НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ІТ-ПРАВО ПІД ЧАС ГІБРИДНОЇ ВІЙНИ: ВІД ПОШУКУ ПАРАДИГМИ ДО ПРАГМАТИЧНИХ РІШЕНЬ

Колективна монографія

За редакцією
Є. Харитонова, О. Харитонової, І. Давидової

Одеса
Фенікс
2025

УДК 340:004:327:355
І-87

Рекомендовано рішенням вченої ради
Національного університету «Одеська юридична академія»
(протокол № 9 від 30 червня 2025 р.)

Рецензенти:

Майданик Р. А. – академік НАПрН України, доктор юридичних наук, професор, професор кафедри цивільного процесу Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка;

Соколов А. В. – доктор технічних наук, професор, професор кафедри кібербезпеки Національного університету «Одеська юридична академія»;

Маковій В. П. – кандидат юридичних наук, професор, завідувач кафедри цивільно-правових дисциплін Одеського державного університету внутрішніх справ.

І-87 **ІТ-право під час гібридної війни: від пошуку парадигми до прагматичних рішень** : кол. монографія / за заг. ред. проф.: Є. Харитонова, О. Харитонової, І. Давидової. – Одеса : Фенікс, 2025. – 588 с.
ISBN 978-617-8430-70-2

Монографія є продовженням циклу праць колективу кафедри цивільного права Національного університету «Одеська юридична академія», присвячених результатам досліджень цивілістичних шкіл університету від часу їхнього формування до гібридної війни, що триває нині. У третьому томі аналізуються в контексті гібридної війни: проблеми визначення концепту «ІТ-право», особливості правового регулювання відносин, що виникають у зв'язку з використанням інформаційних технологій, особливості механізму цивільно-правового регулювання у сфері ІТ, чинник симулякру, значення та роль інформаційного середовища як стратегічного ресурсу, правові рамки для цифрових активів і перспективи цифрової власності, ІТ-правочини, порушення прав інтелектуальної власності в Інтернет, протидія кіберзагрозам у гібридній кібервійні, загрози вербування неповнолітніх через соцмережі та месенджери та юридичні заходи запобігання таким загрозам, правове регулювання стартапів, е-кредитування, цивільно-правова відповідальність за шкоду, завдану кібератаками, забезпечення інформаційної безпеки електронного судочинства в умовах гібридної війни в Україні та ін.

Авторський колектив концентрував увагу на обґрунтуванні необхідності комплексного вирішення практичних питань впорядкування інформаційно-технологічні відносини в умовах гібридної російсько-української війни. Автори прагнули розкрити особливості правового регулювання цих відносин і запропонувати власне бачення шляхів вирішення проблем, що виникають у цій сфері. Усвідомлюючи спірність низки висновків і пропозицій, автори розраховують на продовження плідних дискусій з проблем правового регулювання інформаційних технологій, зокрема в умовах гібридної війни.

Монографія може бути цікавою науковцям, практикуючим юристам, викладачам, аспірантам, здобувачам вищої освіти, а також широкому загалу небайдужих українців, які цікавляться проблемами правового регулювання у сфері ІТ, зокрема під час гібридної війни.

УДК 340:004:327:355

ISBN 978-617-8430-70-2

ЗМІСТ

Авторський колектив

Харитонов Євген (ORCID ID: 0000-0001-5521-0839), доктор юридичних наук, професор, член-кореспондент НАПрН України, зав. кафедри цивільного права НУ «ОЮА»: розділ 1 (у співав. з О. Харитоновою, І. Давидовою); розділ 2 (у співав. з О. Харитоновою); розділ 3 (у співав. з О. Харитоновою); розділ 4 (у співав. з О. Харитоновою); розділ 5 (у співав. з О. Харитоновою); розділ 11 (у співав. з О. Харитоновою); розділ 14 (у співав. з О. Харитоновою);

Харитонова Олена (ORCID ID: 0000-0002-9681-9605), докторка юридичних наук, професорка, членкиня-кореспондент НАПрН України, зав. кафедри права інтелектуальної власності і патентної юстиції НУ «ОЮА»: розділ 1 (у співав. з Є. Харитоновим, І. Давидовою); розділ 2 (у співав. з Є. Харитоновим); розділ 3 (у співав. з Є. Харитоновим); розділ 4 (у співав. з Є. Харитоновим); розділ 5 (у співав. з Є. Харитоновим); розділ 11 (у співав. з Є. Харитоновим); розділ 14 (у співав. з Є. Харитоновим);

Давидова Ірина (ORCID ID: 0000-0001-5622-671X), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 1 (у співав. з Є. Харитоновим, О. Харитоновою); розділ 9;

Некіт Катерина (ORCID ID: 0000-0002-3540-350X), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 7;

Сафончик Оксана (ORCID ID: 0000-0001-6781-8219), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 19;

Бааджи Наталія (ORCID ID: 0000-0002-9889-4879), кандидатка юридичних наук, доцента, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 10;

Берназ-Лукавецька Олена (ORCID ID: 0000-0002-2133-1672), кандидатка юридичних наук, доцента, доцентка кафедри цивільного права НУ «ОЮА»: розділ 17;

Галупова Лариса (ORCID ID: 0000-0001-6263-2773), кандидатка юридичних наук, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 8 (у співав. з А. Кирилюк);

Дрогозюк Крістіна (ORCID ID: 0000-0001-9254-9575), кандидатка юридичних наук, доцента, доцентка кафедри цивільного, нотаріального та виконавчого процесу НУ «ОЮА»: розділ 20;

