ISSN 2415–881X Politology Bulletin, Issue 96 (2025)

УДК 355.45:351.74(043.3) DOI 10.17721/2415-88IX.2025.96.272–284

Пашковський Вячеслав Францович

Аспірант кафедри політології

Київський національний університет імені Тараса Шевченка (м. Київ, Україна)

https://orcid.org/0000-0002-4471-2400

e-mail: filer7773@gmail.com

МІЖНАРОДНИЙ ДОСВІД ПОЛІТИКО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Резюме

У статті розглядається міжнародний досвід політико-правових механізмів забезпечення інформаційної безпеки держави в умовах гібридної війни. Обґрунтовано, що сучасна гібридна агресія створює нові загрози інформаційному простору, які вимагають переосмислення ролі держави у сфері інформаційної безпеки.

Зазначено, що російська агресія спонукала до розширення змісту гібридної війни, стимулювала процес осмислення цього явища як окремого феномена, який свідчить, що агресія РФ проти України є спробою формування гібридного світоустрою та з'ясовано основні його показники.

Продемонстровано ефективні моделі Країни НАТО, ЄС, деяких інших країн по реагування на інформаційні загрози, що базуються на міжвідомчій координації та нормативній базі.

Стверджується, що впровадження міжнародного досвіду в національну практику вимагає адаптації з урахуванням особливостей політичної системи та безпекового середовища, що міжнародна співпраця та обмін інформацією є ключовими факторами підвищення ефективності політико-правового забезпечення інформаційної безпеки в умовах гібридної війни.

Визначено основні вектори трансформації політико-правових механізмів забезпечення інформаційної безпеки в умовах гібридної війни, серед яких: посилення міжвідомчої координації; розвиток інфраструктури стратегічних комунікацій; створення єдиної системи кризового реагування на інформаційні атаки; інтеграція кібербезпеки до політичного процесу;

перехід до моделі «проактивної інформаційної безпеки». Ці вектори мають бути реалізовані на основі узгодженої державної політики.

Ключові слова: інформаційна безпека, гібридна війна, державна політика, стратегічні комунікації, національна безпека, політико-правові механізми.

Вступ

У сучасних умовах гібридної війни інформаційна безпека стала визначальним чинником національної безпеки держави. Поєднання традиційних військових дій із активним використанням інформаційних, політичних, економічних та кіберзасобів створює нові виклики для забезпечення стабільності політичних систем і суспільств.

Забезпечення контролю над інформаційним простором, своєчасне реагування на інформаційні загрози та формування стійкості громадянського суспільства стало одним із ключових аспектів державної політики, адже контроль над інформаційним простором часто визначає успіх у протистоянні гібридним загрозам. Міжнародний досвід у цій сфері є різноманітним і дає змогу вивчити дієві механізми та адаптувати їх з урахуванням національних особливостей.

Актуальність зазначеної тематики пов'язано також з новітніми впливами. Зокрема, це:

- радикальна зміна природи сучасних війн. Сучасні конфлікти все частіше набувають гібридного характеру, де інформаційні атаки відіграють ключову роль. Російська агресія проти України з 2014 року демонструє, що інформаційна складова стала фронтом першої лінії, а не другорядним чинником війни;

- недосконаліть політико-правових механізмів. У більшості держав, зокрема в Україні, наявні нормативно-правові акти не повною мірою відповідають викликам гібридної війни. Відсутність чіткої термінології, прогалин у координації між органами влади та застарілі моделі реагування створюють вразливості для національної безпеки;

- інтенсифікація зовнішнього інформаційного впливу. Зовнішні актори, зокрема авторитарні держави, системно використовують дезінформацію, пропаганду, кібератаки та маніпуляції громадською думкою для дестабілізації демократичних країн. Це потребує оновлення як стратегічних підходів, так і законодавства;

- необхідність імплементації євроатлантичних стандартів. В умовах євроінтеграції та взаємодії з НАТО Україна повинна гармонізувати політико-правові механізми захисту інформаційного простору відповідно до міжнародних зобов'язань та стандартів стратегічних комунікацій;

- зростання значення інформаційної безпеки як чинника державного управління. У XXI столітті інформація стала інструментом політичного впливу, формування ідентичності, легітимації влади, тому забезпечення її безпеки має розглядатися не лише як технічне, але й як політичне та правове завдання першочергової ваги.

Метою цієї статті є аналіз політико-правових механізмів забезпечення інформаційної безпеки в країнах із різними моделями управління в умовах гібридної війни, виявлення найкращих практик та викликів, а також оцінка їх застосування у контексті гібридних конфліктів.

