Адміністративне право і процес

УДК 342.9:004.056

DOI https://doi.org/10.5281/zenodo.21297805

Адміністративна відповідальність за порушення вимог кібербезпеки: проблеми кваліфікації та ефективності санкцій

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: 12.08.2025 | Опубліковано: 30.08.2025

Анотація. Статтю присвячено аналізу адміністративної відповідальності за порушення вимог кібербезпеки в Україні, зокрема проблемам кваліфікації правопорушень та ефективності санкцій. Досліджено доктринальні засади кібербезпекового делікту як самостійного складу із специфічним об'єктом – впорядкованим режимом конфіденційності, цілісності та доступності мережевих та інформаційних систем. Проаналізовано розпорошеність релевантних складів між статтями КУпАП (ст. 188-31, 188-39, 212-2, 212-5, 212-6) та інституційну асиметрію між матеріальними обов'язками операторів критичної інфраструктури, встановленими Законом № 4336-IX, і фрагментарним

санкційним блоком. Виявлено чотири кваліфікаційні проблеми: нечіткість межі між адміністративним і кримінальним кіберправопорушенням, конституційну напругу бланкетних диспозицій, мультикаузальність кіберінцидентів та відсутність диференціації санкцій за типом суб'єкта. Зіставлено українську модель із підходом Директиви NIS 2 та практикою GDPR enforcement. Обґрунтовано напрями реформи: оборотно-прив'язані санкції, compliance-захист, нормативне визнання SIEM/SOC-даних як доказів, добровільне самоповідомлення з амністією та особиста відповідальність керівника з кіберзахисту.

Ключові слова: адміністративна відповідальність, кібербезпека, кваліфікація правопорушень, ефективність санкцій, Директива NIS 2, критична інфраструктура, compliance, GDPR.

Administrative liability for cybersecurity violations: problems of qualification and effectiveness of sanctions

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

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

Abstract. The article examines administrative liability for cybersecurity violations in Ukraine, focusing on the qualification of offences and the effectiveness

of sanctions. The doctrinal foundations of a cybersecurity delict are explored as an autonomous corpus delicti with a specific object – the orderly regime of confidentiality, integrity and availability of network and information systems. The analysis reveals the fragmentation of relevant administrative offence provisions across multiple articles of the Code of Ukraine on Administrative Offences (Art. 188-31, 188-39, 212-2, 212-5, 212-6) and the institutional asymmetry between the substantive obligations of critical infrastructure operators established by Law No. 4336-IX and the fragmentary sanctions framework. Four qualification problems are identified: the blurred boundary between administrative and criminal cyber offences, the constitutional tension of blanket dispositions referencing private technical standards such as ISO/IEC 27001 and NIST CSF, the multi-causal nature of cyber incidents that impedes the establishment of causation under classical doctrines, and the absence of sanction differentiation by entity type, which violates the principle of proportionality. The Ukrainian model is compared with the NIS 2 Directive approach, where fines may reach EUR 10 million or 2% of global turnover, and with GDPR enforcement practice, which has accumulated over EUR 5.65 billion in penalties. Five reform directions are substantiated: turnover-linked sanctions differentiated by entity category, compliance defence through ISO/IEC 27001 certification, normative recognition of SIEM/SOC data as admissible administrative evidence, voluntary self-reporting with amnesty for timely incident disclosure, and personal liability of the cybersecurity officer.

Keywords: administrative liability, cybersecurity, offence qualification, sanction effectiveness, NIS 2 Directive, critical infrastructure, compliance, GDPR.

Постановка проблеми. Якщо спробувати виразити центральну суперечність українського кібербезпекового регулювання однією пропорцією, вона виглядатиме так: верхня межа адміністративного штрафу за найтяжчими статтями Кодексу України про адміністративні правопорушення (далі – КУпАП) становить кілька десятків тисяч гривень, тоді як збитки від одного резонансного

кіберінциденту вимірюються сотнями мільйонів доларів – різниця сягає п'яти порядків [4, 6]. У контексті загальної теорії юридичної відповідальності така диспропорція означає, що санкція перестає виконувати будь-яку з трьох класичних функцій – каральну, превентивну, відновлювальну – і перетворюється на суто символічний жест з боку законодавця. Символізм, утім, не є нейтральним: він сигналізує регульованим суб'єктам, що держава не розглядає кіберзахист як пріоритет, що вартість недбалості є знехтувано малою порівняно з вартістю інвестицій у безпеку. Видається обґрунтованим припустити, що саме ця символічність – а не технічна складність кіберзагроз – є головною причиною системної неспроможності адміністративно-правового інструментарію в цій сфері.

