УДК 355.343.4
DOI https://doi.org/10.24144/2307-3322.2026.93.3.15

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ В УКРАЇНІ: МІЖНАРОДНІ ДОКТРИНАЛЬНІ ПІДХОДИ, НАЦІОНАЛЬНА МОДЕЛЬ ТА НАПРЯМИ ВДОСКОНАЛЕННЯ

Євлампієв А.С.,
аспірант,
Національна академія Служби безпеки України
ORCID: 0009-0001-6082-2220
e-mail: Nikolaev.finance80@gmail.com

Євлампієв А.С. Правове забезпечення спеціальних інформаційних операцій в Україні: міжнародні доктринальні підходи, національна модель та напрями вдосконалення.

У статті здійснено порівняльно-правовий та доктринальний аналіз підходів до спеціальних інформаційних операцій (СІО) у ключових документах США, НАТО та ОБСЄ. Прослідковано еволюцію їх розуміння від переліку «ключових спроможностей» до ефект-орієнтованої діяльності в інформаційному середовищі, інтегрованої у стратегічні комунікації та операційне планування. На цій основі за допомогою системно-структурного методу досліджено сучасний стан нормативно-правового забезпечення СІО в Україні крізь призму законодавства про національну безпеку, оборону, контррозвідку, кібербезпеку та доктринальних актів. Обґрунтовано, що національна модель послідовно фіксує ворожі СІО як загрозу та визначає завдання протидії відповідним суб'єктам (Міністерству оборони, Службі безпеки України). Водночас виявлено системну проблему: законодавство не встановлює достатньо визначеного правового режиму для планування й проведення власних СІО, особливо поза межами воєнного стану. Цей прогалина призводить до дефініційної фрагментації, міжвідомчих колізій, ускладнень у плануванні та оцінці ефективності, а також підвищених правових ризиків у сфері захисту прав людини та демократичного контролю. Наукова новизна дослідження полягає у формулюванні прикладної моделі рамкового правового режиму СІО для України. Запропонована модель поєднує: (1) уніфікацію термінології та узгодження її з міжнародними підходами; (2) чітке розмежування компетенцій між органами оборони, контррозвідки та кібербезпеки; (3) детальну процесуалізацію повного циклу управління СІО (ініціювання, санкціонування, виконання, оцінювання, припинення), що передбачає єдине розуміння цілей, методів та критеріїв завершення; (4) вбудовані правові гарантії пропорційності, підзвітності та обов'язкового аудиту. Практичне значення результатів полягає у можливості використання запропонованої моделі як концептуальної основи для подальших законодавчих ініціатив і розробки підзаконних актів, спрямованих на подолання ідентифікованих правових прогалин, а також для стандартизації міжвідомчих процедур та інструкцій у сфері стратегічних комунікацій та інформаційної безпеки, що сприятиме підвищенню ефективності, керованості та легітимності дій держави в інформаційному просторі.

Ключові слова: спеціальні інформаційні операції; стратегічні комунікації; інформаційне середовище; кіберпростір; інформаційна безпека; Служба безпеки України; правове регулювання.

Yevlampiiev A.S. Legal framework for special information operations in Ukraine: international doctrinal approaches, national model and directions for improvement.

The article conducts a comparative legal and doctrinal analysis of approaches to special information operations (SIO) in key documents of the United States, NATO, and the OSCE. It traces the evolution of their conceptual understanding from a mere list of «key capabilities» towards effects-oriented activities in the information environment, integrated into strategic communications and operational planning. Building on this framework and employing a systemic-structural method, the study examines the current

