесу, а також Індекс готовності до гармонізації, призначений для оцінювання відповідності секторів критичної інфраструктури вимогам Європейського Союзу.

Ключові слова: публічне управління, цифровізація, критична інфраструктура, кібербезпека, директива NIS2, директива CER, євроінтеграція.

Abstract. This article examines the theoretical, methodological, and practical foundations for harmonizing Ukraine's national cyber resilience system for critical infrastructure with European Union law. It is argued that the cyber resilience of critical infrastructure is not a purely technical issue but a complex management challenge, the resolution of which requires the coordinated development of legal, institutional, human resources, financial, and technological mechanisms of public administration, rather than being limited to the transposition of individual legal provisions.

Based on an analysis of the dynamics of cyber incidents and the status of the development of the Register of Critical Infrastructure Objects, it is demonstrated that the scale and complexity of cyber threats are growing at a faster rate than the institutional and human resource capacity of the public administration system to counter them. The content of the requirements of the European Union's NIS2 and CER Directives is examined, and a comparative analysis of the pace of their transposition in member states is conducted, which provides grounds for viewing harmonization as a protracted and uneven process, characteristic even of countries with developed institutional capacity.

The study examined national legal and institutional mechanisms for harmonization, including the legislative framework for the operation of a unified cyber incident response system, the development of human resources in the field of cybersecurity, and the improvement of methodological guidelines for assessing the cybersecurity status of critical infrastructure entities. Particular attention was paid to the human factor in cyber resilience—the evolution of social engineering as a vector for cyberattacks, which complements the technical dimensions of critical infrastructure protection.

The authors propose a model for harmonizing the national cyber resilience system for critical infrastructure, which integrates legal, institutional, human resources, financial, and technological mechanisms within a cyclical management process, as well as a Harmonization Readiness Index designed to assess the compliance of critical infrastructure sectors with European Union requirements.

Keywords: public administration, digitalization, critical infrastructure, cybersecurity, NIS2 Directive, CER Directive, European integration.

Постановка проблеми. Захист критичної інфраструктури від кіберзагроз є однією з визначальних умов забезпечення національної безпеки та реалізації курсу України на європейську інтеграцію. В умовах повномасштабної збройної агресії кіберпростір набуває значення самостійної сфери протистояння: об'єкти енергетики, реєстри державних органів, інфраструктура органів місцевого самоврядування та телекомунікаційні мережі виступають об'єктами систематичних кібероперацій, спрямованих як на отримання розвідувальної інформації, так і на дестабілізацію функціонування державних інституцій.

Одночасно Україна взяла на себе зобов'язання щодо гармонізації національного законодавства у сфері кібербезпеки з правом Європейського Союзу, насамперед з директивами NIS2 та CER, у межах програми Ukraine Facility та переговорного процесу про вступ до ЄС.

Виконання цих зобов'язань пов'язане з визначеними індикаторами Плану України для Ukraine Facility, від дотримання яких залежить надання фінансової підтримки в рамках зазначеної програми [1; 2].

Проблема гармонізації є, однак, управлінською значно більшою мірою, ніж суто юридичною. Ухвалення закону, що відтворює термінологію директиви ЄС, саме собою не забезпечує кіберстійкості: необхідні дієздатні інституції, підготовлений персонал, функціонуючий облік об'єктів критичної інфраструктури, галузеві команди реагування на кіберінциденти та сталі фінансування відповідних заходів. Це зумовлює потребу розглядати гармонізацію національної системи кіберстійкості критичної інфраструктури не лише крізь призму змісту правових норм, а й крізь призму спроможності системи публічного управління їх реалізовувати.

Аналіз останніх досліджень і публікацій. Питання гармонізації законодавства України з правом Європейського Союзу у сфері кібербезпеки перебуває у полі уваги як вітчизняних, так і європейських дослідників. Зокрема, Я.М. Костюченко досліджує механізми співпраці України та ЄС у сфері кібербезпеки, оцінює рівень інтеграції національної системи кіберзахисту в європейський безпековий простір та обґрунтовує необхідність гармонізації національного законодавства з правом ЄС у контексті протидії кіберзлочинності [3]. Питання інституційної координації захисту критичної інфраструктури та методології віднесення об'єктів до критичної інфраструктури в контексті наближення національного законодавства до підходів Європейського Союзу розглядають С.І. Кондратов [4] та О.В. Мельничук [5]. У європейському науковому дискурсі J. Ruohonen на основі систематичного огляду академічної літератури встановлює, що дослідження директиви NIS2 здебільшого зосереджені на її співвідношенні з іншими актами права ЄС у сфері кібербезпеки та вказує на недостатню дослідженість практичних аспектів впровадження директиви в окремих секторах критичної інфраструктури [6], тоді як N. Vandezande здійснює порівняльний аналіз положень NIS2 із попередньою директивою NIS, виявляючи посилення вимог до управління кіберризиками, безпеки ланцюгів постачання та звітування про інциденти [7]. У науковій літературі також наголошується, що ефективна імплементація директиви NIS2 передбачає розширення інституційної спроможності державних органів та вдосконалення механізмів обміну кіберрозвідувальною інформацією між Україною та структурами Європейського Союзу.

У європейському дискурсі директиви NIS2 та CER розглядаються як взаємодоповнювальні регуляторні інструменти: перша спрямована на забезпечення кіберстійкості мереж та інформаційних систем, друга – на фізичну й операційну стійкість критичних суб'єктів до широкого кола загроз, включно з природними, техногенними та терористичними [8; 9]. Обидві директиви охоплюють переважно однакове коло секторів – енергетику, транспорт, охорону здоров'я, банківський сектор, цифрову інфраструктуру, публічне управління, – що зумовлює потребу в скоординованій, а не паралельній, імплементації відповідних вимог [9].

Аналіз практики транспозиції NIS2 у державах-членах Європейського Союзу засвідчує, що гармонізація національного законодавства з правом ЄС є тривалим і нерівномірним процесом навіть для країн із розвинутою інституційною спроможністю [10; 11]. Це формує важливий методологічний орієнтир для оцінювання темпів гармонізації в Україні, оскільки дає підстави розглядати відставання від формальних термінів директиви як типове явище, притаманне процесу гармонізації як такому.

