Адміністративне право

УДК 342.951:004.056

DOI https://doi.org/10.5281/zenodo.21297649

Адміністративно-правове регулювання кібербезпеки критичної інформаційної інфраструктури в умовах воєнного стану

А. А. Васильєв

аспірант, ЗВО «Львівський університет бізнесу та права»

https://orcid.org/0009-0000-6413-783X

Я. О. Бакай

аспірант, ЗВО «Львівський університет бізнесу та права»

https://orcid.org/0009-0003-7890-4567

Прийнято: 15.05.2025 | Опубліковано: 30.05.2025

Анотація: У статті досліджено адміністративно-правове регулювання кібербезпеки критичної інформаційної інфраструктури в Україні в умовах воєнного стану станом на квітень 2025 року. Проаналізовано понятєву тріаду «критична інфраструктура – критична інформаційна інфраструктура – об'єкти КІІ» за Законами України № 1882-IX та № 2163-VIII у зіставленні із суб'єктною логікою Директиви (ЄС) 2022/2555 (NIS2), що оперує категоріями essential та important entities у 18 секторах. Встановлено, що об'єктно-орієнтований підхід українського законодавства створює семантичний розрив з європейською моделлю та ускладнює процес гармонізації. Визначено інституційну архітектуру національної системи кібербезпеки, що охоплює Держспецзв'язку, CERT-UA, СБУ, кіберполіцію, Мінцифри та НКЦК при РНБО, та виявлено структурну проблему «координації без координатора» – дублювання компетенцій за

відсутності єдиного оперативного центру відповідальності. Досліджено трансформацію правового режиму кібербезпеки КІІ під впливом воєнного стану, зокрема розширення дискреційних повноважень регуляторів, спрощення процедур реагування та обмеження публічності реєстрів, із констатацією ризику нормалізації надзвичайних повноважень за відсутності механізмів автоматичного згортання. Здійснено порівняльний аналіз української моделі з європейською системою NIS2 та досвідом Естонії і Литви. На підставі аналізу стратегічних кіберінцидентів 2022–2024 років (Industroyer2, атака на «Київстар», злам реєстрів Мін'юсту) доведено ефективність оперативного реагування за одночасної неспроможності адміністративного механізму превентивного дисциплінування операторів КІІ. Сформульовано пропозиції de lege ferenda щодо повної транспозиції NIS2, гармонізації санкційного механізму, створення єдиного оперативного координатора кіберзахисту та впровадження обов'язкового зовнішнього аудиту.

Ключові слова: кібербезпека, критична інформаційна інфраструктура, адміністративно-правове регулювання, воєнний стан, NIS2, CERT-UA, Держспецзв'язку, адміністративна відповідальність.

Administrative-legal regulation of cybersecurity of critical information infrastructure under martial law conditions

A. A. Vasyliev
Postgraduate Student, HEI "Lviv University of Business and Law"
https://orcid.org/0009-0000-6413-783X

Y. O. Bakai
Postgraduate Student, HEI "Lviv University of Business and Law"
https://orcid.org/0009-0003-7890-4567

Abstract: The article examines the administrative-legal regulation of cybersecurity of critical information infrastructure in Ukraine under martial law conditions as of April 2025. The conceptual triad of critical infrastructure, critical information infrastructure, and CII objects under Ukrainian Laws No. 1882-IX and No. 2163-VIII is analysed in comparison with the entity-based logic of Directive (EU) 2022/2555 (NIS2), which operates with the categories of essential and important entities across 18 sectors. It is established that the object-oriented approach of Ukrainian legislation creates a semantic gap with the European model and complicates the harmonisation process. The institutional architecture of the national cybersecurity system encompassing the SSSCIP, CERT-UA, SSU, Cyber Police, Ministry of Digital Transformation, and NCCC under the NSDC is identified, revealing the structural problem of coordination without a coordinator – overlapping competencies in the absence of a single operational accountability centre. The transformation of the CII cybersecurity legal regime under the influence of martial law is explored, including the expansion of regulatory discretionary powers, simplified incident response procedures, and restricted registry publicity, with the stated risk of normalising emergency powers in the absence of automatic sunset mechanisms. A comparative analysis of the Ukrainian model with the European NIS2 system and the experience of Estonia and Lithuania is conducted. Based on the analysis of strategic cyber incidents in 2022–2024 (Industroyer2, the Kyivstar attack, the Ministry of Justice registry breach), the effectiveness of operational response is demonstrated alongside the inability of the administrative mechanism to perform preventive disciplining of CII operators. De lege ferenda proposals are formulated regarding full NIS2 transposition, harmonisation of the sanctions mechanism, creation of a unified operational cyber defence coordinator, and introduction of mandatory external audits.

Keywords: cybersecurity, critical information infrastructure, administrative-legal regulation, martial law, NIS2, CERT-UA, SSSCIP, administrative liability.

Постановка проблеми. Безпрецедентна інтенсивність кібератак на Україну, що за період 2022–2024 років перевищила 11 000 задокументованих інцидентів [32], зробила адміністративно-правове регулювання кібербезпеки критичної інформаційної інфраструктури (далі – КІІ) одним із пріоритетних напрямів адміністративно-правової науки. Три роки повномасштабної війни оголили як переваги, так і системні дисфункції національного механізму кіберзахисту: ефективне оперативне реагування CERT-UA й Держспецзв'язку співіснувало з повною відсутністю адміністративних санкцій за порушення вимог кіберзахисту навіть після стратегічних інцидентів (атака на «Київстар» у грудні 2023 року, злам державних реєстрів Міністерства юстиції у грудні 2024 року) [24, 27]. Водночас ухвалення Закону № 4336-IX від 27 березня 2025 року, що імплементує близько 80 % положень Директиви (ЄС) 2022/2555 (NIS2), засвідчило готовність законодавця до системних змін [3]. Ця реформа відбувається одночасно з продовженням воєнного стану та прискоренням переговорного процесу про вступ до ЄС, що надає проблемі адміністративно-правового забезпечення кібербезпеки КІІ виняткової актуальності – як практичної, так і доктринальної.