Калітенко Оксана (ORCID ID: 0000-0003-1001-3561)**,** кандидатка юридичних наук, доцентка, професорка кафедри цивільного права НУ «ОЮА»: розділ 6;

Кирилюк Алла (ORCID ID: 0000-0002-3051-6599), кандидатка юридичних наук, доцентка, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 8 (у співав. з Л. Галуповою);

Омельчук Олександр (ORCID ID: 0000-0002-0082-3619), кандидат юридичних наук, доцент, доцент кафедри цивільного права НУ «ОЮА»: розділ 12;

Ткалич Максим (ORCID ID: 0000-0003-4224-7231), кандидат юридичних наук, доцент, доцент кафедри цивільного права Запорізького національного університету: розділ 21 (у співав. з Ю. Толмачевською);

Токарева Віра (ORCID ID: 0000-0002-8409-1477), кандидатка юридичних наук, доцентка, доцентка кафедри цивільного права НУ «ОЮА»: розділ 13;

Толмачевська Юлія (ORCID ID: 0000-0002-7964-8875), докторка філософії (081 право): розділ 21 (у співав. з О. Ткаличем);

Фасій Богдан (ORCID ID: 0000-0002-8715-930X), кандидат юридичних наук, доцент, декан факультету судового та міжнародного права НУ «ОЮА»: розділ 18;

Розумейко Дмитро (ORCID ID: 0000-0001-8206-1031)**,** аспірант кафедри цивільного права НУ «ОЮА»: розділ 16;

Рябченко Вікторія (ORCID ID: 0009-0007-1542-6492)**,** аспірантка кафедри цивільного права НУ «ОЮА»: розділ 15.

Розділ 6

ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ ЯК СТРАТЕГІЧНИЙ РЕСУРС У ГІБРИДНИХ КОНФЛІКТАХ

DOI

Оксана Калітенко
кандидатка юридичних наук, доцента

Гібридні конфлікти як багатовимірне явище сучасності стали результатом трансформації класичних форм воєнного протистояння та еволюції інструментів геополітичної боротьби. Ці конфлікти на сучасному етапі розвитку людства поєднують військові, політичні, економічні, інформаційні, цифрові та кібернетичні елементи, які взаємодіють у межах єдиної стратегії для досягнення складних і багаторівневих цілей. У цифрову епоху гібридні конфлікти набули нових форм, адже стрімкий розвиток інформаційних технологій, глобальна цифровізація, а також зростання ролі кіберпростору в житті кожної людини значно розширили арсенал інструментів, доступних їхнім учасникам. Ідея гібридних конфліктів, хоча й отримала широке визнання лише у XXI столітті, має глибокі історичні корені. Елементи гібридності можна виявити у багатьох конфліктах минулого, які поєднували використання військових і невійськових засобів впливу на населення задля досягнення стратегічних цілей. Наприклад, під час Холодної війни активно використовувалися «проксі-війни», дезінформація, пропаганда конкретних ідей, економічний тиск і дипломатичні маніпуляції. Однак лише у 2000-х роках, з розвитком та активним поширенням цифрових технологій, гібридні конфлікти почали сприйматися як цілісний феномен, що вимагає окремого наукового аналізу.

Перші більш-менш грунтовні дослідження концепції гібридних конфліктів з'явилися у відповідь на події, які продемонстрували на практиці ефективність поєднання різних засобів ведення війни. Зокрема, конфлікт у Грузії у 2008 році можливо став одним із перших

яскравих прикладів гібридної війни у сучасному розумінні цього терміну. У ньому військові дії були інтегровані з активними інформаційними кампаніями, дипломатичним тиском та кібероперацією. Подальший розвиток цієї концепції активно відбувався на тлі подій в Україні у 2014 році, коли гібридні засоби стали основою стратегії агресії росії проти суверенної держави.

Цифрова епоха суттєво трансформувала природу гібридних конфліктів, шляхом значного розширення спектру доступних інструментів і підвищення їх ефективності. Всесвітня цифровізація надала змогу швидко та масштабно впливати на суспільну свідомість, політичні процеси та економічну стабільність, навіть не вдаючись до прямого військового втручання. Основними факторами, що зумовили ці зміни, без сумніву, є розвиток інформаційних технологій, зростання ролі соціальних мереж, значення кіберпростору та активне впровадження технологій штучного інтелекту у всі сфери людського життя.

Стрімкий розвиток інформаційних технологій дозволив реалізувати стратегії асиметричного впливу, коли менш потужні держави або недержавні учасники отримали можливість досягати стратегічних переваг, використовуючи новітні цифрові інструменти. Це створило умови для зміщення акценту від класичних військових операцій до інформаційних і кібернетичних, в тому числі за участі ШІ.

В той же час соціальні мережі стали важливим, або, навіть, ключовим полем для ведення гібридних конфліктів. Завдяки їхній інтерактивності, миттєвості поширення інформації та широкому охопленню аудиторії, вони перетворилися на потужний інструмент для дезінформації, пропаганди та маніпуляції суспільною думкою. Використання алгоритмів соціальних платформ для таргетованого впливу, а також організація інформаційних кампаній через ботоферми створили нові можливості для здійснення інформаційного тиску.

В свою чергу кіберпростір став одним із найважливіших елементів гібридних конфліктів. Кібератаки частішають систематично і дозволяють завдавати значної шкоди економічним системам, критичній інфраструктурі та інформаційним ресурсам будь-якої держави. Завдяки використанню технологій штучного інтелекту та великих даних агресори отримують можливість не лише поширювати інформацію, а й прогнозувати реакції суспільства, адаптувати свої стратегії та підвищувати ефективність своїх дій.

