УДК (341.1/.2:343.34.01):32.019.5:355.02
DOI: https://doi.org/10.37750/2616-6798.2026.2(57).364418

Радзієвська Оксана Григорівна
Державна наукова установа "Інститут інформації, безпеки і права Національної академії правових наук України".
Київ, Україна
ORCID: https://orcid.org/0000-0003-3813-3987

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ СПЕЦІАЛЬНИМ ІНФОРМАЦІЙНИМ І ПСИХОЛОГІЧНИМ ОПЕРАЦІЯМ: НАЦІОНАЛЬНИЙ, МІЖНАРОДНИЙ ТА ЄВРОАТЛАНТИЧНИЙ ВИМІРИ

Анотація. *Стаття присвячена комплексному аналізу правових засад протидії спеціальним інформаційним і психологічним операціям (ІПсО) у контексті сучасної гібридної війни та європейської та євроатлантичної інтеграції України. Розглянуто понятійно-категоріальний апарат та правову природу інформаційного протиборства. Досліджено міжнародно-правову систему безпеки, зокрема концептуальні документи НАТО та ЄС. Досліджено еволюцію поглядів країн НАТО на трансформацію медійних загроз та концептуалізацію "когнітивної війни" (Cognitive Warfare). Здійснено порівняльно-правовий аналіз прогресивного досвіду країн НАТО (США, Естонії, Великої Британії, Польщі) щодо законодавчого врегулювання захисту когнітивної сфери та інформаційного простору. Проаналізовано стан розвитку національного законодавства України під впливом відсічі збройній та інформаційній агресії Російської Федерації. Виявлено ключові колізії між заходами забезпечення національної безпеки та гарантіями прав людини. Сформульовано практичні рекомендації щодо вдосконалення нормативно-правової бази та інституційного механізму протидії ІПсО на національному та міжнародному рівнях.*

Ключові слова: *інформаційні і психологічні операції, інформаційна безпека, когнітивна війна, гібридні загрози, правове забезпечення, країни НАТО, інформаційні права, стратегічні комунікації.*

Oksana H. Radziievska
State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine".
Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-3813-3987

LEGAL REGULATION OF COUNTERING SPECIAL INFORMATION AND PSYCHOLOGICAL OPERATIONS: NATIONAL, INTERNATIONAL, AND EURO-ATLANTIC DIMENSIONS

Summary. *The article is devoted to a comprehensive analysis of the legal frameworks for countering special information and psychological operations (PsyOps) in the context of modern hybrid warfare and Ukraine's European and Euro-Atlantic integration. The conceptual and categorical apparatus, as well as the legal nature of information warfare are examined. The international legal security system, including the conceptual documents of NATO and the EU, is investigated. The study explores the evolution of NATO countries' perspectives on the transformation of media threats and the conceptualization of "Cognitive Warfare". A comparative legal analysis of the progressive*

experience of NATO member states (the USA, Estonia, the United Kingdom, and Poland) regarding the legislative regulation of cognitive sphere and information space protection is carried out. The current state of development of Ukraine's national legislation under the influence of repelling the armed and information aggression of the Russian Federation is analyzed. Key conflicts between national security measures and human rights guarantees are identified. Practical recommendations are formulated to improve the regulatory framework and institutional mechanism for countering PsyOps at both national and international levels.

Keywords: *information and psychological operations, information security, cognitive warfare, hybrid threats, legal framework, NATO countries, information rights, strategic communications.*

Постановка проблеми. Стрімкий розвиток цифрових технологій, штучного інтелекту та поява нових мережевих інструментів маніпулювання індивідуальною й суспільною свідомістю в глобалізованому інформаційному просторі фундаментально змінили характер сучасних геополітичних конфліктів, суттєво трансформувавши систему міжнародної безпеки. Спеціальні інформаційні та психологічні операції (далі – ІПсО) перестали бути виключно допоміжним елементом кінетичних воєнних дій, а перетворилися на самостійні неконвенційні інструменти впливу. Для них характерним є прихованість, непередбачуваність, використанням невійськових інструментів, у тому числі нових технологій й можливостей для досягнення поставлених цілей у всіх сферах життя сучасного суспільства. Спеціальні інформаційні та психологічні операції сьогодні широко застосовуються в політиці, економіці, соціальних комунікаціях тощо. Методи та способи проведення сучасних ІПсО виходять за межі загальноприйнятих правил, норм міжнародного права чи конвенційних (традиційних) способів ведення війни. Наразі ІПсО виступають як самостійна, високотехнологічна та деструктивна зброя, спроможна дестабілізувати конституційний лад, зруйнувати суспільний консенсус і паралізувати систему державного управління без застосування прямої військової сили.

В умовах повномасштабної агресії Російської Федерації (далі – РФ) проти України питання перманентного скоординованого інформаційного тиску та спеціальних інформаційних і психологічних операцій, спрямованих на деморалізацію населення, розкол суспільства та дискредитацію військово-політичного керівництва нашої держави у світі набули особливих масштабів. Разом із тим, загроза ІПсО – це проблема не лише для України. Спеціальні інформаційні та психологічні операції сьогодні стають глобальним викликом для всієї євроатлантичної системи безпеки, оскільки спрямовані на руйнацію базових демократичних цінностей, процедур виборів та суспільної стійкості країн. Це підтверджується численними фактами втручання у виборчі процеси, проведенням кампаній із дезінформації та штучним роздмухуванням внутрішніх соціальних конфліктів у країнах-членах НАТО.

Ефективна протидія ІПсО потребує не лише технічних, технологічних та контррозвідувальних заходів, а й створення надійної правової та інституційної системи. Водночас, сучасне міжнародне та національне право постає перед серйозними викликами: з одного боку, існує потреба в жорсткому обмеженні шкідливих інформаційних впливів для захисту національного суверенітету та безпеки громадян, з іншого – виникає ризик порушення засадничих прав людини, зокрема свободи вираження поглядів та доступу до інформації.

Для України формування ефективного правового механізму протидії спеціальним інформаційним та психологічним операціям є не лише безпековою потребою, а й невід'ємною частиною стратегічного курсу на набуття повноправного членства в Європейському Союзі (ЄС) та Північноатлантичному альянсі (НАТО). Процес євро- та євроатлантичної інтеграції вимагає від законодавця розв'язання надскладної правової

дилеми: створення жорстких юридичних інструментів захисту інформаційного простору за одночасного безумовного дотримання європейських стандартів прав людини, верховенства права та свободи вираження поглядів.