Водночас недостатньо дослідженою залишається взаємодія між юридичною гармонізацією, тобто транспозицією правових норм, та управлінською спроможністю її практичної реалізації – кадровим забезпеченням, фінансуванням, інституційною координацією. Саме цей аспект визначає спрямованість цього дослідження.

Метою статті є теоретичне обґрунтування та розроблення практичних рекомендацій щодо гармонізації національної системи кіберстійкості критичної інфраструктури України з вимогами та стандартами Європейського Союзу на основі інтеграції правового, інституційного, кадрового, фінансового та технологічного механізмів публічного управління.

Виклад основного матеріалу. Правове регулювання захисту критичної інфраструктури в Україні пройшло шлях від розрізнених галузевих актів до системного закону. Базовим нормативним актом є Закон України «Про критичну інфраструктуру» від 16.11.2021 р. № 1882-IX, який визначив критичну інфраструктуру як сукупність об'єктів, порушення функціонування яких загрожує національній безпеці, економіці або довкіллю, встановив рівні управління національною системою захисту критичної інфраструктури та запровадив категоризацію об'єктів критичності [12]. Закон набув чинності 15.12.2021 р., водночас його оперативна дія розпочалася з 15.06.2022 р., тобто в умовах повномасштабного вторгнення, що позначилося на перших етапах його впровадження.

Ключовим інструментом реалізації Закону є Реєстр об'єктів критичної інфраструктури, Порядок ведення якого затверджено постановою Кабінету Міністрів України від 28.04.2023 р. № 415 [13]. Держателем та адміністратором Реєстру визначено Державну службу спеціального зв'язку та захисту інформації України як уповноважений орган у сфері захисту критичної інфраструктури. Доповненням системи є Національний план захисту та забезпечення безпеки і стійкості критичної інфраструктури, затверджений розпорядженням Кабінету Міністрів України від 19.09.2023 р. № 825-р [14].

Окремим етапом гармонізації є ухвалення Закону України від 27.03.2025 р. №4336-IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» [15]. Закон передбачає розбудову національної, галузевих та регіональних команд реагування на кіберінциденти з урахуванням підходів, визначених директивою NIS2, запроваджує в державних органах і на об'єктах критичної інфраструктури штатні посади фахівців з кібербезпеки, стандартизує криптографічний та технічний захист інформації, а також систему оцінювання рівня кіберзахисту [15; 16]. Ухвалення цього закону було умовою виконання Плану України для Ukraine Facility [2; 16].

Стратегічний рівень регулювання представлений Стратегією кібербезпеки України, затвердженою Указом Президента України від 26.08.2021 р. №447/2021 на період до 2025 р. [17]. Аналітичне узагальнення результатів її реалізації свідчить про часткове виконання поставлених завдань, зокрема щодо формування переліку об'єктів критичної інформаційної інфраструктури та розвитку цифрової грамотності населення. Бюджетне забезпечення відповідних заходів на завершальний рік дії Стратегії залишалося обмеженим порівняно з масштабом визначених завдань [18].

Правовою основою кіберстійкості в Європейському Союзі є дві директиви, ухвалені одночасно 14 грудня 2022 р.: Директива (ЄС) 2022/2555 про заходи для забезпечення високого спільного рівня кібербезпеки в Союзі (NIS2) та Директива (ЄС) 2022/2557 про стійкість критичних суб'єктів (CER) [19; 20]. Обидві директиви підлягали транспозиції державами-членами до національного законодавства до 17 жовтня 2024 р.

NIS2 встановлює обов'язкові заходи з управління кіберризиками для «істотних» та «важливих» суб'єктів у вісімнадцяти секторах – від енергетики й транспорту до публічного управління та цифрової інфраструктури, – включно з обов'язковим повідомленням про інциденти у визначені строки [19; 21]. CER, своєю чергою, зосереджена на фізичній та операційній стійкості критичних суб'єктів до широкого спектра загроз – природних катастроф, техногенних аварій, терористичних актів, саботажу, – і передбачає ухвалення кожною державою-членом національної стратегії підвищення стійкості критичних суб'єктів [20].

Порівняльний аналіз стану транспозиції засвідчує суттєву нерівномірність цього процесу в межах Європейського Союзу: на встановлений термін вимоги виконала лише незначна частина держав-членів, після чого Європейська Комісія відкрила процедури порушення щодо переважної більшості з них [10; 11]. Станом на середину 2026 р. транспозицію NIS2 завершили близько чотирьох п'ятих держав-членів, тоді як частина країн залишалася серед відстаючих і отримала вмотивовані висновки Комісії, а окремі справи було передано до Суду Європейського Союзу [22]. Зазначені дані слугують важливим орієнтиром для оцінювання темпів гармонізації в Україні, оскільки засвідчують, що узгодження національного законодавства з правом ЄС у сфері

кібербезпеки є довготривалим і ресурсомістким процесом навіть для країн із розвинутою інституційною спроможністю.

Дані урядової команди реагування на комп'ютерні надзвичайні події (CERT-UA), що функціонує у складі Державного центру кіберзахисту Держспецзв'язку, свідчать про стійке зростання інтенсивності кібератак упродовж останніх років. У 2023 р. опрацьовано 2541 кіберінцидент, у 2024 р. – 4315, що становить приріст на 69,8 % [23]. У другому півріччі 2024 р. кількість зафіксованих кібератак зросла на 48 % порівняно з першим півріччям, а загалом за рік – приблизно на 70 % [24; 25]. У 2025 р. кількість опрацьованих кіберінцидентів становила близько 6000, що на 37 % більше, ніж роком раніше [26].

Структура цілей кібератак у 2025 р. свідчить про стійку концентрацію на суб'єктах публічного сектору: найбільша частка інцидентів припадала на органи місцевої влади (35,7 % від загальної кількості, порівняно з 31,8 % роком раніше), урядові організації (19,7 %), сектор безпеки й оборони (17,5 %) та енергетичний сектор (4,7 %) [26; 27]. Водночас кількість інцидентів критичного та високого рівнів у другому півріччі 2024 р. скоротилася приблизно на три чверті порівняно з першим півріччям, тоді як кількість інцидентів, пов'язаних із розповсюдженням шкідливого програмного забезпечення, та підтверджених фактів зараження суттєво зросла. Ця тенденція свідчить про перехід до менш точкових, але більш чисельних кампаній кібератак.