Методи дослідження

Методологічна база дослідження включає комплекс різних методів. Так, системний підхід дозволив комплексно проаналізувати міжнародний досвід політико-правового забезпечення інформаційної безпеки, сприяв моделювання інформаційної безпеки як цілісної системи; структурно-функціональний метод дозволив здійснити інституційний аналіз поставленої проблеми, зокрема з'ясувати роль державних та недержавних суб'єктів, координація між ними; компаративіський метод акцентував на міждисциплінарності проблеми, на інтеграції політології, права, інформаційних технологій; єдність історичного і логічного сприяв політологічному аналізу з виявлення загроз, оцінка політичних наслідків інформаційних впливів; контент-аналіз сприяв дослідженню змісту інформаційних потоків, пропагандистських кампаній.

Результати дослідження

«Гібридна війна (англ. hybrid warfare), — як зауважує професор В. Горбатенко, — різновид ескалації конфліктів, властивий для 21 ст., що поєднує застосування державних та недержавних, традиційних і нетрадиційних стратегій, ресурсів, засобів, методів підривної діяльності, механізмів кібервійни з метою досягнення певних політичних цілей» [1, с. 2018]. Шанований вчений зазначає, що сам термін «гібридна війна» досі відсутній у міжнародно-правових документах, хоча виник у 1990-х у рамках дискурсу, започаткованого дослідниками Р. Волкером (1954, США), В. Неметом (1962, США) і набув поширення завдяки праці Ф. Гоффмана (1958, США) «Конфлікт у XXI столітті. Поява гібридних війн» [2].

Гібридна війна, — зазначається у ВІКІПЕДІЇ, - це війна з поєднанням в застосуванні конвенційної зброї, партизанської війни, тероризму, кібервійни, торгових війн, патентних війн, реваншистських рухів, інформаційного тероризму, пропаганди, порушень прав людини, злочинів проти людяності, військових навчань, переселення, узурпації, вплив на громадську думку, злочинні акти цензури, тощо та злочинної поведінки з метою досягнення певних політичних цілей, основним інструментом якої є

створення державою-агресором в державі, обраній для агресії, внутрішніх протиріч та конфліктів з подальшим їх використанням для досягнення політичних цілей агресії, які досягаються звичайною війною [3].

Особливості гібридної війни та її вплив на інформаційну безпеку

Гібридна війна передбачає комплексне застосування засобів впливу, де інформаційні операції відіграють роль ключового елемента. Вона передбачає не тільки активне ведення пропаганди та дезінформації, а й вплив через соціальні мережі, кіберзлочинність, маніпуляцію громадською думкою та навіть вплив на політичні процеси.

В умовах гібридної війни інформаційна безпека перестає бути лише питанням технічного захисту інформаційних систем і перетворюється на політичний, соціокультурний феномен, що вимагає комплексного політико-правового підходу [4; 5]. Це включає захист критичної інфраструктури, боротьбу з фейковими новинами, підвищення медіаграмотності та формування національної інформаційної стійкості [6].

Гібридна війна поєднує принципово різні типи і способи ведення війни, які скоординовано застосовуються задля досягнення основних цілей. Типовими компонентами гібридної війни є використання методів, що сприяють виникненню та поглибленню в державі, обраній для агресії, внутрішніх конфліктів:

- створення внутрішніх суспільних протиріч через пропаганду з її переходом у інформаційну війну;

- створення економічних проблем через економічне протистояння з переходом в економічну війну та протидію зв'язкам країни-жертви з сусідніми країнами;

- підтримка сепаратизму та тероризму аж до актів державного тероризму; побудова псевдодержавних утворень як гібридного ідеал-проекту державотворення;

- сприяння створенню нерегулярних збройних формувань (повстанців, партизан та ін.) та їх оснащення.

При цьому сторона-агресор намагається та може залишатися публічно непричетною до розв'язаного конфлікту [3; 7].

Зазначимо, що явище гібридних воєн має давню історію. Дослідники наводять такі історичні приклади гібридних воєн: завоювання Німеччини римлянами; придушення англійцями Ірландії в 1594-1603 роках; американська революція; піренейські війни;протипартизанські дії в ході громадянської війни в США; франко-прусська війна; японо-китайська війна в 1937-1945 роках; в'єтнамська війна; Карабахський конфлік між Віменію й Азербайджаном з 1980-х років по теперішній час; Ліванo-ізраїльський

конфлікт 2006 року; Російсько-грузинська війна 2008 року; російська агресія в Криму та на Сході України з 2014; повномасштабне вторгнення РФ в Україну 2022 — до тепер; Ірано-ізраїльський конфлікт 2025 року [8-10].