Відтак, теоретичне осмислення та практичне вирішення правових колізій у сфері протидії ІПсО з урахуванням досвіду держав Альянсу є надзвичайно актуальним науковим завданням.

Результати аналізу наукових публікацій свідчать про те, що проблемам правового забезпечення інформаційної безпеки у контексті протидії інформаційній агресії та спеціальним інформаційним і психологічним операціям в умовах гібридних протистоянь у світі приділено достатньо уваги у працях вітчизняних та зарубіжних дослідників. Зокрема, питаннями аналізу глобальних цифрових загроз в умовах воєнних конфліктів, протидії інструментам гібридної війни та асиметричних конфліктів в інформаційній сфері, а також проблемами інформаційно-психологічного протиборства та негативними наслідками інформаційного впливу на індивідуальну і суспільну свідомість займалися такі вчені як О. Баранов, В. Брижко, О. Довгань, Я. Жарков, Б. Кормич, В. Ліпкан, О. Олійник, В. Пилипчук, В. Петрик, П. Прибутько, М. Присяжнюк, В. Фурашев та інші [3; 4; 10; 22; 23; 26].

Проблематику протидії дезінформації та проведення ІПсО в контексті сучасного міжнародного права та військової доктрини досліджували й зарубіжні фахівці. Зокрема, М. Шмітт [5; 12] зробив вагомий внесок у розвиток підходів до застосування норм міжнародного права щодо кібероперацій та інформаційного втручання у цифровому середовищі. У працях Д. Дженіні [9] висвітлено специфіку адаптації оборонних доктрин НАТО до сучасних некінетичних викликів та гібридних загроз, викликаних масштабними кампаніями з дезінформації. Питання юридичної відповідальності технологічних гігантів (BigTech) за поширення координованої неавтентичної поведінки та нормативні підходи ЄС до регулювання цифрових платформ аналізувалися у працях європейських дослідників [42], зокрема й у працях Р. О'Фагея [24]. Юридичні та політико-комунікаційні аспекти концепції стратегічних комунікацій (StratCom) та нормативні обмеження інформаційного впливу у практиці США та Великої Британії стали предметом вивчення таких західних аналітиків, як Н. Болт, В. Беннетт та С. Лівінгстон [25; 40].

Попри наявність ґрунтовних праць, питання порівняльно-правового аналізу спеціальних нормативних інструментів країн НАТО та їх імплементації в правове поле України в умовах тривалого воєнного стану залишається недостатньо вивченим. Поза увагою дослідників залишається також юридична сумісність національних оборонних заходів із новими регуляторними актами ЄС (зокрема, Актом про цифрові послуги / Digital Services Act (DSA) [8] та концептуальними підходами НАТО щодо когнітивної війни (Cognitive Warfare) [19, 20].

Більшість праць розглядають ІПсО окремо від євроінтеграційних зобов'язань, тоді як гармонізація законодавства України та доктринальних підходів НАТО щодо StratCom потребує системного переосмислення інституційних повноважень і подальшого реформування сектору безпеки.

Наукова новизна дослідження полягає у комплексному порівняльно-правовому аналізі механізмів протидії ІПсО в державах-членах НАТО та визначенні шляхів імплементації відповідних стандартів у правову систему України з урахуванням вимог ЄС щодо цифрового врядування та захисту прав людини.

Метою статті є здійснення комплексного аналізу системи правового забезпечення протидії спеціальним інформаційним і психологічним операціям в Україні крізь призму євроінтеграційних та євроатлантичних зобов'язань держави в умовах активної

цифровізації суспільних відносин та збройної агресії, проведення порівняльно-правового аналізу досвіду окремих країн НАТО щодо законодавчого захисту інформаційного простору та когнітивної сфери, визначення векторів гармонізації вітчизняного законодавства із безпековими стандартами ЄС та НАТО з розробкою пропозицій рекомендацій для органів державної влади.

Виклад основного матеріалу. Для побудови логічно послідовної, цілісної та ефективної системи правового регулювання протидії спеціальним інформаційним та психологічним операціям в Україні першочерговим завданням є уніфікація понятійно-категоріального апарату, оскільки розмитість дефініцій унеможливлює чітку правову кваліфікацію правопорушень у судовому порядку.

Аналіз доктринальних підходів країн НАТО, міжнародно-правових джерел та вітчизняного законодавчого поля свідчить про наявність вираженої динаміки у визначенні досліджуваного явища. У військовій доктрині НАТО AJP-3.10.1 2014 року психологічні операції (PsyOps) позиціонувалися як самостійний інструмент і визначалися як: "запланована психологічна діяльність з використання методів комунікації та інших засобів, спрямована на затверджені аудиторії з метою впливу на їхнє сприйняття, ставлення та поведінку, для сприяння досягненню політичних та військових цілей" [28]. Проте сучасна доктринальна трансформація Альянсу привела до переходу від концепції ізольованих інформаційних чи психологічних операцій до інтегрованої моделі. Відповідно до чинної базової доктрини НАТО AJP-10 (Strategic Communications), усі інформаційні заходи та когнітивні спроможності (включаючи PsyOps, Info Ops та кібероперації) тепер інтегровані в єдину систему стратегічних комунікацій (StratCom) [41]. У межах цієї оновленої системи інформаційні операції в офіційній базі термінів NATO Term розглядаються як інтегруюча штабна функція військового командування [6].

Деталізація цього підходу закріплена у положеннях базової профільної доктрини НАТО AJP-10.1 "Allied Joint Doctrine for Information Operations", де інформаційні операції (Info Ops) визначаються як штабна функція, що забезпечує аналіз, планування, інтеграцію та координацію інформаційної діяльності для досягнення визначених ефектів [29]. Таким чином, сучасний євроатлантичний підхід розглядає інформаційні операції не як окремий вид "інформаційної зброї", а як інтегруючу штабну функцію. Вона забезпечує горизонтальну синхронізацію військових дій для реалізації стратегічних комунікацій (StratCom) та координацію суміжних спроможностей – від психологічних операцій (PsyOps) до військового маскування – задля досягнення цілеспрямованого когнітивного ефекту [25; 29].

У правовому полі Сполучених Штатів Америки (далі – США) класичний термін PsyOps у внутрішньому нормативному обігу поступово замінюється дефініцією MISO (Military Information Support Operations) – операції з військової інформаційної підтримки, під якими розуміють: "спланові операції з доведення вибраної інформації та індикаторів до іноземних аудиторій з метою впливу на їхні емоції, мотиви, раціональне мислення і, зрештою, на поведінку іноземних урядів, організацій, груп та окремих осіб". Це поняття закріплене у військовій директиві Joint Publication 3-13.2 "Military Information Support Operations" Міністерства оборони США [39].