Одним із інцидентів досліджуваного періоду, що мав системний вплив на функціонування державних інформаційних систем, стала кібератака кінця 2024 р. на реєстри Міністерства юстиції України, яка призвела до тимчасового припинення роботи низки ключових державних реєстрів і ускладнила надання пов'язаних із ними адміністративних та інших публічних послуг. Цей інцидент засвідчив залежність надання публічних послуг від кіберстійкості окремих інформаційних систем і вплинув на прискорення ухвалення Закону № 4336-IX.

Формування Реєстру об'єктів критичної інфраструктури розпочалося у 2023 р. відповідно до постанови Кабінету Міністрів України № 415. Держателем Реєстру визначено Держспецзв'язку, секторальні органи подають відомості про об'єкти I та II категорій критичності на погодження уповноваженому органу [13]. Станом на початок 2026 р. загальна кількість об'єктів у Реєстрі перевищила 4600, з яких значну частину внесено протягом 2025 р.; за цей самий період погоджено понад тисячу паспортів безпеки – документів, обов'язкових для об'єктів I та II категорій критичності [28]. Наведена динаміка свідчить про прискорення наповнення Реєстру порівняно з початковими роками його формування, коли основна увага приділялася розробленню методології категоризації.

Водночас Реєстр не є публічним документом: доступ до відомостей, що в ньому містяться, обмежений уповноваженими співробітниками Держспецзв'язку та посадовими особами суб'єктів національної системи захисту критичної інфраструктури. З управлінського погляду це створює двоїсту ситуацію: закритість Реєстру обумовлена безпековими міркуваннями воєнного часу, однак ускладнює незалежну оцінку повноти категоризації та її відповідності переліку секторів, визначеному додатком до директиви CER, який охоплює, зокрема, виробництво, переробку та розподілення харчових продуктів – сектор, що в українській моделі категоризації представлений менш системно.

Технологічне посилення засобів кіберзахисту супроводжується паралельною еволюцією методів соціальної інженерії – сукупності прийомів психологічного впливу, спрямованих на спонукання особи до розкриття конфіденційної інформації або вчинення дій, що створюють умови для несанкціонованого доступу до інформаційних систем. На відміну від атак, орієнтованих на технічні вразливості, соціальна інженерія використовує як об'єкт впливу людину – учасника інформаційних відносин, – що зумовлює її стійку ефективність незалежно від рівня технічної захищеності системи.

Аналітичні матеріали профільного органу у сфері кіберзахисту фіксують ускладнення прийомів соціальної інженерії: від класичних форм, як-от фішинг, вішинг і смішинг, до сценаріїв, що поєднують психологічний тиск, імітацію офіційних комунікацій та використання технологій штучного інтелекту для створення правдоподібних фальшивих матеріалів [37]. Це зумовлює потребу

розглядати підготовку персоналу до розпізнавання прийомів соціальної інженерії як самостійний, невід'ємний складник кадрового механізму гармонізації національної системи кіберстійкості поряд із суто технічними заходами захисту.

Закон № 4336-IX встановлює єдину координаційну рамку для суб'єктів забезпечення кібербезпеки, замінюючи попередні, менш комплексні нормативні підходи до цього питання [15]. До складу національної системи реагування на кіберінциденти передбачено включення CERT-UA, галузевих та регіональних команд реагування, що утворюються органами державної влади або місцевого самоврядування, а також, за окремою процедурою, приватних команд реагування [16; 29]. Закон запроваджує обов'язкове формування підрозділів (фахівців) з кіберзахисту в державних установах, які працюють із чутливою інформацією, стандартизує криптографічний і технічний захист інформації, протидію технічним розвідкам, а також систему оцінювання стану кіберзахисту [15; 29].

Практика впровадження реформи засвідчує наявність інституційних дискусій щодо розподілу повноважень між координаційним органом та іншими суб'єктами сектору безпеки й оборони [29]. Це ілюструє типову управлінську дилему гармонізації: вимоги права ЄС передбачають існування єдиного координаційного центру кіберзахисту, тоді як інституційна архітектура сектору безпеки і оборони України історично характеризується функціональною автономією окремих відомств.

Складовою поточного етапу гармонізації є вдосконалення методичного інструментарію оцінювання стану кіберзахисту суб'єктів національної системи захисту критичної інфраструктури. Наказом Адміністрації Держспецзв'язку від 07.08.2026 р. №607 внесено зміни до методичних рекомендацій і форми звіту про результати оцінювання стану кіберзахисту [38; 39]. Оновлена форма передбачає деталізоване відображення кількісних і якісних показників окремо за напрямом виконання вимог законодавства у сфері кіберзахисту та за шістьма функціями кіберзахисту – управлінням, ідентифікацією, забезпеченням захисту, виявленням, реагуванням і відновленням, – з окремим визначенням загального стану кіберзахисту суб'єкта [39].

Змінено також структуру звіту, який відтепер складається з трьох розділів – загальних відомостей, узагальнених результатів оцінювання стану кіберзахисту та рекомендацій і плану дій, – за результатами чого формується загальний висновок щодо стану кіберзахисту суб'єкта. У розділі рекомендацій передбачено визначення пріоритетності узагальнених рекомендацій за критичними напрямками, встановленими за результатами оцінювання. Наведені зміни методичного забезпечення відповідають логіці запропонованої в цьому дослідженні моделі гармонізації, оскільки переводять оцінювання стану кіберзахисту з площини формальної констатації відповідності до площини структурованого, функціонально диференційованого й орієнтованого на подальші управлінські дії аналізу.

Кадрова спроможність є одним із обмежувальних чинників гармонізації. За оцінками фахівців галузі, дефіцит кадрів у сфері захисту інформації та кібербезпеки в Україні є значним і, за окремими оцінками, сягає близько 100 тис. фахівців [30]. У відповідь здійснюється реформування системи професійної підготовки: до класифікатора професій внесено новий перелік професій у сфері кібербезпеки, затверджено відповідні професійні стандарти [31]. Запроваджено також платформу для підготовки керівників і фахівців з кіберзахисту державного сектору [32; 33] – захід, безпосередньо пов'язаний із запровадженням посади фахівця з кібербезпеки Законом № 4336-IX [33].