Ситуацію додатково загострює хронологічна асинхронія між розвитком матеріального та санкційного права. Закон № 2163-VIII «Про основні засади забезпечення кібербезпеки України» (2017) у редакції закону № 4336-IX від 27.03.2025 фактично гармонізував матеріальні обов'язки регульованих суб'єктів із вимогами Директиви NIS 2 (2022/2555) Європейського Союзу: з'явилися категорії підрозділів з кіберзахисту, керівників з кіберзахисту, авторизації з безпеки, обов'язкової інцидентної звітності [12]. Проте санкційний блок КУпАП, покликаний забезпечити виконання цих обов'язків, залишився розпорошеним між чотирма статтями Особливої частини, кожна з яких сконструйована під інший, більш загальний об'єкт регулювання. Європейський Союз, зіткнувшись із аналогічною проблемою після ухвалення першої Директиви NIS (2016), відреагував створенням єдиного санкційного режиму зі стелями штрафів у 10 млн євро або 2 % світового обороту для essential entities [4]. Україна ж перебуває у стані, який можна було б назвати «матеріальним випередженням при санкційному відставанні» – стані, що набуває особливої гостроти в умовах воєнного стану, коли серйозні кіберінциденти автоматично переходять у площину кримінального переслідування, а адміністративні справи залишаються

без руху через нечіткість диспозицій і брак правозастосовної практики. За таких умов постає фундаментальне питання: чи здатна адміністративна відповідальність у нинішній конфігурації виконувати хоча б мінімальну регулятивну функцію, чи вона потребує системної реконструкції на засадах, уже апробованих у праві Європейського Союзу?

Аналіз останніх досліджень і публікацій. Проблематика адміністративної відповідальності у сфері кібербезпеки перебуває на перетині кількох дослідницьких традицій, що розвиваються переважно автономно, хоча їхнє предметне поле перетинається. Одне з перших системних досліджень адміністративної відповідальності саме у сфері забезпечення кібербезпеки України здійснили В. В. Топчій та О. М. Бодунова, обґрунтувавши необхідність розмежування кібербезпекового делікту та суміжних складів в інформаційній сфері [1]. Дещо іншу оптику пропонує В. А. Мазійчук, зосереджуючись на характеристиці адміністративних правопорушень в інформаційній сфері загалом, не виокремлюючи кібербезпекову специфіку, проте її типологія складів корисна для порівняльного аналізу нормативної бази [2]. Доктринальне розмежування дефініцій «інформаційна безпека» і «кібербезпека» здійснив Г. А. Гончаренко, продемонструвавши, що нечітке розмежування цих понять у законодавстві породжує конкуренцію норм при кваліфікації правопорушень [3].

Європейський вимір проблеми глибоко розкрито у працях зарубіжних дослідників. Комплексне порівняння Директиви NIS 2 з її попередницею здійснила N. Vandezande, акцентувавши увагу на санкційних механізмах та їхній стримувальній функції [4]. Питання про формування самостійного права на кібербезпеку в праві ЄС порушила P. G. Chiara, концептуально обґрунтовуючи перехід від карально-репресивної до превентивно-регулятивної моделі відповідальності [5]. Інституційну архітектуру кібербезпекового регулювання ЄС через призму взаємодії NIS, ENISA та GDPR розкрито у фундаментальній праці D. Markopoulou, V. Papakonstantinou та P. De Hert, де запропоновано

аналітичну рамку, придатну для зіставлення із фрагментованою українською моделлю [11]. Розширене коло суб'єктів NIS 2 та їхні обов'язки проаналізував T. Sievers, а санкційні механізми Директиви щодо критичної інфраструктури деталізував F. Teichmann [14, 16]. Проблему визначення порогу звітності про кіберінциденти – порогу, від якого залежить сама можливість порушення адміністративної справи – дослідив S. Schmitz-Berndt [9]. Механізм конкуренції секторальних і горизонтальних норм виявив C. Ducuing на прикладі правила переважності у NIS Directive [18].

Практичний вимір вітчизняної проблематики розкривають кілька напрямів досліджень. Правове забезпечення кібербезпеки об'єктів критичної інфраструктури аналізує О. А. Алексеєва, фіксуючи розрив між обов'язками операторів і відсутністю ефективних санкцій за їх невиконання [6]. Кібербезпеку в контексті повномасштабного вторгнення досліджує О. М. Романова, показуючи, як воєнний стан змістив баланс між адміністративними та кримінальними механізмами реагування [7]. Детальний аналіз кібератак та діяльності APT-груп в Україні здійснив М. Опанович, забезпечивши емпіричну базу для оцінки адекватності чинних санкцій масштабу реальної загрози [8]. Адміністративно-правові механізми захисту персональних даних у системах автоматизованого прийняття рішень дослідив Н. Т. Головацький, виявивши спільне з кібербезпековим регулюванням проблемне поле – бланкетність диспозицій і мізерність штрафів [10]. Правове регулювання кібербезпеки критичної інфраструктури в умовах воєнного стану аналізує О. Д. Довгань, встановлюючи зв'язок між матеріальними обов'язками та їхнім санкційним забезпеченням [12]. Систему виявлення вразливостей і реагування на кіберінциденти досліджує І. А. Білан, пропонуючи процесуальні механізми, здатні підтримати доказування адміністративних деліктів [13]. Механізм повідомлення про кібербезпекові події об'єктів критичної інфраструктури розкрили В. Цуркан і В. Ракович [15].