Також заслуговують на увагу альтернативні підходи, які розглядають інформаційно-психологічні операції не лише як військовий інструмент, а і як форму прихованого зовнішньополітичного впливу. Зокрема, в американській правовій та безпековій практиці відповідні дії часто аналізуються крізь призму концепції "covert action", ключовими ознаками якої є прихований характер діяльності та ускладнена атрибуція державної участі [12].

Своєю чергою, сучасні європейські дослідження у сфері протидії гібридним загрозам дедалі більше акцентують увагу на технологічних аспектах інформаційного впливу, пов'язаних із використанням алгоритмічних систем, бот-мереж, платформених механізмів поширення контенту та генеративного штучного інтелекту [8; 27]. У дослідженнях Європейського центру передових технологій з протидії гібридним загрозам (European Centre of Excellence for Countering Hybrid Threats) підкреслюється роль AI-driven influence operations та алгоритмічного маніпулювання інформаційним середовищем як складових сучасних гібридних загроз [27].

Водночас у вітчизняній юридичній літературі зазначені процеси розглядаються крізь призму захисту інформаційного суверенітету та забезпечення інформаційної безпеки держави [23].

Особливу загрозу для євроатлантичного простору становить підхід РФ, де інформаційно-психологічний вплив розглядається як складова ширшого комплексу засобів "інформаційної боротьби", що включає використання інформаційних і психологічних інструментів для досягнення стратегічних цілей у політичній та безпековій сферах. У науковій літературі, присвяченій аналізу російських підходів до інформаційного протиборства, зазначається, що інформаційний вплив може бути спрямований не лише на поведінковий рівень, але й на ціннісні та когнітивні структури суспільства, включаючи історичну пам'ять та ідентичність [3; 23].

Отже, сучасна ІПсО має комплексний характер і поєднує ознаки інформаційної диверсії, кіберзлочину та елементів агресивного впливу у віртуальному просторі.

Нормативно-правові акти сектору безпеки і оборони України, зокрема Закон України "Про національну безпеку України" [1] та профільні документи оборонного планування, не містять уніфікованого юридичного визначення інформаційно-психологічної операції, однак закріплюють загальні підходи до забезпечення інформаційної безпеки та протидії деструктивним інформаційним впливам. Таким чином, на національному рівні це поняття використовується переважно в операційно-безпековому та доктринальному значенні, що сформувалося в умовах протидії гібридним загрозам.

Вказаний підхід підтримується і представниками вітчизняної правової школи. Так, у наукових працях В. Ліпкана інформаційно-психологічні операції розглядаються не просто як медійний феномен, а як деструктивний складник інформаційного протиборства, спрямований на дезорганізацію систем державного управління та деструктивний вплив на суспільну свідомість з метою завоювання стратегічної переваги [3].

У низці наукових досліджень з проблематики інформаційної безпеки та гібридних загроз ІПсО також інтерпретуються як елемент ширшого концепту "смислового впливу", що охоплює трансформацію колективних уявлень, ідентичності та суспільних наративів через нав'язування альтернативних смислових конструкцій [11; 23].

Порівняльний аналіз свідчить, що в доктринальних підходах НАТО та США акцент робиться переважно на поведінкових і когнітивних ефектах інформаційного впливу на цільові аудиторії – видозміні поведінки, мотивів та емоцій реципієнтів, тоді як в українському правовому та науковому дискурсі більша увага приділяється безпековим наслідкам таких впливів та їх значенні для національної безпеки і суверенітету держави [1; 11].

Підсумовуючи зазначені підходи до понять та опираючись на базові нормативні акти у сфері інформаційної та кібернетичної безпеки, пропонується під спеціальною інформаційно-психологічною операцією розуміти скоординовану й технологічно детерміновану систему заходів інформаційного, психоемоційного та організаційного спрямування, що реалізується формальними або неформальними суб'єктами впливу

(зокрема, державою-агресором або підконтрольними їй проксі-структурами) шляхом трансляції свідомо деформованої, маніпулятивної, конфіденційної чи сфабрикованої (неавтентичної) інформації, об'єктивна спрямованість якої полягає в деструктивній трансформації емоційного стану, ціннісних орієнтирів та поведінкових моделей суспільства задля реалізації стратегічних військово-політичних інтересів замовника впливу.

Правова природа ІПсО має доволі виражений транскордонний, асиметричний та латентний характер. Як правило, джерело впливу, технологічна інфраструктура (сервери, платформи) та об'єкти впливу (громадяни) перебувають у різних юрисдикціях, що не дозволяє застосовувати лише засоби національного права, а потребує додаткового регулювання на міждержавному рівні. Крім того, суб'єкт ІПсО витрачає мінімальні ресурси для досягнення руйнівних наслідків, тоді як для протидії операціям держава змушена застосовувати масштабні та високовартісні правові й оборонні системи реагування. Зовнішній прояв таких дій часто маскується під законну реалізацію права на свободу слова, думки, громадську дискусію чи журналістську діяльність.

Об'єктом правопорушення у цьому контексті виступає суспільна свідомість, ментальна (когнітивна) стійкість громадян, а також легітимність функціонування державних інституцій. Головна правова дилема, яка заважає ефективній протидії ІПсО на етапі євроінтеграційного зближення України, полягає в тому, що більшість методів впливу (поширення оціночних суджень, чуток, експлуатація суспільних наративів, гіперболізація соціальних проблем) формально перебувають у правовому полі цивільних свобод, якщо оцінювати кожен елемент окремо, проте у своїй системній сукупності вони створюють деструктивний ефект, що загрожує основам державності.

Трансформація інформаційних загроз змушує країни Північноатлантичного альянсу відходити від класичного розуміння ІПсО, як засобу контролю за потоками інформації (що люди читають і чують), та схилятися до концепції "когнітивної війни" (Cognitive Warfare), метою якої є зміна алгоритмів людського сприйняття, критичного мислення та обробки інформації (як люди мислять і чому вони ухвалюють ті чи інші рішення) [19]. У цьому випадку людський розум стає головним об'єктом впливу. У низці доктринальних досліджень НАТО когнітивна сфера розглядається як перспективний операційний домен ведення сучасних конфліктів [20].