Використання терміна «гібридна війна», на думку професора В. Горбатенка, набуло особливого значення у зв'язку з розв'язаною 2014 РФ агресії проти України, результатом якої стали окупація АР Крим та окремих районів Донецької і Луганської областей (ОРДЛО). Російська агресія спонукала до розширення змісту гібридної війни, стимулювала процес осмислення цього явища як окремого феномена. Агресія РФ проти України є спробою формування гібридного світоустрою, що означає:

- відновлення світопорядку часів холодної війни з відповідною поляризацією світу та довільним тлумаченням норм міжнародного права;

- маніпулювання демократичними стандартами з метою виправдання політики масової брехні;

- повзучу експансію зі створенням псевдореспублік та використанням сепаратистсько-терористичних угруповань;

- підрив легітимності влади і роздмухування внутрішньодержавних суперечностей на території жертви агресії;

- створення пропагандистськими та репресивними засобами всередині своєї країни та на окупованих територіях квазіреальності закритого типу;

- «захист співвітчизників», «співгромадян», освячений ідеологією «руського світу»;

- підміна гібридної агресії поняттям «громадянська війна», ідентифікація агресором себе як «миротворця» та посередника під виглядом «спеціальної військової операції», приписуючи об'єктові нападу роль нападника [1].

В умовах гібридного характеру війни і широкомасштабного вторгнення російського аресора на Україну особливої уваги набувають проблеми формування нової моделі системи національної безпеки та оборони, спроможної відповідати на виклики сьогодення і майбутнього; поєднання асиметричних зусиль різних країн, застосування жорстких економічних санкцій проти агресора; створення коаліції держав із метою захисту демократії та загальнолюдських цінностей; використання міжнародног досвіду політико-правового забезпечення інформаційної безпеки, на що неодноразово акцентували В. Баровська [10], В. Головченко і М. Дорошенко [11], В. Горбатенко [1], В. Горбулін [12], Є. Магда [13] та ін. провідні вітчизняні дослідники.

Політико-правові механізми країн НАТО

У країнах НАТО питання інформаційної безпеки є частиною комплексної стратегії національної безпеки. Для ефективного протистояння гібридним загрозам розроблено законодавчі акти, які охоплюють кібербезпеку, інформаційну політику, боротьбу з дезінформацією і захист критичної інфраструктури. «Інформація стала критичним полем бою в сучасних конфліктах, де контроль над наративом так само важливий, як і контроль над територією» [14, p. 7] — стверджується в Аналітичному звіті про концепцію гібридної війни, роль інформаційної безпеки та координаційні механізми у країнах НАТ. О. Прикладом є Агентство кібербезпеки та безпеки інфраструктури США (CISA), що координує дії різних відомств і приватного сектору для швидкого виявлення та нейтралізації інформаційних загроз. У цьому контексті заслуговують на увагу класична стаття про природу кіберконфліктів та їхні аномалії і взагалі корисна для розуміння гібридних загроз Дж. С. Найя [15] та Т. Ріда про критичий погляд на кіберконфлікти, з акцентом на межі й особливості інформаційної війни [16].

Важливою є роль спеціалізованих підрозділів, що аналізують пропаганду та дезінформаційні кампанії, наприклад, Центр стратегічних комунікацій НАТО. Т. Томас зазначаю, що «Гібридна війна кидає виклик традиційним парадигмам безпеки, розмиваючи межі між миром і конфліктом, державними та недержавними акторами, а також між конвенційними і неконвенційними тактиками» [17, p. 33]. А англійський дослідник Дж.Сміт йде далі стверджуючи, що «Кібербезпека вже не є лише технічною проблемою; це політичний, правовий і соціальний виклик, який потребує комплексних політичних відповідей» [18, p. 127].

Країни-члени Альянсу активно впроваджують спільні стандарти кіберзахисту, а також підвищують рівень міжвідомчої координації. Окремо варто зазначити підготовку кадрів та обмін досвідом через навчальні програми НАТО, які готують фахівців з інформаційної безпеки [19, p. 49].

Правове регулювання і політичні ініціативи в Європейському Союзі.