Сучасні науковці останнім часом приділяють значну увагу дослідженню загальних характеристик та особливостей гібридних конфліктів. Так, наприклад Харитонов Є. О. та Харитонова О. І. в своїй роботі, що присвячується дослідженню людського виміру в гібридній війні, визначають гібридну війну як зіткнення багатовекторних інтересів – політичних, правових, психологічних і гуманітарних – у межах сучасного конфлікту. Особливу увагу науковці приділяють людському виміру війни, тобто тій сфері, де інформаційні, правові та ментальні впливи перетинаються і формують правосвідомість, поведінку, реакцію на агресію, відчуття справедливості й правової захищеності. У тезах наголошено, що гібридна війна – це не лише збройна агресія, а й «вплив на людську свідомість, цінності та правові орієнтири через інструменти масової комунікації, маніпуляції, дезінформації». У цьому контексті інформаційне середовище функціонує як стратегічний інструмент формування сприйняття конфлікту і правової легітимності держави. «Гібридна війна – це не лише протистояння збройних підрозділів, а й конфлікт на рівні ментальності, права, моралі, історичної пам'яті та інституційної довіри. У центрі цього конфлікту – людина, її вибір, її ставлення до подій, її здатність протистояти маніпуляції».[1]

У публікації аналізується світоглядна вразливість особистості в умовах гібридної агресії, підкреслюється, що правові механізми не можуть бути ефективними, якщо не враховують фактори інформаційного впливу, особливо в межах окупованих територій або за умови систематичного інформаційного тиску на свідомість.

«Інформаційна атака, як складова гібридної війни, формує не лише уявлення про реальність, а й підміняє правові критерії її оцінки».

Цей підхід розширює межі традиційного розуміння гібридної війни, вводячи у фокус дослідження взаємозв'язок між правовою системою та інформаційною екосистемою, в якій функціонує людина як адресат і суб'єкт впливу.

Узденова Ю. М. в своєму дослідженні "Гібридна війна: сутність, складові та ключові поняття" доходить висновку, що гібридна вій-

[1] Харитонов Є. О., Харитонова О. І. Гібридна війна як зіткнення інтересів: людський вимір. *Одеські грудневі цивілістичні читання: приватне право як концепт в умовах війни*: матеріали наук. конф. (м. Одеса, 12 груд. 2024 р.). Одеса: Фенікс, 2025. С. 13.

на – це нова форма ведення війни, війна четвертого покоління, потужний монстр, діяльність якого спрямована на досягнення політичних цілей.[1] Тут же вона зазначає: “Неабияка участь під час ведення гібридної війни приділяється інформаційній сфері, адже саме вона має неабиякий вплив на формування стабільності, довіри до влади та формування та збереження і підтримку ідеології країни.” Однак при цьому залишає дослідження інформаційної складової завданням для своїх подальших досліджень.

Кундеус О. М. пропонує чітку дефініцію гібридної війни як поєднання прямих (збройних) та непрямих (кібернетичних, інформаційних, диверсійних тощо) операцій, спрямованих на підрив суверенітету України. Політична агресія реалізується не класичним військовим шляхом, а через «комплекс інструментів» гібридного впливу, що включає: приховані операції, диверсії, підтримку незаконних збройних формувань, інформаційну та кібернетичну стратегію. Автор відзначає, що основна загроза полягає у втраті або субстанційному обмеженні суверенітету України. «Інформаційний фронт “гібридної війни” розгортається… серед населення в зоні конфлікту… проти внутрішньої держави… серед громадян країни агресора та міжнародного співтовариства» – зазначає автор.[2]

В низці інших наукових досліджень також виділяються різні характерні ознаки гібридних війн і конфліктів, більшість з яких перекликаються та є співзвучними. Однак при цьому майже відсутні дослідження гібридних конфліктів з акцентом на цифрові реалії людського суспільства. Хоча саме цифрові технології сьогодення, на нашу думку, і надають особливої специфіки сучасним гібридним війнам.

Гібридні конфлікти в цифрову епоху сучасності характеризуються низкою специфічних рис, які відрізняють їх від традиційних форм протистояння. Перш за все, вони мають глобальний характер, адже цифрові інструменти дозволяють вести операції у глобальному (планетарному) масштабі, впливаючи на різні регіони світу одночасно.

---

[1] Узденова Ю. М. Гібридна війна: сутність, складові та ключові поняття. *Вчені записки ТНУ імені В. І. Вернадського.* Серія: Публічне управління та адміністрування. 2024. № 4. С. 178. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2024/4_2024/28.pdf?utm_source=chatgpt.com

[2] Кундеус О. М. Теоретичні аспекти гібридної війни РФ проти України. *Регіональні студії.* 2020. № 20. С. 120–124.

Крім того, такі конфлікти характеризуються високим рівнем інтеграції між різними засобами впливу, включаючи військові, політичні, інформаційні, економічні, та кібернетичні. При цьому не залишається осторонь і емоційна складова кожної людини та людства в цілому. Також варто зазначити, що внаслідок використання цифрових технологій сучасні гібридні конфлікти відрізняються також асиметричністю – потенційно менш потужні у військовому аспекті учасники конфлікту можуть досягати стратегічних цілей, використовуючи сучасні технології та інструменти.