Enforcement-вимір проблеми розкривають кілька зарубіжних досліджень. Співвідношення кібербезпекового регулювання та боротьби з кіберзлочинністю аналізує L. Bartoli, порушуючи питання конкуренції адміністративних і кримінальних санкцій за один і той самий кіберінцидент [17]. Ефективність інцидентної звітності як інструменту від виявлення загроз до формування регуляторної політики емпірично досліджують S. Busetti та F. M. Scanni [19]. Метод DEMATEL для моделювання бар'єрів комплаєнсу з NIS 2 застосовують A. Vavoula, V. Triantafyllou та P. Triantafyllou [20]. Санкції ЄС у відповідь на кібератаки як кризові заходи розглядає Y. Miadzvetskaya, окреслюючи альтернативні інструменти стримування [21]. Фреймворк визнання допустимості цифрових доказів, отриманих за допомогою інструментів з відкритим кодом, розробили I. Ismail та K. A. Zainol Ariffin – підхід, безпосередньо застосовний до SIEM-логів як доказової бази в адміністративних кіберсправах [22].

Виділення невирішених раніше частин загальної проблеми. Попри значний обсяг досліджень, у літературі залишається незаповненою ніша комплексного аналізу, який поєднував би доктринальний рівень (конструкція складу кібербезпекового делікту), нормативний рівень (конкретні статті КУпАП у зіставленні з NIS 2) та емпіричний рівень (зіставлення розмірів санкцій із реальними збитками від кіберінцидентів). Більшість вітчизняних робіт обмежуються описом чинного законодавства, тоді як зарубіжні зосереджені на європейському контексті без проєкції на українські реалії.

Формулювання цілей статті. Метою статті є комплексний аналіз адміністративної відповідальності за порушення вимог кібербезпеки в Україні крізь призму проблем кваліфікації та ефективності санкцій із формулюванням обґрунтованих пропозицій щодо реформування санкційного механізму. Для досягнення цієї мети необхідно: визначити доктринальні засади кібербезпекового делікту як самостійного складу; проаналізувати нормативну базу України, виявивши прогалини кваліфікації; дослідити чотири ключові

кваліфікаційні проблеми, що паралізують правозастосування; емпірично зіставити розміри санкцій із реальними збитками; порівняти українську модель із підходом NIS 2 та GDPR enforcement; обґрунтувати напрями реформи – від оборотно-прив'язаних санкцій до доказового визнання SIEM/SOC-даних.

Виклад основного матеріалу. Будь-яка спроба осмислити адміністративну відповідальність за порушення вимог кібербезпеки неминуче починається з онтологічного питання: чи існує кібербезпековий делікт як самостійна правова реальність, чи він є лише одним із проявів ширшої категорії «інформаційного правопорушення», успадкованої від радянської кодифікації? Якщо прийняти першу тезу, то перед дослідником постає завдання виявити конститутивні ознаки, що відрізняють цей делікт від суміжних складів; якщо другу – доведеться визнати, що чинна структура КУпАП є адекватною, а проблема полягає лише в розмірах штрафів. Аналіз нормативного матеріалу переконує у правильності першого підходу: об'єктом кібербезпекового делікту виступає не інформація як абстрактне благо, а впорядкований режим конфіденційності, цілісності та доступності мережевих та інформаційних систем у поєднанні з публічним інтересом безперервного функціонування критичної інфраструктури [1, 6]. Саме ця подвійна природа об'єкта – технічна і публічна водночас – породжує п'ять конститутивних особливостей складу: бланкетну диспозицію, що відсилає до приватних технічних стандартів; ризик-орієнтовану конструкцію, в якій відповідальність настає за порушення обов'язку обачності, а не лише за матеріальний результат; формалізовану протиправність, за якої вже саме порушення вимоги утворює делікт; спеціального суб'єкта – регульовану організацію або керівника з кіберзахисту; переважно необережну форму вини. Ці ознаки, взяті сукупно, описують склад, що не вкладається в жодну з наявних рубрик КУпАП, – а отже, потребує або спеціальної статті, або спеціального розділу, подібно до того, як NIS 2 і Закон № 4336-IX описують матеріально нову

 ISSN: 3041-2110

нормативну реальність, у якій захищеним благом виступає сам режим комплаєнсу [12, 16].