Когнітивна війна за своєю суттю є інтегрованою сукупністю кібернетичних атак, психологічного маніпулювання, соціальної інженерії та використання нейротехнологій і штучного інтелекту. Однією з її ознак, які потребують відображення в нормативних актах, є порушення ментального суверенітету. Посягання на індивідуальну волю громадян актуалізує питання про захист нового об'єкта правової охорони – "когнітивну свободу" та права на ментальну недоторканність [21]. Це актуалізує необхідність формування правових механізмів захисту людини від автоматизованого маніпулювання її емоціями з боку суб'єкта впливу. Зважаючи на те, що когнітивна війна ведеться приховано, перманентно, у мирний час, без оголошення війни, то класичні міжнародно-правові інструменти реагування на агресію не можуть бути активовані, оскільки операції впливу не досягають порогу "збройного нападу" у розумінні ст. 51 Статуту ООН [12]. Використання нейромережевих та генеруючих технологій, зокрема застосування алгоритмів когнітивного профайлінгу на основі Big Data, що дозволяє агентам впливу здійснювати мікротаргетинг деструктивного контенту, чи створення "діпфейків" за допомогою штучного інтелекту, істотно ускладнює застосування традиційних стандартів доказування та верифікації інформації.

Впровадження концепції когнітивної війни в доктрини НАТО вимагатиме від України модернізації понятійної системи в Законі України "Про національну безпеку України" [1] та Стратегії інформаційної безпеки [2]. Україні доведеться запровадити термін "когнітивної війни", а відповідно "когнітивного захисту" та "когнітивної безпеки" в національне законодавство, що дозволить гармонізувати оборонне планування із стандартами NATO Allied Command Transformation [19].

Єдиного уніфікованого багатостороннього договору, який би безпосередньо забороняв або регулював інформаційні і психологічні операції на міжнародному рівні немає, а система нормативно-правового регулювання протидії ІПсО характеризується фрагментарністю. У 2017 році під егідою Спільного центру передових технологій з кібероборони НАТО (CCDCOE) було розроблено Талліннське керівництво 2.0 (Tallinn Manual 2.0) [5]. Відповідно до цього документу, ІПсО можуть оцінюватися через фундаментальні принципи міжнародного публічного права, зокрема: принцип суверенітету, принцип невтручання (non-intervention) і принцип незастосування сили (ст. 2(4) Статуту ООН). Відповідно до цих принципів, якщо ІПсО призвела до порушення належного функціонування державних органів або завдала шкоди державній інфраструктурі, то такі дії класифікуються як протиправне порушення державного суверенітету. ІПсО визнається неправомірним втручанням, якщо вона має елемент примусу (coercion), тобто має на меті примусити суверенну державу ухвалити рішення щодо її політичного, економічного чи соціального устрою, яке вона за звичайних умов не ухвалила б. У виняткових випадках, якщо ІПсО за своїми масштабами та наслідками (наприклад, викликаний операцією масовий хаос, що призвів до загибелі людей або колапсу критичної інфраструктури) є еквівалентною кінетичному нападу, вона може бути кваліфікована як "застосування сили" або "акт агресії", що відкриває право на індивідуальну чи колективну самооборону згідно зі ст. 51 Статуту ООН.

На рівні Європейського Союзу у 2022 році був прийнятий Акт про цифрові послуги (Digital Services Act – DSA) [8], який встановив правові основи здійснення нагляду за цифровим середовищем. Це дозволило перейти від декларативних норм до діючих правових механізмів регулювання цифрових послуг. Зокрема DSA покладає на технологічні гіганти (Very Large Online Platforms – VLOPs, такі як Meta, Google, X, TikTok) юридичну відповідальність за системні ризики, які виникають унаслідок функціонування їхніх алгоритмів [24; 42]. Також згідно зі статтями 34 та 35 DSA, ці платформи зобов'язані щорічно проводити оцінку ризиків та впроваджувати заходи з їх пом'якшення у питаннях поширення протиправного контенту, будь-якого негативного впливу на реалізацію основоположних прав (включаючи свободу вираження поглядів) та навмисного маніпулювання послугами, що має реальний або передбачуваний негативний вплив на демократичні процеси, вибори та громадську безпеку.

Для України, як кандидата на вступ до ЄС, наближення законодавства України до положень DSA є одним із напрямів адаптації до спільного європейського ринку. Це вимагає створення національного регулятора (Координатора цифрових послуг), який матиме правові інструменти для фіксації порушень з боку платформ та взаємодіятиме із Європейською комісією.

Залежно від своїх історичних та правових традицій країни Північноатлантичного альянсу демонструють різні правові підходи до протидії інформаційним і психологічним операціям. Проте всі вони еволюціонують у напрямку посилення відповідальності за транскордонний вплив.

Американська правова модель базується на чіткому розмежуванні між операціями за кордоном та захистом внутрішнього простору. Це зумовлено жорсткими рамками Першої

поправки до Конституції США, яка максимально захищає свободу слова і унеможливлює пряму державну цензуру. Головними правовими елементами оборони є Закон "Про повноваження на національну оборону (NDAA)", який розширив мандат Центру глобальної взаємодії (Global Engagement Center – GEC) при Державному департаменті, наділивши його повноваженнями координувати протидію іноземній пропаганді [30].

Також ключовим є Розділ 10 Кодексу США (Title 10 US Code), який регламентує діяльність Збройних сил США (зокрема, Кіберкомандування США та Сил спеціальних операцій) та створює нормативні передумови для реалізації концепції "Defend Forward" (захист на випередження) [12; 31]. Такий підхід нормативно закріплює можливість превентивного виявлення та нейтралізації інфраструктури ворожих ІПсО безпосередньо в мережах супротивника ще до того, як вони завдадуть шкоди національній безпеці США. Для фінансового контролю використовується Закон "Про реєстрацію іноземних агентів (FARA)", який зобов'язує осіб, що діють в інтересах іноземних урядів, розкривати свої джерела фінансування [32].

Естонська модель національної безпеки часто розглядається в науковій літературі як одна з найбільш розвинених у Європі завдяки впровадженню концепції "всеохоплюючої оборони" (Comprehensive National Defence) [43], яка передбачає залучення державних інституцій, приватного сектору та громадянського суспільства до системи оборони держави [9; 26]. Закон "Про надзвичайний стан" та Закон "Про національну оборону" визначають чіткі юридичні алгоритми взаємодії між оборонним відомством, спецслужбами, приватним сектором та волонтерськими організаціями [33]. Юридично врегульований статус Ліги оборони "Кайтселійт" (Kaitseliit) та її підрозділу з кібероборони дозволяє залучати цивільних ІТ-фахівців та експертів з комунікацій до завдань оборонного характеру, включаючи кіберзахист у межах відповідних програм і ініціатив [34]. Естонія також є місцем розташування Об'єднаного центру передових технологій з кібероборони НАТО (NATO CCDCOE), який виконує функції науково-аналітичного центру НАТО у сфері кібероборони та сприяє розвитку спільних підходів держав-членів Альянсу. [5].