state of Ukraine's legal and regulatory framework for SIO through an analysis of national security, defense, counterintelligence, cybersecurity legislation, and relevant doctrinal instruments. The research substantiates that the national model consistently identifies hostile SIO as a threat and assigns counter-SIO mandates to relevant actors (the Ministry of Defense, the Security Service of Ukraine). However, a critical systemic gap is identified: the legislation fails to establish a sufficiently defined legal regime for planning and conducting Ukraine's own SIO, particularly outside the context of martial law. This regulatory vacuum leads to definitional fragmentation, inter-agency conflicts, complications in planning and effectiveness assessment, and elevated legal risks concerning human rights protection and democratic oversight, potentially undermining international legitimacy. The scientific novelty of the research lies in formulating an applied model of a framework legal regime for SIO in Ukraine. The proposed model integrates: unification of terminology aligned with international approaches; clear delineation of competencies among defense, counterintelligence, and cybersecurity agencies; detailed proceduralization of the full SIO management cycle (initiation, authorization, execution, assessment, termination), establishing a common understanding of objectives, methods, and exit criteria; embedded legal safeguards of proportionality, accountability, and mandatory audit. The practical significance of the findings is that the proposed model can serve as a conceptual foundation for future legislative initiatives and the development of secondary legislation aimed at bridging the identified legal gaps. Furthermore, it provides a basis for standardizing inter-agency procedures and instructions within strategic communications and information security governance, thereby enhancing the effectiveness, controllability, and legitimacy of state actions in the information domain while aligning with international norms.

Key words: special information operations; strategic communications; information environment; cyberspace; information security; Security Service of Ukraine; legal regulation.

Постановка проблеми. Досвід сучасних конфліктів показує, що інформаційний простір став повноцінним «театром» протиборства, де вплив на сприйняття, мотивацію та ухвалення рішень здатний забезпечувати стратегічний ефект без класичного застосування сили. Відповідно, спеціальні інформаційні операції (СІО) трансформувалися з допоміжного елементу інформаційного супроводу у самостійний інструмент досягнення цілей національної безпеки – як у наступальному, так і у захисному вимірі (протидія дезінформації, деморалізації, підриву довіри до інститутів держави, управлінських рішень тощо).

Паралельно міжнародні інституції почали формувати підходи до зниження ризиків ескалації у кібер- та інформаційному середовищі, зокрема через «м'які» інструменти прозорості і довіри. Важливим прикладом є рішення Постійної ради ОБСЄ від 3 грудня 2013 року про початковий перелік заходів зміцнення довіри щодо використання інформаційно-комунікаційних технологій як чинника конфліктності [1]. Для України це має подвійне значення: як рамка очікувань партнерів щодо належної обачності та пропорційності, та як орієнтир на внутрішню процедурність і контроль за «інформаційними інструментами» сектору безпеки і оборони.

Аналіз останніх досліджень і публікацій. Проблематика нормативно-правового регулювання спеціальних інформаційних операцій знаходить відображення у працях вітчизняних та зарубіжних дослідників. В Україні цій темі приділяли увагу такі вчені, як М.А. Дмитренко, О.О. Верголяс, В.П. Горбулін, О.Г. Додонов, Д.В. Ланде, І.Н. Панарин, П.О. Яковлєв та інші. У їхніх роботах розглядаються різні аспекти інформаційної безпеки, правові засади протидії інформаційно-психологічним загрозам.

Міжнародний досвід регулювання СІО досліджувався у контексті діяльності таких організацій, як NATO, а також у працях зарубіжних експертів, зокрема L.S. Johnson, та в офіційних документах, серед яких Joint Publication 3-13 «Information Operations» США, доктринальні матеріали країн ЄС та Російської Федерації.

Разом із тим, у наявних дослідженнях недостатньо системно розкрито глибину системної кризи українського законодавства щодо СІО, зокрема конфлікт між конституційними обмеженнями та операційними потребами, а також не запропоновано цілісної концепції реформування з урахуванням сучасних цифрових викликів та міжнародного досвіду. Це обумовлює необхідність подальшого комплексного аналізу та розробки конкретних пропозицій щодо вдосконалення правового поля.

Мета дослідження: показати еволюцію доктринального розуміння спеціальних інформаційних операцій, їх інтеграцію у стратегічні комунікації. Визначити сучасний стан правового забез-

печення СІО в Україні і роль ключових суб'єктів (Міністерства оборони України/Служби безпеки України) та запропонувати напрямки вдосконалення правового режиму СІО.