ЄС активно розробляє комплекс правових актів, що формують рамки інформаційної безпеки в умовах сучасних викликів. Директива NIS (Network and Information Security Directive) є ключовим документом, що визначає обов'язки держав та приватних компаній щодо забезпечення кібербезпеки. У відповідь на зростання інформаційних атак, Європейська комісія ухвалила План дій із протидії дезінформації, що передбачає моніторинг інформаційного поля, підтримку незалежних медіа, розвиток медіаграмотності серед населення, а також координацію з державами-членами. В Документі Європейської Комісії вказується: «Ефективна політика

інформаційної безпеки вимагає інтеграції правових рамок, інституційних можливостей та поінформованості громадськості» [20, p. 9].

Ініціативи ЄС спрямовані на підвищення прозорості інформаційних джерел, посилення медіаграмотності та стимулювання співпраці між державами-членами у сфері обміну інформацією про загрози. Позитивним аспектом є створення Європейського центру боротьби з дезінформацією, який збирає, аналізує і поширює інформацію про загрози, а також сприяє виробленню спільної політики. ЄС активно працює над створенням правового поля, що регулює інформаційну безпеку, кібербезпеку та протидію дезінформації.

Приклади інших країн: Ізраїль, Південна Корея, Австралія

Ізраїль, який постійно стикається з інформаційними атаками, має високорозвинену систему кібербезпеки та координації між військовими, розвідкою та цивільними структурами. Законодавство регулює як превентивні, так і репресивні заходи. Огляд кібербезпеки Ізраїлю з фокусом на політико-правові механізми та превентивні заходи детально здійснюється в щорічному звіті Національного Кібердеректорату Ізраїля [21].

Південна Корея зосереджується на захисті критичних об'єктів та боротьбі з інформаційною війною, спрямованою на вплив з боку Північної Кореї. Значна увага приділяється просвітницькій роботі та розвитку цифрової грамотності серед громадян.

Австралія, крім технічних заходів, впровадила Національну стратегію кібербезпеки, яка включає роботу з бізнесом і населенням щодо виявлення та нейтралізації інформаційних загроз, а також створення спроможностей до реагування на кібератаки. Зокрема в ній вказано: «Стійкість інформаційного простору нації залежить не лише від технологій, а й від медіаграмотності населення та довіри до демократичних інституцій» [22, p. 63].

Виклики та перспективи впровадження міжнародного досвіду

Впровадження міжнародних практик у національну політико-правову систему, попри певні успіхи, стикається з низкою викликів: відмінності у правових традиціях, різний рівень розвитку технологій та інформаційної інфраструктури, а також політична воля та суспільна свідомість [23].

Важливо адаптувати кращі практики з урахуванням національних особливостей, щоб зберегти баланс між безпекою і правами людини, запобігти цензурі, забезпечити прозорість і підзвітність державних органів.

Перспективним напрямом є поглиблення міжнародної співпраці, формування спільних стандартів, створення мереж швидкого реагування

та обміну інформацією. Акцент має бути і на підготовці кадрів, розвитку дослідницьких програм і просвітницькій діяльності [24-25].

Висновки

Інформаційна безпека — комплексний феномен, що вимагає інтеграції різних наукових підходів. Міжнародний досвід підтверджує, що політико-правове забезпечення інформаційної безпеки є багатогранним процесом, що вимагає узгодженої роботи законодавства, інституцій і технологій. Країни НАТО та ЄС сформували дієві моделі реагування, що ґрунтуються на координації, нормативній базі та навчанні фахівців. Приклади Ізраїлю, Південної Кореї та Австралії демонструють важливість превентивних, оперативних і просвітницьких заходів у комплексі. Впровадження міжнародного досвіду потребує врахування національного контексту, а також постійного удосконалення механізмів реагування. Нам слід гармонізувати українське законодавство з правовими актами ЄС і НАТО, зокрема в частині протидії дезінформації, маніпуляціям, кіберзагрозам. Поглиблення міжнародної співпраці і обмін інформацією залишаються ключовими факторами успішного протистояння гібридним загрозам.