Проблема має кілька взаємопов'язаних вимірів. Концептуальний вимір полягає у фрагментації дефініцій «критична інфраструктура», «критична інформаційна інфраструктура» та «об'єкти КІІ», що зумовлює невизначеність адміністративно-правового статусу оператора. Інституційний вимір проявляється у дублюванні компетенцій між Держспецзв'язку, СБУ, кіберполіцією, Мінцифри та НКЦК при РНБО. Санкційний вимір – у мінімальних розмірах штрафів і фактичній незастосовності адміністративної відповідальності до великих операторів КІІ. Воєнний вимір – у ризику нормалізації надзвичайних повноважень після завершення бойових дій. Кожен із цих вимірів потребує окремого наукового осмислення, але саме їхня сукупність визначає унікальність української ситуації: жодна інша європейська держава не

ISSN: 3041-2110

здійснює повномасштабну реформу кібербезпеки в умовах активного збройного конфлікту та одночасного руху до членства в ЄС.

Аналіз останніх досліджень і публікацій. Проблематика адміністративно-правового регулювання кібербезпеки КІІ перебуває на перетині кількох дослідницьких традицій – адміністративного права, інформаційного права, порівняльного правознавства та безпекових студій. Українські дослідники розробляють переважно нормативно-догматичний аспект, тоді як зарубіжні автори зосереджуються на порівняльному та функціональному аналізі.

О. А. Алексеєва дослідила правове забезпечення кібербезпеки об'єктів критичної інфраструктури, акцентувавши увагу на прогалинах нормативного регулювання та необхідності узгодження базових законів [12]. Я. С. Мануілов зосередився на забезпеченні кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни, виокремивши специфіку правового регулювання в період активних бойових дій та роль міжнародного співробітництва [13]. Ю. Третяк здійснила систематизацію суб'єктів адміністративно-правового забезпечення кібербезпеки, запропонувавши їхню класифікацію за функціональним критерієм та визначивши межі компетенції кожного органу [14]. О. І. Скіцько проаналізував нормативно-правове забезпечення кібербезпеки об'єктів критичної інфраструктури, зосередившись на підзаконному рівні регулювання та проблемах імплементації [15].

О. П. Метелев та О. В. Плетньов розглянули протидію впливу на державні електронні інформаційні ресурси та об'єкти критичної інфраструктури в умовах воєнного стану, зафіксувавши трансформацію адміністративних процедур реагування під тиском реальних кіберінцидентів [16]. Г. А. Гончаренко присвятила увагу проблемі визначення та розмежування дефініцій «інформаційна безпека» і «кібербезпека», що має принципове значення для окреслення предмета адміністративно-правового регулювання та усунення термінологічних колізій [17]. К. Р. Корощенко та О. В. Ільченко дослідили

правоохоронні органи як суб'єктів забезпечення кібербезпеки в інформаційному просторі України, визначивши компетенційні межі кіберполіції та СБУ у сфері протидії кіберзлочинності [18].

Зарубіжна література представлена низкою фундаментальних робіт. N. Vandezande порівняв Директиву NIS2 з її попередницею і показав, що нова директива суттєво розширює наглядові повноваження та зміщує модель з реактивної на проактивну для essential entities [19]. S. Schmitz-Berndt та P. G. Chiara здійснили випереджальний аналіз німецького й італійського законодавства про кібербезпеку на відповідність проєкту NIS2, виявивши значний ступінь попередньої гармонізації цих правопорядків [20]. D. D. S. Ferguson дослідив outcome-ефективність вимог NIS2 щодо управління ризиками суб'єктів, доводячи, що ці вимоги мають реальний превентивний ефект лише за наявності дієвої загрози санкції [21]. T. Sievers розглянув розширене коло суб'єктів NIS2 та їхні обов'язки, констатувавши принципово новий рівень адміністративного навантаження для essential та important entities [22]. D. Markopoulou та V. Papakonstantinou дослідили регуляторну рамку захисту критичної інфраструктури від кіберзагроз у секторі охорони здоров'я, продемонструвавши секторальну специфіку імплементації загальних вимог [23].

I. Fyshchuk, M. Trofimenko, T. Tropina та T. Janowski опублікували одне з перших комплексних досліджень управління кібератаками у воєнний час на матеріалі України, встановивши, що проблеми мирного часу (обмежені ресурси, кадрові дефіцити, нечіткі гайдлайни) у воєнний час не зникають, а посилюються [24]. M. N. Schmitt у рамках Українського симпозіуму проаналізував кібератаки з позиції міжнародного права, наголосивши на необхідності чіткого розмежування між антикризовими повноваженнями та системним регулюванням [25]. R. Cormac, C. Walton та D. Van Puyvelde дослідили кібервимір російсько-української війни, зафіксувавши конфігураційні вразливості, що не закриваються жодним обсягом нормативних вимог без зміни архітектурних

ISSN: 3041-2110

рішень [26]. C. Bronk, G. Collins та D. S. Wallach проаналізували інформаційну та кібервійну в Україні з технічної та стратегічної перспектив [27]. L. Maglaras, H. Janicke та M. A. Ferrag систематизували виклики та рішення у сфері кібербезпеки критичних інфраструктур, запропонувавши багаторівневу модель захисту [28]. D. Sharma, S. Reddy та H. Shahid дослідили enforcement gap – розрив між нормативними зобов'язаннями з кібербезпеки та їхнім реальним застосуванням, що є ключовою проблемою й для України [29]. A. Davydiuk та O. Potii підготували для NATO CCDCOE комплексний огляд національного управління кібербезпекою в Україні, деталізувавши інституційну архітектуру та компетенційні межі суб'єктів [30]. Звіт ENISA Threat Landscape 2024 зафіксував, що головним рушієм європейського кіберландшафту за липень 2023 – червень 2024 року була саме війна Росії проти України [31].