Фінансовий вимір гармонізації залишається слабким місцем: бюджетне забезпечення заходів Стратегії кібербезпеки на завершальний 2025 р. становило менше 0,5 млрд грн [18], що є незіставно малою сумою порівняно з масштабом завдань – розбудовою галузевих команд реагування у щонайменше 18 секторах критичної інфраструктури, впровадженням систем моніторингу для понад 4600 об'єктів Реєстру ОКІ та підготовкою десятків тисяч фахівців. Це змушує розглядати фінансування гармонізації не як разову витрату на ухвалення законів, а як довгострокову інвестиційну програму, порівнянню за логікою з фінансуванням Ukraine Facility.

Гармонізація системи кіберстійкості критичної інфраструктури є складовою ширшого процесу приведення законодавства України у відповідність до права Європейського Союзу в рамках

вступних переговорів. За результатами самостійного скринінгу, проведеного Урядом України у 2023 р., встановлено необхідність повної або часткової імплементації значного масиву актів права ЄС [34]. Роз'яснювальна зустріч за розділом «Цифрова трансформація та медіа», що охоплює й питання кібербезпеки, відбулася у квітні 2024 р. в межах офіційного скринінгового процесу [35]. Перемовини організовано в шести тематичних кластерах, перший з яких, що охоплює верховенство права та реформу державного управління, відкривається першим і закривається останнім, а темпи його проходження значною мірою визначають загальну динаміку вступного процесу [36].

Гармонізація кібербезпекового законодавства безпосередньо пов'язана з фінансовою підтримкою в межах програми Ukraine Facility, надання якої обумовлене виконанням визначених індикаторів Плану України, одним з яких було ухвалення Закону № 4336-IX [1; 2; 16]. Таким чином, кіберстійкість критичної інфраструктури набуває значення не лише безпекового питання, а й індикатора інституційної готовності України до членства в Європейському Союзі.

На основі проведеного аналізу пропонується модель, яка інтегрує п'ять взаємопов'язаних механізмів гармонізації (табл. 1).

Таблиця 1

Модель гармонізації національної системи кіберстійкості критичної інфраструктури України з вимогами ЄС

Механізм	Основний зміст	Очікуваний результат
Правовий	транспозиція норм NIS2 і CER, усунення колізій між законами	відповідність <i>acquis</i> ЄС у сфері кібербезпеки
Інституційний	єдина система реагування, галузеві та регіональні CSIRT	скоординоване реагування на інциденти
Кадровий	професійні стандарти, підготовка CISO, кваліфікаційні центри	подолання дефіциту фахівців
Фінансовий	бюджетування захисту OKI, узгодження з індикаторами Ukraine Facility	стале фінансування реформи
Технологічний	наповнення Реєстру OKI, системи моніторингу та раннього попередження	повнота обліку та швидкість виявлення загроз

[Джерело: сформовано авторами].

Принциповою особливістю запропонованої моделі є розгляд гармонізації не як одноразового акту транспозиції норм, а як циклічного управлінського процесу: скринінг відповідності, усунення прогалин, інституційна розбудова, кадрове забезпечення, фінансування, моніторинг результату та повторний скринінг. Застосування такого циклу до сфери кіберстійкості критичної інфраструктури дає змогу уникнути ситуації, за якої формальна відповідність тексту закону директиві ЄС не супроводжується реальною спроможністю системи протидіяти кіберзагрозам.

Для практичного застосування моделі на рівні окремого сектору критичної інфраструктури або суб'єкта національної системи захисту пропонується Індекс готовності до гармонізації (ІГГ):

$$\text{ІГГ} = 0,25\Gamma_1 + 0,20\Gamma_2 + 0,20\Gamma_3 + 0,20\Gamma_4 + 0,15\Gamma_5,$$

де Γ_1 – відповідність внутрішніх регламентів вимогам NIS2 щодо управління кіберризиками; Γ_2 – наявність призначеного CISO та функціонуючої команди реагування; Γ_3 – повнота внесення об'єктів до Реєстру OKI та наявність паспортів безпеки; Γ_4 – дотримання строків повідомлення про інциденти (24 години/72 години/1 місяць); Γ_5 – рівень підготовки персоналу з кіберзахисту.

Кожен компонент оцінюється за шкалою 0–100 балів; пропонувано чотири рівні готовності: 0–49 – критично недостатній, 50–69 – базовий, 70–84 – достатній, 85–100 – високий, відповідний вимогам ЄС.

Практична цінність ІГГ полягає в можливості перейти від формальної констатації «закон ухвалено» до вимірювання фактичної готовності конкретного сектору чи об'єкта протистояти кіберзагрозам і взаємодіяти із системами реагування держав-членів ЄС.

Висновки. Проведене дослідження дає підстави розглядати кіберстійкість критичної інфраструктури як комплексну управлінську проблему, розв'язання якої потребує не лише транспозиції норм директив NIS2 і CER, а й розбудови інституційної, кадрової, фінансової та технологічної спроможності системи публічного управління. Динаміка кіберінцидентів в Україні та розвиток обліку об'єктів критичної інфраструктури засвідчують випереджальне зростання масштабу загроз порівняно з темпами інституційної розбудови, а порівняльний аналіз транспозиції директив ЄС у державах-членах підтверджує, що гармонізація є тривалим і нерівномірним процесом навіть для країн із розвиненою інституційною спроможністю, унаслідок чого тимчасове відставання України від формальних термінів директив не є ознакою кризи національної системи.