Нормативно-правова база Сполученого Королівства у сфері протидії гібридним загрозам зазнала масштабної модернізації. Закон "Про національну безпеку" (National Security Act 2023) реформував застарілі акти про державну таємницю та запровадив нові, сучасні склади кримінальних правопорушень, зокрема статтю про "іноземне втручання" (Foreign Interference) [7]. Ця стаття криміналізує поведінку, яка здійснюється за дорученням або в інтересах іноземної держави, якщо вона включає елементи примусу, чи введення в оману, і спрямована на втручання в реалізацію конституційних прав, вибори чи роботу державних органів [7].

Одночасно Закон "Про безпеку в Інтернеті" (Online Safety Act 2023) зобов'язав технологічні компанії мінімізувати ризики поширення шкідливого та протиправного контенту, що загрожує національній безпеці. Незалежний медійний регулятор Ofcom наділений повноваженнями накладати фінансові санкції (до 18 млн фунтів стерлінгів або 10% від глобального річного обороту компанії) у разі виявлення порушень [35]. Крім того, зазначений акт передбачає кримінальну відповідальність за умисне поширення завідомо неправдивих повідомлень (false communications offence) особою, яка усвідомлювала недостовірність та потенційну шкідливість інформації [35].

Польська правова модель зазнала суттєвої трансформації після 2022 року у зв'язку з безпосередньою близькістю до зони конфлікту та штучно створеною прикордонною кризою біля білоруського кордону. Фундаментальний Закон "Про захист Вітчизни" (Ustawa o obronie Ojczyzny) юридично закріпив нову систему організації національної

оборони та нормативно визначив функціонування Військ оборони кіберпростору (Wojska Obrony Cyberprzestrzeni – WOC) як окремого компонента Збройних Сил Польщі [13]. WOC наділені законодавчим мандатом не лише на захист військової інфраструктури, а й на виконання завдань у сфері кібероборони та інформаційної протидії [13; 37].

Крім того, реформа Кримінального кодексу Польщі (далі – КК РП) (зокрема, радикальні зміни до ст. 130 щодо шпигунства та диверсійної діяльності) значно посилила відповідальність за проведення деструктивних дезінформаційних операцій в інтересах іноземних розвідок [15; 36]. Відповідно до нової редакції § 9 ст. 130 КК РП, участь в діяльності іноземної спецслужби, яка полягає у поширенні дезінформації з метою дестабілізації устрою чи створення загрози національній безпеці, карається позбавленням волі на строк не менше ніж 8 років або навіть довічним ув'язненням [15; 36], що є одним із найсуворіших підходів серед держав-членів НАТО. Польський досвід демонструє остаточний перехід від розуміння ІПсО як суто "медійної проблеми" до її трактування як форми державної диверсії, яка потребує скоординованої військово-кримінальної протидії [14; 37].

Порівняльний аналіз свідчить, що держави НАТО поступово переходять від переважно декларативних механізмів інформаційної безпеки до моделей, які передбачають комплексне поєднання кримінально-правових, кібербезпекових та адміністративно-регуляторних інструментів протидії ІПсО.

Базовою нормативною основою у сфері протидії інформаційним та психологічним операціям в Україні є Закон України "Про національну безпеку України" [1] та Стратегія інформаційної безпеки, схвалена РНБО та введена в дію Указом Президента України у грудні 2021 року [2]. Стратегія системно замінила застарілу та скасовану Доктрину інформаційної безпеки, концептуально переорієнтувавши безпековий сектор держави на проактивне виявлення гібридних загроз, захист ментального простору громадян та стратегічну координацію з євроатлантичними інституціями.

Відповідно до ч. 1 ст. 3 цього Закону України "Про національну безпеку України", "державна політика у сферах національної безпеки та оборони спрямовується на захист: людини і громадянина... суспільства та держави – від зовнішніх і внутрішніх загроз" [1]. Деталізація правових інструментів в інформаційній сфері міститься у Стратегії інформаційної безпеки, де констатується, що "інформаційна політика Російської Федерації загрожує не лише Україні, а й іншим демократичним державам", а серед головних загроз прямо названо "дезінформаційні кампанії, спрямовані на розкол суспільства, дискредитацію державних інститутів та послаблення міжнародної підтримки України" [2].

Ефективність національного правового механізму протидії інформаційним та психологічним операціям найкраще ілюструється практикою його застосування, яка в умовах воєнного стану набула рішучого характеру. Практичним прикладом масштабного обмеження інструментів ведення ІПсО стало введення в дію рішень РНБО щодо застосування санкцій проти телеканалів "групи Медведчука" ("112 Україна", ZIK, NewsOne) та телеканалу "НАШ". З юридичної точки зору, ці рішення базувалися на Законі України "Про санкції" та були обґрунтовані тим, що фінансування та редакційна політика цих суб'єктів здійснювалися державою-агресором, а їхня інфраструктура використовувалася для системного поширення наративів ворожих ІПсО [16]. Це рішення витримало перевірку у Верховному Суді, який визнав правомірність обмеження свободи слова задля захисту територіальної цілісності та нацбезпеки у згаданих вище випадках.

Аналіз Єдиного державного реєстру судових рішень [18] свідчить про формування стійкої судової практики за статтями Кримінального кодексу України (ККУ) [38].

Зокрема, узагальнення правозастосовчої діяльності [17] дозволяє виокремити такі підходи:

У судовій практиці трапляються випадки кваліфікації дій так званих "інтернет-агітаторів" та адміністраторів проросійських груп у соціальних мережах як здійснення деструктивної інформаційної діяльності у співпраці з державою-агресором за ч. 6 ст. 111-1 ККУ "Колабораційна діяльність", що передбачає відповідальність за організацію та проведення заходів політичного характера чи здійснення інформаційної діяльності у співпраці з державою-агресором;

У випадках, коли особа не просто висловлювала власні погляди, а отримувала фінансування та конкретні завдання від кураторів із РФ для проведення ІПсО (наприклад, щодо зриву мобілізаційних заходів чи поширення панічних настроїв через координовану мережу), її дії кваліфікуються за ст. 111 ККУ "Державна зрада" у формі надання допомоги іноземній державі в проведенні підривної діяльності проти України. Суди наголошують, що інформаційна підтримка агресора за своїм деструктивним потенціалом прирівнюється до матеріально-технічної допомоги ворогу;

Кримінальна відповідальність застосовується також до організаторів "ботоферм", які використовували спеціалізоване програмне забезпечення та SIM-банки для автоматизованого створення тисяч фейкових акаунтів, через які розповсюджувалися ворожі ІПсО. Такі дії кваліфікуються за ст. 361 ККУ "Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж".