Ще однією важливою особливістю гібридних конфліктів сучасності є, на нашу думку, розмитість меж між державними та недержавними суб'єктами таких протистоянь. У гібридних конфліктах сьогодні активно використовуються недержавні структури, такі як приватні компанії, хакерські угруповання, громадські організації, окремі фахівці, які діють у взаємозв'язку з офіційними державними структурами.

Нарешті, такі конфлікти часто мають прихований характер, коли операції проводяться так, щоб уникнути прямої відповідальності агресора за завдану людству шкоду.

Еволюція концепту гібридних конфліктів у цифрову епоху свідчить про те, що ці конфлікти стали більш складними, багатокомпонентними та ефективними. Інтеграція цифрових технологій, розвиток кіберпростору та значення інформаційного середовища зумовили появу нових форм протистояння, які значно розширили арсенал інструментів впливу обох сторін конфлікту на людські маси. У таких умовах для ефективної протидії гібридним загрозам необхідне використання міждисциплінарного підходу, розвиток інноваційних технологій і вдосконалення міжнародного співробітництва у сфері забезпечення інформаційної безпеки.

Описані вище складність і багатовимірність гібридних конфліктів у цифрову епоху підкреслюють зростаюче значення інформаційного середовища як ключового ресурсу сучасного протистояння. Його інтеграція в стратегії ведення конфліктів обумовлює не лише необхідність використання новітніх технологій, але й вимагає глибокого розуміння структури, функцій і впливу інформаційних потоків на глобальному та національному рівнях. Як наслідок, інформаційне середовище стає центральним елементом як у забезпеченні безпеки,

так і в реалізації агресивних стратегій, що відкриває нові горизонти для його дослідження.

Розглянемо основні етапи формування інформаційного середовища в Україні. Зрозуміло, що розвиток концепту інформаційного середовища в Україні відбувався у взаємозв'язку з трансформаціями політичної системи, безпековими викликами та правовим оформленням державної інформаційної політики. Формування теоретичних і практичних засад цього концепту супроводжувалося поступовим становленням відповідного законодавства, зростанням усвідомлення стратегічної ваги інформації як ресурсу впливу, а також еволюцією доктрини національної безпеки в умовах зростання всебічних загроз.

На початковому етапі самостійності і суверенності України (у 1990-х роках) інформаційне середовище не розглядалося як цілісний об'єкт правового регулювання чи як елемент системи національної безпеки. Першочергову увагу законодавець в ті часи приділяв проблемам свободи слова, доступу до інформації, діяльності засобів масової інформації, тощо. Так, Закони України «Про інформацію» (1992 р.), «Про друковані засоби масової інформації (пресу) в Україні» (1992 р.), «Про телебачення і радіомовлення» (1993 р.) та інші стали основою для поступового формування інформаційного простору як системи обміну повідомленнями у межах конституційно-правової моделі демократичного суспільства. Водночас, у ці ж роки в юридичній науці зароджувалося усвідомлення того, що інформація – це не лише об'єкт цивільного обігу чи засіб масової комунікації, а й потенційно вразливий стратегічний ресурс.[1] Саме на цьому ґрунті у 2000-х роках починає формуватись уявлення про інформаційне середовище як цілісну, багатофункціональну систему, яка включає в себе не лише ЗМІ, а й канали електронного зв'язку, мережеву інфраструктуру, суб'єктів генерування і споживання інформації, алгоритмічні механізми її поширення, а також правові механізми її контролю та захисту. Цей підхід було частково зафіксовано в редакції Закону України «Про інформацію» 2011 року, в якому було вперше чітко визначено поняття інформаційних ресурсів, інформаційної інфраструктури, носіїв інформації та прав на неї.

[1] Пожуєв В. І. Інформатизація як ресурс розвитку сучасного українського суспільства. *Гуманітарний вісник ЗДІА*. 2009. Вип. 38. С. 4-12; Марущак А. І. Інформаційні ресурси держави: зміст та проблема захисту. *Правова інформатика.* 2009. № 1(21).С. 65-71. URL: https://ippi.org.ua/sites/default/files/09maizpz_0.pdf та інші.

Важливим етапом у розвитку концепту інформаційного середовища стало прийняття у 2016 році Доктрини інформаційної безпеки України (Указ Президента № 47/2017)[1], яка вперше на рівні стратегічного правового документа закріпила ідею про інформаційне середовище як фактор, що прямо впливає на національну безпеку, громадську стабільність, суверенітет держави та інтеграцію в євроатлантичний простір. Доктрина констатувала, що одним із ключових викликів для України є інформаційна агресія з боку іноземних держав, насамперед Російської Федерації, яка активно використовує пропаганду, дезінформацію, інформаційно-психологічні операції та інші інструменти для дестабілізації суспільства та делегітимації влади.

У зв'язку з анексією Криму (2014 р.) та початком збройного конфлікту на Донбасі, інформаційне середовище починає розглядатися не лише як сфера комунікацій, а і як поле ведення війни – «інформаційний фронт». Це призвело до активного розвитку теоретичних уявлень про інформаційно-психологічні операції, інформаційний суверенітет, інформаційну гігієну.[2] На законодавчому рівні з'являються положення, що прямо спрямовані на обмеження шкідливого впливу інформації, зокрема щодо блокування іноземних пропагандистських ресурсів (рішення РНБО, введені в дію указами Президента), законодавчі ініціативи щодо боротьби з дезінформацією, посилення відповідальності за поширення неправдивої інформації в умовах воєнного стану.