Запропонована в дослідженні модель гармонізації, що поєднує правовий, інституційний, кадровий, фінансовий і технологічний механізми в межах циклічного управлінського процесу, а також розроблений Індекс готовності до гармонізації становлять теоретико-методичну основу для вимірювання фактичної, а не лише формальної відповідності секторів критичної інфраструктури вимогам Європейського Союзу. Перспективним напрямом подальших досліджень є апробація запропонованого індексу на рівні окремих секторів критичної інфраструктури та встановлення статистичного зв'язку між рівнем їхньої готовності й результативністю протидії кіберінцидентам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Ukraine Facility: Рамкова угода щодо фінансування з боку Європейського Союзу. Міністерство економіки України. URL: <https://www.ukrainefacility.me.gov.ua/> (дата звернення: 20.08.2026).
2. Кабінет Міністрів України. План України для Ukraine Facility. URL: <https://eu-ua.kmu.gov.ua/> (дата звернення: 20.08.2026).
3. Костюченко Я. М. Співпраця України та ЄС у сфері кібербезпеки: механізми боротьби з кіберзлочинністю. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. URL: <https://reicst.com.ua/pmtl/article/download/2025-15-01-10/2025-15-01-10/1613> (дата звернення: 20.08.2026).
4. Кондратов С.І. Про забезпечення координації дії, взаємодії та обміну інформацією при створенні державної системи захисту критичної інфраструктури. Київ: НІСД. URL: <https://niss.gov.ua/> (дата звернення: 20.08.2026).
5. Мельничук О. В. Управління критичною інфраструктурою держави: базові методи та критерії ідентифікації об'єктів. *Державне управління та місцеве самоврядування*. Вип. 3 (42). 2019. С. 13–27. DOI: <https://doi.org/10.35432/1993-8330appa1812020201816/>.
6. Ruohonen J. A Systematic Literature Review on the NIS2 Directive. University of Southern Denmark. URL: <https://arxiv.org/abs/2412.08084> (дата звернення: 20.08.2026).
7. Vandezande, N. Cybersecurity in the EU: How the NIS2-Directive Stacks up against Its Predecessor. *Computer Law & Security Review*, 52, Article 105890. URL: <https://www.sciencedirect.com/science/article/abs/pii/S0267364923001000> (дата звернення: 20.08.2026).
8. Wavestone. CER Directive: where does Europe stand on critical infrastructure resilience? Електронний URL: <https://www.wavestone.com/en/insight/critical-infrastructure-cybersecurity-cer-directive/> (дата звернення: 20.08.2026).
9. OpenKRITIS. EU NIS2 and CER Directives for European Critical Infrastructures. URL: <https://www.openkritis.de/eu/eu-nis-2-rce-directive.html> (дата звернення: 20.08.2026).
10. ECSO. NIS2 Directive Transposition Tracker. URL: <https://ecs-org.eu/policy/nis2-directive-transposition-tracker/> (дата звернення: 20.08.2026).
11. European Commission. The Commission calls on 23 Member States to fully transpose the NIS2 Directive. URL: <https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive> (дата звернення: 20.08.2026).
12. Закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20> (дата звернення: 20.08.2026).
13. Кабінет Міністрів України. Постанова від 28.04.2023 № 415 «Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього». URL: <https://zakon.rada.gov.ua/laws/show/415-2023-p> (дата звернення: 20.08.2026).
14. Кабінет Міністрів України. Розпорядження від 19.09.2023 № 825-р «Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури». URL: <https://www.kmu.gov.ua/> (дата звернення: 20.08.2026).
15. Закон України від 27.03.2025 № 4336-IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури». URL: <https://zakon.rada.gov.ua/laws/show/4336-IX> (дата звернення: 20.08.2026).
16. Державна служба спеціального зв'язку та захисту інформації України. Президент України Володимир Зеленський підписав Закон № 4336-IX про кіберзахист державних інформаційних ресурсів. URL: <https://cip.gov.ua/ua/news/>

- prezident-ukrayini-volodimir-zelenskii-pidpisav-zakon-4336-ix-pro-kiberzakhist-derzhavnikh-informaciinikh-resursiv (дата звернення: 20.08.2026).
17. Указ Президента України від 26.08.2021 № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»». URL: <https://zakon.rada.gov.ua/laws/show/447/2021> (дата звернення: 20.08.2026).
 18. dev.ua. Під заходи зі «Стратегії кібербезпеки» від Держспецзв'язку на 2025 рік зарезервовано в бюджеті трохи менше ніж 0,5 млрд грн. URL: <https://dev.ua/news/strategii-kiberbezpeky-2025> (дата звернення: 20.08.2026).
 19. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive). URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng> (дата звернення: 20.08.2026).