Виділення невирішених раніше частин загальної проблеми. Попри значний обсяг досліджень, поза увагою залишається комплексний аналіз адміністративно-правового регулювання кібербезпеки КІІ саме в умовах воєнного стану з одночасним урахуванням трьох аспектів: інституційної архітектури, санкційного механізму та вимог NIS2. Більшість українських робіт зосереджені на описі нормативної бази, тоді як зарубіжні дослідження не враховують специфіку українського воєнного досвіду. Потребу у синтезі цих підходів і покликана задовольнити ця стаття.

Формулювання цілей статті. Метою статті є комплексний аналіз адміністративно-правового регулювання кібербезпеки критичної інформаційної інфраструктури в Україні в умовах воєнного стану станом на квітень 2025 року. Для досягнення цієї мети передбачено: розмежувати понятєвий апарат КІ/КІІ за національним та європейським правом; дослідити інституційну архітектуру суб'єктів кібербезпеки та виявити компетенційні колізії; оцінити вплив воєнного стану на адміністративно-правовий режим кіберзахисту КІІ; здійснити порівняльний аналіз української моделі з Директивою NIS2 та досвідом Естонії

і Литви; проаналізувати ефективність реагування на стратегічні кіберінциденти 2022–2024 років; сформулювати пропозиції de lege ferenda щодо гармонізації з acquis ЄС.

Виклад основного матеріалу. Будь-яка спроба осмислити адміністративно-правове регулювання кібербезпеки КІІ неминуче наштовхується на питання про межі самого об'єкта регулювання, і саме тут виявляється перша, можливо найглибша, дисфункція українського правопорядку. Закон «Про критичну інфраструктуру» № 1882-IX від 16 листопада 2021 року оперує поняттям «об'єкти критичної інфраструктури» як систем, важливих для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [1]. Закон «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року звужує цей широкий контур до критичної інформаційної інфраструктури, розуміючи під нею комунікаційні та технологічні системи, кібератака на які безпосередньо вплине на сталу роботу об'єкта КІ [2]. Директива (ЄС) 2022/2555 (NIS2) рухається принципово іншим шляхом: вона взагалі не оперує поняттям «критична інформаційна інфраструктура», а будує регуляторний каркас навколо суб'єктної логіки essential entities та important entities, ідентифікованих за об'єктивним size-cap критерієм у 18 секторах [10]. Якщо спробувати дати цій ситуації телеологічне тлумачення, то виявиться, що NIS2 робить юридичний статус суб'єкта похідним від об'єктивних економічних показників і тим самим мінімізує дискрецію регулятора, тоді як українська модель залишає його результатом адміністративного рішення секторального органу, зберігаючи простір для регуляторного арбітражу [10, 12, 17, 19]. Це дає підстави стверджувати, що при формальному перенесенні європейських норм у національне право без повної ревізії базових законів виникне семантичний розрив: український регулятор і

 ISSN: 3041-2110

далі оперуватиме об'єктами, а європейський наглядовий механізм очікуватиме звітності від суб'єктів.

Наслідки цієї понятійної асиметрії проявляються, зокрема, в архітектурі реєстрів. Секторальні органи разом з операторами категоризують об'єкти КІ за рівнями критичності I–IV відповідно до постанови Кабінету Міністрів № 1109 від 9 жовтня 2020 року, тоді як Адміністрація Держспецзв'язку на підставі постанови № 943 від 9 жовтня 2020 року відносить комунікаційні та технологічні системи до об'єктів КІІ і вносить їх до окремого Державного реєстру [8, 9]. Існування двох паралельних реєстрів (реєстру КІ та реєстру КІІ) створює для оператора подвійне адміністративне навантаження і розмиває критерії включення, що О. А. Алексеєва та О. І. Скіцько концептуалізують як розмитість дефінітивного простору [12, 15]. В умовах воєнного стану обидва реєстри отримали обмежений доступ, що унеможливлює зовнішній контроль повноти охоплення; станом на квітень 2025 року публічна верифікація переліку об'єктів КІІ залишається неможливою [30]. Видається обґрунтованим припустити, що доки ці два реєстри існуватимуть паралельно з різними критеріями формування, дотоді проблема конкуренції секторальних і центральних регуляторів за повноваження категоризації не зникне, а лише набуватиме нових форм із кожною хвилею законодавчих змін. Найгостріше ця різниця проявляється в обсязі обов'язків: за NIS2 essential entity автоматично потрапляє під ex-ante нагляд із регулярними аудитами, сканування вразливостей та виїзними інспекціями, тоді як в Україні аналогічний обсяг превентивного контролю прив'язаний виключно до приналежності об'єкта до КІІ I категорії і деталізований лише постановою Кабінету Міністрів № 367 від 1 квітня 2025 року [3, 22].

Від понятійних засад аналіз закономірно переміщується до інституційної площини, бо навіть ідеально сформульована дефініція не працює без суб'єкта, здатного забезпечити її застосування. Національна система кібербезпеки України формально включає шістьох ключових суб'єктів, кожен із яких має

ISSN: 3041-2110

власну правову підставу існування та окремий мандат: Держспецзв'язку з підпорядкованим Державним центром кіберзахисту і CERT-UA, СБУ з Ситуаційним центром забезпечення кібербезпеки, Департамент кіберполіції Національної поліції, Міністерство цифрової трансформації, Національний банк України (для фінансового сектора) та Національний координаційний центр кібербезпеки при РНБО [6, 14, 18, 30]. Закон № 4336-IX від 27 березня 2025 року додав до цієї структури мережу галузевих CSIRT і обов'язкову посаду керівника з кіберзахисту в кожному операторі КІ [3]. Якщо подивитися на цю архітектуру крізь призму системного підходу, впадає в око парадоксальна ситуація: кожен елемент системи функціонально обґрунтований і має чітке правове підґрунтя, але система як ціле позбавлена єдиного оперативного координатора. Це дає підстави ввести поняття «координація без координатора», яке описує стан, коли всі суб'єкти зобов'язані обмінюватися інформацією, але жоден не несе відповідальності за збій координації як такої.