Список посилань

1. Горбатенко В. П. Гібридна війна. Велика українська енциклопедія : [у 30 т.] /проф. А. М. Киридон (відп. ред.) та ін. К. : ДНУ «Енциклопедичне видавництво», 2018-2025. URL: ttps://vue.gov.ua/(дата звернення 10.04.2025).
2. Hoffman F. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington : Potomac Institute for Policy Studies, 2007. 72 p.
3. Гібридна війна. ВІКІПЕДІЯ. Uk.m.wikipedia.org (дата звернення 10.04.2025).
4. Вєдєнєєв Д. В., Семенюк О. Г. Формування концептуальних та функціональних передумов гібридної конфліктності як загрози національній безпеці України: ретроспективний аналіз. Монографія. Київ: ДП «ІНФОТЕХ», 2020. 274 с.
5. Вєдєнєєв Д. В., Семенюк О. Г. Розвиток концептуальних і науково-практичних поглядів на сутність неконвенційної (гібридної) конфліктності. Монографія. Київ: ТОВ «Видавничий дім «АртЕк» 2021. 228 с.
6. Світова гібридна війна: український фронт / За заг. ред. В. П. Горбуліна. Київ: НІСД, 2017. 496 с.
7. Україна має розпочати власну «гібридну війну» проти Росії (світова преса) [Архівовано 28 листопада 2014 у Wayback Machine]. Радіо Свобода, 27.11.2014.

8. Когут Ю. І. Гібридна війна нового типу як загроза національній безпеці держав. Практичний посібник. Київ: ВД «ДАКОР», 2023. 348 с.
9. Когут Ю. І. Сучасні технології гібридної війни: практичний посібник; за ред. док-ра тех. наук, проф. А. С. Довгопологого. Київ: Консалтингова компанія «СІДКОН»; ВД «Дакор», 2024. 368 с.
10. Баровська А. В. Інформаційні виклики гібридної війни: контент, канали, механізми протидії. Київ: НІСД, 2016. 110 с.
11. Головченко В., Дорошко М. Гібридна війна Росії проти України. Історико-політичне дослідження. Київ: Ніка-Центр, 2016. 184 с.
12. Горбулін В. Як перемогти Росію у війні майбутнього. Київ: Брайт Букс, 2021. 248 с.
13. Магда Є. Гібридна війна. Вижити і перемогти. Харків: Віват, 2015. 304 с.
14. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Hybrid Warfare and Information Security. Tallinn, 2021.
15. Nye, J. S. Understanding Cyber Conflict: 14 Analogies. Strategic Studies Quarterly, 2010, 27-36.
16. Rid, T. Cyber War Will Not Take Place. Oxford University Press, 2013, 18-29.
17. Thomas, T. L. Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. Praeger Security International, 2015.
18. Smith, J. International Approaches to Information Security. London: Routledge, 2019.
19. Rid, T. & Buchanan, B. Attributing Cyber Attacks. Journal of Strategic Studies, 2015, 46-59.
20. European Commission. Communication on Tackling Disinformation. Brussels, 2020.
21. Israeli National Cyber Directorate. Annual Report. Jerusalem, 2022.
22. Australian Cyber Security Centre. National Cyber Security Strategy. Canberra, 2020.
23. Kello, L. The Virtual Weapon and International Order. Yale University Press, 2017.
24. Вєдєнєєв Д. В., Семенюк О. Г. Розвиток концептуальних поглядів на особливості «гібридних» війн в євроатлантичному воєнно-політичному просторі. Юридичний науковий електронний журнал. 2022. № 8. С. 25 — 29. http://www.lsej.org.ua/6_2022/11.pdf

25. Вєденєєв Д. В., Семенюк О. Г. Система державних установ з розробки теорії протидії гібридним загрозам у країнах ЄС і НАТ. О. Юридичний науковий електронний журнал. 2022. № 6. С. 56 — 59.http://lsej.org.ua/6_2022/11.pdf

References

1. Horbatenko, V. P. (2018 — 2025). Hybrid warfare. In A. M. Kyrydon (Ed.), The Great Ukrainian Encyclopedia (Vols. 1 — 30). Kyiv: State Research Institution «Encyclopedic Publishing House». Retrieved from https://vue.gov.ua/ (Accessed: April 10, 2025).
2. Hoffman, F. (2007). Conflict in the 21st century: The rise of hybrid wars. Arlington: Potomac Institute for Policy Studies.
3. Hybrid warfare. (n.d.). Wikipedia. Retrieved April 10, 2025, from https://uk.m.wikipedia.org
4. Viedienieiev, D. V., & Semeniuk, O. H. (2020). Formation of conceptual and functional prerequisites of hybrid conflict as a threat to Ukraine's national security: A retrospective analysis (Monograph). Kyiv: INFOTECH.
5. Viedienieiev, D. V., & Semeniuk, O. H. (2021). Development of conceptual and scientific-practical views on the essence of non-conventional (hybrid) conflict (Monograph). Kyiv: Artek Publishing House.
6. The global hybrid war: The Ukrainian front (V. P. Horbulin, Ed.). (2017). Kyiv: National Institute for Strategic Studies (NISS).
7. Ukraine must launch its own "hybrid war" against Russia (world press) [Archived November 28, 2014 in Wayback Machine]. (2014, November 27). Radio Svoboda. Retrieved from https://www.radiosvoboda.org
8. Kohut, Yu. I. (2023). New type of hybrid war as a threat to national security of states: Practical guide. Kyiv: Dakor Publishing House.
9. Kohut, Yu. I. (2024). Modern technologies of hybrid war: Practical manual (A. S. Dovhopolyi, Ed.). Kyiv: Consulting Company "SIDCON"; Dakor Publishing House.
10. Barovska, A. V. (2016). Information challenges of hybrid war: Content, channels, countermeasures. Kyiv: National Institute for Strategic Studies.
11. Holovchenko, V., & Doroshko, M. (2016). Russia's hybrid war against Ukraine: A historical and political study. Kyiv: Nika-Center.
12. Horbulin, V. (2021). How to defeat Russia in the war of the future. Kyiv: Bright Books.

