Кадяйкін К. В.,
курсант факультету службово-бойової діяльності НГУ Київського інституту Національної гвардії України
(м. Київ, Україна)

Науковий керівник:
Бейкун А.Л.,
кандидат юридичних наук, доцент доцент кафедри правового забезпечення та правоохоронної діяльності факультету забезпечення державної безпеки Київського інституту Національної гвардії України
(м. Київ, Україна)

МІЖНАРОДНО-ПРАВОВІ СТАНДАРТИ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ПРОБЛЕМАТИКА ЇХ ІМПЛЕМЕНТАЦІЇ В УКРАЇНСЬКЕ ЗАКОНОДАВСТВО

Відповідно до теоретичного надбання, національна безпека України концептуально мислиться через поєднання міжнародно-правових стандартів і внутрішнього законодавства, що забезпечує сумісність цілей, принципів і процедур із європейським та глобальним правопорядком. Базовою точкою відліку є Статут Організації Об'єднаних Націй, який у статті 51 визнає невід'ємне право держави на індивідуальну та колективну самооборону від збройного нападу до моменту, поки Рада Безпеки ООН не вживе необхідних заходів. Ця норма задає межі легітимності безпекової політики, включно з оборонними, санкційними та кооперaційними інструментами, і є вихідною передумовою для тлумачення «національної безпеки» в умовах збройної агресії проти України [1].

Одночасно із «жорстким» міжнародним виміром меж оборони діє і т.з. «гуманітарне» обмеження: європейський правопорядок, що спирається на Конвенцію про захист прав людини і основоположних свобод [2], допускає обмеження прав громадян воюючої країни (тобто, такої, що функціонує в умовах особливого правового режиму) лише настільки, наскільки це необхідно у демократичному суспільстві, а у виключних обставинах - дерогацію за статтею 15 із процесуальним повідомленням Генерального секретаря Ради Європи. Таким чином, міжнародний стандарт безпеки інтегрує як дозволи, так і стримування, аби запобігти «правовим аб'юзам» під приводом необхідності забезпечення безпеки.

Як зазначає нам Д. А. Чижов, ці дві опори: право на оборону за Статутом ООН і права людини за ЄКПЛ - формують т.з. «раму сумісності», у якій має діяти як законодавчі органи держави, що зазнала агресії, так і виконавчі та інші державні органи та посадові особи, насамперед, оборонно-безпекового сектору [3, с. 127].

Європейський вектор деталізує стандарти через зобов'язання асоціації Україна-ЄС: Угода про асоціацію між Україною та ЄС, чинна у консолідованій редакції, фіксує політичну асоціацію та правове зближення, у тому числі у сферах безпеки, юстиції, кіберстійкості, захисту даних і критичної інфраструктури [4].

В останні роки цей вектор доповнюється секторальними рамками: Директива (ЄС) 2022/2555 (NIS2) встановлює високий рівень кібербезпеки в 18 критичних секторах і вимагає відповідної дієвої національної стратегії, обов'язкової оцінки ризиків, інцидент-репортингу та санкційної підзвітності операторів суттєвих/важливих послуг; «Інструментарій безпеки 5G» (EU 5G Toolbox) задає критерії ризиків і повноваження національних регуляторів щодо «високоризикових постачальників». Практична імплементація зближення підтверджена регулярними Кібер-діалогами Україна-ЄС: так, у жовтні 2025 року сторони погодили подальше узгодження політик, включно з імплементацією NIS2, застосуванням 5G-Toolbox, взаємодією у кіберрозвідці та доступом до Європейського резерву кібербезпеки; ці кроки важливі не лише технічно, а й інституційно, бо пришвидшують «вмонтованість» українських правил у європейську систему нагляду і співпраці [5].

У ширшому безпековому контексті діють і політичні гарантії: у 2024 році Україна підписала з ЄС рамкову угоду про довгострокові безпекові зобов'язання (постачання, тренування, розмінування, оборонна індустрія), що підсилює юридичну та операційну сторону євроінтеграції у сфері безпеки [5].