Закон № 4336-IX намагається розв'язати цю проблему розмежуванням функцій: Держспецзв'язку отримує роль стандартизатора й валідатора відповідності, СБУ зосереджується на контррозвідувальній складовій, Нацполіція – на розслідуванні кіберзлочинів [3]. Водночас Держспецзв'язку отримало розширені повноваження щодо погодження кандидатур керівників з кіберзахисту в державних органах і операторах КІ, причому лише після перевірки СБУ. Ця багатошарова процедура здатна блокувати оперативні кадрові рішення саме тоді, коли кіберінцидент вимагає негайної заміни відповідальної особи, і в цьому виявляється онтологічне протиріччя між безпековою логікою (перевіряти все) та управлінською ефективністю (діяти швидко). НКЦК при РНБО, який інституційно мав би стати центром стратегічної координації за зразком естонського RIA чи литовського NKSC, залишається робочим органом без оперативних повноважень: він координує політику, але не має права видавати приписи операторам чи накладати санкції [6, 30].

Адміністративні процедури (категоризація, обов'язковий аудит, повідомлення про інциденти CERT-UA, видача приписів і моніторинг рівня безпеки) формально утворюють замкнений цикл [7, 8], проте кейс «Київстара» грудня 2023 року продемонстрував його формальність: зловмисники перебували в ядрі мережі національного оператора зв'язку щонайменше сім місяців без виявлення ані внутрішнім аудитом, ані зовнішнім моніторингом [24, 27]. Розрив між наявністю норми й застосуванням санкцій (enforcement gap у термінології D. Sharma, S. Reddy та H. Shahid [29]) залишається найслабшою ланкою: формально-правовий каркас існує, але регуляторна санкційна функція фактично не активована.

Таблиця 1

Таблиця 1. Порівняльна характеристика адміністративно-правових моделей кіберзахисту КІІ: Україна та Директива NIS2

Критерій	Україна (станом на квітень 2025 р.)	Директива NIS2 (ЄС)
Об'єкт / суб'єкт регулювання	Об'єкти КІІ, що визначаються адміністративним рішенням секторального органу та Держспецзв'язку і вносяться до закритого Державного реєстру; оператор набуває обов'язків лише після внесення	Essential та important entities у 18 секторах за об'єктивним size-cap критерієм (кількість працівників, оборот); статус виникає автоматично
Санкційний механізм	КУпАП, ст. 188-47: штрафи від 1700 до 5100 грн (40–120 EUR); жодного публічно задокументованого випадку застосування після великих інцидентів 2022–2024 рр.	До 10 млн EUR або 2 % світового обороту для essential entities; до 7 млн EUR або 1,4 % для important; персональна відповідальність керівних органів за ст. 20
Повідомлення про інциденти	Обов'язок повідомляти CERT-UA «негайно», конкретні строки не формалізовані у годинах	Триетапна схема: 24 год (раннє попередження), 72 год (повідомлення), 1 місяць (фінальний звіт)

ISSN: 3041-2110

Координуючий орган	НКЦК при РНБО – стратегічна координація без оперативних повноважень; Держспецзв'язку – цивільний нагляд; СБУ – контррозвідка. Відсутність єдиної точки відповідальності	Кожна держава-член призначає один або кілька competent authorities та єдиний single point of contact; ENISA – координація на рівні ЄС
Безпека ланцюга постачання	Не врегульовано на рівні закону; окремі вимоги в підзаконних актах	Обов'язкова вимога ст. 21(2)(d): оцінка ризиків постачальників, включно з критеріями для вибору
Аудит	Обов'язковий для об'єктів КІІ І категорії за постановою КМУ № 367 від 01.04.2025; для інших категорій – рекомендаційний	Регулярні аудити, сканування вразливостей та виїзні інспекції для essential entities (ex-ante); перевірки ex-post для important entities за наявності підстав

Джерело: складено автором на підставі [3, 10, 19, 29]

Якщо інституційна архітектура визначає суб'єктів кіберзахисту, то воєнний стан кардинально змінив умови, в яких ці суб'єкти діють, і саме це перетворення заслуговує на окремий концептуальний розгляд. Указ Президента № 64/2022 від 24 лютого 2022 року, що вводив воєнний стан і продовжувався безперервно до квітня 2025 року, фундаментально розширив адміністративний розсуд органів кібербезпеки [4]. Серія підзаконних актів (постанова Кабінету Міністрів № 991 від 2 вересня 2022 року, постанови № 1174 і № 1175 від 14 жовтня 2022 року, постанова № 299 від 4 квітня 2023 року) запровадила спеціальний регламент обміну інформацією, прискорені перевірки, спрощені процедури реагування та легалізувала оперативне переміщення даних державних інформаційних ресурсів [7]. Стратегія кібербезпеки України (Указ Президента № 447/2021 від 26 серпня 2021 року), доповнена Планом реалізації (Указ Президента № 37/2022) та розпорядженням Кабінету Міністрів № 204-р від 7 березня 2025 року з фінансуванням 468,8 млн грн, забезпечує бюджетну, організаційну та кадрову координацію між суб'єктами кібербезпеки у воєнний

період [5]. Усе це виглядає раціональним в антикризовій логіці, проте саме тут виникає глибша проблема: конструкція українського законодавства не передбачає sunset clauses для воєнних режимних норм, унаслідок чого розширений розсуд адміністрації, обмеження публічності реєстрів та спрощені процедури блокування ризикують стати постійним фоновим режимом регулювання і після завершення бойових дій.