У 2020-х роках під впливом загальносвітових трендів цифровізації та технологій штучного інтелекту, а також в умовах повномасштабного вторгнення РФ в Україну (з 24 лютого 2022 року), концепт інформаційного середовища набуває ще більшої стратегічної значущості. Тепер його розуміють як складний соціотехнічний конструкт, в якому поєднуються технологічна інфраструктура, контент, алгоритми його розповсюдження (включно з бот-мережами та автоматизованими системами), інституційна спроможність до реагування, рівень цифрової грамотності населення, тощо. У практичній площині це виражається

[1] Про доктрину інформаційної безпеки України. Указ Президента України № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/514/2009#Text

[2] Довгань О. Д. Національний інформаційний суверенітет – об'єкт інформаційної безпеки. *Інформація і право.* 2014. № 3 (12); Дубов Д. В. Проблеми нормативно-правового забезпечення інформаційного суверенітету в Україні. *Вісник Національної Академії керівних кадрів культури і мистецтв.* 2014. № 1. С. 233-238. та інші.

в тому, що інформаційні кампанії стають невід'ємною частиною воєнної стратегії: від застосування платформ Telegram, TikTok і Twitter для оперативного інформування та мобілізації, до протидії російському інформаційному впливу через СБУ, Центр протидії дезінформації при РНБО, а також на рівні громадянського суспільства.

Водночас, триває процес кодифікації інформаційного законодавства України відповідно до стандартів ЄС. Так, у 2022-2023 роках ухвалено нову редакцію Закону України «Про медіа»[1], який адаптує українське законодавство до Директиви Європейського Союзу про аудіовізуальні медіапослуги. Закон також закладає основи для саморегуляції ринку медіа, захисту прав споживачів інформації, прозорості власності та розподілу відповідальності за дезінформацію. Таким чином, українська правова система поступово переходить від фрагментарного до системного правового регулювання інформаційного середовища.

Підсумовуючи, можна констатувати, що концепт інформаційного середовища в українському праві сформувався як відповідь на нові форми загроз – від політичної дестабілізації до кібервтручань і маніпуляцій суспільною свідомістю. На сучасному етапі українське правове поле перебуває у процесі активної трансформації, в якому інформаційне середовище визнається не лише об'єктом захисту, але й активним елементом національної стратегії протидії гібридним впливам. Інформаційне середовище в сучасних умовах стало одним із ключових елементів національної та міжнародної безпеки. Його значення виходить далеко за межі традиційного людського уявлення про медіа та комунікації, охоплюючи цифрові платформи, соціальні мережі, кіберпростір і технології штучного інтелекту. В епоху глобальної цифровізації інформаційне середовище набуло статусу стратегічного ресурсу, здатного не лише впливати на соціально-економічний і політичний розвиток держав, але й визначати основні напрямки та методику перебігу збройних конфліктів, переділу світу. На сьогодні можна із впевненістю заявити, що у сучасних конфліктах інформаційне середовище відіграє вирішальну роль, адже воно слугує платформою для формування суспільної думки, дестабілізації державних інституцій та координації військових і невійськових дій. Інформаційні кампанії, засновані на пропаганді та маніпуляції, здатні змінювати

[1] Про медіа: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text

громадське сприйняття конфліктів, впливати на настрої населення та політичні рішення. Інформаційні атаки підривають довіру до органів влади, створюють соціальний хаос та провокують громадянські протистояння. У конфліктах сучасності інформаційні платформи використовуються для комунікації між учасниками бойових дій, передачі даних та організації інформаційних операцій. Як зазначалось вище, особливістю сучасних гібридних конфліктів є активне використання інформаційного середовища для досягнення стратегічних цілей. До основних викликів інформаційному середовищу в таких умовах належать: дезінформація та пропаганда, які включають поширення фейкових новин, маніпулятивних повідомлень та спотворення реальних фактів; кіберзагрози, що полягають у кібератаках на державні установи, інфраструктуру та медіа; маніпуляції через соціальні мережі, які дозволяють таргетовано впливати на різні групи населення, поширюючи контент, що сприяє загостренню конфліктів; а також руйнування інформаційної довіри, яке інтенсивно використовується для зниження довіри населення до офіційних джерел і породження інформаційного хаосу в суспільстві і державі.

Інформаційне середовище сьогодні є складною та багатокомпонентною системою, яка включає технологічні, соціальні, політичні, економічні та культурні аспекти. Його дослідження вимагає комплексного підходу, який враховує різноманіття чинників, що впливають на його функціонування та трансформацію. У цьому контексті міждисциплінарний підхід дослідження набуває особливого значення, адже він дозволяє інтегрувати знання з різних галузей науки для глибокого аналізу інформаційного середовища, його ролі в сучасних суспільних процесах та викликів, які воно створює. Міждисциплінарний підхід передбачає об'єднання методологій, концептів і практичних інструментів різних наукових дисциплін для дослідження складних проблем, які виходять за межі окремої наукової галузі. У випадку інформаційного середовища такий підхід є особливо важливим, адже це явище охоплює різні сфери: від технічних аспектів функціонування цифрових платформ до соціокультурного впливу інформаційних потоків на суспільство. Аналіз інформаційного середовища на основі міждисциплінарного підходу дозволяє створювати цілісну картину його розвитку, виявляти основні тенденції та прогнозувати потенційні наслідки змін. Для аналізу інформаційного середовища в сучас-

ному суспільстві використовуються різні ключові дисципліни. Так, наприклад, інформатика та технології забезпечують технічну основу для аналізу інформаційного середовища. Інформатика надає інструменти для вивчення великих даних, алгоритмів штучного інтелекту, функціонування цифрових платформ, соціальних мереж і кібербезпеки. Завдяки використанню сучасних технологій, таких як машинне навчання та блокчейн, можливе ефективне виявлення дезінформації, прогнозування поведінки користувачів і забезпечення захисту даних.