Визнання автономності кібербезпекового делікту з неминучістю ставить питання про його межі – і тут стає зрозумілим, чому правозастосування потрапляє у глухий кут. Кримінальна відповідальність за статтями 361, 361-1, 361-2, 362, 363, 363-1 Кримінального кодексу України спрацьовує в ситуаціях активного несанкціонованого втручання: створення, розповсюдження шкідливого програмного забезпечення, проникнення до інформаційно-комунікаційних систем. Адміністративна ж покликана реагувати на інший тип протиправної поведінки – невиконання вимог про захисні заходи, несвоєчасне повідомлення, непідготовленість персоналу [1, 9]. Дисциплінарна відповідальність, що накладається паралельно на службовців і військовослужбовців за порушення внутрішніх регламентів кіберзахисту, утворює третій, автономний трек. Проте стаття 9 КУпАП проголошує субсидіарність адміністративної відповідальності щодо кримінальної, і в поєднанні з мізерними штрафами це створює своєрідну гравітаційну воронку: будь-яка справа, що набуває хоча б мінімального резонансу, перетягується в кримінальний трек; дрібні ж порушення зосереджуються в дисциплінарному. Адміністративний інструмент, покликаний заповнювати простір між цими полюсами, фактично залишається незадіяним – і не тому, що він непотрібний, а тому, що його конструкція робить його непривабливим для будь-якого правозастосовця.

Цю тезу підтверджує аналіз нормативної архітектури, яка, якщо подивитися на неї з телеологічної перспективи, виявляє парадоксальний розрив між амбіцією матеріального права та інерцією санкційного. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII у редакції від 19.10.2025 містить статтю 11, яка обмежується порожньою бланкетною формулою про відповідальність «згідно із законодавством», не створюючи

жодного власного санкційного складу – це, по суті, відкладання відповідальності на потім, яке триває вже вісім років від ухвалення базового закону. Закон № 4336-IX від 27.03.2025 пішов далі, запровадивши принципово важливі категорії – підрозділи з кіберзахисту, керівників з кіберзахисту, авторизацію з безпеки – і фактично перенісши архітектуру NIS 2 у матеріальне право [12]. Проте відповідні санкційні норми у КУпАП так і не з'явилися, і оператор критичної інформаційної інфраструктури, який не виконав вимог постанов Кабінету Міністрів України № 518 (2019), № 1426 (2021), № 299 (2023), № 367 та № 1470 (2025), опиняється у правовому вакуумі: формально він несе відповідальність, але конкретної норми про штраф для нього не існує. Якщо скористатися метафорою з архітектури, це нагадує будівлю, у якій зведено стіни, прокладено комунікації, але не встановлено замків на дверях.

Релевантні склади, які законодавець розкидав між главами 13 і 15 КУпАП, підтверджують цю тезу з емпіричною наочністю. Стаття 188-31 передбачає відповідальність за перешкоджання Держспецзв'язку зі штрафом 50–100 неоподатковуваних мінімумів доходів громадян; стаття 188-39 – за порушення режиму захисту персональних даних (до 2000 НМДГ при повторності); стаття 212-2 – за порушення режиму державної таємниці; стаття 212-5 – за порушення обліку та зберігання носіїв конфіденційної інформації, що є власністю держави; стаття 212-6 – за незаконний доступ до інформації в інформаційних системах (5–100 НМДГ із конфіскацією) [2, 3]. Показовим є те, що в академічному дискурсі іноді цитуються неіснуючі або помилково названі статті 188-47 чи 212-16, які насправді присвячені дозвільній системі та виборчим бюлетеням, – сама ця плутанина свідчить про те, наскільки непрозорою є нормативна карта. Ні в Особливій частині КУпАП, ні в Законі № 1882-IX «Про критичну інфраструктуру» (2021) не передбачено окремого складу про порушення обов'язків з реагування на кіберінциденти, попри те що відповідні матеріальні обов'язки визначені підзаконними актами Національного координаційного

центру кібербезпеки та Держспецзв'язку [6, 15]. Інституційна асиметрія між матеріальним і санкційним блоками – це не технічна недоробка, а структурна вада, що визначає саму природу чинної моделі.