Якщо припустити, що воєнний стан завершиться протягом найближчих років, постане питання: яку частину надзвичайного регуляторного режиму держава збереже як «оптимальну» і яку поверне до мирного стандарту? I. Fyshchuk та співавтори на основі інтерв'ю з представниками публічних органів фіксують, що проблеми мирного часу (обмежені фінансові ресурси, кадрові дефіцити, нечіткі гайдлайни) у воєнний час не зникають, а посилюються, і саме це створює спокусу зберегти спрощені процедури як звичний режим роботи [24]. M. N. Schmitt з позиції міжнародного права підкреслює необхідність чіткого розмежування між антикризовими повноваженнями та системним регулюванням, бо без такого розмежування губиться адресат гарантій: оператор КІІ опиняється в режимі перманентної невизначеності щодо обсягу обов'язків і прав на оскарження [25]. Баланс між оперативністю реагування та адміністративно-правовими гарантіями для операторів КІІ наразі схилений у бік першого: скорочення процесуальних строків і підвищена секретність технічних деталей атак сприяють швидкості, але одночасно блокують ефективний внутрішній комплаєнс і незалежний аудит. Литовська модель, де NKSC підпорядковано Міністерству національної оборони, а адміністративні штрафи зрівняні з планкою NIS2 у 10 млн EUR, демонструє, що поєднання військового підпорядкування з прозорою санкційною функцією є досяжним і не вимагає жертвування правовою визначеністю [20, 23]. Естонський досвід Data Embassy у Люксембурзі та X-Road як децентралізованої магістралі обміну даними показує, що цифрова стійкість критичної інфраструктури досяжна без обмеження

 ISSN: 3041-2110

прозорості [11, 28]. Отже, українська дилема (як забезпечити кризове реагування, не нормалізуючи правового винятку) поки що розв'язується на користь винятку, що породжує довгостроковий ризик ерозії адміністративно-правових гарантій.

Від внутрішнього контексту логічно перейти до зовнішнього орієнтира, який одночасно є і моделлю, і зобов'язанням. Директива (ЄС) 2022/2555 від 14 грудня 2022 року, що скасувала NIS1 і встановила кінцевий термін транспозиції 17 жовтня 2024 року, запроваджує кілька принципових інновацій [10]. До них належать двохрівнева класифікація essential/important entities у 18 секторах, гармонізована шкала адміністративних штрафів (10 млн EUR або 2 % світового обороту для essential, 7 млн EUR або 1,4 % для important entities), персональна відповідальність керівних органів, обов'язкове повідомлення про значущий інцидент за схемою 24 години / 72 години / 1 місяць та управління безпекою ланцюга постачання [10, 19, 22]. У сукупності вони формують модель, де кібербезпека стає предметом корпоративного фідуціарного обов'язку: N. Vandezande показує, що NIS2 суттєво зміщує парадигму з реактивної (NIS1) на проактивну для essential entities [19], а D. D. S. Ferguson доводить, що вимоги управління ризиками мають реальний превентивний ефект лише за наявності дієвої загрози санкції [21]. ENISA, мандат якого посилено Регламентом (ЄС) 2019/881 (Cybersecurity Act), функціонує як координаційний хаб через CSIRT Network, EU-CyCLONe та сертифікаційну рамку, а щорічний Threat Landscape Report фіксує, що головним рушієм європейського кіберландшафту за липень 2023 – червень 2024 року була саме війна Росії проти України [11, 31].

Українська адаптація NIS2 наразі відбувається фрагментарно, хоча і з відчутним прискоренням. Закон № 4336-IX від 27 березня 2025 року імплементує авторизацію систем з безпеки замість обов'язкового КСЗІ, ризик-орієнтований підхід, посаду керівника з кіберзахисту, єдину національну систему реагування та публічний перелік авторизованих систем, а постанова Кабінету Міністрів № 367 від 1 квітня 2025 року деталізує управління ризиками для об'єктів I категорії

[3]. Однак ключові елементи NIS2 (гармонізована санкційна шкала з планкою 10 млн EUR, персональна адміністративна відповідальність керівників, формалізовані строки повідомлення 24/72 годин / 1 місяць, обов'язкове регулювання безпеки ланцюга постачання) поки що не отримали еквівалентного національного оформлення [19, 21]. Зобов'язання за Додатком XVII Угоди про асоціацію Україна–ЄС та результати білатерального скринінгу за Розділом 10 «Цифрова трансформація і медіа» (31 березня – 1 квітня 2025 року) формують зовнішній юридичний тиск, який Україна змушена конвертувати у внутрішні норми протягом найближчого циклу. Якщо припустити, що до моменту відкриття переговорного кластера 4 санкційний механізм не буде гармонізований до мінімумів NIS2, переговорна позиція України буде ослаблена структурно, а не лише політично, бо йдеться про відповідність acquis, а не про політичну волю. Це дає підстави стверджувати, що гармонізація з NIS2 є не побажанням, а юридичним зобов'язанням із чітким дедлайном, порушення якого має конкретні переговорні наслідки.