Проблеми євроінтеграційної гармонізації. Ключовою проблемою для України є те, що чинна система є переважно реактивною та санкційною, адаптованою до умов воєнного стану. Законодавство України адаптується до загрози після того, як ця загроза завдала матеріальних чи репутаційних збитків. Блокування ворожих інформаційних ресурсів здійснюється за допомогою надзвичайних процедур у рамках адміністративно-санкційних механізмів (рішення РНБО, листи НКЕК), які мають обмежену легітимність у мирний час і викликають критику з боку європейських інституцій. Крім того, в Україні відсутні законодавчо закріплені правові механізми примусу транснаціональних корпорацій до виконання національних безпекових вимог. У процесі європейської та євроатлантичної інтеграції Україна має трансформувати ці надзвичайні заходи у постійно діючі, прозорі інституційні механізми [26]. Європейські партнери вимагають, щоб обмеження в інформаційній сфері суворо відповідали трискладовому тесту ст. 10 Конвенції про захист прав людини (бути встановленими законом, переслідувати легітимну мету та бути необхідними в демократичному суспільстві). Тому реформа українського права має відбуватися не через розширення позасудових блокувань, а через імплементацію європейських стандартів відповідальності платформ (DSA) та розбудову системи стратегічних комунікацій за стандартами НАТО.

Недоліком моделі Європейського Союзу щодо протидії ІПсО є те, що хоча DSA і є потужним регуляторним актом, проте його бюрократична процедура розгляду системних ризиків займає місяці. У випадку ведення інтенсивних бойових дій, коли ворожа ІПсО розгортається і досягає мети за кілька годин (наприклад, штучне роздування паніки навколо техногенної катастрофи або військових невдач), механізми DSA можуть виявитися недостатньо оперативними. Крім того, ЄС робить акцент на цивільних суб'єктах, приділяючи обмежену увагу ролі військових структур.

Недоліком моделі НАТО у питаннях протидії ІПсО є те, що документи Альянсу щодо StratCom та Cognitive Warfare мають виключно рекомендаційний, м'який правовий статус (soft law). Вони не є обов'язковими для виконання національними парламентами

країн-членів, що призводить до фрагментації правового поля. Для прикладу: якщо Польща вводить жорстку відповідальність за дезінформацію, інші країни-члени Альянсу можуть залишати медіапростір повністю відкритим для ворожого впливу під приводом захисту ліберальних цінностей, створюючи "проломи" в загальній системі колективної безпеки.

Висновки. Підводячи підсумки слід зазначити, що спеціальні інформаційні і психологічні операції в умовах глобальної цифровізації еволюціонували у вищу, більш руйнівну форму – когнітивну війну (Cognitive Warfare), об'єктом експлуатації якої є людський розум, критичне мислення та процеси ухвалення рішень. У доктринальних підходах НАТО когнітивна сфера розглядається як перспективний операційний домен, що свідчить про те, що окремі прояви ІПсО можуть набувати ознак правопорушень, які одночасно поєднують у собі ознаки транскордонної інформаційної диверсії, кіберзлочину проти суверенітету та акту прихованої агресії, що часто ведеться нижче порогу "збройного нападу" у розумінні ст. 51 Статуту ООН. Правова природа когнітивної війни характеризується субпороговістю, транскордонністю та асиметричністю, що обмежує адаптованість класичних інструментів міжнародного права (зокрема, ст. 2(4) Статуту ООН) до некінетичних форм впливу для захисту держав від некінетичної агресії.

Процес європейської та євроатлантичної інтеграції вимагає від України докорінної зміни філософії правового регулювання у сфері безпеки. Доцільним є поступовий відхід держави від суто реактивних і тимчасових санкційних інструментів обмеження інформаційних загроз, що застосовуються під час воєнного стану. Набуття членства в ЄС та НАТО потребує створення прозорої, постійно діючої та інституційно стійкої правової рамки, здатної захищати ментальний (когнітивний) суверенітет суспільства без порушення європейських стандартів прав людини, верховенства права та свободи вираження поглядів.

Порівняльно-правовий аналіз досвіду країн НАТО виявив ефективні національні моделі нормативного реагування на ІПсО, які доцільно імплементувати в правове поле України. Зокрема, американська модель демонструє ефективність проактивної концепції "захисту на випередження" (Defend Forward) та фінансового контролю (FARA); естонська модель доводить дієвість залучення цивільного та волонтерського секторів у межах "Всеохоплюючої оборони"; британська модель успішно модернізувала карне право через інститут "іноземного втручання" та впровадила жорстку фінансову відповідальність платформ BigTech через регулятор Ofcom; польська модель може розглядатися як одна з найбільш релевантних для України, оскільки юридично закріпила статус Військ оборони кіберпростору (WOC) із мандатом на контр-інформаційні операції та суттєво посилила відповідальність за дезінформаційні диверсії іноземних розвідок (ст. 130 КК РП).

З метою системної гармонізації законодавства України із безпековими стандартами ЄС та НАТО запропоновано три ключові вектори реформ:

по-перше, ухвалення національного аналога європейського Акта про цифрові послуги (DSA) для покладання юридичної відповідальності за системні ризики поширення дезінформації на технологічні гіганти (VLOPs);

по-друге, модернізацію Закону України "Про національну безпеку України" та Стратегії інформаційної безпеки шляхом нормативного закріплення категорій "когнітивна війна" та "когнітивна безпека";

по-третє, чітке нормативне уточнення правових меж діяльності суб'єктів сектору безпеки (зокрема ССО ЗСУ та профільних інституцій) щодо ведення проактивних контр-інформаційних дій у цифровому просторі.

ПОДЯКИ: Немає
КОНФЛІКТ ІНТЕРЕСІВ: Немає

Використана література

1. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України». Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2469-19 (дата звернення: 18.05.2026).

2. Про Стратегію інформаційної безпеки: Указ Президента України від 28.12.2021 № 685/2021 // Офіційний вебсайт Президента України. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 18.05.2026)

3. Ліпкан В. А. Сучасний зміст інформаційних операцій проти України. // *Актуальні проблеми міжнародних відносин*. 2011. Вип. 102 (ч. 1). С. 34–43. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=apmv_2011_102(1)__7 (дата звернення: 18.05.2026).