Методи дослідження. Методологічну основу становлять порівняльно-правовий і доктринальний аналіз офіційних документів США, НАТО та ОБСЄ, системно-структурний підхід до розкриття місця СІО у стратегічних комунікаціях, а також аналіз норм національного законодавства України у сфері національної безпеки, оборони, контррозвідки та інформаційної безпеки.

Виклад основного матеріалу. У фаховому оборонному дискурсі США термін information operations набув системного поширення у польових статутах (field manuals), що закладали підходи до інформаційної підтримки операцій у мирний і воєнний час. Зокрема, у FM 100-23 «Peace Operations» фіксувалися питання інформаційного впливу і взаємодії з цивільним середовищем у контексті миротворчих дій [2]. Водночас FM 33-5 (у різних редакціях) історично розвивав концепцію психологічної війни/психологічних операцій як інструменту впливу на поведінку противника і населення [3].

Подальша доктриналізація відбулася у документах ВПС США. Показовим є Air Force Doctrine Document 2-5 «Information Operations» (11 січня 2005 року; пізніше перенумеровано як AFDD 3-13), який визначав СІО як інтеграцію спроможностей впливу, електронної боротьби та мережевих операцій для впливу, порушення, спотворення або узурпації процесів ухвалення рішень противника при одночасному захисті власних процесів [4]. Важливо, що у цьому підході СІО виходили за межі «пропаганди» і включали технологічні, організаційні та процедурні компоненти.

Еволюція особливо чітко простежується у Joint Publication 3-13 «Information Operations». Редакція 2006 року зосереджувалася на інтегрованому застосуванні ключових можливостей (електромагнітні засоби, комп'ютерні мережі, психологічні операції, військове мистецтво і безпекові операції тощо) для впливу на процес ухвалення рішень противником при одночасному захисті власного процесу [5]. Редакція 2012 року (з подальшими змінами) змістила акцент: СІО трактуються як інтегроване застосування під час військових операцій «інформаційно-релевантних можливостей» разом з іншими засобами для досягнення ефектів у інформаційному середовищі [6].

У меморандумі Міністерства оборони США «Strategic Communication and Information Operations in the Department of Defense» (25 січня 2011 року) додатково наголошувалося, що попередні визначення СІО надмірно фокусувалися на «переліку спроможностей» і недостатньо – на інформаційному середовищі та досягненні бажаних ефектів; також підкреслювалась потреба кращого управління і контролю за ключовими спроможностями [7]. З точки зору правового забезпечення це важливо: зміщення акценту від «інструментів» до «ефектів» посилює вимогу процедурного контролю (обґрунтованість цілей, пропорційність, оцінювання результатів, припинення операції).

У межах стратегічних комунікацій НАТО СІО визначаються як військові рекомендації та координація інформаційних військових заходів для створення бажаного впливу на наміри, розуміння та здатність противника й інших суб'єктів на підтримку операцій, місій та цілей Альянсу [8]. Паралельно НАТО виділяє психологічні операції як сплановану психологічну діяльність із застосуванням комунікаційних і інших засобів впливу на визначені аудиторії.

Практичний висновок для українського правового поля полягає в тому, що у сучасних західних моделях СІО переважно не є «ізольованою» діяльністю, а інтегруються у ширшу архітектуру стратегічних комунікацій і планування операцій. Це посилює вимогу до уніфікованої термінології між відомствами, прозорого розмежування «публічних» і «прихованих» інструментів та формалізації процедур санкціонування і контролю.

У кібер- та інформаційному середовищі міжнародні механізми стримування ескалації часто спираються на CBMs (confidence-building measures) – інструменти прозорості, комунікацій і координації. Рішення ОБСЄ 2013 року («Initial Set of OSCE Confidence-Building Measures…») стало одним із перших регіональних прикладів, що інституціоналізував такі заходи для зниження ризиків конфліктів через використання ІКТ [1]. Хоча CBMs не є «прямим дозволом» або «забороною» інформаційних операцій, вони формують стандарт поведінки: держави мають будувати внутрішні режими, які мінімізують помилкові атрибуції, забезпечують керованість та відповідальність за дії в кібер- та інформаційному просторі.