Навіть якщо абстрагуватися від проблеми розмірів штрафів, правозастосуванню перешкоджають чотири кваліфікаційні бар'єри, кожен із яких заслуговує окремого аналізу, оскільки вони діють кумулятивно, підсилюючи один одного. Перший бар'єр – розмита межа між адміністративним і кримінальним кіберправопорушенням. Уявімо ситуацію: адміністратор корпоративної мережі не оновив критичний патч протягом регламентованих 72 годин, і саме через цю вразливість зловмисник проник у систему. Чи є адміністратор деліквентом, який порушив вимогу захисту, – а отже, суб'єктом адміністративної відповідальності, – чи він стає співучасником кримінального правопорушення з необережності? Судова практика, замість того щоб провести чітку межу, тяжіє до крайнощів: або взагалі не порушувати справу, або переходити на статтю 367 Кримінального кодексу (службова недбалість), що знецінює всю адміністративну вертикаль [3, 6]. Другий бар'єр – конституційна напруга бланкетних диспозицій. Диспозиції відповідних статей КУпАП відсилають до постанов Кабінету Міністрів та наказів Держспецзв'язку, які, своєю чергою, відсилають до приватних стандартів ISO/IEC 27001:2022, NIST CSF 2.0, ETSI EN 303 645 [11, 18]. Стандарти ISO видає недержавна організація, проте їхній текст фактично визначає об'єктивну сторону адміністративного делікту, – а це означає, що межі протиправності встановлює не законодавець і навіть не уряд, а приватний суб'єкт стандартизації, що створює напругу з принципом nullum crimen sine lege.

Третій кваліфікаційний бар'єр стосується причинного зв'язку між порушенням вимоги та настанням шкоди – зв'язку, який у класичній доктрині має бути необхідною умовою, але в кіберпросторі набуває зовсім іншої природи. Кіберінциденти мультикаузальні за визначенням: нульовий день, соціальна

інженерія, ланцюг постачання, людський фактор діють одночасно і часто нерозривно, що робить виокремлення якоїсь однієї «необхідної умови» методологічно сумнівним. NIS 2 обходить цю складність елегантним рішенням: конструюючи формальний делікт, за якого відповідальність настає за саме порушення вимоги, незалежно від того, чи стався інцидент [4]. Українське ж право досі мислить причинність у класичних термінах conditio sine qua non, що робить доказування у важких справах майже нездійсненним. Це дає підстави стверджувати, що без переходу до моделі формального делікту або хоча б моделі підвищення ризику – де причинний зв'язок презумується, якщо порушений обов'язок існував саме для запобігання тому виду шкоди, що настав, – адміністративна відповідальність у сфері кібербезпеки залишатиметься здебільшого теоретичною конструкцією. Четвертий бар'єр – відсутність диференціації за суб'єктом: однакова ставка штрафу для фізичної особи-підприємця і для оператора телекомунікацій загальнонаціонального масштабу [10] породжує парадокс зворотної регуляції, за якого великі гравці ігнорують правила, бо штраф мізерний, а малий бізнес платить непропорційно.

Усі ці кваліфікаційні проблеми набувають особливої гостроти, коли їх зіставити з масштабом реальних збитків від кіберінцидентів, – і саме тут декоративність санкцій стає очевидною навіть без юридичного аналізу. Глобальні втрати від атаки NotPetya у червні 2017 року, за оцінкою Білого дому, становили близько 10 млрд доларів США; одна лише компанія Maersk втратила приблизно 300 млн доларів, Merck – 870 млн, FedEx – 400 млн [4, 8]. Для України, де цю атаку розпочали через бухгалтерське програмне забезпечення M.E.Doc, наслідки були не менш катастрофічними, хоча й гірше задокументованими. Атака на «Київстар» 12 грудня 2023 року вивела з ладу до 40 % інфраструктури найбільшого мобільного оператора країни, торкнулася понад 24 мільйонів абонентів, паралізувала системи повітряної тривоги в кількох областях; материнська компанія VEON оцінила лише прямий вплив на виторг у 3,6 млрд

гривень, не рахуючи близько 90 млн доларів інвестицій у відновлення [6, 7]. Атака на державні реєстри 19 грудня 2024 року заблокувала близько 60 реєстрів Міністерства юстиції та більшість сервісів «Дії». На тлі цих цифр максимальний штраф за статтею 212-5 КУпАП – близько 28 900 гривень – виглядає не просто недостатнім, а ірраціональним: співвідношення з типовими збитками сягає 1:150 000.

Стримувальний ефект будь-якої санкції, якщо розглядати його через призму раціонального вибору, є функцією двох змінних – ймовірності виявлення порушення та розміру покарання. У сфері кібербезпеки обидва множники критично низькі: латентність деліктів колосальна через цифровий характер слідів, а нечіткість бланкетних диспозицій ускладнює доказування навіть виявлених порушень [9, 13]. Державна судова адміністрація не виокремлює кібербезпекові адміністративні справи в окрему рубрику, тож точна статистика недоступна, проте фрагментарний моніторинг Єдиного державного реєстру судових рішень свідчить про одиничні постанови за статтею 188-39 і фактичну відсутність застосування статті 212-6, яка витісняється кримінальними складами [1, 9]. Показовою є позиція голови Держспецзв'язку, який у 2024 році публічно заявив про намір запровадити повноцінні санкції для операторів критичної інфраструктури лише після завершення воєнного стану [12]. Видається парадоксальним, що саме в найкритичніший для кіберзахисту період регулятор свідомо відмовляється від санкційного інструменту – ніби лікар, який відкладає лікування до моменту, коли хвороба мине сама.

