УДК 004.056:34(477:4-67)
DOI https://doi.org/10.32782/2312-1815/2026-23-19

Андрій Пролорензо
ORCID: 0009-0008-3704-2219

ПОЛІТИКО-ПРАВОВІ ЗАСАДИ ГАРМОНІЗАЦІЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ ІЗ ЗАКОНОДАВСТВОМ ЄВРОПЕЙСЬКОГО СОЮЗУ: ІМПЛЕМЕНТАЦІЯ NIS2 ТА ІНСТИТУЦІЙНА СПРОМОЖНІСТЬ

У статті досліджено політико-правові засади гармонізації системи кібербезпеки України із законодавством Європейського Союзу в умовах європейської інтеграції та триваючої збройної агресії РФ. Методологічну основу становлять порівняльно-правовий аналіз Директиви (ЄС) 2022/2555 (NIS2) та інституційний підхід до оцінки координації суб'єктів кібербезпеки.

Виявлено, що окрім нормативних розбіжностей, ключовими бар'єрами імплементації є політико-інституційні чинники: конкуренція за повноваження між основними суб'єктами сектору безпеки (Держспецзв'язку, СБУ, РНБО), конфлікт інтересів між вимогами євроінтеграції та ресурсними обмеженнями бізнесу, а також суперечність між необхідністю обміну інформацією та каральною парадигмою чинного кримінального законодавства. Обґрунтовано необхідність законодавчого закріплення принципу «безпечної гавані» (safeharbor) для стимулювання звітування про інциденти та уникнення ризику перетворення вимог NIS2 на «нефінансовані мандати» для критичної інфраструктури. Наголошено на критичному навантаженні на систему реагування: за даними CERT-UA кількість опрацьованих інцидентів зросла з 4315 у 2024 р. до майже 6000 у 2025 р. Запропоновано рекомендації щодо інституційної консолідації та зміни моделі відносин «держава-бізнес» у кіберсфері.

Ключові слова: *кібербезпека, гармонізація законодавства, кіберзахист, Європейський Союз, критична інфраструктура, NIS2, інституційна конкуренція, безпечна гавань, управління кіберризиками.*

Вступ. Кібербезпека є системною складовою державної політики та національної безпеки, оскільки цифровізація публічних послуг, економіки та оборонної сфери одночасно створює нові можливості і множить вектори кібератак. Для України цей виклик посилюється гібридним характером агресії Російської Федерації, де кібероперації застосовуються як інструмент дестабілізації, підриву довіри та порушення функціонування критичної інфраструктури [1]. Динаміка інцидентів, зафіксована урядовою командою CERT-UA, демонструє зростання навантаження на національну систему реагування: 4315 опрацьованих кіберінцидентів у 2024 р. та майже 6000 – у 2025 р., а також повідомлене зростання ворожих атак на 37% у 2025 р. [13, 14].

У контексті європейської інтеграції України гармонізація законодавства з правом ЄС у сфері кібербезпеки набуває прикладного значення: йдеться про сумісність вимог до управління кіберризиками, повідомлення про інциденти, нагляду та відповідальності, а також про здатність України інтегруватися до європейського простору кіберстійкості. Базовим орієнтиром сучасної європейської регуляторної рамки є Директива (ЄС) 2022/2555 (NIS2), яка встановлює «заходи для високого спільного рівня кібербезпеки в Союзі» та скасовує Директиву (ЄС) 2016/1148 (NIS1), яка стала першим базовим стандартом кібербезпеки у Європі, проте з часом перестала відповідати масштабу нових гібридних загроз [16, 19]. Суміжними актами є Регламент (ЄС) 2019/881 (CybersecurityAct) щодо ролі ENISA та системи європейської сертифікації кібербезпеки [23], а також Директива (ЄС) 2022/2557 про стійкість

критичних суб'єктів (CER), що доповнює NIS2 у площині загальної стійкості критичної інфраструктури [17].

Україна вже має базовий каркас правового регулювання: Закон України «Про основні засади забезпечення кібербезпеки України» [9], Закон України «Про критичну інфраструктуру» [8], а також Стратегію кібербезпеки України, введену в дію Указом Президента № 447/2021 [10]. Водночас наукові публікації українських дослідників засвідчують наявність «розривів» між національним регулюванням і вимогами ЄС, зокрема у частині інституційної архітектури, нагляду, управління ризиками та механізмів реагування [1, 2, 4, 5, 6, 7, 11, 12].

Постановка проблеми. Наявний рівень нормативної визначеності та інституційної узгодженості української системи кібербезпеки не повною мірою відповідає ризик-орієнтованій логіці NIS2, що ускладнює гармонізацію з правом ЄС, взаємосумісність процедур реагування та впровадження європейських стандартів кіберстійкості.

Аналіз останніх досліджень і публікацій. В українському академічному дискурсі проблематика гармонізації кібербезпеки з правом ЄС розкривається в роботах, присвячених правовому забезпеченню національного кіберпростору у воєнний часта в євроінтеграційному вимірі (А. Лисеюк і Т. Свінцицька) [4], викликам гармонізації актів ЄС у сфері кібербезпеки (С. Савчук) [11, 12], імплементації європейських правових норм у національне законодавство (С. Мазепа) [5], організаційно-правовим заходам забезпечення безпеки цифрових послуг (О. Передерій, Л. Кулачок-Тітова) [7], кіберзахисту об'єктів критичної інфраструктури в умовах кібервійни (Я. Мануілов) [6], а також правовим проблемам цифрового розвитку і національної безпеки (І. Доронін) [2]. Зарубіжні дослідження додатково висвітлюють практичні виклики впровадження NIS2 у державах ЄС (Ф. Тайхманн) [24] та значення публічно-приватних партнерств (К. Хоєцька) [15].

Мета статті. Виявити політико-правові бар'єри гармонізації системи кібербезпеки України із законодавством ЄС (насамперед NIS2) та обґрунтувати напрями їх подолання.

Завдання статті. Охарактеризувати нормативний каркас кібербезпеки України та проблемні вузли правозастосування; окреслити ключові новели NIS2 і суміжних актів ЄС (CybersecurityAct, CER) як рамку гармонізації; виокремити основні розриви між українським регулюванням і вимогами NIS2 (охоплення суб'єктів, управління ризиками, повідомлення про інциденти, нагляд і відповідальність); узагальнити релевантні підходи українського й зарубіжного наукового дискурсу; сформулювати практико-орієнтовані рекомендації нормативного та інституційного характеру.