 20. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive). URL: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng> (дата звернення: 20.08.2026).
 21. Softline Defense. NIS2 для українських операторів КІІ: чек-лист. URL: <https://softline.org.ua/kb-nis2-chek-list-kii/> (дата звернення: 20.08.2026).
 22. ISMS Copilot. NIS 2 transposition tracker: national status in all 27 EU Member States. URL: <https://www.ismscopilot.com/learn/nis-2-transposition-tracker> (дата звернення: 20.08.2026).
 23. MediaSapiens. Урядові кіберфахівці за 2024 рік опрацювали 4315 кіберінцидентів. URL: <https://ms.detector.media/kiberbezpeka/post/37156/2025-01-08-uryadovi-kiberfakhivtsi-za-2024-rik-opratsyuvay-4315-kiberintsydentiv/> (дата звернення: 20.08.2026).
 24. cybersec.net.ua. В CERT-UA підготували аналітичний звіт «російські кібероперації» H2'2024. URL: <https://cybersec.net.ua/statti/868-v-cert-ua-pidhotuvaly-analitychnyi-zvit-rosiiski-kiberoperatsii-h22024-kilkist-kiberintsydentiv-zroslo-na-48protsent.html> (дата звернення: 20.08.2026).
 25. AIN.ua. Україна зазнала 2 576 російських кібератак у другому півріччі 2024-го – звіт CERT-UA. URL: <https://ain.ua/2025/04/30/kiberataki-na-ukrayinu-u-drugomu-pivricchi-2024/> (дата звернення: 20.08.2026).
 26. poda.gov.ua. Топік CERT-UA опрацювала майже 6000 кіберінцидентів: кількість ворожих атак зросла на 37 %. URL: <https://poda.gov.ua/news/251006> (дата звернення: 20.08.2026).
 27. Interfax-Ukraine. CERT-UA зафіксувала нові кібератаки на державні організації під виглядом сертифікатів від платформи Prometheus. URL: <https://interfax.com.ua/news/general/1170034.html> (дата звернення: 20.08.2026).
 28. Державна служба спеціального зв'язку та захисту інформації України. До Реєстру об'єктів критичної інфраструктури вже внесено відомості про понад 4600 об'єктів. URL: <https://ns-gromada.gov.ua/news/1768407787/> (дата звернення: 20.08.2026).
 29. AIN.ua. В Україні реформують кіберзахист після атаки на реєстри. URL: <https://ain.ua/2025/03/31/vr-uxvalila-zakonoprojekt-iaiki-reformuje-kiberzaxist/> (дата звернення: 20.08.2026).
 30. UKR.NET. Названа кількість фахівців з кібербезпеки, яких бракує Україні. URL: <https://www.ukr.net/news/details/society/110428568.html> (дата звернення: 20.08.2026).
 31. qc.csi.cip.gov.ua. Ставка на освіту: Україна посилює стійкість у кіберпросторі через професійну підготовку. URL: https://qc.csi.cip.gov.ua/uk/posts/stavka_osvita (дата звернення: 20.08.2026).
 32. DOU.ua. В Україні навчатимуть кіберфахівців для державного сектору. URL: <https://dou.ua/lenta/news/cybersecurity-training-in-th-public-sector/> (дата звернення: 20.08.2026).
 33. Кабінет Міністрів України. Мінцифри: Запускаємо CISO Campus – національну платформу підготовки керівників із кібербезпеки. URL: <https://www.kmu.gov.ua/news/mintsyfry-zapuskaiemo-ciso-campus-natsionalnu-platformu-pidhotovky-kerivnykiv-iz-kiberbezpeky> (дата звернення: 20.08.2026).
 34. Урядовий портал європейської інтеграції. Переговори про вступ України до ЄС: повний гід у 12 питаннях. URL: <https://eu-ua.kmu.gov.ua/en/news/peregovory-pro-vstup-ukrayiny-do-yes-povnyj-gid-u-12-pytannyah-i-10-mifah-2/> (дата звернення: 20.08.2026).
 35. Міністерство внутрішніх справ України. Переговори про вступ до ЄС. URL: <https://mvs.gov.ua/jeuropeiska-integraciia/peregovori-pro-vstup-do-jes-1> (дата звернення: 20.08.2026).
 36. MediaSapiens. Шість кластерів і одна проблема: як відбуваються переговори про вступ України до ЄС. URL: <https://ms.detector.media/trendi/post/38298/2025-08-10-shist-klasteriv-i-odna-problema-yak-vidbuvayutsya-peregovory-pro-vstup-ukrainy-do-ies/> (дата звернення: 20.08.2026).
 37. Державна служба спеціального зв'язку та захисту інформації України. Зламати людину, а не систему: як еволюціонувала соціальна інженерія і як не потрапити у пастку. URL: <https://cip.gov.ua/ua/news/zlamati-lyudinu-a-ne-sistemu-yak-evolyucionovala-socialna-inzheneriya-i-yak-ne-potrapiti-u-pastku> (дата звернення: 20.08.2026).
 38. Державна служба спеціального зв'язку та захисту інформації України. Внесено зміни до методичних рекомендацій і форми звіту про результати оцінювання стану кіберзахисту. URL: <https://cip.gov.ua/ua/news/vneseno-zmini-do-metodichnikh-rekomendacii-i-formi-zvitu-pro-rezultati-ocinyuvannya-stanu-kiberzakhistu> (дата звернення: 20.08.2026).
 39. Адміністрація Держспецзв'язку. Наказ від 07.08.2026 № 607 «Про внесення змін до наказу Адміністрації Держспецзв'язку від 16.04.2026 № 285». URL: <https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-07-08-2026-607-pro-vnesennya-zmin-do-nakazu-administraciyi-derzhspeczv-yazku-vid-16-04-2026-285> (дата звернення: 20.08.2026).