Як вбачаємо, українське законодавство, розвиваючи ці стандарти, зберігає «каркасну» роль Закону «Про національну безпеку України»: він визначає принципи політики, архітектуру демократичного цивільного контролю за оборонно-безпековим сектором, планування у сферах оборони і безпеки та інтеграцію процедур органів державної влади [6].

Стратегія національної безпеки України «Безпека людини – безпека країни» 2020 року, введена в дію Указом Президента №392/2020, концептуалізує триаду: «стримування - стійкість - взаємодія» як вісь державної політики, а її оновлення січня 2025 року фокусуються на доповненні пріоритетів у зв'язку з тривалою агресією російської федерації та цифровими загрозами [7].

У секторальному вимірі Закон України «Про критичну інфраструктуру» [8] створює правові та організаційні засади національної системи захисту критичної інфраструктури, вводить дефініції стійкості, режимів реагування та координації з Держспецзв'язком.

У сфері кібербезпеки чинний Закон «Про основні засади забезпечення кібербезпеки України» (із актуальними змінами 2024 року), - наближує

понятійний апарат і механізми до acquis ЄС (стратегії, суб'єкти кіберзахисту, інцидент-менеджмент, публічно-приватна взаємодія) [9].

Разом ці акти демонструють, як міжнародні стандарти «перекладаються» на національні повноваження, процедури нагляду і відповідальність суб'єктів критичних систем та електронних комунікацій.

Як видно з теоретичних викладів, імплементація міжнародних стандартів завжди має подвійний вимір: матеріальний (що саме держава зобов'язується робити) і процесуальний (як вона це робить, не виходячи за межі прав людини).

У матеріальному сенсі згадані вище NIS2 і 5G-Toolbox вимагають від держави створити спроможності ризик-менеджменту, визначити національні органи, встановити критерії критичності та забезпечити пропорційні санкції за порушення; у процесуальному: кожне обмеження повинне відповідати змісту законності, легітимної мети та необхідності у демократичному суспільстві, який напрацьований практикою ЄСПЛ.

Національні правові норми щодо критичної інфраструктури та кібербезпеки формально відповідають першій вимозі, але їх ефективність залежить від підзаконних актів, інституційної координації (Кіберцентр, урядові уповноважені органи, галузеві регулятори), а також від здатності виконувати міждержавні запити та обмін інформацією у транскордонних інцидентах, чого вимагає як європейська мережа CSIRT, так і Будапештська конвенція Ради Європи про кіберзлочинність та робота над Другим додатковим протоколом (е-докази та міжнародне співробітництво). Саме через такий «процесуальний міст» міжнародні стандарти стають не декларацією, а дієвими практиками: від оцінок постачальницьких ризиків у 5G до обов'язкового інцидент-репортингу й санкцій за невиконання [10].

У 2024–2025 роках імплементаційний трек підкріплюється політико-правовими кроками: безпекові пакти з Європейським Союзом і державами-членами посилюють оперативну взаємодію та спільні відгуки на майбутню агресію. Паралельно Кібер-діалоги системно фіксують синхронізацію міждержавної політики (NIS2, 5G Toolbox, санкційні режими в кіберсфері, доступ до Європейського резерву кібербезпеки), що на практиці означає поступове наближення до стандартів ринку ЄС у сферах резилієнтності мереж, supply-chain security та публічних закупівель [11].

Водночас імплементаційні виклики для всього європейського простору: дефіцит інвестицій у критичних секторах, фрагментація нагляду, різні темпи транспозиції NIS2, - вимагають від України реалістичного планування, а саме, пріоритетної уваги держави до секторів високого ризику, інвентаризації активів, призначення відповідальних осіб (CISO-функції), поетапного впровадження інцидент-менеджменту та вимог до ланцюгів постачання і, головне, стійкого міжвідомчого управління, що зменшує регуляторні узгодження між кібер-, енергетичною та комунікаційною політиками. Таким чином, міжнародні стандарти перетворюються на внутрішні практики через скоординований набір правових, інституційних та технічних рішень, а не лише шляхом формального ухвалення актів законодавства [11].