Матеріал дослідження. Нормативно-правові акти України у сфері кібербезпеки та критичної інфраструктури [8, 9, 10]; акти права ЄС – NIS2 [16], CybersecurityAct [23] та CER [17]; офіційні дані CERT-UA про кіберінциденти [13, 14]; сучасні наукові праці українських і зарубіжних авторів щодо правового регулювання кібербезпеки, управління кіберризиками, захисту критичної інфраструктури, сертифікації та публічно-приватного партнерства.

Методи дослідження. Порівняльно-правовий метод (зіставлення вимог NIS2 із положеннями українського законодавства), нормативно-догматичний метод (аналіз юридичних конструкцій обов'язків, нагляду та відповідальності), інституційний підхід (оцінка координаційних механізмів, CSIRT-спроможностей і взаємодії держави з операторами критичної інфраструктури), а також системний підхід, який дозволяє розглядати кібербезпеку у зв'язку із ширшими рамками стійкості критичних суб'єктів, кіберстандартизації та європейської сертифікації.

Робочі дефініції. «Кібербезпека» у національному праві розуміється через правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави у кіберпросторі [9]. «Критична інфраструктура» визначається як об'єкти, системи та ресурси, порушення функціонування яких може спричинити негативні наслідки для національної безпеки, економіки, довкілля та життєдіяльності населення [8].

Під «гармонізацією законодавства» розуміється цілеспрямоване наближення норм, процедур і інституцій до acquis ЄС з метою забезпечення правової сумісності та ефективної імплементації стандартів ЄС. "NIS2" – це Директива (ЄС) 2022/2555 про заходи для високого спільного рівня кібербезпеки в Союзі, яка оновлює NIS1 та встановлює мінімальні вимоги до кіберстійкості, управління ризиками і повідомлення про інциденти [16]. "CSIRT" (Computer Security Incident Response Team) – команда реагування, що забезпечує оперативне реагування та координацію у разі кіберінцидентів [16].

Виклад основного матеріалу. Нормативний каркас кібербезпеки України визначається базовими актами, які встановлюють суб'єктний склад, принципи координації та підходи до захисту критичних об'єктів. Зокрема, Закон України «Про основні засади забезпечення кібербезпеки України» закріплює систему суб'єктів і загальні принципи координації [9]. Закон України «Про критичну інфраструктуру» формує організаційно-правові основи захисту критичних об'єктів [8], а Стратегія кібербезпеки України визначає стратегічні пріоритети та очікувані результати розвитку системи кібербезпеки [10]. Водночас правозастосовна практика засвідчує, що наявність базових законів і стратегічних документів сама по собі не гарантує єдності регуляторних підходів: як практики, так і академічні джерела вказують на фрагментарність підзаконного «пакета» та нерівномірність вимог у різних секторах. Унаслідок цього ускладнюються стандартизація управління кіберризиками, уніфікація методик оцінювання ризиків і проведення аудитів/контролю, а також належна взаємодія між державою та операторами критичної інфраструктури, зокрема в частині обміну інформацією про інциденти та загрози. Так, С. Савчук наголошує на потребі посилення інституційної спроможності та нормативної конкретизації вимог до управління ризиками й звітності про інциденти у логіці ЄС, що безпосередньо корелює з підходами NIS2 до комплаєнсу та нагляду [11, 12]. А. Лисеюк і Т. Свінцицька підкреслюють, що умови воєнного стану додатково актуалізують необхідність єдиних підходів до регуляторного контролю, процедур реагування та координації між суб'єктами системи кібербезпеки, оскільки фрагментарність норм і практик підвищує вразливість критичних сервісів [4].

З огляду на ці висновки українських дослідників, подальший аналіз доцільно вибудовувати через зіставлення національного регуляторного підходу з тим стандартом, який нині визначає рамку кіберстійкості в ЄС і фактично задає орієнтир для держав-кандидатів. Саме в такій ролі виступає Директива (ЄС) 2022/2555 (NIS2), що концентрує ключові вимоги до управління ризиками, повідомлення про інциденти та наглядової моделі.

NIS2 розширює перелік секторів, уточнює категоризацію суб'єктів, підсилює нагляд і відповідальність керівництва та робить акцент на безпеці ланцюгів постачання [16]. З огляду на практику ЄС, NIS2 розглядається як перехід від «мінімального узгодження» до більш жорсткого комплаєнсу, що вимагає готовності як суб'єктів, так і державних наглядових структур [24].

Водночас регуляторна рамка ЄС у сфері кібербезпеки не обмежується лише NIS2, а функціонує як взаємопов'язаний пакет інструментів, що підсилюють один одного. Зокрема, CybersecurityAct розширює мандат ENISA (Агентства Європейського Союзу з кібербезпеки – головної інституції, що відповідає за стандартизацію та координацію дій держав-членів), а також формує єдину європейську рамку сертифікації інформаційно-комунікаційних технологій (ІКТ), що є критично важливим для забезпечення довіри до цифрових продуктів на внутрішньому ринку [23], що істотно впливає на питання довіри до цифрових продуктів і послуг, у тому числі при транскордонній взаємодії. CER, своєю чергою, задає логіку стійкості критичних суб'єктів, включно з плануванням безперервності та управлінням кризами [17]. У сукупності ці акти формують нормативний «каркас» ЄС, у межах якого гармонізація для України означає не тільки формальне наближення норм, а й практичне узгодження процедур управління ризиками, нагляду, звітності та координації.

У цьому контексті порівняльний аналіз дозволяє виокремити ключові «розриви» гармонізації України з підходами NIS2. Насамперед, у NIS2 правовий статус суб'єкта визначає обсяг обов'язків, режим нагляду та санкційні наслідки [16]. Україна має базові визначення та механізми категоризації критичної інфраструктури [8], однак потребує більш деталізованих критеріїв охоплення і диференціації обов'язків залежно від критичності послуг і профілю ризику, що є важливим для пропорційності регулювання. На цю проблему опосередковано вказують і вітчизняні дослідження: Я. Мануілов підкреслює ознаки критичності та фактори вразливості об'єктів в умовах кібервійни, що може бути використано як наукове підґрунтя для уточнення критеріїв віднесення та пріоритизації захисних вимог [6].