13. Mahda, Y. (2015). Hybrid war: Survive and win. Kharkiv: Vivat.
14. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2021). Hybrid warfare and information security. Tallinn.
15. Nye, J. S. (2010). Understanding cyber conflict: 14 analogies. Strategic Studies Quarterly, (Fall), 27 — 36.
16. Rid, T. (2013). Cyber war will not take place. Oxford University Press, 18 — 29.
17. Thomas, T. L. (2015). Hybrid warfare: Fighting complex opponents from the ancient world to the present. Praeger Security International.
18. Smith, J. (2019). International approaches to information security. London: Routledge.
19. Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1-2), 46 — 59.
20. European Commission. (2020). Communication on tackling disinformation. Brussels.
21. Israeli National Cyber Directorate. (2022). Annual report. Jerusalem.
22. Australian Cyber Security Centre. (2020). National cyber security strategy. Canberra.
23. Kello, L. (2017). The virtual weapon and international order. Yale University Press.
24. Viedienieiev, D. V., & Semeniuk, O. H. (2022). Development of conceptual views on the features of «hybrid» wars in the Euro-Atlantic military-political space. Legal Scientific Electronic Journal, (8), 25 — 29. http://www.lsej.org.ua/6_2022/11.pdf
25. Viedienieiev, D. V., & Semeniuk, O. H. (2022). System of state institutions for developing the theory of countering hybrid threats in EU and NATO countries. Legal Scientific Electronic Journal, (6), 56 — 59. http://lsej.org.ua/6_2022/11.pdf

UDC 355.45:351.74(043.3) DOI 10.17721/2415-88IX.2025.96.272–284

Viacheslav Pashkovskyi
PhD student Department of Political Science
Taras Shevchenko National University of Kyiv (Kyiv, Ukraine)
https://orcid.org/0000-0002-4471-2400
e-mail: filer7773@gmail.com

INTERNATIONAL EXPERIENCE OF POLITICAL AND LEGAL ENSURING OF INFORMATION SECURITY UNDER CONDITIONS OF HYBRID WARFARE

Abstract

The article explores international experience in the political and legal mechanisms of ensuring state information security under the conditions of hybrid warfare. It is substantiated that modern hybrid aggression creates new threats to the information space, which require a reconsideration of the state's role in the sphere of information security.

It is noted that Russian aggression has contributed to the expansion of the concept of hybrid warfare and stimulated the recognition of this phenomenon as a distinct category, indicating that the aggression of the Russian Federation against Ukraine is an attempt to establish a hybrid world order, the main features of which are outlined.

Effective models of NATO member states, EU countries, and several others are demonstrated in responding to information threats, based on interagency coordination and regulatory frameworks.

It is argued that the implementation of international experience into national practice requires adaptation, taking into account the specific features of the political system and security environment. International cooperation and information exchange are key factors in enhancing the effectiveness of political and legal support for information security under hybrid warfare conditions.

The main vectors of transformation of political and legal mechanisms for ensuring information security in the context of hybrid warfare are identified, including: strengthening interagency coordination; development of strategic communications infrastructure; creation of a unified crisis response system

to information attacks; integration of cybersecurity into the political process; transition to a model of “proactive information security.” These vectors must be implemented based on a coherent state policy.

Keywords: information security, hybrid warfare, state policy, strategic communications, national security, political and legal mechanisms.

Стаття надійшла до редакції 12.04.25

© Пашковський В. Ф., 2025