Отже, зрештою, як відомо, імплементація - це не «разова подія», а безперервний процес узгодження норм і практик. Українська система права, залишаючись у руслі Статуту ООН та європейських правозахисних стандартів, повинна поєднати ефективність безпекових заходів і пропорційність втручань.

На рівні правових нормативів це означає підтримувати актуальність законів України: «Про національну безпеку України», «Про критичну інфраструктуру» і «Про основні засади забезпечення кібербезпеки України» з урахуванням NIS2 і 5G-Toolbox.

На рівні підзаконних актів - гармонізувати методики оцінки ризиків, критерії «суттєвих/важливих» операторів, порядок інцидент-репортингу та санкцій.

На рівні інституцій - забезпечити сталість координації, незалежність профільних регуляторів і здатність виконувати міжнародні запити у кримінальному провадженні щодо кіберзлочинів.

Таке «правове зближення через практику» і є фактичною імплементацією міжнародних стандартів у сфері національної безпеки, що посилює обороноздатність і, одночасно, гарантує повагу до прав людини - ядра європейського правопорядку.

Список використаних джерел:

1. Статут Організації Об'єднаних Націй. Офіційний текст. URL: https://www.un.org/en/about-us/un-charter/full-text (дата звернення: 09.10.2025).
2. Конвенція про захист прав людини і основоположних свобод (ЄКПЛ). Офіційний текст ЄСПЛ. URL: https://www.echr.coe.int/documents/d/echr/convention_ENG (дата звернення: 09.10.2025).
3. Чижов Д. А. Міжнародні стандарти забезпечення прав людини у сфері національної безпеки / *Актуальні проблеми політики*. 2022. Вип. 69. С. 124-131. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/e57577f8-893d-463a-9778-8d2d8766b3f7/content (дата звернення: 09.10.2025).
4. Угода про асоціацію між Україною та ЄС (чинна консолідована версія). EUR-Lex. URL: https://eur-lex.europa.eu/eli/agree_internation/2014/295/oj/eng (дата звернення: 09.10.2025).
5. Бродовський Сергій. Україна підписала 28 двосторонніх безпекових угод - що вони передбачають. 8 жовтня 2025. [Інформаційний портал: ГОЛОВНЕinUA]. URL: https://glavnoe.in.ua/news/ukrayina-pidpysala-28-dvostoronnih-bezpekovyh-uhod-i-odnu-z-yes-shho-vony-peredbachayut (дата звернення: 09.10.2025).
6. Про національну безпеку України: Закон України від 21.06.2018 №2469-VIII. База «Законодавство України». URL: https://zakon.rada.gov.ua/go/2469-19 (дата звернення: 09.10.2025).
7. Про Стратегію національної безпеки України: Указ Президента України від 14.09.2020 №392/2020 (із змінами). Офіційне інтернет-

представництво Президента та База «Законодавство України». URL: https:// zakon.rada.gov.ua/go/392/2020 (дата звернення: 09.10.2025).

8. Про критичну інфраструктуру: Закон України від 16.11.2021 №1882-IX. База «Законодавство України». URL: https://zakon.rada.gov.ua/go/ 1882-20 (дата звернення: 09.10.2025).

9. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 №2163-VIII. База «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 09.10.2025).

10. У НАДС відбувся воркшоп щодо формування сучасної системи кібербезпеки, наближеної до стандартів ЄС, на основі нового Закону України № 4336-IX. [Офіційний портал Національного агентства України з питань державної служби]. 13 серпня 2025 року. URL: https://nads.gov.ua/news/u-nads-vidbuvsia-vorkshop-shchodo-formuvannia-suchasnoi-systemy-kiberbezpeky-nablyzhenoi-do-standartiv-ies-na-osnovi-novoho-zakonu-ukrainy-4336-ikh (дата звернення: 09.10.2025).

11. Reuters. Security pacts between the European Union and Ukraine (червень 2024) - контекст довгострокових безпекових зобов'язань ЄС. URL: https://www.reuters.com/world/europe/ukraine-signs-security-pacts-with-eu-lithuania-estonia-2024-06-27/ (дата звернення: 09.10.2025).