Далі, NIS2 трактує управління кіберризиками як юридичний обов'язок суб'єктів і прямо вимагає впровадження комплексу заходів, серед яких інцидент-менеджмент, управління вразливостями, політики доступу, безпека ланцюгів постачання, навчання персоналу та забезпечення безперервності [16]. Українська практика, натомість, демонструє нерівномірність упровадження таких заходів у різних секторах, що відображено у працях вітчизняних авторів, які наголошують на потребі стандартизованих методик і національних керівництв для операторів [4, 5, 6, 11]. Унаслідок цього виникає проблема зіставлення рівнів готовності, а також ускладнюється регуляторний контроль та аудит.

Окремий блок розривів стосується повідомлення про інциденти, інформаційного обміну та довіри. NIS2 передбачає поетапне повідомлення про «значні інциденти», включно з раннім повідомленням протягом 24 годин [16]. В українських умовах інтенсивність атак робить критичною здатність швидко виявляти, класифікувати та повідомляти інциденти, а також обмінюватися технічними індикаторами компрометації. Дані CERT-UA фіксують зростання інцидентів і підтверджують потребу у правовому оформленні процедур обміну інформацією, у тому числі з приватним сектором, із гарантіями конфіденційності повідомлень [13, 14]. Додатково, праці О. Передерія та Л. Кулачок-Тітової підкреслюють значення довіри до цифрових послуг та організаційно-правових заходів кіберзахисту при їх наданні, що прямо впливає на готовність суб'єктів до своєчасного і повного репортингу [7].

Нарешті, критичним є розрив у наглядовій моделі, що ускладнюється політико-інституційним фактором. NIS2 вимагає чіткого визначення компетентних органів та посилення відповідальності керівництва (top management accountability) [16]. Однак для України ключовим політико-правовим бар'єром виступає не лише технічна потреба уникнення дублювання, а й фактична інституційна конкуренція та боротьба за повноваження між основними суб'єктами сектору безпеки і оборони – Держспецзв'язку, профільними підрозділами СБУ, апаратом РНБО та Міністерством цифрової трансформації.

Ця міжвідомча фрагментація створює ризик розмивання відповідальності, коли кожен орган намагається зберегти вплив на регулювання кіберсфери, але уникає повної відповідальності за провали в кіберзахисті. Без політичного вирішення цього питання – чіткого розмежування сфер впливу та визначення єдиного (або чітко скоординованого) центру прийняття рішень згідно з логікою «компетентного органу» (Competent Authority) в NIS2 – будь-яка нормативна гармонізація залишатиметься декларативною та нежиттєздатною на практиці. Як слушно зазначає І. Доронін, цифровий розвиток без належного державного планування та гарантій безпеки породжує системні ризики [2], і в умовах України ці ризики посилюються саме відсутністю консолідованої політичної волі до завершення інституційної реформи сектору.

Емпіричним підтвердженням цієї конкуренції є низка нормативних колізій та публічних дискусій, що супроводжували реформу сектору безпеки.

По-перше, боротьба за статус Національного регулятора критичної інфраструктури. Під час розробки Закону «Про критичну інфраструктуру» (2021) [8] тривала прихована апаратна боротьба між СБУ та Держспецзв'язку за контроль над Реєстром об'єктів критичної

інфраструктури. Компромісним рішенням стало надання Держспецзв'язку статусу «Уповноваженого органу», проте СБУ зберегла за собою фактичний контроль через механізми контрозвідувального захисту та погодження паспортів безпеки, що створило систему «подвійного ключа» в управлінні.

По-друге, колізія навколо реформи СБУ. Законопроєкт № 3196-Д щодо реформи СБУ викликав гостру критику з боку експертної спільноти та європейських партнерів саме через намагання спецслужби зберегти невластиві їй функції регулювання економіки та кіберсфери, які дублюють повноваження Кіберполіції та Держспецзв'язку. Фактично йдеться про конфлікт між моделлю «сервісної служби» (яку просуває Держспецзв'язку та Мінцифри) і моделлю «силового контролю» (СБУ).

По-третє, дискусія щодо системи КСЗІ (Комплексна система захисту інформації). Тривалий конфлікт між Мінцифри (яке виступає за дерегуляцію та швидку цифровізацію) та блоком Держспецзв'язку/СБУ (які відстоюють жорстку атестацію систем) є прикладом ціннісного розколу. Хоча війна тимчасово згладила ці суперечності, спроби блокування впровадження хмарних технологій для держреєстрів у перші дні вторгнення під приводом «вимог КСЗІ» яскраво ілюструють, як інституційна інерція та боротьба за контроль гальмують технологічну стійкість.

Політичний аналіз імплементації NIS2 потребує також висвітлення конфлікту інтересів ключових стейкхолдерів. Роль «драйверів» гармонізації виконують органи, відповідальні за європейську інтеграцію та цифрову трансформацію, для яких пріоритетом є виконання політичних зобов'язань перед ЄС (acquisconditionality). Натомість прихований опір формується у двох інших площинах. По-перше, бізнес-середовище та оператори критичної інфраструктури (як приватні, так і комунальні) розглядають жорсткі вимоги комплаєнсу як надмірний фінансовий тягар, намагаючись лобіювати «пом'якшення» регуляцій або відтермінування їх введення [24]. По-друге, представники сектору безпеки і оборони в умовах війни схильні до «сек'юритизації» (securitization) даних: вони чинять опір ідеї транскордонного звітування про інциденти та наданню доступу до чутливої інформації цивільним органам ЄС (наприклад, ENISA або CSIRT network). Варто визнати, що ця позиція має під собою реальне підґрунтя: в умовах активної діяльності російських розвідувальних мереж у країнах ЄС, побоювання українських спецслужб щодо того, що технічні деталі про вразливості національних систем можуть потрапити до ворога через наднаціональні бази даних, є раціональною безпековою дилемою, а не лише проявом бюрократичної закритості [4, 6]. Балансування цього трикутника інтересів (євроінтеграція – вартість для бізнесу – операційна безпека) є головним політичним викликом реформи.

Зазначене підводить до важливого методологічного висновку: дискусія про гармонізацію з правом ЄС не може обмежуватися лише порівнянням норм NIS2 та українського законодавства, адже вирішальним є поєднання правових приписів із реальною інституційною спроможністю, організаційними механізмами та ресурсними можливостями їх виконання. Саме тому доцільно окремо окреслити український науковий доробок, який формує аналітичну базу для удосконалення національної моделі кібербезпеки та її зближення з європейськими стандартами.