Соціологія та психологія допомагають зрозуміти, як інформаційне середовище впливає на суспільну свідомість і поведінку індивідів. Соціологічний аналіз дозволяє виявляти динаміку формування громадської думки, механізми соціальної поляризації та роль інформації у створенні соціальних груп і спільнот. Психологія досліджує когнітивні механізми сприйняття інформації, впливу пропаганди та маніпулятивних повідомлень на особистість.

Політологія та міжнародні відносини також є підґрунтям для досліджень. Політологія аналізує інформаційне середовище як інструмент політичного впливу, розглядаючи його роль у виборчих кампаніях, політичних кризах та гібридних конфліктах. Міжнародні відносини зосереджуються на транснаціональному вимірі інформаційної політики, зокрема, у контексті інформаційних воєн, дипломатії та формування міжнародного порядку.

Право і правова наука України відіграють фундаментальну роль у формуванні, функціонуванні та захисті інформаційного середовища як складової національного простору в умовах демократичного устрою, глобалізації та гібридної агресії. У межах сучасної правової доктрини інформаційне середовище дедалі частіше трактується не лише як інфраструктурно-комунікаційна система, а як складний соціально-правовий феномен, що охоплює сукупність відносин, пов'язаних із створенням, збиранням, передачею, обробкою, зберіганням, використанням і захистом інформації у цифрову епоху. Саме правовий вимір визначає межі допустимого, моделі поведінки суб'єктів, баланс між приватною автономією і публічними інтересами, а також механізми реагування на інформаційні загрози.

У національному правопорядку України, що активно еволюціонує під впливом євроінтеграційного курсу та потреб протидії зовнішнім загрозам, право виконує як регулятивну, так і стратегічну функції у

сфері інформаційної політики. Починаючи з основоположних актів, як-от Закони України «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», «Про медіа», правова система забезпечує нормативно-правове поле для реалізації інформаційних прав і свобод громадян, прозорості діяльності органів влади, відповідальності журналістики та платформ цифрової комунікації. Водночас, у період збройного конфлікту та гібридної агресії з боку Російської Федерації, пріоритетним стає захист національного інформаційного простору від зовнішнього втручання, кіберзагроз, деструктивних наративів та дезінформаційних кампаній.

Зміна безпекової парадигми після 2014 року, а особливо з початком повномасштабної війни у 2022 році, спричинила необхідність радикального переосмислення ролі права у сфері інформаційної безпеки. Правові механізми почали застосовуватись не лише з метою регулювання обігу інформації, а й як інструмент протидії гібридним впливам. Зокрема, запровадження індивідуальних та секторальних санкцій, блокування ворожих інформаційних ресурсів, криміналізація колабораціонізму у сфері мас-медіа та введення додаткових обмежень під час воєнного стану свідчать про перехід до концепції «активного права», зорієнтованого на захист суверенітету у сфері інформації. Законодавчі ініціативи щодо боротьби з дезінформацією, медіаграмотності, цифрової етики та кібергігієни підсилюють цю трансформацію. У свою чергу, правова наука в Україні виконує важливу функцію методологічного осмислення нових форм правовідносин у межах інформаційного середовища. Сучасні наукові дослідження концентруються на розробці дефініційного апарату, зокрема категорій «інформаційна безпека», «інформаційний суверенітет», «дезінформація», «інформаційний тероризм», «гібридна інформаційна агресія» тощо. Увага приділяється також аналізу національного законодавства в порівняльно-правовій перспективі, зокрема в контексті імплементації актів Європейського Союзу – таких як Директива про аудіовізуальні медіапослуги, Резолюція Європарламенту про боротьбу з дезінформацією, рекомендації Ради Європи щодо свободи вираження у цифрову епоху. Наукові розвідки правників також охоплюють проблематику юрисдикційного суверенітету в кіберпросторі, законодавчого регулювання функціонування соціальних мереж, алгоритмічного моделювання контенту та право-

вого статусу автоматизованих агентів комунікації (наприклад, ботів або систем штучного інтелекту).

У межах міждисциплінарного підходу, що поєднує цивільне, інформаційне, адміністративне, міжнародне публічне та кримінальне право, розробляються концепції змішаного регулювання інформаційного середовища. Правова наука в цьому аспекті не лише фіксує правові прогалини чи суперечності в чинному законодавстві, а й формує нові вектори його розвитку – від інституціоналізації незалежних регуляторів у сфері цифрових комунікацій до запровадження моделей спільного управління даними та етичних стандартів цифрової поведінки.

Відтак, право в Україні не лише забезпечує нормативну основу для функціонування інформаційного середовища, а й виконує роль активного чинника стратегічного реагування, що здатен протидіяти загрозам, трансформувати інститути публічного управління, сприяти демократичному розвитку, а також формувати національну ідентичність і стійкість у межах глобального цифрового простору. Правова наука, в цьому контексті, постає не лише як аналітична система, а як фактор формування правового дискурсу майбутнього, здатного адаптуватися до постійної зміни форм, каналів та технологій комунікації.

Культурологічний підхід дозволяє дослідити вплив інформаційного середовища на культурні цінності, традиції та національну ідентичність. Комунікаційні науки зосереджуються на вивченні процесів передачі інформації, механізмів медіа-ефектів, особливостей роботи традиційних і цифрових медіа.