Для України, яка перебуває під постійним впливом деструктивних інформаційних кампаній держави-агресора, релевантним є поєднання: міжнародної легітимації власних захисних кроків, внутрішньої правової визначеності процедур і меж застосування інструментів СІО, щоб уникати вторинних ризиків – правових, репутаційних і міжнародно-політичних.

Конституція України закріплює обов'язок держави захищати суверенітет і територіальну цілісність, а також гарантує права і свободи людини як базову межу діяльності державних органів [9]. Закон України «Про національну безпеку України» визначає загрози як явища, тенденції і чинники, що ускладнюють або унеможливлюють реалізацію національних інтересів та збереження національних цінностей; він також встановлює систему планування і координації політики у сфері безпеки і оборони [10].

Стратегія національної безпеки України (Указ Президента № 392/2020, зі змінами 2025 року) прямо пов'язує стійкість держави з протидією дезінформації, інформаційним втручанням та гібридним загрозам, закладаючи підґрунтя для комплексних інструментів реагування [11]. У сфері оборони ключовим є Закон України «Про оборону України», який визначає воєнні дії та допускає проведення спеціальних операцій у визначених законом формах і за рішенням уповноважених суб'єктів [12].

Нормативна база інформаційної безпеки в Україні характеризується поєднанням законів і доктринальних документів. Доктрина інформаційної безпеки України (Указ Президента № 47/2017) визначає як актуальні загрози в інформаційній сфері здійснення СІО, спрямованих на підрив обороноздатності, деморалізацію, провокування паніки та дестабілізацію, а також проведення СІО у третіх країнах для формування негативного іміджу України [13]. Важливо, що Доктрина розподіляє відповідальність: МОУ і Генеральний штаб забезпечують протидію СІО проти ЗСУ і супроводження оборонних завдань інформаційними засобами, а СБУ протидіє СІО проти України, спрямованим на підрив конституційного ладу, суверенітету та територіальної цілісності [13].

Разом із тим Доктрина фактично описує режим протидії (counter-SIO), а не режим проведення власних СІО. Вона не встановлює процедур санкціонування, контролю, звітності, а також межі застосування інструментів впливу – що є критичним з точки зору прав людини, міжнародної легітимації та управління ризиками.

Закон України «Про Службу безпеки України» визначає СБУ як спеціальний орган державної безпеки, на який покладаються завдання захисту державного суверенітету, конституційного ладу, територіальної цілісності, економічного та оборонного потенціалу, законних інтересів держави та прав громадян від розвідувально-підривної діяльності [14]. Закон України «Про контррозвідувальну діяльність» встановлює правові засади контррозвідувального забезпечення державної безпеки, включно з протидією діяльності іноземних спецслужб і підривним загрозам [15].

У цифровому вимірі важливим є Закон України «Про основні засади забезпечення кібербезпеки України», який визначає принципи і суб'єктів кібербезпеки, у тому числі у контексті захисту критичної інфраструктури і державних інформаційних ресурсів [16]. Сукупно ці акти створюють підстави для діяльності СБУ у частині протидії інформаційним і кіберзагрозам, однак не формують окремого, чітко окресленого правового режиму «СІО як інструмента» (цілі, межі, процедури, контроль).

Практичні підходи відображені у відомчих матеріалах і методичних документах, які пропонують операційно-організаційне бачення СІО як комплексу заходів інформаційного впливу і контрвпливу, синхронізованого з іншими складовими сектору безпеки і оборони. Проте такі документи мають обмежену публічну легітимність і не можуть замінити законодавчого врегулювання, якщо йдеться про потенційний вплив на інформаційні права громадян, репутаційні та міжнародні наслідки.