Українські дослідники поступово формують міждисциплінарний масив знань, релевантний гармонізації із правом ЄС. С. Савчук аналізує нормативну архітектуру ЄС: директиви NIS/NIS2, CybersecurityAct, Загальний регламент про захист даних (GDPR) та Регламент щодо цифрової операційної стійкості (DORA), підкреслюючи потребу інституційного посилення і сертифікації цифрових продуктів для входження до єдиного цифрового ринку ЄС [11, 12]. С. Мазепа у фокусі інформаційної безпеки комплексно оцінює європейську модель правового регулювання та бар'єри імплементації в українське право, зокрема розбіжності правових традицій, інституційні й фінансові обмеження [5].

А. Лисеюк і Т. Свінцицька розкривають нормативні виклики забезпечення кібербезпеки у воєнний період та акцентують на необхідності зближення правових підходів із ЄС за умови збереження керованості й оперативності управління в умовах надзвичайних викликів [4]. О. Передерій та Л. Кулачок-Тітова пропонують систематизацію організаційно-правових заходів безпеки цифрових послуг у контексті протидії кіберзлочинності, що є важливим для осмислення довіри, прозорості та механізмів публічно-приватного партнерства [7]. Я. Мануілов деталізує проблематику кіберзахисту критичної інфраструктури в умовах кібервійни та обґрунтовує потребу конкретизації ознак критичності й ризиків як передумови для встановлення пропорційних обов'язків та пріоритетів захисту [6].

Додатково, праці, присвячені правовому забезпеченню кібербезпеки критичної інформаційної інфраструктури та цифровій безпеці, акцентують на необхідності синхронізації правових і організаційних механізмів, зокрема у сфері критичної інформаційної інфраструктури [21]. Узагальнення наведених підходів дозволяє зробити висновок, що практична гармонізація із правом ЄС потребує поєднання двох взаємодоповнювальних вимірів: нормативного (чіткі юридичні обов'язки, процедури, стандарти та правила звітності) й інституційного (координація, нагляд, спроможності реагування та взаємодія з приватним сектором).

У нормативному вимірі доцільно адаптувати логіку NIS2 щодо класифікації суб'єктів і встановлення диференційованих обов'язків (essential/important) [16]. Необхідно на рівні закону закріпити мінімальний перелік заходівуправління кіберризиками для критичної інфраструктури (інцидент-менеджмент, управління вразливостями, доступами, безперервністю, навчанням персоналу, безпекою постачання) у ризик-орієнтованій формі [4, 6, 11, 12,16, 21]. Окремої уваги потребує наближення повідомлення про інциденти до NIS2: етапність повідомлення, строки, критерії «значного інциденту», а також правила конфіденційності, які одночасно забезпечують правову визначеність і стимулюють добросовісне повідомлення [13, 14, 16].

Важливо, щоб нормативні зміни враховували взаємозв'язок NIS2 із CybersecurityAct (сертифікація ІКТ) [23] та CER (стійкість критичних суб'єктів) [17]. Така зв'язка відповідає європейській логіці, за якої кіберстійкість розглядається як елемент загальної стійкості критичних сервісів. У національному вимірі це означає правове поєднання кіберзаходів із плануванням безперервності та кризовим управлінням.

В інституційному вимірі варто деталізувати компетенційну матрицю органів (формування політики, нагляд, координація реагування, стандартизація, міжнародна взаємодія), що зменшить ризики дублювання і конфліктів компетенцій та підвищить передбачуваність регуляторного середовища [4, 9, 8, 10, 11, 12]. З огляду на зростання кількості інцидентів, доцільно посилювати спроможності CSIRT, включно зі стандартизованими протоколами взаємодії з операторами та локальними центрами реагування, щоб забезпечити швидкість обміну інформацією та узгодженість дій під час інцидентів [13, 14].

Суттєвим елементом інституційного виміру є правові стимули для публічно-приватного партнерства та обміну інформацією. Зарубіжні дослідження підкреслюють, що публічно-приватне партнерствоможе підвищувати стійкість за рахунок «колективного захисту», однак потребує нормативних гарантій конфіденційності, прозорого розподілу відповідальності та визначених правил доступу до чутливої інформації [15]. Український контекст також підтверджує потребу у довірчих механізмах обміну інформацією, що узгоджується з вітчизняними оцінками безпеки цифрових послуг та організаційно-правових заходів кіберзахисту [7].

Логічним продовженням цієї тези є питання не лише про те, що саме слід змінити у нормах і інституціях, а й про те, яким способом забезпечити послідовне наближення до acquis ЄС – із прозорою процедурою, визначеними відповідальними суб'єктами та вимірюваними результатами. Відповідно, доцільно окреслити механізм адаптації у сфері кібербезпеки

як «дорожню карту», що поєднує законодавчі рішення, підзаконну регламентацію та операційну готовність системи реагування.

Правовий механізм наближення до acquis ЄС у сфері кібербезпеки доцільно розглядати як складову загальної політики адаптації права, яка в практиці держав-кандидатів зазвичай включає послідовні етапи: (1) «скринінг» відповідності; (2) розроблення плану імплементації; (3) прийняття законодавчих змін і підзаконних актів; (4) інституційне зміцнення та навчання; (5) моніторинг виконання і корекція. У кіберсфері ці етапи мають бути доповнені технічною стандартизацією та підтриманням операційної готовності CSIRT, адже без них формальна відповідність нормам ЄС не трансформується у реальну кіберстійкість мереж, сервісів і критичних процесів [16, 23, 13, 14].

Для України доцільно закріпити «дорожню карту» гармонізації із NIS2 як комплексний пакет: а) зміни до профільних законів (визначення суб'єктів/секторів, обов'язків, нагляду, відповідальності); б) секторальні підзаконні акти та методики (оцінювання ризиків, аудит, безперервність, класифікація інцидентів); в) регламентація інформаційного обміну (правила конфіденційності, відповідальність за розголошення, «безпечні гавані» для добросовісного повідомлення); г) інтеграція сертифікації ІКТ у критичних секторах; ґ) кадровий та фінансовий план нарощування спроможностей. Такий підхід узгоджується із висновками С. Савчука щодо потреби незалежної координації, комплаєнсу та сертифікації як практичних умов входження до єдиного цифрового простору ЄС [11, 12].