4. Кормич Б. А. Організаційно-правові основи забезпечення інформаційної безпеки України : монографія. Одеса : Юридична література, 2004. 384 с.

5. Schmitt M. N. (ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press. 2017. 638 p. DOI: 10.1017/9781316822524.URL: https://ccdcoe.org/news/2017/tallinn-manual-2-0-on-the-international-law-applicable-to-cyber-operations-to-be-launched/ (дата звернення: 18.05.2026).

6. NATO Term. NATO Terminology Database / NATO Standardization Office.URL: https://nso.nato.int/natoterm/Web.mvc (дата звернення: 18.05.2026).

7. National Security Act 2023: UK Public General Acts. 2023. c. 32. URL: https://www.legislation.gov.uk/ukpga/2023/32/contents (дата звернення: 18.05.2026).

8. Digital Services Act (DSA). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022. Official Journal of the European Union. 2022. L 277. p. 1–102. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng (дата звернення: 18.05.2026).

9. Genini D. Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine / *New Perspectives*. 2025. Vol. 33, no. *33*(2). P. 122–149. URL: https://journals.sagepub.com/doi/10.1177/2336825X251322719 (дата звернення: 18.05.2026).

10. Жарков Я. М., Петрик В. М., Присяжнюк М. М. та ін. Історія інформаційно-психологічного протиборства: підручник / за заг. ред. Є. Д. Скулиша. Київ: Наук.-вид. відділ НА СБ України, 2012. 212 с. URL: https://viknu.mil.gov.ua/files/books/історія%20інформаційно-психологічного%20протиборства.pdf (дата звернення: 18.05.2026).

11. State information policy in the context of hybrid threats: Legal and political aspects / S. Balan and ather. *Соціально-правові студії* [Social and Legal Studies]. 2025. Vol. 8. No. 1. P. 165–178. URL: https://sls-journal.com.ua/web/uploads/pdf/Social_and_Legal_Studois_Vol.8_No.1_2025-165-178.pdf (дата звернення: 18.05.2026).

12. Schmitt M. N. Foreign Cyber Interference in Democratic Elections under International Law. Harvard National Security Journal. 2021. Vol. 11. P. 45–72. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3816748 (дата звернення: 18.05.2026).

13. Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny: Dziennik Ustaw Rzeczypospolitej Polskiej. 2022. Poz. 655. URL: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20220000655 (дата звернення: 18.05.2026).

14. Grabowska-Siwiec A., Hoc S. Aspekty prawno-operacyjne dezinformacji w ujęciu art. 130 § 9 k.k. Nowa Kodyfikacja Prawa Karnego. Wrocław: Wydawnictwo Uniwersytetu Wrocławskiego, 2024. Tom LXXI. S. 25–44. URL: https://repozytorium.uni.wroc.pl/Content/142360/PDF/03_A_Grabowska-Siwiec_S_Hoc_Aspekty_prawno-operacyjne_dezinformacji_w_ujeciu_art._130_9_k.k..pdf (дата звернення: 18.05.2026).

15. Burczaniuk M. Przestępstwo szpiegostwa po nowemu: analiza nowelizacji Kodeksu karnego z 17 sierpnia 2023 r. Warszawa: Wydawnictwo UKSW, 2024. 32 s. URL: https://bazawiedzy.uksw.edu.pl/docstore/download/UKSW567608a2d18647e286eca69e60b137e4/Burczaniuk-2024-Przestepstwo-szpiegostwa-po-nowemu.pdf?entityType=article&entityId=UKSW2185de67e06044a38731137e89b6d153 (дата звернення: 18.05.2026).

16. Про санкції : Закон України від 14.08.2014 № 1644-VII // Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/1644-18#Text (дата звернення: 18.05.2026).

17. Узагальнення судової практики щодо розгляду кримінальних проваджень про злочини проти основ національної безпеки України в умовах воєнного стану. Судова апеляція. 2025. № 3 (78). С. 12–26. URL: sudapp.gov.ua (дата звернення: 18.05.2026).

18. Єдиний державний реєстр судових рішень України. URL: https://reyestr.court.gov.ua/ (дата звернення: 18.05.2026).

19. Cognitive Warfare: A New Domain of Competitive Advantage / NATO Allied Command Transformation. Norfolk: NATO ACT, 2024. URL: https://www.nato.int (дата звернення: 18.05.2026).

20. Claverie B., Du Cluzel F. Cognitive Warfare: The Next Domain of Warfare. Bordeaux: NATO Innovation Hub; ENSC, 2022. 245 p. URL: https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf (дата звернення: 18.05.2026).

21. Cognitive Warfare: The Future of Cognitive Dominance : Papers presented at the First NATO Scientific Meeting on Cognitive Warfare (Bordeaux, France, 21 June 2021) / ed. by B. Claverie, B. Prébot, N. Buchler, F. du Cluzel. NATO Collaboration Support Office, 2022. 254 p. URL: https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare-Symposium-ENSC-March-2022-Publication.pdf (дата звернення: 18.05.2026).

22. Брижко В.М., Фурашев В.М. Інформаційне право та інформаційне законодавство: наукове видання. Київ: АртЕК, 2020. 288 с. URL: https://ippi.org.ua/informatsiine-pravo-ta-informatsiine-zakonodavstvo (дата звернення: 18.05.2026).

23. Правове забезпечення інформаційної безпеки України в умовах військової агресії: монографія / за заг. ред. В. Г. Пилипчука, О. Д. Довганя. Київ: КНТ, 2023. 244 с.

24. The Regulation of Disinformation Under the Digital Services Act / T. Ó Fathaigh et al. *Media and Communication*. 2025. Volume. 13. Article 9615. URL: https://www.researchgate.net/publication/392162549_The_Regulation_of_Disinformation_under_the_Digital_Services_Act ;

25. Bolt N. Strategic communications and disinformation in the early 21st century, EUI RSC PP. 2021. No. 12, Global Governance Programme. https://hdl.handle.net/1814/74494 (дата звернення: 18.05.2026).

26. Пилипчук В. Г., Баранов О. А., Гиляка О. С. Проблема правового регулювання у сфері штучного інтелекту в контексті розвитку законодавства Європейського Союзу. *Вісник Національної академії правових наук України*. 2022. Т. 29, № 2. С. 35–51. URL: https://visnyk.kh.ua/uk/journals/visnik-naprnu-2-2022-r/problema-pravovogo-regulyuvannya-u-sferi-shtuchnogo-intelektu-v-konteksti-rozvitku-zakonodavstva-yevropeyskogo-soyuzu (дата звернення: 18.05.2026).