Підходи до стратегічних комунікацій у системі МО України тривалий час визначалися відомчою Концепцією 2017 року (наказ МО України № 612), яка, серед іншого, містила дефініції інформаційних і психологічних операцій та вводила обмеження щодо їх застосування, зокрема принцип непроведення таких операцій стосовно громадян України (з окремими винятками) і поза визначеними районами застосування сил [17].

Водночас у 2025 році наказ МО України № 612 втратив чинність у зв'язку з ухваленням наказу Міністерства оборони № 653-нм, який визначив нові організаційні засади реалізації стратегічних комунікацій у МОУ [18]. Для правового аналізу це означає, що дефініції і обмеження 2017 року слід оцінювати як історичний етап становлення, а актуальні правила 2025 року – як предмет окремої верифікації і нормотворчої синхронізації з законами.

Законодавче визначення загроз і національних інтересів задає рамку для інструментів реагування [10; 11]. У практичному вимірі заходи протидії загрозам національній безпеці можуть групуватися як: політико-дипломатичні; військові; правові; інформаційно-психологічні; еконо-

мічні; науково-технологічні; організаційні; фізичні; технічні тощо. У такій системі СІО логічно розглядати як різновид інформаційно-психологічних і водночас організаційно-технічних заходів, що поєднують комунікаційні, аналітичні, кіберкомпонентні та процедурні елементи.

Функціонально СІО можуть виконувати три взаємопов'язані ролі:

1) Превентивну – нейтралізація ворожих наративів і каналів до настання кризової фази, підвищення інформаційної стійкості, недопущення паніки та міжгрупової ворожнечі [13; 16]

2) Оперативну – підтримка стійкості управління та ухвалення рішень під час криз/воєнних дій, включно з інформаційним супроводом оборонних завдань, контрнаративами, протидією ворожим СІО [12; 13]

3) Компенсаторну – асиметричне посилення спроможностей держави в умовах обмежених ресурсів, коли пряме військове або економічне реагування є недостатнім або надмірно затратним

Разом із тим, легітимність і ефективність СІО прямо залежать від визначеності правових підстав, процедур та меж, інакше СІО ризикують перетворитися на ситуативний інструмент, що складно контролюється, важко оцінюється і створює вторинні ризики (правові, репутаційні, політичні).

На основі аналізу національної нормативної бази і наукових підходів можна виокремити такі системні проблеми.

В українському праві співіснують різні пов'язані терміни («інформаційні операції», «інформаційно-психологічні операції», «стратегічні комунікації», «кібероперації»), але їх визначення або відсутні на рівні закону, або містяться у підзаконних і доктринальних актах, що мають різну юридичну силу [10; 12; 13; 17; 18]. Це породжує різночитання при плануванні, координації та контролі, особливо коли діяльність перетинає межі компетенції між обороною, розвідкою, контррозвідкою, кіберзахистом і урядовими комунікаціями.

Окрему увагу слід приділити конституційним межам. Стаття 17 Конституції України, з одного боку, покладає на державу обов'язок забезпечувати інформаційну безпеку як складову національної безпеки, а з іншого – містить застереження щодо недопустимості використання військових формувань для обмеження прав і свобод громадян [9]. Отже, будь-яка діяльність, яка може трактуватися як вплив на інформаційні права громадян, має спиратися на чітко визначені правові підстави та процедури, бути пропорційною меті і супроводжуватися дієвими механізмами контролю

СІО за своєю природою часто є прихованими, міжвідомчими і здатними впливати на інформаційні права громадян. Відтак потрібні чіткі «запобіжники»: порядок санкціонування, вимоги пропорційності, облік і аудит, ex post контроль, а також механізми внутрішнього комплаєнсу. Наявні акти визначають загальні завдання і загрози, але не формують повного процесуального циклу (planning–execution–assessment–termination) [9–13].