Водночас навіть добре вибудувана «дорожня карта» ризикує залишитися декларативною, якщо вимоги NIS2 не будуть перекладені на рівень зрозумілих і відтворюваних процедур для операторів. Саме тому наступним кроком має бути операціоналізація ризик-орієнтованих обов'язків через стандарти, методики та сертифікаційні інструменти, які дозволяють перетворити принципи директиви на конкретні політики, контрольні заходи, метрики і документообіг (зокрема для управління вразливостями, планування безперервності та повідомлення про інциденти) [16, 23]. Практична проблема «паперової імплементації» полягає в тому, що директивні вимоги формулюються на рівні загальних приписів і переліків заходів, тоді як організаціям потрібні керовані інструкції: методики оцінювання ризиків, шаблони планів безперервності, процедури внутрішнього контролю, формати раннього/повного повідомлення про інциденти та протоколи взаємодії з CSIRT [13, 14, 16]. Відтак для України принципово важливо на нормативному рівні визначити, які саме рамки та стандарти можуть слугувати «належною практикою» виконання вимог NIS2, а також яким чином їх застосування враховуватиметься під час нагляду та оцінювання відповідності. Тому операціоналізація NIS2 має спиратися на NIST CSF 2.0, ISO/IEC 27001 та пов'язані з ними методики контролю й аудиту із чітким визначенням їхнього статусу в національному праві, а також з механізмом узгодження з європейською системою сертифікації та підходами ENISA, закріпленими CybersecurityAct [23].

У міжнародній практиці широко використовується NIST CybersecurityFramework (CSF), який у версії 2.0 пропонує структуру функцій і категорій для побудови системи кіберстійкості організації (ідентифікація, захист, виявлення, реагування, відновлення) [22]. Для побудови системи управління інформаційною безпекою (ISMS) одним із базових стандартів є ISO/IEC 27001:2022 [20]. Включення посилань на такі рамки у підзаконні акти (наприклад, як допустимі еквіваленти) може підвищити передбачуваність вимог та забезпечити єдиний підхід до аудитів і самооцінювання.

Європейський вимір доповнюється сертифікацією ІКТ за CybersecurityAct, який передбачає європейські схеми сертифікації та посилює роль ENISA [23]. ENISA у своїх матеріалах додатково роз'яснює логіку й елементи рамки сертифікації ЄС та практичні аспекти її застосування, що важливо для коректного впровадження цих підходів у критичних секторах [18]. Для критичних секторів це має прикладне значення: вимоги NIS2 щодо безпеки ланцюгів

постачання можуть реалізовуватися через мінімальні рівні сертифікації для постачальників та критичних компонентів, що зменшує ризик системних вразливостей.

В українському науковому дискурсі акцент на стандартизації також присутній. Зокрема, дослідження щодо критичної інформаційної інфраструктури підкреслюють необхідність поєднання правових норм із технічними та організаційними вимогами, а також формалізації процесів контролю й аудиту як передумови керованої кіберстійкості операторів [21]. Водночас навіть найбільш якісні стандарти та методики не забезпечують результату без практичного середовища, у якому суб'єкти готові своєчасно повідомляти про інциденти, ділитися технічними даними та координувати реагування. Саме тому питання стандартизації логічно доповнюється питанням організації довірчого інформаційного обміну та правових гарантій участі приватного сектору в системі кібербезпеки.

Ефективність NIS2 значною мірою залежить від налагодженого обміну інформацією між державою, CSIRT та операторами, оскільки на практиці йдеться про передачу індикаторів компрометації, описів тактик і технік атак, даних про вразливості, а також координацію реагування на інциденти, які можуть мати каскадний характер. Водночас для бізнесу існують природні бар'єри участі в такому обміні: репутаційні ризики, ризики адміністративної або договірної відповідальності, а також загроза розкриття комерційної таємниці. Тому політико-правове завдання України полягає у формуванні правового режиму, який одночасно стимулює повідомлення та захищає добросовісних суб'єктів. У європейській логіці такий режим передбачає, по-перше, чіткі правила конфіденційності й доступу до даних; по-друге, розмежування інформації, що підлягає публічному розкриттю, та інформації, яка використовується виключно для реагування й запобігання; по-третє, процедури безпечного обміну через уповноважені канали та визначені ролі компетентних органів і CSIRT [16]. Окремо доцільно закріплювати «безпечні гавані» для добросовісного повідомлення: правові гарантії, що передання технічної інформації про інцидент у встановленому порядку не призводитиме до непропорційних санкцій або вторинного використання даних поза цілями реагування, за винятком випадків умисного приховування або грубої недбалості.

Дослідження К. Хоєцька підкреслює роль публічно-приватних партнерств у посиленні стійкості, але водночасвказує на потребу чітких правил і механізмів відповідальності сторін [15]. Українські автори, аналізуючи безпеку цифрових послуг, також наголошують на важливості організаційно-правових заходів, що забезпечують довіру до цифрового середовища [7].

Практичним інструментом подолання бар'єрів довіри має стати законодавче закріплення принципу «безпечної гавані» (safeharbor). Однак в українських реаліях це наштовхується на фундаментальний політико-правовий конфлікт між вимогами NIS2 щодо добровільного обміну інформацією та репресивною логікою чинного кримінального законодавства (зокрема, статей 361, 363 КК України) [3]. На сьогодні бізнес сприймає державу не як партнера у подоланні кризи, а як джерело додаткових ризиків: повідомлення про інцидент часто тягне за собою вилучення серверів, блокування роботи та звинувачення посадових осіб у службовій недбалості.

Тому гармонізація вимагає не лише технічних правок, а й політичної зміни парадигми відносин «держава – бізнес»: від каральної моделі до партнерської. На рівні закону доцільно запровадити режим «безпечної гавані» (safeharbor), за яким своєчасне повідомлення про кіберінцидент і добросовісна співпраця з CSIRT враховуються як підстава для звільнення від кримінальної відповідальності або суттєвого обмеження застосування кримінально-правових заходів щодо жертви інциденту, за винятком випадків умисного сприяння ворогу чи іншої протиправної поведінки. Без таких правових гарантій невтручання правоохоронних органів і стимули до обміну інформацією залишатимуться декларативними, а реальна картина кіберзагроз – неповною та частково прихованою.

Разом із тим запровадження таких стимулів має спиратися на перевірені підходи до нагляду, щоб уникнути ситуації, коли комплаєнс зводиться до формального виконання вимог «для звіту». Досвід імплементації NIS2 у державах ЄС демонструє, що «жорсткість» вимог повинна супроводжуватися реалістичністю їх виконання та підкріплюватися наглядовими спроможностями. Зарубіжні оцінки звертають увагу на те, що розширення переліку секторів і суб'єктів робить критичною здатність держави здійснювати ризик-орієнтований нагляд: пріоритезувати перевірки за рівнем критичності, застосовувати аудит і тестування, а також розвивати секторні CSIRT та центри компетенцій як інституційну опору виконання вимог [24].