Міждисциплінарний підхід базується також на інтеграції кількісних та якісних методів дослідження. Кількісні методи, такі як аналіз великих даних, соціометрія та статистичне моделювання, дозволяють виявляти масштабні тенденції, визначати закономірності функціонування інформаційного середовища та прогнозувати його розвиток. Якісні методи, включаючи інтерв'ю, контент-аналіз, дискурс-аналіз і кейс-стаді, забезпечують глибоке розуміння конкретних явищ, їхнього контексту та значення для окремих груп.

Особливу роль у міждисциплінарному аналізі відіграє системний підхід, який дозволяє розглядати інформаційне середовище як цілісну систему, що взаємодіє з іншими сферами суспільного життя.

Використання системного підходу сприяє розумінню взаємозв'язків між окремими елементами інформаційного середовища, такими як технології, суспільні інститути та індивідуальні суб'єкти.

Міждисциплінарний підхід до аналізу інформаційного середовища має низку переваг. По-перше, він дозволяє подолати обмеження окремих дисциплін і отримати більш повне уявлення про складні явища. По-друге, інтеграція знань з різних галузей сприяє розробці комплексних рішень для вирішення актуальних проблем, таких як інформаційна безпека чи протидія дезінформації. По-третє, міждисциплінарний підхід стимулює розвиток інноваційних методів дослідження, які поєднують технічні, соціальні та гуманітарні аспекти.

Сьогоднішня актуальність аналізу інформаційного середовища особливо виражена в умовах гібридної агресії, яку переживає Україна. З 2014 року країна стала об'єктом масштабних інформаційних атак, спрямованих на підрив її територіальної цілісності, економічної стабільності та міжнародного авторитету. В інформаційному середовищі України реалізуються масштабні дезінформаційні кампанії через медіа та соціальні платформи, здійснюються кібератаки на державні інформаційні системи та об'єкти критичної інфраструктури, а також поширюються ідеї, спрямовані на розпалювання гендерних, міжетнічних та політичних конфліктів. У таких умовах для України важливим завданням є розробка ефективних механізмів захисту інформаційного середовища, враховуючи як міжнародний досвід, так і особливості національного контексту та всі можливості сучасного цифрового світу.

У глобальному масштабі інформаційне середовище впливає не лише на локальні конфлікти, а й на міжнародну безпеку. Приклади кібератак, поширення дезінформації та використання інформаційних кампаній у міждержавних протистояннях демонструють важливість розробки міжнародно-правових механізмів протидії цим викликам. Дослідження інформаційного середовища у контексті гібридних конфліктів дозволяє розкрити сутність та динаміку впливу інформаційних загроз, запропонувати ефективні механізми захисту, сприяти зміцненню інформаційної стійкості держави та підвищенню рівня міжнародної безпеки. Таким чином, аналіз інформаційного середовища як стратегічного ресурсу стає невід'єм-

ною складовою сучасних наукових досліджень, що забезпечує не лише теоретичну, але й практичну цінність у протидії сучасним викликам.

Інформаційне середовище є одним із основних (а можливо вже і єдиним основним) елементів, що формує не тільки повсякденне життя сучасного суспільства, але й взаємодію між державами, політичними структурами та іншими соціальними інститутами. В умовах глобалізації та інтенсивного розвитку цифрових технологій інформаційне середовище стає не просто складовою комунікаційного процесу, а й глобальним ресурсом, здатним впливати на всі соціально-політичні процеси, економічні трансформації та національну безпеку. У контексті сучасних конфліктів, зокрема гібридних, інформаційне середовище відіграє ключову роль, визначаючи напрямки і способи ведення боротьби на інформаційних фронтах. Настали часи коли поняття інформаційного середовища охоплює не лише засоби масової інформації, але й численні новітні технології, які утворюють складну мережу взаємозв'язків і процесів, що формують загальну картину сучасного світу.

На сучасному етапі розвитку людства інформаційне середовище можна визначити також як сукупність всіх інформаційних потоків, що циркулюють у суспільстві, а також інститутів, організацій і технологій, які беруть участь у виробництві, передачі, обробці та сприйнятті інформації. Це середовище складається з різноманітних елементів, які взаємодіють між собою, створюючи динамічну систему, що постійно змінюється під впливом зовнішніх і внутрішніх факторів. Інформаційне середовище охоплює не лише традиційні форми комунікації, такі як телевізійні канали, газети, радіо, а й в першу чергу новітні форми цифрових медіа, соціальні мережі, онлайн-платформи, а також технології, що використовуються для збору та обробки даних, такі як великі дані (big data), штучний інтелект (ШІ) та інші інноваційні рішення.

Таким чином, інформаційне середовище можна визнавати і інтегрованою мережею, яка складається з різних компонентів, що взаємодіють між собою через безліч каналів і платформ. Це середовище впливає на способи комунікації, формує суспільну думку та змінює політичні, соціальні і економічні реалії на глобальному та національному рівнях.

При всій глобальності концепту інформаційне середовище можна умовно розподілити на кілька основних складових, кожна з яких має свої функції та специфіку взаємодії.

Комунікаційні канали – це основні канали, через які передається інформація. До них відносяться традиційні засоби масової інформації, такі як телебачення, радіо, газети, а також нові медіа – соціальні мережі, блоги, веб-сайти, відеохостинги, месенджери, платформи для обміну контентом та інші інтернет-ресурси. З розвитком цифрових технологій роль останніх у формуванні інформаційного середовища постійно і швидко зростає, оскільки вони забезпечують миттєву комунікацію між різними учасниками глобального процесу.