Цифрове середовище ускладнює атрибуцію інформаційних кампаній і кібератак, що створює ризики як помилкових рішень, так і надмірних обмежень прав. Це вимагає особливих правил документування інцидентів, зберігання цифрових доказів, взаємодії з провайдерами та міжнародної кооперації. Законодавство про кібербезпеку задає загальні принципи, але не деталізує режим доказовості для «інформаційних» компонентів СІО [16].

Скасування (втрата чинності) ключових відомчих документів і заміна їх новими (як у випадку стратегічних комунікацій Міністерства оборони України у 2025 році) посилює ризик нормативних розривів. Це аргумент на користь стабільнішого «рамкового» законодавчого регулювання, яке забезпечить сталі дефініції і базові процедури незалежно від відомчих циклів.

Ще у 2017 році у парламентському дискурсі порушувалося питання розширення правового поля для спеціальних операцій (зокрема, інформаційно-психологічних) поза межами воєнного стану як елемент підготовки держави до оборони. На це вказує згадка законопроєкту № 7272 (09.11.2017) у матеріалах комітетів Верховної Ради України [19]. Незалежно від долі конкретного законопроєкту, сама постановка питання залишається актуальною: гібридні загрози існують у «сірій зоні» між миром і війною, але держава має діяти у межах права і під контролем демократичних інститутів.

Першочерговим завданням удосконалення правового забезпечення СІО є подолання дефініційної фрагментації, що склалася через паралельне використання суміжних термінів («інформаційні операції», «інформаційно-психологічні операції», «стратегічні комунікації», «кібероперації») у документах різної юридичної сили та відомчої належності. У практичному вимірі це створює різночитання під час планування і координації, ускладнює контроль і оцінювання результативності,

а також підвищує юридичні ризики у сфері прав людини та демократичного нагляду, що особливо чутливо з огляду на конституційні межі діяльності органів сектору безпеки і оборони [9–13]. Відтак, на рівні закону доцільно синхронізувати понятійний апарат і узгодити його із сучасними доктринальними підходами, де СІО розуміються не як набір розрізнених інструментів, а як керована діяльність у інформаційному середовищі, орієнтована на досягнення визначених ефектів і підкріплена процедурністю [5–8].

У цьому контексті наукова новизна дослідження полягає у формулюванні прикладної моделі рамкового правового режиму СІО для України як стійкого «каркаса» у системі стратегічних комунікацій сектору безпеки і оборони. Такий каркас має закріплювати уніфіковані дефініції СІО та базових категорій інформаційного середовища, визначати легітимні цілі і межі застосування СІО відповідно до національних інтересів та актуальних загроз, а також забезпечувати чітке розмежування компетенцій між ключовими суб'єктами (оборона, контррозвідка/держбезпека, кібербезпека) без «розмивання відповідальності» [10; 12–16]. Саме відсутність такого законодавчого «ядра» нині зумовлює ситуацію, коли нормативна база достатньо розвинена для фіксації загрози ворожих СІО та організації протидії, але недостатня для правомірного, передбачуваного і підконтрольного застосування власних СІО, особливо поза режимом воєнного стану [11–13].

Процесуальна частина запропонованої моделі передбачає правове відтворення повного циклу управління СІО, що робить її юридично перевірюваною і контрольованою. Ініціювання СІО має спиратися на документовану оцінку загрози та формулювання очікуваних ефектів у інформаційному середовищі; на етапі санкціонування необхідні визначені законом рівні ухвалення рішення, обов'язкова юридична експертиза і фіксація меж повноважень, допустимих методів, часових параметрів та критеріїв пропорційності. Виконання СІО доцільно поєднувати із внутрішніми механізмами комплаєнсу й управління ризиками (облік дій, контроль доступу до спроможностей, мінімізація побічної шкоди), а оцінювання - із стандартизованими показниками ефектів і визначеними підставами припинення операції (exit criteria) та подальшою звітністю й ex post аудитом у формах, сумісних із режимами таємності [9–13; 16]. Така процесуалізація не лише підвищує легітимність застосування інструментів впливу, а й знижує ризики помилкових рішень і надмірного втручання у права та свободи.