Ключовим ризиком є «формальний комплаєнс», коли суб'єкти створюють документи і політики без реальної зміни практик. Для уникнення цього потрібні: (1) мінімальні технічні та організаційні вимоги, які можна перевірити; (2) регулярні навчання та вправи з реагування; (3) інтеграція вимог безпеки у закупівлі та контракти з постачальниками; (4) прозорі процедури нагляду. У контексті України ці підходи корелюють з тезою про необхідність інституційної та кадрової спроможності, яку підкреслюють українські дослідники [4, 5, 11].

Особливістю України є воєнний контекст: частина заходів може бути впроваджена у прискореному порядку, однак важливо, щоб прискорення не призвело до хаотичності регулювання та «нашарування» взаємно неузгоджених вимог. Навпаки, саме стандартизовані підходи, типові методики й уніфіковані процедури (для оцінювання ризиків, класифікації інцидентів, повідомлення про інциденти, аудитів і перевірок) здатні скоротити час впровадження, зберігаючи керованість і відповідність логіці NIS2 [16]. У цьому сенсі пріоритетом має бути не кількість нормативних змін, а їхня узгодженість і здатність породжувати відтворювану практику в різних секторах.

Вимоги NIS2 (цілодобовий моніторинг, функціонування Security Operations Centers (SOC) – центрів оперативного реагування на кіберінциденти, регулярні аудити, конкурентні зарплати фахівцям) є високовитратними [16, 24]. Для критичної інфраструктури, значна частина якої в Україні є державною, комунальною або тарифно-регульованою (енергетика, водопостачання), це створює політичний конфлікт між вимогами безпеки та соціальною чутливістю тарифів [8].

Перекладання витрат на споживача через підвищення тарифів в умовах війни є політично ризикованим, а фінансування з держбюджету – обмеженим через пріоритет фронтових видатків. Крім того, оператори критичної інфраструктури змушені обирати між фізичним відновленням пошкоджених об'єктів та інвестиціями у цифрові бар'єри. Без вирішення цього питання на рівні Кабінету Міністрів (наприклад, через цільові субвенції або міжнародні донорські фонди) законодавчі вимоги NIS2 ризикують перетворитися на «нефінансовані мандати», що призведе до імітації комплаєнсу замість реального захисту.

С. Мазепа у контексті імплементації європейських норм наголошує на значенні інституційних і кадрових рішень, які мають супроводжувати нормотворчість [5]. Війна робить це питання ще гострішим: кадровий потенціал кіберсфери є обмеженим, а підготовка фахівців займає час. Тому важливі «швидкі» інструменти – типові політики, централізовані сервіси безпеки для критичних секторів, стандартизовані вимоги до підрядників і постачальників.

Узгодження з CER [17] дозволяє розглядати кібербезпеку як частину загальної стійкості: у критичних секторах потрібні не лише кіберконтроли, а й плани кризового управління, альтернативні канали комунікації, резервні потужності та відпрацьовані процедури відновлення послуг. Включення цих елементів у правові та підзаконні акти підвищить практичну цінність гармонізації.

Висновки. Гармонізація системи кібербезпеки України із законодавством ЄС (NIS2) виходить за межі суто техніко-юридичного процесу адаптації норм і становить складну політичну реформу, успіх якої залежить від збалансування євроінтеграційних зобов'язань,

економічної спроможності бізнесу та вимог секретності сектору безпеки і оборони. Ключовим політико-інституційним бар'єром імплементації виступає наявна конкуренція за повноваження між основними суб'єктами національної системи кібербезпеки (Держспецзв'язку, СБУ, РНБО, Мінцифри). Відсутність консолідованої політичної волі до визначення єдиного «компетентного органу» (CompetentAuthority) згідно з логікою NIS2 створює ризики дублювання наглядових функцій та розмивання відповідальності за стан захищеності критичної інфраструктури.

Ефективність нормативних змін, зокрема у частині обміну інформацією про інциденти, суттєво обмежується каральною парадигмою чинного кримінального законодавства. Впровадження принципу «безпечної гавані» (safeharbor) для добросовісного бізнесу вимагає декриміналізації дій жертв кібератак та докорінної зміни підходів правоохоронних органів: від вилучення серверів до партнерської допомоги у відновленні стійкості. Водночас реалізація високих стандартів NIS2 містить ризик перетворення нових обов'язків на «нефінансовані мандати». В умовах війни перекладання витрат на кіберзахист критичної інфраструктури виключно на тариф для населення або обігові кошти підприємств є політично ризикованим, що без державних програм співфінансування загрожує зведенням реформи до «формального комплаєнсу». Відтак, на тлі динаміки кіберзагроз (зростання кількості інцидентів до майже 6000 у 2025 р.), перспектива гармонізації полягає у переході від фрагментарних рішень до ресурсно забезпеченої та інституційно узгодженої моделі управління кіберризиками.

Література:

1. Горлинський В., Горлинський Б. Кібервійна як системний виклик кібербезпеці України. Information Technology and Security. 2025. Vol. 13, Iss. 1(24). С. 118–130. DOI:10.20535/2411-1031.2025.13.1.328980.URL:https://ela.kpi.ua/bitstreams/104512e0-daf1-4a10-9c49-5d635cd2b318/download (дата звернення: 18.12.2025)

2. Доронін І. М. Цифровий розвиток та національна безпека у контексті правових проблем. Інформація і право. 2019. № 1(28). С. 29–38. URL: https://ippi.org.ua/sites/default/files/5_12.pdf (дата звернення: 15.12.2025)

3. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2341-14 (дата звернення: 16.12.2025)

4. Лисеюк А., Свінцицька Т. Правове забезпечення кібербезпеки України в умовах воєнного стану та євроінтеграції. Право та інновації. 2024. № 4(48). DOI: 10.37772/2518-1718-2024-4(48)-4. URL: https://pti.org.ua/ndipzir/uk/article/view/1212(дата звернення: 20.12.2025)

5. Мазепа С. Міжнародний досвід захисту інформаційної безпеки: імплементація європейських правових норм в законодавство України. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Т. 4, № 90. DOI: 10.24144/2307-3322.2025.90.3.42. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/09/44-2.pdf(дата звернення: 22.12.2025)

6. Мануілов Я. С. Забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни. Інформація і право. 2023. № 1(44). С. 154–167. DOI: 10.37750/2616-6798.2023.1(44).287780. URL: https://ippi.org.ua/manuilov-yas-zabezpechennya-kiberbezpeki-ob%E2%80%99%D1%94ktiv-kritichnoi-infrastrukturi-v-umovakh-kiberviini-s-1(дата звернення: 19.12.2025)