Перевірка сформованого регуляторного каркасу реальними кіберінцидентами дозволяє оцінити не так наявність норм, як їхню дієвість, і саме цей емпіричний вимір аналізу виявляє найбільш тривожну закономірність. Перша хвиля (січень-квітень 2022 року) включала кампанії WhisperGate, HermeticWiper, IsaacWiper, атаку AcidRain проти Viasat KA-SAT і спробу розгортання Industroyer2 проти регіонального обленерго на 2 млн абонентів [25, 26]. CERT-UA у взаємодії з ESET та Microsoft продемонструвала високу здатність до спільного виявлення і нейтралізації: 8 квітня 2022 року атаку Sandworm на енергетичну інфраструктуру було зупинено до виконання деструктивного компонента. Атака AcidRain паралізувала зв'язок українських військових, вивела з ладу десятки тисяч модемів у Європі і спричинила безпрецедентну колективну атрибуцію Російській Федерації з боку США, ЄС, Великої Британії, Канади, Австралії й Нової Зеландії [26, 27]. Адміністративно-

ISSN: 3041-2110

правова відповідь на цю хвилю була переважно технічною й оперативною; системного нормативного оновлення вона майже не спричинила, за винятком постанови № 991 від 2 вересня 2022 року, що косметично адаптувала підзаконний рівень.

Друга хвиля кульмінувала кібератакою на «Київстар» 12 грудня 2023 року, яка стала найбільшою деструктивною атакою на телеком-інфраструктуру в історії. Атака знищила 40 % віртуальної інфраструктури оператора, що обслуговував 24,3 млн мобільних і 1,1 млн фіксованих абонентів; перестали працювати сирени повітряної тривоги в Києві та Сумах, банкомати й платіжні термінали [27]. Атрибуцію Sandworm/ГРУ підтвердив Департамент кібербезпеки СБУ; зловмисники перебували в мережі щонайменше з травня 2023 року, повний доступ здобули у листопаді. Координація СБУ, Держспецзв'язку та CERT-UA забезпечила відновлення фіксованого зв'язку за 8 годин, голосового – за добу, повне відновлення базових сервісів – за дев'ять днів; збитки Veon оцінив у близько 100 млн доларів [24]. СБУ відкрила кримінальне провадження та збирає докази для Міжнародного кримінального суду в Гаазі. Адміністративно-правова відповідь виявилась асиметричною: швидке оперативне реагування не супроводжувалося жодною адміністративною санкцією щодо самого оператора за прогалини у комплаєнсі, які дозволили зловмисникам сім місяців перебувати в ядрі мережі. Це спостереження набуває концептуального значення, бо ставить під сумнів саму ідею «замкненого циклу» адміністративних процедур: якщо цикл не генерує санкції навіть після стратегічного інциденту, він є не циклом, а ритуалом.

Третя хвиля продемонструвала вразливість іншого типу. Атака на державні реєстри Міністерства юстиції 19 грудня 2024 року зупинила понад 60 систем, зокрема Єдиний державний реєстр юридичних осіб, ДРАЦС, Реєстр речових прав на нерухоме майно [32]. Повне відновлення тривало 32 дні; завдяки резервним копіям дані не було втрачено остаточно. Кабінет Міністрів

постановою № 1445 від 20 грудня 2024 року тимчасово зупинив строки адміністративного провадження по реєстрах. CERT-UA прямо констатувала, що інцидент продемонстрував критичну залежність державних процесів від функціонування реєстрів і потребує перегляду підходів до резервування [32]. Якщо підійти до цього інциденту з позиції системного аналізу, його ключовий урок полягає не стільки в технічній вразливості, скільки у проблемі вендорлоку: монопольна залежність держави від єдиного приватного підрядника на критичні реєстри без архітектурно вбудованого децентралізованого резервування перетворює будь-який нормативний захист на фікцію, якщо атака спрямована саме на цю єдину точку відмови [26, 27]. Сукупна оцінка реагування 2022–2025 років дозволяє сформулювати авторську тезу: адміністративно-правовий механізм дозволяє ефективно реагувати на кризу, але не здатний дисциплінувати операторів превентивно, бо державна машина не активувала жодного значущого адміністративного провадження проти операторів КІІ за прогалини у виконанні вимог кіберзахисту [21, 29].

На підставі проведеного аналізу доцільно запропонувати авторську модель адміністративно-правового циклу кіберзахисту КІІ, яку можна візуалізувати у вигляді блок-схеми (рис. 1). Схема охоплює шість послідовних етапів: ідентифікація та категоризація об'єкта КІІ (секторальний орган → Держспецзв'язку → внесення до Реєстру), встановлення вимог захисту (відповідно до категорії I–IV), обов'язковий аудит (внутрішній або зовнішній, періодичність залежить від категорії), моніторинг і повідомлення про інциденти (CERT-UA як центральний хаб), видача приписів та накладення адміністративних санкцій (Держспецзв'язку), зворотний зв'язок (перегляд категорії та вимог за результатами інциденту). Принципово важливо, що п'ятий етап (санкції) наразі фактично не функціонує: стрілка від «виявлення порушень» до «накладення санкцій» існує нормативно, але не активується практично, що і було продемонстровано кейсами «Київстара» та реєстрів Мін'юсту. Саме цей

розрив перетворює циклічну модель на лінійну, де реагування завершується відновленням, а не дисциплінуванням.

Гармонізація з acquis ЄС зобов'язує Україну в наступному циклі реформ закрити чотири стратегічні розриви, кожен із яких потребує не лише нормотворчої, а й інституційної дії. Перший розрив полягає в ревізії базового Закону № 2163-VIII: об'єктно-орієнтовану термінологію необхідно замінити на суб'єктно-орієнтовану модель essential/important entities, що автоматично синхронізує сферу регулювання з NIS2 та усуне асиметрію з європейським наглядом [10, 17, 19]. Другий розрив стосується санкційного механізму, і він є, мабуть, найбільш чутливим політично: без адміністративних штрафів, кратних світовому обороту оператора, і персональної відповідальності керівників за аналогією зі статтею 20 NIS2 український регулятор залишатиметься неспроможним у комерційному сегменті КІІ, де оператори є великими приватними компаніями з потужними юридичними службами [21, 29]. Третій розрив пов'язаний з множинністю реєстрів: реєстр КІ та реєстр КІІ доцільно об'єднати в єдину федеровану інформаційну систему з прозорими критеріями включення і публічним базовим шаром, обмеживши доступ лише до технічної атрибутики [12, 15]. Четвертий розрив – інституційна архітектура після завершення воєнного стану, яка потребує чіткого ієрархічного центру: або через посилення НКЦК до рівня операційного координатора (литовська модель), або через концентрацію цивільного нагляду в Держспецзв'язку як єдиної точки входу (естонська модель RIA), із залишенням за СБУ суто контррозвідувальної компетенції [14, 30].