Європейська модель, до якої Україна за Угодою про асоціацію зобов'язана наближатися, пропонує принципово інший підхід до калібрування санкцій – і саме тому порівняння з нею є не просто академічною вправою, а методологічною необхідністю. NIS 2 захищає системний рівень мережевих та інформаційних систем, GDPR – рівень персональних даних, а стаття 35(2) NIS 2 запобігає подвійному покаранню за одне й те саме діяння, формуючи двоконтурну, але не

дублюючу архітектуру [4, 11]. Стаття 34 NIS 2 встановлює мінімальні стелі штрафів для держав-членів: 10 млн євро або 2 % світового обороту для essential entities та 7 млн євро або 1,4 % для important entities, доповнені можливістю періодичних штрафних платежів і тимчасовою забороною обіймати керівні посади для топ-менеджерів повторних порушників (стаття 32(5)(b)) [4, 16]. Практика GDPR через статтю 83 та Настанови EDPB 04/2022 емпірично продемонструвала працездатність оборотно-прив'язаної моделі: станом на березень 2025 року сукупний обсяг штрафів перевищив 5,65 млрд євро у понад 2 245 рішеннях, а одне рішення проти Meta Ireland у 2023 році сягнуло 1,2 млрд євро [11]. Цей досвід свідчить: пропорційні санкції не залишаються на папері – за умови інституційної спроможності наглядових органів вони працюють як реальний інструмент стримування.

Утім, було б інтелектуально нечесним замовчувати складнощі, з якими зіткнувся сам ЄС. Попри жовтневий 2024 року дедлайн транспозиції, до жовтня 2025-го повністю імплементували NIS 2 близько двадцяти з двадцяти семи держав-членів, а проти решти Європейська Комісія видала вмотивовані висновки про порушення [20]. Водночас жоден публічно відомий штраф за NIS 2 ще не накладений, тож емпіричний стримувальний ефект Директиви залишається теоретичним [4, 16]. Для України з цього випливає парадоксальний, але повчальний урок: формальне ухвалення жорстких санкцій є необхідною, але недостатньою умовою стримування – потрібна ще й спроможність наглядових органів, прозорість статистики та політична готовність до перших високопрофільних рішень. За Угодою про асоціацію (Глава 14, статті 389–394) і Цифровим розділом Плану України Київ зобов'язаний наближатися до acquis у сфері електронних комунікацій і цифрових послуг; Закон № 4336-IX матеріально цю вимогу значною мірою виконує, проте санкційний розрив залишається найвідчутнішою точкою невідповідності [12, 20].

Виявлені проблеми та апробований зарубіжний досвід дають підстави запропонувати авторську модель реформування, що складається з п'яти взаємопов'язаних елементів. Перший і найфундаментальніший – диференціація санкцій за трьома критеріями (тип суб'єкта, повторність, обсяг потенційної шкоди) із заміною плоских НМДГ на оборотно-прив'язані ставки. Конкретно це означає трирівневу шкалу: для операторів критичної інформаційної інфраструктури I категорії – до 2 % річного обороту або 50 млн гривень, для важливих суб'єктів – до 1 %, для інших регульованих – до 0,5 % з абсолютним мінімумом для малого та середнього бізнесу. Така архітектура відтворює логіку статті 34 NIS 2, знімає доктринальне заперечення про порушення пропорційності й водночас зберігає захисну межу для МСБ [4, 16]. Другий елемент – compliance-захист: чинна сертифікація системи управління інформаційною безпекою за ISO/IEC 27001 або еквівалентним стандартом має ставати пом'якшувальним фактором, що знижує штраф до 50 %, на зразок методології EDPB Guidelines 04/2022 [9, 14]. Ідея compliance-захисту принципово змінює телеологію санкції: з покарання вона перетворюється на регулятивний стимул, що заохочує сумлінних суб'єктів інвестувати в безпеку, а не вишукувати способи мінімізувати штрафні ризики.