7. Передерій О. С., Кулачок-Тітова Л. В. Організаційно-правові заходи забезпечення безпеки цифрових послуг в аспекті протидії кіберзлочинності в Україні. Вісник Кримінологічної асоціації України. 2025. Т. 34, № 1. С. 570–578. DOI: 10.32631/vca.2025.1.44. URL: https://vca.univd.edu.ua/index.php/vca/article/view/473(дата звернення: 24.12.2025)

8. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1882-20(дата звернення: 17.12.2025)

9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 17.12.2025)

10. Про Стратегію кібербезпеки України : Рішення РНБО від 14.05.2021, введено в дію Указом Президента України від 26.08.2021 № 447/2021. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/n0055525-21 (дата звернення: 21.12.2025)

11. Савчук С. О. Виклики гармонізації законодавства ЄС в галузі кібербезпеки для України. Економіка, управління та адміністрування. 2024. № 1(107). С. 207–213. DOI: 10.26642/jen-2024-1(107)-207-213. URL: https://ema.ztu.edu.ua/article/view/319745/310337 (дата звернення: 21.12.2025)

12. Савчук С. О. Виклики та можливості інтеграції України в систему кібербезпеки ЄС. Економіка, управління та адміністрування. 2024. № 2(108). С. 198–203. DOI: 10.26642/jen-2024-2(108)-198-203. URL: https://ema.ztu.edu.ua/article/view/319739/310325 (дата звернення: 26.12.2025)

13. CERT-UA минулого року опрацювала 4315 кіберінцидентів. Державна служба спеціального зв'язку та захисту інформації України. 2025. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (дата звернення: 10.01.2026)

14. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів: кількість ворожих атак зросла на 37%. Державна служба спеціального зв'язку та захисту інформації України. 2026. URL: https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37 (дата звернення: 10.01.2026)

15. Chojecka K. Cybersecurity, resilience and sustainability: evaluating theroleofpublic-private partnerships. Yearbookof Antitrust and Regulatory Studies. 2025. DOI: 10.7172/1689-9024. YARS.2025.18.32.9. URL: https://press.wz.uw.edu.pl/cgi/viewcontent.cgi?article=1487&context=yars(дата звернення: 28.12.2025)

16. Directive (EU) 2022/2555 of th eEuropean Parliamentandof the Councilof 14 December 2022 onmeasuresfor a highcommonlevelofcybersecurityacrosstheUnion, amendingRegulation (EU) No 910/2014 andDirective (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union. 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (дата звернення: 15.12.2025)

17. Directive (EU) 2022/2557 oft he European Parliamentandofthe Councilof 14 December 2022 on theres ilienceofcriticalentitiesandrepealing Council Directive 2008/114/EC. Official Journal of the European Union. 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng (дата звернення: 15.12.2025)

18. ENISA. European Union Agency for Cybersecurity. Aboutthe EU cybersecuritycertificationframework (Cybersecurity Act). URL: https://www.enisa.europa.eu/topics/cybersecurity-certification (дата звернення: 29.12.2025)

19. EuropeanCommission. The NIS2 Directive: strengtheningcybersecurityrules (overview/summary). URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (дата звернення: 29.12.2025)

20. ISO. ISO/IEC 27001:2022 – Information security management systems – Requirements. URL: https://www.iso.org/standard/27001.html (дата звернення: 30.12.2025)

21. Kovaliv M., Skrynkovskyi R., NazarYu., Yesimov S., Krasnytskyi I., KaidrovychKh., Kniaz S., KemskaYu. Pravove zabezpechennia kiberbezpeky krytychnoi informatsiinoi infrastruktury Ukrainy. Traektoriâ Nauki = Pathof Science. 2021. Vol. 7, No. 4. DOI: 10.22178/pos.69-12 .(дата звернення: 04.01.2026)

22. NIST. The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. URL: https://www.nist.gov/cyberframework (дата звернення: 04.01.2026)

23. Regulation (EU) 2019/881 of the European Parliamentand of the Councilof 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union. 2019. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj (дата звернення: 16.12.2025)

24. Teichmann F. Cybersecurity of critical infrastructure in Europe: the NIS2 directive in focus. Zeitschrift für die gesamte Versicherungswissenschaft. 2025. DOI: 10.1365/s43439-025-00154-4. URL: https://link.springer.com/article/10.1365/s43439-025-00154-4 (дата звернення: 06.01.2026)

References:

1. Horlynskyi, V., &Horlynskyi, B. (2025). Kiberviina yak systemnyivyklykkiberbezpetsiUkrainy [Cyberwar as a systemic challenge to Ukraine's cybersecurity]. Information Technology and Security, 13(1), 118–130. https://doi.org/10.20535/2411-1031.2025.13.1.328980(accessed: 18.12.2025) [in Ukrainian].

2. Doronin, I. M. (2019). Tsyfrovyirozvytok ta natsionalnabezpeka u kontekstipravovykh problem [Digital development and national security in the context of legal problems]. Informatsiiaipravo, 1(28), 29–38. https://ippi.org.ua/sites/default/files/5_12.pdf(accessed: 15.12.2025) [in Ukrainian].

3. Verkhovna Rada of Ukraine. (2001). KryminalnyikodeksUkrainy [Criminal Code of Ukraine] No. 2341-III. https://zakon.rada.gov.ua/go/2341-14(accessed: 16.12.2025) [in Ukrainian].

4. Lyseiuk, A., &Svintsytska, T. (2024). Pravove zabezpechennia kiberbezpeky Ukrainy v umovakh voiennoho stanu ta yevrointehratsii [Legal support of cybersecurity of Ukraine under martial law and European integration]. Pravo ta innovatsii, 4(48). https://doi.org/10.37772/2518-1718-2024-4(48)-4(accessed: 20.12.2025) [in Ukrainian].

5. Mazepa, S. (2025). Mizhnarodnyi dosvid zakhystu informatsiinoi bezpeky: implementatsiia yevropeiskykh pravovykh norm v zakonodavstvo Ukrainy [International experience of information security protection: implementation of European legal norms in Ukrainian legislation]. Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo, 4(90). https://doi.org/10.24144/2307-3322.2025.90.3.42(accessed: 22.12.2025) [in Ukrainian].

6. Manuilov, Ya. S. (2023). Zabezpechenniakiberbezpekyobiektivkrytychnoiinfrastruktury v umovakhkiberviiny [Ensuring cybersecurity of critical infrastructure objects in conditions of cyberwar]. Informatsiiaipravo, 1(44), 154–167. https://doi.org/10.37750/2616-6798.2023.1(44).287780(accessed: 19.12.2025) [in Ukrainian].