REFERENCES

1. Ministerstvo ekonomiky Ukrainy. (2024). Ukraine Facility: Ramkova uhoda shchodo finansuvannia z boku Yevropeiskoho Soiuzu [Ukraine Facility: Framework Agreement on financing from the European Union]. www.ukrainefacility.me.gov.ua. Retrieved from <https://www.ukrainefacility.me.gov.ua/> [in Ukrainian].
2. Kabinet Ministriv Ukrainy. (2024). Plan Ukrainy dlia Ukraine Facility [Ukraine Plan for the Ukraine Facility]. eu-ua.kmu.gov.ua. Retrieved from <https://eu-ua.kmu.gov.ua/> [in Ukrainian].
3. Kostiuchenko, Ya.M. (2025). Spivpratsia Ukrainy ta YeS u sferi kiberbezpeky: mekhanizmy borotby z kiberzlochynnistiu [Cooperation between Ukraine and the EU in the field of cybersecurity: mechanisms for combating cybercrime]. *Problemy suchasnykh transformatsii. Seriya: pravo, publichne upravlinnia ta administruvannia – Issues in Contemporary Transformations. Series: Law, Public Management, and Administration*. Retrieved from <https://reicst.com.ua/pmtl/article/download/2025-15-01-10/2025-15-01-10/1613> [in Ukrainian].
4. Kondratov, S.I. (2018). *Pro zabezpechennia koordynatsii dii, vzaємodii ta obminu informatsiieu pry stvorenni derzhavnoi systemy zakhystu krytychnoi infrastruktury* [On ensuring the coordination of actions, interaction and information exchange in the creation of the state system for the protection of critical infrastructure]. Kyiv: NISD. Retrieved from <https://niss.gov.ua/> [in Ukrainian].
5. Melnychuk, O.V. (2019). Upravlinnia krytychnoiu infrastrukturoiu derzhavy: bazovi metody ta kryterii identyfikatsii ob'ektiv [Management of the state's critical infrastructure: basic methods and criteria for identifying objects]. *Derzhavne upravlinnia ta mistseve samovriaduvannia – Public Administration and Local Self-Government*, 3 (42), 13–27. DOI: <https://doi.org/10.35432/1993-8330appa1812020201816> [in Ukrainian].
6. Ruohonen, J. (2024). A Systematic Literature Review on the NIS2 Directive. University of Southern Denmark. Retrieved from <https://arxiv.org/abs/2412.08084> [in English].
7. Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-Directive Stacks up against Its Predecessor. *Computer Law & Security Review*, 52, Article 105890. Retrieved from <https://www.sciencedirect.com/science/article/abs/pii/S0267364923001000> [in English].
8. Wavestone. (2026). *CER Directive: where does Europe stand on critical infrastructure resilience?* Retrieved from <https://www.wavestone.com/en/insight/critical-infrastructure-cybersecurity-cer-directive/> [in English].
9. OpenKRITIS. (2024). *EU NIS2 and CER Directives for European Critical Infrastructures*. Retrieved from <https://www.openkritis.de/eu/eu-nis-2-rce-directive.html> [in English].
10. ECSO. (2026). *NIS2 Directive Transposition Tracker*. Retrieved from <https://ecs-org.eu/policy/nis2-directive-transposition-tracker/> [in English].
11. European Commission. (2024). *The Commission calls on 23 Member States to fully transpose the NIS2 Directive*. Retrieved from <https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive> [in English].
12. Pro krytychnu infrastrukturu: Zakon Ukrainy No 1882-IX vid 16 lystopada 2021 r. [On Critical Infrastructure: Law of Ukraine No. 1882-IX from November 16, 2021]. zakon.rada.gov.ua. Retrieved from <https://zakon.rada.gov.ua/laws/show/1882-20> [in Ukrainian].
13. Kabinet Ministriv Ukrainy. (2023). Postanova vid 28 kvitnia 2023 r. No 415 Pro zatverdzhennia Poriadku vedennia Reiestru ob'ektiv krytychnoi infrastruktury, vkluchennia takykh ob'ektiv do Reiestru, dostupu ta nadannia informatsii z noho [Resolution No. 415 of April 28, 2023 On approval of the Procedure for maintaining the Register of Critical Infrastructure Objects]. zakon.rada.gov.ua. Retrieved from <https://zakon.rada.gov.ua/laws/show/415-2023-p> [in Ukrainian].
14. Kabinet Ministriv Ukrainy. (2023). Rozporiadzhennia vid 19 veresnia 2023 r. No 825-r Pro zatverdzhennia Natsionalnoho planu zakhystu ta zabezpechennia bezpeky ta stikosti krytychnoi infrastruktury [Order No. 825-r of September 19, 2023 On approval of the National Plan for the protection and resilience of critical infrastructure]. kmu.gov.ua. Retrieved from <https://www.kmu.gov.ua/> [in Ukrainian].
15. Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo zakhystu informatsii ta kiberzakhystu derzhavnykh informatsiinykh resursiv, ob'ektiv krytychnoi informatsiinoi infrastruktury: Zakon Ukrainy No 4336-IX vid 27 bereznia 2025 r. [On Amendments to Certain Laws of Ukraine Concerning Information Protection and Cyber Defence of State Information Resources and Critical Information Infrastructure Objects: Law of Ukraine No 4336-IX dated March 27, 2025]. zakon.rada.gov.ua. Retrieved from <https://zakon.rada.gov.ua/laws/show/4336-IX> [in Ukrainian].
16. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. (2025). Prezydent Ukrainy Volodymyr Zelenskyi pidpysav Zakon No 4336-IX pro kiberzakhyst derzhavnykh informatsiinykh resursiv [President of Ukraine signed Law No. 4336-IX on cyber defence of state information resources]. cip.gov.ua. Retrieved from <https://cip.gov.ua/ua/news/prezydent-ukrayini-volodimir-zelenskii-pidpisav-zakon-4336-ix-pro-kiberzakhyst-derzhavnykh-informatsiinykh-resursiv> [in Ukrainian].
17. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku Pro Stratehiiu kiberbezpeky Ukrainy: Ukaz Prezydenta Ukrainy No 447/2021 vid 26 serpnia 2021 r. [On the Decision of the National Security and Defence Council of Ukraine of May 14, 2021 On the Cybersecurity Strategy of Ukraine: Decree of the President of Ukraine No. 447/2021 dated August 26, 2021]. zakon.rada.gov.ua. Retrieved from <https://zakon.rada.gov.ua/laws/show/447/2021> [in Ukrainian].