Окремого унормування потребує цифровий вимір СІО, де атрибуція інформаційних впливів і доведення їх зв'язку з конкретними суб'єктами часто є складнішими, ніж у традиційних операційних середовищах. У межах рамкового режиму доцільно закріпити мінімальні стандарти документування інцидентів, збереження цифрових даних і доказовості щодо «інформаційних» компонентів СІО, а також принципи взаємодії з суб'єктами кібербезпеки та захисту критичної інфраструктури. Це створює підґрунтя для керованого застосування аналітичних інструментів OSINT/AI у правомірний спосіб - як допоміжного засобу верифікації, оцінювання ризиків і вимірювання ефектів, але з урахуванням потреби аудиту, прозорих критеріїв і запобігання системним помилкам [16; 20–23].

Нарешті, інституційний вимір запропонованої моделі передбачає не формальне декларування координації, а її юридичне закріплення через визначення постійного механізму міжвідомчої синхронізації СІО у системі стратегічних комунікацій. Саме процедурно оформлена координація із чітким розподілом ролей, відповідальністю та наглядом забезпечує практичну сумісність оборонних, контррозвідувальних та кібербезпекових інструментів і знижує ризики нормативних розривів, що виникають унаслідок зміни відомчих документів [10; 12–16].

Враховуючи, що держави-агресори інституціоналізують інформаційний вплив як елемент державної політики та воєнного планування, Україні доцільно вести порівняльний аналіз таких моделей і враховувати їх у власній правовій архітектурі протидії та стійкості.

Висновки. За результатами дослідження систематизовано міжнародні доктринальні підходи до спеціальних інформаційних операцій і простежено їх еволюцію в документах США, НАТО та ОБСЄ, а також проаналізовано сучасний стан нормативно-правового забезпечення СІО в Україні. Було встановлено, що західні моделі поступово змістили акцент від переліку «спроможностей» до ефект-орієнтованого розуміння СІО як діяльності в інформаційному середовищі, інтегрованої в архітектуру стратегічних комунікацій і підкріпленої процедурністю, керованістю та контролем ризиків

Водночас українська нормативно-правова база послідовно фіксує ворожі СІО як актуальну загрозу і визначає компетенції ключових суб'єктів щодо протидії. Проте, вітчизняне законодавство

не формує достатньо визначеного правового режиму для планування і проведення власних СІО, особливо поза межами воєнного стану, що зумовлює дефініційну фрагментацію, міжвідомчу неузгодженість і підвищені юридичні ризики у чутливій площині прав людини та демократичного контролю

У дослідженні сформульовано прикладну модель рамкового правового режиму СІО для України, яка поєднує уніфіковану термінологію, розмежування компетенцій та процесуалізацію повного циклу управління СІО із вбудованими гарантіями пропорційності, підзвітності й аудиту