7. Perederii, O. S., &Kulachok-Titova, L. V. (2025). Orhanizatsiino-pravovizakhodyzabezpechenniabezpekytsyfrovykhposluh v aspektiprotydiikiberzlochynnosti v Ukraini [Organisational and legal measures to ensure the security of digital services in countering cybercrime in Ukraine]. Visnyk Kryminolohichnoiasotsiatsiiukrainy, 34(1), 570-578. https://doi.org/10.32631/vca.2025.1.44(accessed: 24.12.2025) [in Ukrainian].

8. Verkhovna Rada of Ukraine. (2021). Zakon Ukrainy "Pro krytychnuinfrastrukturu" No. 1882-IX [Law of Ukraine "On Critical Infrastructure" No. 1882-IX]. https://zakon.rada.gov.ua/laws/show/1882-20(accessed: 17.12.2025) [in Ukrainian].

9. Verkhovna Rada of Ukraine. (2017). Zakon Ukrainy "Pro osnovnizasadyzabezpechenniakiberbezpekyUkrainy" No. 2163-VIII [Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" No. 2163-VIII]. https://zakon.rada.gov.ua/go/2163-19(accessed: 17.12.2025)

10. National Security and Defense Council of Ukraine. (2021). Pro StratehiiukiberbezpekyUkrainy (Rishennia RNBO vid 14.05.2021, enacted by Presidential Decree No. 447/2021) [On the Cybersecurity Strategy of Ukraine]. https://zakon.rada.gov.ua/go/n0055525-21(accessed: 21.12.2025)

11. Savchuk, S. O. (2024). VyklykyharmonizatsiizakonodavstvaYeS v haluzikiberbezpekydliaUkrainy [Challenges of harmonising EU cybersecurity legislation for Ukraine]. Ekonomika, upravlinnia ta administruvannia, 1(107), 207-213. https://doi.org/10.26642/jen-2024-1(107)-207-213(accessed: 21.12.2025) [in Ukrainian].

12. Savchuk, S. O. (2024). Vyklyky ta mozhlyvostiintehratsiiUkrainy v systemukiberbezpekyYeS [Challenges and opportunities for integrating Ukraine into the EU cybersecurity system]. Ekonomika, upravlinnia ta administruvannia, 2(108), 198–203. https://doi.org/10.26642/jen-2024-2(108)-198-203(accessed: 26.12.2025) [in Ukrainian].

13. State Service of Special Communications and Information Protection of Ukraine. (2025). CERT-UA last year processed 4315 cyber incidents [CERT-UA mynulohorokuopratsiuvala 4315 kiberintsydentiv]. https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv(accessed: 10.01.2026) [in Ukrainian].

14. State Service of Special Communications and Information Protection of Ukraine. (2026). CERT-UA in 2025 processed nearly 6000 cyber incidents; hostile attacks increased by 37% [CERT-UA u 2025 rotsiopratsiuvalamaizhe 6000 kiberintsydentiv: kilkistvorozhykhatakzroslana 37%]. https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37(accessed: 10.01.2026) [in Ukrainian].

15. Chojecka, K. (2025). Cybersecurity, resilience and sustainability: Evaluating the role of public-private partnerships. Yearbook of Antitrust and Regulatory Studies. https://doi.org/10.7172/1689-9024.YARS.2025.18.32.9(accessed: 28.12.2025)

16. Directive (EU) 2022/2555 (NIS 2 Directive). (2022). Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng(accessed: 15.12.2025)

17. Directive (EU) 2022/2557 (CER). (2022). Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng(accessed: 15.12.2025)

18. European Union Agency for Cybersecurity (ENISA). (n.d.). EU cybersecurity certification framework (Cybersecurity Act). https://www.enisa.europa.eu/topics/cybersecurity-certification(accessed: 29.12.2025)

19. European Commission. The NIS2 Directive: strengthening cybersecurity rules (overview/summary). https://digital-strategy.ec.europa.eu/en/policies/nis2-directive(accessed: 29.12.2025)

20. ISO. (n.d.). ISO/IEC 27001:2022 – Information security management systems – Requirements. https://www.iso.org/standard/27001.html(accessed: 30.12.2025)

21. Kovaliv, M., Skrynkovskyi, R., Nazar, Y., Yesimov, S., Krasnytskyi, I., Kaidrovych, K., Kniaz, S., &Kemska, Y. (2021). PravovezabezpechenniakiberbezpekykrytychnoiinformatsiinoiinfrastrukturyUkrainy [Legal provision of cybersecurity of critical information infrastructure of Ukraine]. TraektoriâNauki = Path of Science, 7(4). https://doi.org/10.22178/pos.69-12(accessed: 04.01.2026) [in Ukrainian].

22. NIST.The NIST Cybersecurity Framework (CSF) 2.0. https://www.nist.gov/cyberframework(accessed: 04.01.2026)

23. Regulation (EU) 2019/881 (Cybersecurity Act). (2019). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2019/881/oj(accessed: 16.12.2025)

24. Teichmann, F. (2025). Cybersecurity of critical infrastructure in Europe: The NIS2 directive in focus. Zeitschrift für die gesamteVersicherungswissenschaft. https://doi.org/10.1365/s43439-025-00154-4(accessed: 06.01.2026)

Andrii Prolorenzo. Political and legal foundations for harmonising Ukraine's cybersecurity system with EU law: NIS2 implementation and institutional capacity

The article examines the political and legal foundations for harmonising Ukraine's cybersecurity system with European Union law in the context of European integration and ongoing armed aggression by the Russian Federation. The methodological basis includes a comparative legal analysis of Directive (EU) 2022/2555 (NIS2) and an institutional approach to assessing cybersecurity coordination.

The study identifies that, beyond regulatory gaps, the key barriers to implementation are political and institutional factors: competition for powers among key security sector actors (SSSCIP, SBU, NSDC).

Key words: *cybersecurity, harmonization of legislation, cyber defense, European Union, critical infrastructure, NIS2, institutional competition, safe harbor, cyber risk management.*

Відомості про автора:

Пролорензо Андрій – аспірант кафедри політичних наук,
Карпатський національний університет імені Василя Стефаника.

Дата першого надходження статті до видання: 10.03.2026
Дата прийняття статті до друку після рецензування: 05.04.2026
Дата публікації (оприлюднення) статті: 27.05.2026