18. dev.ua. (2025). Pid zakhody zi Stratehii kiberbezpeky vid Derzhspetssviazku na 2025 rik zarezerovano v biudzheti trokhy menshe nizh 0,5 mlrd hrn [Just under UAH 0.5 billion reserved in the budget for 2025 Cybersecurity Strategy measures]. *dev.ua*. Retrieved from <https://dev.ua/news/strategii-kiberbezpeky-2025> [in Ukrainian].
19. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). (2022). *eur-lex.europa.eu*. Retrieved from <https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng> [in EU].
20. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive). (2022). Retrieved from <https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng> [in English].
21. Softline Defense. (2025). NIS2 dlia ukrainskykh operatoriv KII: chek-lyst [NIS2 for Ukrainian critical information infrastructure operators: a checklist]. *softline.org.ua*. Retrieved from <https://softline.org.ua/kb-nis2-chek-list-kii/> [in Ukrainian].
22. ISMS Copilot. (2026). NIS 2 transposition tracker: national status in all 27 EU Member States. *www.ismscopilot.com*. Retrieved from <https://www.ismscopilot.com/learn/nis-2-transposition-tracker> [in EU].
23. MediaSapiens. (2025). Uriadovi kiberfakhivtsi za 2024 rik opratsiuvaly 4315 kiberintsydentiv [Government cyber specialists processed 4,315 cyber incidents in 2024]. *ms.detector.media*. Retrieved from <https://ms.detector.media/kiberbezpeka/post/37156/2025-01-08-uryadovi-kiberfakhivtsi-za-2024-rik-opratsyuvay-4315-kiberintsydentiv/> [in Ukrainian].
24. cybersec.net.ua. (2025). V CERT-UA pidhotuvaly analitychnyi zvit rosiiskii kiberoperatsii H2'2024 [CERT-UA prepared an analytical report Russian cyber operations H2'2024]. *cybersec.net.ua*. Retrieved from <https://cybersec.net.ua/statti/868-v-cert-ua-pidhotuvaly-analitchnyi-zvit-rosiiskii-kiberoperatsii-h2024-kilkist-kiberintsydentiv-zroslo-na-48protsent.html> [in Ukrainian].
25. AIN.ua. (2025). Ukraina zaznala 2 576 rosiiskykh kiberatak u druhomu pivrichchi 2024-ho – zvit CERT-UA [Ukraine suffered 2,576 Russian cyberattacks in the second half of 2024 – CERT-UA report]. *ain.ua*. Retrieved from <https://ain.ua/2025/04/30/kiberataki-na-ukrayinu-u-drugomu-pivricci-2024/> [in Ukrainian].
26. poda.gov.ua. (2025). Torik CERT-UA opratsiuvala maizhe 6000 kiberintsydentiv: kilkist vorozhykh atak zroslo na 37 % [CERT-UA processed almost 6,000 cyber incidents last year: hostile attacks increased by 37 %]. *poda.gov.ua*. Retrieved from <https://poda.gov.ua/news/251006> [in Ukrainian].
27. Interfax-Ukraine. (2026). CERT-UA zafiksuvala novi kiberatomy na derzhavni orhanizatsii pid vyhliadom sertyfikativ vid platformy Prometheus [CERT-UA recorded new cyberattacks on state organisations disguised as Prometheus platform certificates]. *interfax.com.ua*. Retrieved from <https://interfax.com.ua/news/general/1170034.html> [in Ukrainian].
28. Derzhavna sluzhba spetsialnogo zviazku ta zakhystu informatsii Ukrainy. (2026). Do Reiestru obektiv krytychnoi infrastruktury vzhe vneseno vidomosti pro ponad 4600 obektiv [More than 4,600 objects have already been entered into the Register of Critical Infrastructure Objects]. *ns-gromada.gov.ua*. Retrieved from <https://ns-gromada.gov.ua/news/1768407787/> [in Ukrainian].
29. AIN.ua. (2025). V Ukraini reformuiut kiberzakhyst pislia ataky na reiestry [Ukraine reforms cyber defence after the registries attack]. *ain.ua*. Retrieved from <https://ain.ua/2025/03/31/vr-uxvaila-zakonoprojekt-iakii-reformuje-kiberzaxist/> [in Ukrainian].
30. UKR.NET. (2025). Nazvana kilkist fakhivtsiv z kiberbezpeky, yakykh brakuie Ukraini [The number of cybersecurity specialists Ukraine lacks has been named]. *www.ukr.net*. Retrieved from <https://www.ukr.net/news/details/society/110428568.html> [in Ukrainian].
31. qc.csi.cip.gov.ua. (2024). Stavka na osvitu: Ukraina posyliuie stiikist u kiberprostorii cherez profesiinu pidhotovku [Betting on education: Ukraine strengthens cyberspace resilience through professional training]. *qc.csi.cip.gov.ua*. Retrieved from https://qc.csi.cip.gov.ua/uk/posts/stavka_osvita [in Ukrainian].
32. DOU.ua. (2025). V Ukraini navchatymut kiberfakhivtsiv dlia derzhavnogo sektoru [Ukraine to train cyber specialists for the public sector]. *dou.ua*. Retrieved from <https://dou.ua/lenta/news/cybersecurity-training-in-th-public-sector/> [in Ukrainian].
33. Kabinet Ministriv Ukrainy. (2025). Mintsyfry: Zapuskaemo CISO Campus – natsionalnu platformu pidhotovky kerivnykiv iz kiberbezpeky [Ministry of Digital Transformation: Launching CISO Campus – a national platform for training cybersecurity leaders]. *www.kmu.gov.ua*. Retrieved from <https://www.kmu.gov.ua/news/mintsyfry-zapuskaemo-ciso-campus-natsionalnu-platformu-pidhotovky-kerivnykiv-iz-kiberbezpeky> [in Ukrainian].
34. Uriadovyi portal yevropeiskoi intehtatsii. (2025). Perehovory pro vstup Ukrainy do YeS: povnyi hid u 12 pytanniakh [Ukraine's EU accession negotiations: a complete guide in 12 questions]. *www.kmu.gov.ua*. Retrieved from <https://eu-ua.kmu.gov.ua/en/news/peregovory-pro-vstup-ukrayiny-do-yes-povny-gid-u-12-pytannyah-i-10-mifah-2/> [in Ukrainian].
35. Ministerstvo vnutrishnikh sprav Ukrainy. (2024). Perehovory pro vstup do YeS [EU accession negotiations]. *mvs.gov.ua*. Retrieved from <https://mvs.gov.ua/jeuropeiska-integraciia/peregovori-pro-vstup-do-jes-1> [in Ukrainian].
36. MediaSapiens. (2025). Shist klasteriv i odna problema: yak vidbuvauiatsia perehovory pro vstup Ukrainy do YeS [Six clusters and one problem: how Ukraine's EU accession negotiations proceed]. *ms.detector.media*. Retrieved from <https://ms.detector.media/trendi/post/38298/2025-08-10-shist-klasteriv-i-odna-problema-yak-vidbuvauiatsia-peregovory-pro-vstup-ukrainy-do-ies/> [in Ukrainian].
37. Derzhavna sluzhba spetsialnogo zviazku ta zakhystu informatsii Ukrainy. (2026). Zlamaty liudynu, a ne systemu: yak evoliutsionuvala sotsialna inzheneriia i yak ne potrapyty u pastku [Hacking the human, not the system: how social engineering has evolved and how to avoid the trap]. *cip.gov.ua*. Retrieved from <https://cip.gov.ua/ua/news/zlamati-lyudinu-a-ne-sistemu-yak-evolyucionuvala-socialna-inzheneriya-i-yak-ne-potrapiti-u-pastku> [in Ukrainian].

38. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. (2026). Vneseno zminy do metodichnykh rekomendatsii i formy zvituvannia pro rezultaty otsiniuvannia stanu kiberzakhystu [Amendments to the methodological recommendations and the cyber defence assessment report form]. *cip.gov.ua*. Retrieved from <https://cip.gov.ua/ua/news/vneseno-zmini-do-metodichnykh-rekomendatsii-i-formi-zvituvannia-ocinyuvannya- stanu-kiberzakhystu> [in Ukrainian].
39. Pro vnesennia zmin do nakazu Administratsii Derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii Ukrainy vid 16 kvitnia 2026 r. No 285: Nakaz Administratsii Derzhspetszviazku No 607 vid 7 serpnia 2026 r. [On Amendments to Order No. 285 of the Administration of the State Service of Special Communications and Information Protection of Ukraine of April 16, 2026: Order No. 607 dated August 7, 2026]. *cip.gov.ua*. Retrieved from <https://cip.gov.ua/ua/docs/nakaz-administratsii-derzhspetszv-yazku-vid-07-08-2026-607-pro-vnesennia-zmin-do-nakazu-administratsii-derzhspetszv-yazku-vid-16-04-2026-285> [in Ukrainian].

Історія статті / Article history:

Подано до редакції / Submitted to the editorial office (30.08.2026);

Прийнято до друку / Accepted for publication (30.09.2026);

Опубліковано / Published (10.10.2026)