Видається доцільним запропонувати також модель цільової інституційної архітектури кіберзахисту КІІ у post-war умовах (рис. 2). Схема передбачає три рівні: стратегічний (РНБО/НКЦК з оперативними повноваженнями координації та затвердження національних стандартів), операційний (Держспецзв'язку як єдиний цивільний регулятор із функціями аудиту, авторизації та санкцій, плюс

CERT-UA як технічний хаб реагування) та секторальний (галузеві CSIRT у секторах енергетики, телекому, фінансів, транспорту, що підпорядковуються операційному рівню). СБУ у цій моделі зберігає контррозвідувальну компетенцію і взаємодіє з операційним рівнем через захищений канал обміну індикаторами компрометації, але не дублює функції цивільного нагляду. Кіберполіція залишається в контурі Нацполіції і зосереджується на кримінальному розслідуванні. Ключовою відмінністю від нинішньої моделі є наявність єдиної вертикалі відповідальності та усунення дублювання координаційних функцій.

Окреме завдання, яке не вичерпується нормотворчістю, стосується формування культури обов'язкового зовнішнього аудиту і кіберігієни в приватному сегменті КІІ. Звіт CERT-UA за II півріччя 2024 року вказує, що приватний бізнес значно менш підготовлений до кібератак, ніж державні установи, і не завжди готовий відкрито ділитися інформацією про інциденти [32]. Цю асиметрію не закриє жодне розширення повноважень регулятора без позитивної мотивації: податкових стимулів для інвестицій у кіберзахист, механізму обмеженої відповідальності за умови повного комплаєнсу та обов'язкового страхування кіберризиків для операторів I і II категорії [23, 28]. Капасіті Держспецзв'язку лишається вузьким місцем: розширення мандата Законом № 4336-IX без пропорційного зростання штату, бюджету та технічної експертизи створить ілюзію регулювання без його реальної дії, і саме цей ризик слід артикулювати як один із найбільш імовірних сценаріїв найближчих років.

Висновки. Адміністративно-правове регулювання кібербезпеки критичної інформаційної інфраструктури в Україні станом на квітень 2025 року перебуває на історичному переломі. Закон № 4336-IX, постанова Кабінету Міністрів № 367 і розпорядження № 204-р у сукупності з результатами скринінгу за Розділом 10 формують дорожню карту, яка вперше робить європеїзацію не риторичною, а нормативною реальністю.

Проведений аналіз підтверджує: Україна побудувала ефективну машину кризового кіберреагування, але не побудувала адміністративного механізму превентивного дисциплінування операторів КІІ. Усі великі інциденти 2022–2024 років – від Industroyer2 до атак на реєстри Мін'юсту – закінчувалися відновленням систем і кримінальними провадженнями проти зовнішніх атакантів, але жодним адміністративним провадженням проти внутрішніх носіїв обов'язку дотримуватися вимог кіберзахисту. Це перетворює норми про аудит, повідомлення та категоризацію на формальні, а не примусові.

Виявлені прогалини концентруються в трьох пластах. У концептуальному пласті йдеться про фрагментацію дефініцій КІ, КІІ та об'єктів КІІ, несумісну із суб'єктною логікою NIS2. Інституційний пласт охоплює координацію без оперативного координатора, дублювання компетенцій Держспецзв'язку, СБУ та НКЦК і відсутність єдиної точки відповідальності. Санкційний пласт стосується мінімальних розмірів штрафів, нечіткості процедури їхнього накладення, фактичної незастосовності до великих операторів та повної відсутності персональної адміністративної відповідальності керівників.

Воєнний стан загострив, а не створив ці проблеми. Ризик нормалізації надзвичайних повноважень існує не тому, що ці повноваження надмірні, а тому, що в українському праві відсутній автоматичний механізм їхнього згортання після завершення кризи. Внесення sunset clauses до воєнних постанов у сфері кіберзахисту та періодична парламентська ревізія цих норм мають стати елементом наступного циклу реформ.

Пропозиції de lege ferenda зводяться до інтегрованого пакета: повна транспозиція NIS2 із суб'єктною класифікацією, гармонізованою шкалою штрафів та персональною відповідальністю керівників; об'єднання реєстрів КІ і КІІ з прозорими критеріями включення; створення єдиного оперативного координатора кіберзахисту з повноваженнями приписів; обов'язковий зовнішній аудит для операторів I–II категорії; запровадження кіберстрахування і

ISSN: 3041-2110

податкових стимулів для приватного сегмента; формалізація строків повідомлення про значущий інцидент за моделлю 24/72 годин – 1 місяць; зобов'язання децентралізованого резервування критичних реєстрів на принципі відсутності залежності від єдиного підрядника.

Принциповий висновок полягає в тому, що Україна першою в Європі отримала практичний досвід кіберзахисту КІІ в умовах повномасштабної війни, і саме цей досвід має стати капіталом для оновлення європейської моделі. Але тільки за умови, що внутрішня адміністративно-правова реформа дозволить конвертувати оперативну стійкість у системну спроможність – інакше післявоєнний інституційний пейзаж відтворить нинішню фрагментацію в збільшеному масштабі.

Адміністративне право у сфері кібербезпеки КІІ повинне відмовитися від каркасної логіки переліків і прийняти ризик-орієнтовану логіку результату. Тільки такий поворот зробить регулювання сумісним і з NIS2, і з реальністю гібридного протистояння, у якому Україна перебуватиме ще довго після формального завершення воєнного стану.