27. Artificial Intelligence and Foreign Information Manipulation. Hybrid CoE Paper 29 / The European Centre of Excellence for Countering Hybrid Threats. Helsinki: Hybrid CoE, 2026. 24 p. URL: https://www.hybridcoe.fi/wp-content/uploads/2026/03/Artificial-Intelligence-and-Foreign-Information-Manipulation-Hybrid-CoE-Paper-29.pdf (дата звернення: 18.05.2026).

28. AJP-3.10.1. Allied joint doctrine for psychological operations. Edition A, Version 1 / North Atlantic Treaty Organization: NATO Standardization Office, 2014. URL: https://assets.publishing.service.gov.uk/media/6a0452f88cc72d2f863ea875/ARCHIVED-AJP_3_10_1_B_PSYOPS_with_UK_Green_pages.pdf (дата звернення: 18.05.2026).

29. AJP-10.1. Allied joint doctrine for information operations. Edition A, Version 1 / North Atlantic Treaty Organization: NATO Standardization Office, 2023. URL:

https://assets.publishing.service.gov.uk/media/650c03bf52e73c000d9425bb/AJP_10_1_Info_Ops_UK_web.pdf (дата звернення: 18.05.2026).

30. Global Engagement Center Authorities Act: H.R. 5681, 115th Congress (2017–2018) / United States Congress. Washington, D.C.: Government Publishing Office, 2018. URL: https://www.congress.gov/bill/115th-congress/house-bill/5681/text (дата звернення: 18.05.2026).

31. Armed Forces: Title 10, United States Code (Section 394: Authority to conduct military operations in cyberspace)) / Office of the Law Revision Counsel. Washington, D.C., 2024. URL: https://house.gov (дата звернення: 18.05.2026).

32. Foreign Agents Registration Act (FARA): 22 United States Code (U.S.C.) § 611 et seq. / National Security Division. Washington, D.C.: U.S. Department of Justice, 2025. URL: https://www.justice.gov/nsd-fara/fara-index-and-act (дата звернення: 18.05.2026).

33. National Defence Act : RT I, 12.03.2015, 1 / Riigikogu (Parliament of Estonia). Tallinn: Riigi Teataja, 2026. URL: https://www.riigiteataja.ee/en/eli/ee/526042022004/consolide/current (дата звернення: 18.05.2026).

34. The Estonian Defence League Act: RT I, 02.04.2019, 11 / Riigikogu (Parliament of Estonia). Tallinn: Riigi Teataja, 2026. URL: https://www.riigiteataja.ee/en/eli/502042019011/consolide (дата звернення: 18.05.2026).

35. Online Safety Act 2023: UK Public General Acts. 2023. c. 50 / Parliament of the United Kingdom. London: The Stationery Office. 2023. URL: https://www.legislation.gov.uk/ukpga/2023/50 (дата звернення: 18.05.2026).

36. Kodeks karny: Ustawa z dnia 6 czerwca 1997 r. (Zmiany wprowadzone Ustawą z dnia 17 sierpnia 2023 r. o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw): Dziennik Ustaw Rzeczypospolitej Polskiej. 2023. Poz. 1860. URL: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19970880553 ; https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20230001860 (дата звернення: 18.05.2026).

37. Rosiak P. Wojska Obrony Cyberprzestrzeni a kształtowanie polityki bezpieczeństwa Polski. *Wydawnictwo Uniwersytetu Wrocławskiego*. 2024. No. 35. S. 111–124. URL: https://www.ceeol.com/search/article-detail?id=1392305 (дата звернення: 18.05.2026).

38. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 18.05.2026).

39. Joint Publication 3-13.2: Military Information Support Operations / Joint Chiefs of Staff. Washington, D.C.: Department of Defense, 2010 (Reprint 2011). 108 p. URL: https://www.jcs.mil/doctrine/joint-doctrine-pubs/3-0-operations-series/ (дата звернення: 18.05.2026).

40. The disinformation age: politics, technology, and disruptive communication in the United States / ed. by W. L. Bennett, S. Livingston. Cambridge; New York: Cambridge University Press, 2020. 293 p. (SSRC anxieties of democracy). URL: https://doi.org/10.1017/9781108914628 (дата звернення: 19.05.2026).

41. AJP-10. Allied Joint Doctrine for Strategic Communications. Edition A, Version 1 / North Atlantic Treaty Organization. Brussels: NATO Standardization Office, 2023. 78 p. URL: https://assets.publishing.service.gov.uk/media/6525459d244f8e00138e7343/AJP_10_Strat_Comm_Change_1_web.pdf (дата звернення: 18.05.2026).

42. Beyond phase-in: assessing impacts on disinformation of the EU Digital Services Act / Nannini, L., Bonel, E., Bassi, D. et al. *AI Ethics 5*. 2025. P. 1241–1269. https://doi.org/10.1007/s43681-024-00467-w URL: https://link.springer.com/article/10.1007/s43681-024-00467-w (дата звернення: 19.05.2026).

43. Comprehensive National Defence / Ministry of Defence of Estonia. URL: https://kaitseministeerium.ee/en/estonian-national-defence/structure-and-principles/comprehensive-national-defence (дата звернення: 18.05.2026).

Оксана Григорівна Радзієвська
кандидат юридичних наук, старший дослідник
завідувач наукової лабораторії інформаційних прав та безпеки людини Державної наукової установи "Інститут інформації, безпеки і права Національної академії правових наук України"
04053, Україна, м. Київ, пров. Несторівський, 4
email: radeoksa@gmail.com

Oksana H. Radziievska
Candidate of Legal Sciences, Senior Researcher,
Head of the Scientific Laboratory of Information Rights and Human Security State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"
4 Nestorivskyi Lane, Kyiv, 04053, Ukraine
email: radeoksa@gmail.com

Рекомендоване цитування: Радзієвська О.Г. Правове забезпечення протидії спеціальним інформаційним і психологічним операціям: національний, міжнародний та євроатлантичний виміри. *Інформація і право*. № 2(57)/2026. 2026. С. 169-183. https://doi.org/10.37750/2616-6798.2026.2(57).364418

Suggested Citation: Radziievska O. (2026) Legal Regulation of Countering Special Information and Psychological Operations: National, International, and Euro-Atlantic Dimensions. *Information and Law*. 2(57)/2026. 169-183. https://doi.org/10.37750/2616-6798.2026.2(57).364418

Дата надходження статті до редакції: 15.05.2026 р.
Дата прийняття статті до друку після рецензування: 25.05.2026 р.
Дата публікації (оприлюднення): 26.05.2026 р.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~