Третій елемент авторської моделі – доказова реформа, без якої навіть найдосконаліші санкції залишатимуться мертвою буквою. Логи SIEM-систем, тікети SOC, події з міткою MITRE ATT&CK потребують прямого нормативного визнання як допустимі адміністративні докази – за умови криптографічного підпису, незмінного зберігання й відповідності стандартам ISO/IEC 27037, 27041–27043 [22]. Чинний Кодекс адміністративного судочинства й постанова Кабінету Міністрів № 518 цього прямо не регулюють, змушуючи суди застосовувати загальні правила оцінки доказів і породжуючи процесуальну невизначеність, яку досвідчений адвокат з легкістю використає на користь відповідача. Четвертий елемент – добровільне самоповідомлення з амністією:

суб'єкт, який повідомив CERT-UA про інцидент протягом 24 годин, повністю співпрацює зі слідством і виконує план коригувальних дій, отримує імунітет від адміністративного штрафу [13, 19]. Ця модель спирається на статті 23 і 30 NIS 2, європейську практику імунітету у конкурентному праві та емпіричні дані про поведінкові ефекти добровільного звітування; її цінність полягає в тому, що вона атакує головну перешкоду ефективності – латентність деліктів – не через посилення контролю, а через створення позитивного стимулу до прозорості. П'ятий елемент – особиста відповідальність керівника з кіберзахисту: стаття 5-1 Закону № 4336-IX створила цього суб'єкта, але без санкційного дзеркала – конкретного складу в КУпАП – посада ризикує стати декоративною [17, 21]. Наскрізно через усі п'ять елементів проходить вимога відмови від презумпції класичної причинності на користь моделі підвищення ризику: якщо обов'язок існував саме для запобігання тому виду шкоди, що настав, і його порушення суттєво підвищило ймовірність такої шкоди, причинний зв'язок презумується [4, 16, 20].

Висновки. Українська адміністративна відповідальність за порушення вимог кібербезпеки опинилася у потрійній пастці, кожен елемент якої підсилює два інших: матеріальне право рухається в напрямку NIS 2 швидше, ніж у багатьох держав-членів ЄС, проте санкційне застрягло в логіці плоских неоподатковуваних мінімумів; статистична прозорість відсутня, що унеможливлює оцінку ефективності; правозастосування витісняється у кримінальний трек через мізерність штрафів, а адміністративний інструмент перетворюється на порожню норму.

Воєнний контекст не може виправдовувати відтермінування реформи – навпаки, саме він робить її екзистенційно необхідною. Приватні оператори критичних послуг перетворилися на фронт, не менш значущий за військовий, і щоденні кібератаки на державні реєстри, телекомунікаційних операторів та

ISSN: 3041-2110

енергетичну інфраструктуру створюють загрозу, яку символічні адміністративні санкції нездатні ані стримати, ані компенсувати.

Оборотно-прив'язані санкції, диференційовані за категорією суб'єкта, повторністю та обсягом потенційної шкоди, дозволять закрити найглибший розрив між українським правом і європейським acquis. Compliance-захист перетворить санкцію з інструменту покарання на регулятивний стимул, заохочуючи системне інвестування в кіберзахист замість разових формальних перевірок.

Доказова реформа, що визнає логи SIEM-систем, тікети SOC та події з міткою MITRE ATT&CK допустимими адміністративними доказами за умови криптографічного підпису й незмінного зберігання, усуне процесуальну невизначеність, яка сьогодні робить доказування кібербезпекових деліктів майже нездійсненним. Механізм добровільного самоповідомлення з амністією зменшить латентність – ключову перешкоду ефективності будь-якого регулятивного режиму у цифровому середовищі.

Без реалізації запропонованого комплексу заходів розрив між сотнями мільйонів доларів збитків і кількома тисячами гривень штрафу залишатиметься системною субсидією для нерадивості. Подальші дослідження мають бути спрямовані на розробку конкретних законопроєктних пропозицій щодо внесення змін до КУпАП, а також на емпіричний аналіз перших рішень за NIS 2 у державах-членах ЄС, що забезпечить порівняльну базу для калібрування українських санкцій.

Список використаних джерел

1. Топчій В. В., Бодунова О. М. Адміністративна відповідальність у сфері забезпечення кібербезпеки України. *Науковий вісник публічного та приватного права*. 2021. Вип. 5, т. 3. С. 31–35. DOI: https://doi.org/10.32844/2618-1258.2021.5.3.5

2. Мазійчук В. А. Характеристика адміністративних правопорушень в інформаційній сфері. *Аналітично-порівняльне правознавство*. 2025. Вип. 2.2. DOI: 10.24144/2788-6018.2026.02.2.27. URL: https://journal-app.uzhnu.edu.ua/article/view/357611

3. Гончаренко Г. А. До проблеми визначення та розмежування дефініцій «інформаційна безпека» і «кібербезпека». *Аналітично-порівняльне правознавство*. 2024. № 5. С. 466–471. DOI: 10.24144/2788-6018.2024.05.73. URL: https://journal-app.uzhnu.edu.ua/article/view/313097