У підсумку обґрунтовано необхідність переходу від переважно реактивної моделі до рамкового, процедурно визначеного регулювання СІО, узгодженого з конституційними гарантіями та сучасними доктринальними стандартами, із посиленням координації, підзвітності й методичного забезпечення оцінювання ефектів. Перспективи подальших досліджень пов'язані з розробленням цілісної концепції правового режиму СІО, уточненням компетенцій суб'єктів сектору безпеки і оборони, а також із виробленням стандартів атрибуції, доказовості та комплаєнсу в умовах цифровізації й використання аналітичних та автоматизованих інструментів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies: Permanent Council Decision No. 1106, PC.DEC/1106, 3 December 2013 // Organization for Security and Co-operation in Europe. URL: https://www.osce.org/pc/109168 (дата звернення: 06.01.2026).
2. Field Manual FM 100-23: Peace Operations. Washington, DC: Department of the Army, 1994. URL: https://gsacep-assets.s3.amazonaws.com/asset-manager/X7FR32DFQ9A1.pdf (дата звернення: 09.01.2026).
3. Field Manual FM 33-5: Psychological Warfare in Combat Operations. Washington, DC: Department of the Army, 1949.
4. Air Force Doctrine Document 3-13 (formerly 2-5): Information Operations (11 January 2005; incorporating Change 1, 28 July 2011). Washington, DC: United States Air Force, 2005. URL: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB558/AFDD3-13.pdf (дата звернення: 12.01.2026).
5. Joint Publication JP 3-13: Information Operations. Washington, DC: Joint Chiefs of Staff, 13 February 2006. URL: https://irp.fas.org/doddir/dod/jp3_13.pdf (дата звернення: 14.01.2026).
6. Joint Publication JP 3-13: Information Operations (27 November 2012; Change 1, 20 November 2014). Washington, DC: Joint Chiefs of Staff, 2012. URL: https://informationsecurity.info/_files/IO/jp3_13.pdf (дата звернення: 16.01.2026).
7. Strategic Communication and Information Operations in the Department of Defense: Memorandum (25 January 2011). U.S. Department of Defense. URL: https://pdnetworks.wordpress.com/wp-content/uploads/2011/03/stategic-commmunication-and-information-operations-in-the-department-of-defense1.pdf (дата звернення: 18.01.2026).
8. NATO Strategic Communications Policy (29 September 2009). URL: https://info.publicintelligence.net/NATO-STRATCOM-Policy.pdf (дата звернення: 20.01.2026).
9. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/ 254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 07.01.2026).
10. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 10.01.2026).
11. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 № 392/2020 (зі змінами, внесеними Указом Президента України від 13.01.2025 № 16/2025). URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text; https://zakon.rada.gov.ua/ laws/show/16/2025#Tex t (дата звернення: 22.01.2026).
12. Про оборону України: Закон України від 06.12.1991 № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 24.01.2026).
13. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017

№ 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 26.01.2026).
14. Про Службу безпеки України: Закон України від 25.03.1992 № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 28.01.2026).
15. Про контррозвідувальну діяльність: Закон України від 26.12.2002 № 374-IV. URL: https://zakon.rada.gov.ua/laws/show/374-15#Text (дата звернення: 30.01.2026).
16. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 13.01.2026).
17. Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України: наказ Міністерства оборони України від 22.11.2017 № 612 (втратив чинність). URL: https://zakon.rada.gov.ua/laws/show/v0612322-17#Text (дата звернення: 15.01.2026).
18. Про затвердження організаційних засад реалізації стратегічних комунікацій у Міністерстві оборони України: наказ Міністерства оборони України від 02.10.2025 № 653-нм. URL: https://zakon.rada.gov.ua/laws/show/v0653322-25#Text (дата звернення: 17.01.2026).
19. Картка законопроєкту № 7272 від 09.11.2017 «Про внесення змін до Закону України «Про оборону України» щодо деяких питань підготовки держави до оборони» // Верховна Рада України. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/38039 (дата звернення: 21.01.2026).
20. Горбулін В.П., Додонов О.Г., Ландэ Д.В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. Київ: Інтертехнологія, 2009. 164 с.
21. Верголяс О.В. Протидія спеціальним інформаційним операціям: організаційно-правовий аспект. *Інформація і право*. 2018. № 4. С. 121–128. URL: https://ippi.org.ua/sites/default/files/vergolyas_diser..pdf.
22. Дмитренко М. Проблемні питання нормативно-правового регулювання спеціальних інформаційних операцій в Україні. *Юридична Україна*. 2025. № 11. С. 55–59. URL: http://nbuv.gov.ua/UJRN/iblsd_2013_3_7.
23. Слюсарчук Х. Спеціальна інформаційна операція: історія становлення. *Часопис Київського університету права*. 2019. № 4. DOI: 10.36695/2219-5521.4.2019.22.

Дата першого надходження рукопису до видання: 04.02.2026
Дата прийняття до друку рукопису після рецензування: 20.02.2026
Дата публікації: 5.03.2026