Список використаних джерел

1. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. *Відомості Верховної Ради України*. 2022. № 9-10. Ст. 65. URL: https://zakon.rada.gov.ua/laws/show/1882-IX

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19

3. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. *Відомості Верховної Ради України*. 2025. № 35. URL: https://zakon.rada.gov.ua/laws/show/4336-20

4. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 № 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022

5. Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021

6. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07.06.2016 № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016

7. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п

8. Деякі питання об'єктів критичної інформаційної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-п

9. Деякі питання об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п

10. 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). *Official Journal of the European Union*. L 333, 27.12.2022. P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

11. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act). *Official Journal of the European Union*. L 151, 07.06.2019. P. 15–69. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj

12. Алексеєва О. А. Правове забезпечення кібербезпеки об'єктів критичної інфраструктури. *Інформація і право*. 2023. № 4 (47). С. 168–176. DOI: https://doi.org/10.37750/2616-6798.2023.4(47).291633

13. Мануілов Я. С. Забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни. *Інформація і право*. 2023. № 1 (44). С. 154–167. DOI: https://doi.org/10.37750/2616-6798.2023.1(44).287780

14. Третяк Ю. Система суб'єктів адміністративно-правового забезпечення кібербезпеки. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки*. 2024. Т. 11, № 2 (42). С. 197–205. DOI: https://doi.org/10.23939/law2024.42.197

15. Скіцько О. І. Нормативно-правове забезпечення кібербезпеки об'єктів критичної інфраструктури. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2024. № 2. URL: http://journals.lvduvs.lviv.ua/index.php/law/article/view/870

16. Метелев О. П., Плетньов О. В. Протидія впливу на державні електронні інформаційні ресурси та об'єкти критичної інфраструктури в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2023. № 10. URL: http://lsej.org.ua/10_2024/73.pdf

17. Гончаренко Г. А. До проблеми визначення та розмежування дефініцій «інформаційна безпека» і «кібербезпека». *Аналітично-порівняльне правознавство*. 2024. № 5. С. 466–471. DOI: https://doi.org/10.24144/2788-6018.2024.05.73

18. Корощенко К. Р., Ільченко О. В. Правоохоронні органи як суб'єкти забезпечення кібербезпеки в інформаційному просторі України. *Аналітично-порівняльне правознавство*. 2022. № 1. DOI: https://doi.org/10.24144/2788-6018.2022.01.30

19. Vandezande N. Cybersecurity in the EU: How the NIS2-Directive Stacks Up Against Its Predecessor. *Computer Law & Security Review*. 2024. Vol. 52. Article 105890. DOI: https://doi.org/10.1016/j.clsr.2023.105890

20. Schmitz-Berndt S., Chiara P. G. One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. *International*

Cybersecurity Law Review. 2022. Vol. 3, No. 2. P. 289–311. DOI: https://doi.org/10.1365/s43439-022-00058-7

21. Ferguson D. D. S. The outcome efficacy of the entity risk management requirements of the NIS 2 Directive. *International Cybersecurity Law Review*. 2023. Vol. 4. P. 161–195. DOI: https://doi.org/10.1365/s43439-023-00097-8

22. Sievers T. Proposal for a NIS Directive 2.0: companies covered by the extended scope of application and their obligations. *International Cybersecurity Law Review*. 2021. Vol. 2. P. 223–231. DOI: https://doi.org/10.1365/s43439-021-00033-8

23. Markopoulou D., Papakonstantinou V. The regulatory framework for the protection of critical infrastructures against cyberthreats: The case of the health sector. *Computer Law & Security Review*. 2021. Vol. 41. Article 105502. DOI: https://doi.org/10.1016/j.clsr.2020.105502

24. Fyshchuk I., Trofimenko M., Tropina T., Janowski T. Managing cyberattacks in wartime: The case of Ukraine. *Public Administration Review*. 2025. DOI: https://doi.org/10.1111/puar.13895

25. Schmitt M. N. Ukraine, Cyberattacks, and the Lessons for International Law. *American Journal of International Law*. 2022. Vol. 116. URL: https://doi.org/10.1017/ajil.2022.37

26. Cormac R., Walton C., Van Puyvelde D. The Cyber Dimension of the Russia–Ukraine War. *Survival*. 2022. Vol. 64, No. 5. P. 7–26. DOI: https://doi.org/10.1080/00396338.2022.2126193

27. Bronk C., Collins G., Wallach D. S. The Ukrainian Information and Cyber War. *The Cyber Defense Review*. 2023. Vol. 8, No. 3. P. 33–50. URL: https://www.jstor.org/stable/48755360

28. Maglaras L., Janicke H., Ferrag M. A. Cybersecurity of Critical Infrastructures: Challenges and Solutions. *Sensors*. 2022. Vol. 22, No. 14. Article 5105. DOI: https://doi.org/10.3390/s22145105

29. Sharma D., Reddy S., Shahid H. Cybersecurity Obligations for Critical Infrastructure: Emerging Legal Norms, Enforcement Gaps, and Governance Challenges. *Legal Studies in Digital Age*. 2023. Vol. 2, No. 3. P. 49–63. URL: https://jlsda.com/index.php/lsda/article/view/322

30. Davydiuk A., Potii O. National Cybersecurity Governance: Ukraine. *CCDCOE Tallinn Papers*. Tallinn : NATO CCDCOE, 2024. URL: https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf

31. ENISA Threat Landscape 2024 / European Union Agency for Cybersecurity. Athens : ENISA, 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

32. Російські кібероперації: аналітика за II півріччя 2024 / CERT-UA. Київ : Держспецзв'язку, 2025. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=68769

 ISSN: 3041-2110