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

5. Chiara P. G. Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review*. 2024. Vol. 53. Art. 105961. DOI: 10.1016/j.clsr.2024.105961. URL: https://doi.org/10.1016/j.clsr.2024.105961

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

7. Романова О. М. Кібербезпека під час повномасштабного вторгнення РФ. *Часопис Київського університету права*. 2024. № 2. С. 56–59. DOI: 10.36695/2219-5521.2.2024.9. URL: https://chasprava.com.ua/index.php/journal/article/view/1075

8. Опанович М. Аналіз кібератак та діяльності APT груп в Україні. *Кібербезпека: освіта, наука, техніка*. 2024. Т. 4, № 24. С. 172–184. DOI: 10.28925/2663-4023.2024.24.172184. URL: https://doi.org/10.28925/2663-4023.2024.24.172184

9. Schmitz-Berndt S. Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*.

2023. Vol. 9, Iss. 1. Art. tyad009. DOI: 10.1093/cybsec/tyad009. URL: https://doi.org/10.1093/cybsec/tyad009

10. Головацький Н. Т. Адміністративно-правові механізми захисту персональних даних у системах автоматизованого прийняття рішень як превенція корупційних ризиків. *Аналітично-порівняльне правознавство*. 2025. № 6. Ст. 85. DOI: 10.24144/2788-6018.2025.06.3.85. URL: https://journal-app.uzhnu.edu.ua/article/view/347422

11. Markopoulou D., Papakonstantinou V., De Hert P. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*. 2019. Vol. 35, Iss. 6. Art. 105336. DOI: 10.1016/j.clsr.2019.06.007. URL: https://doi.org/10.1016/j.clsr.2019.06.007

12. Довгань О. Д. Правове регулювання кібербезпеки критичної інфраструктури в умовах воєнного стану. *Інформація і право*. 2024. № 4 (51). С. 113–122. URL: http://jnas.nbuv.gov.ua/j-pdf/Infpr_2024_4_13.pdf

13. Білан І. А. Формування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. *Інформація і право*. 2024. № 4 (51). С. 153–163. URL: http://jnas.nbuv.gov.ua/j-pdf/Infpr_2024_4_17.pdf

14. 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: 10.1365/s43439-021-00045-7. URL: https://doi.org/10.1365/s43439-021-00045-7

15. Цуркан В., Ракович В. Механізм повідомляння про події кібербезпеки об'єктів критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2025. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/1200

16. Teichmann F. Cybersecurity of critical infrastructure in Europe: the NIS2 directive in focus. *International Cybersecurity Law Review*. 2025. Vol. 6. P. 207–220.

DOI: 10.1365/s43439-025-00154-4. URL: https://doi.org/10.1365/s43439-025-00154-4

17. Bartoli L. Cybersecurity and the Fight against Cybercrime: Partners or Competitors? *European Journal of Risk Regulation*. 2025. Vol. 16, Iss. 2. P. 498–513. DOI: 10.1017/err.2025.31. URL: https://doi.org/10.1017/err.2025.31

18. Ducuing C. Understanding the rule of prevalence in the NIS Directive: C-ITS as a case study. *Computer Law & Security Review*. 2021. Vol. 40. Art. 105514. DOI: 10.1016/j.clsr.2020.105514. URL: https://doi.org/10.1016/j.clsr.2020.105514

19. Busetti S., Scanni F. M. Evaluating incident reporting in cybersecurity: From threat detection to policy learning. *Government Information Quarterly*. 2025. Vol. 42, Iss. 1. Art. 102000. DOI: 10.1016/j.giq.2024.102000. URL: https://doi.org/10.1016/j.giq.2024.102000

20. Vavoula A., Triantafyllou V., Triantafyllou P. Identifying and Modeling Barriers to Compliance with the NIS2 Directive: A DEMATEL Approach. *Journal of Cybersecurity* and Privacy. 2025. Vol. 5, Iss. 4. Art. 97. DOI: 10.3390/jcp5040097. URL: https://doi.org/10.3390/jcp5040097

21. Miadzvetskaya Y. EU Sanctions in Response to Cyber-Attacks as Crime-Based Emergency Measures. *Computer Law & Security Review*. 2024. Vol. 54. Art. 105977. DOI: 10.1016/j.clsr.2024.105977. URL: https://doi.org/10.1016/j.clsr.2024.105977

22. Ismail I., Zainol Ariffin K. A. The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLOS ONE*. 2025. Vol. 20, Iss. 9. Art. e0331683. DOI: 10.1371/journal.pone.0331683. URL: https://doi.org/10.1371/journal.pone.0331683