Інформаційні продукти – це конкретний зміст, який передається через комунікаційні канали. Вони можуть бути різного формату: текстовими, аудіовізуальними, графічними, інтерактивними тощо. Ці продукти створюються для того, щоб впливати на аудиторії різного масштабу: від локальних до глобальних. Вони можуть включати новини, статті, доповіді, дослідження, рекламу, соціальні кампанії, меми, що поширюються через цифрові платформи, а також пропагандистські та маніпулятивні матеріали.

Зазвичай суб'єктами, що створюють інформацію є державні органи, медіа-компанії, громадські організації, політичні партії, міжнародні організації, а також інші групи та індивіди, які активно формують та поширюють інформаційний контент. Вони відіграють важливу роль у визначенні інформаційних стратегій, контролюванні інформаційних потоків і маніпулюванні суспільною думкою. Вони є основними суб'єктами, які виробляють, обробляють та впливають на інформаційні потоки в суспільстві.

Сучасні новітні технології обробки та зберігання інформації включають в себе інструменти для збору, аналізу, зберігання та передавання великих обсягів даних. Сюди входять технології обробки великих даних, системи управління базами даних, платформи для штучного інтелекту, автоматизація контенту, аналіз соціальних мереж і навіть інструменти для боротьби з кіберзагрозами.

Слід звернути увагу на той факт, що у контексті гібридних конфліктів інформаційне середовище виконує не лише інструментальну, а й структуроутворюючу роль. Його функції виходять за межі простої трансляції повідомлень: вони впливають на стратегічне плану-

вання, юридичну легітимацію, моральний стан населення, політичну стабільність, а також на міжнародну реакцію. Проаналізувавши життя України і українців в умовах воєнного конфлікту з нападником, пропонуємо виділити наступні функції (місії) які виконує інформація щодня.

Когнітивно-психологічна функція – вплив на свідомість, емоції, поведінкові установки і реакції населення або військових підрозділів. Прикладом може бути масове поширення фейків про «здачу міст», «зраду командування», «втрати» з метою деморалізації цивільного населення і військових (РФ активно застосовувала це під час наступу на південь України у 2022 р.). Як свідчить практика, ця функція найбільш активно реалізується через Telegram, TikTok, Facebook і пов'язана з «вірусним» ефектом поширення.

Мобілізаційна функція – здатність інформаційного середовища консолідувати населення навколо певних цілей, цінностей або рішень. Без сумніву прикладом цієї функції є інформаційні кампанії на підтримку ЗСУ (#паляниця, #Байрактар, #єПідтримка, волонтерський рух) у 2022–2023 рр. Ця функція працює через емоційну ідентифікацію, формується наративами «ми» проти «ворога», виховує та актуалізує патріотизм, жертовність, соціальну згуртованість.

Дестабілізаційна функція (протилежність мобілізаційній) – використання інформації для послаблення довіри до влади, інституцій, економіки, судової системи, тощо. Яскравим прикладо є випадки поширення дезінформації про «втечу урядовців», «продаж територій», «інфляційний колапс», "єврейське заселення територій", тощо. Названа функція породжує стратегію дезорієнтації та деморалізації супротивника в мирний спосіб, підрив правової ідентичності.

Маніпуляційна функція – контроль над формулюванням понять, підміна причинно-наслідкових зв'язків, створення фальшивих альтернатив. На прикладі обставин життя сьогоднішніх українців вона проявляється у трактуванні окупації як «визволення», війни – як «спецоперації», геноциду – як «захист російськомовних», тощо. Як свідчить практика, маніпуляція здійснюється за рахунок підбору лексики, візуальних образів, музичного супроводу, «фактів» без джерел.

Юридично-легітимаційна функція – нформаційне середовище використовується для створення або імітації правової легітимності

(псевдореферендуми, «угоди», «звернення громадян»). Наприклад, інформаційний супровід фіктивних «референдумів» у Херсоні та на Донеччині у 2022 р. В ході реалізації цієї функції медіапростір створює ілюзію юридичної форми, що підкріплює політичні рішення агресора.

Міжнародно-репутаційна функція – це вплив на формування міжнародного образу держави – як жертви, як агресора або як союзника. Ця функція проявляється в діяльності Ukraine.ua, UNITED24, у вигляді звернення Президента до парламентів світу, у викритті злочинів (Буча, Ізюм) для міжнародного обурення. В цих випадках інформаційне середовище є полем дипломатичної конкуренції – чия правда буде сприйнята легітимною світовою спільнотою.

Інституційно-захисна функція – це інформаційна підтримка інституційного авторитету, правопорядку, судової системи, правоохоронних органів. Прикладами реалізації такої функції в Україні є сучасні кампанії проти корупції в обороні, інформування про судові рішення щодо воєнних злочинів, робота Центру стратегічних комунікацій, тощо. Таким чином інформація виконує роль посередника між державою і громадянином, формує довіру до легітимної влади.

Навігаційна (інформаційно-орієнтуюча) функція – це надання достовірної, оперативної, життєво важливої інформації – тривоги, евакуація, загрози. Прикладами реалізації цієї функції можуть бути застосунок «Повітряна тривога», телемарафон, офіційні Telegram-канали Міноборони, ДСНС, тощо. Для пересічних громадян, туристів, іноземців ця функція є ключовою в умовах воєнного стану. Саме вона допомагає населенню приймати правильні, швидкі та чіткі рішення в умовах небезпеки.

Розвідувально-аналітична функція проявляється у зборі відкритих даних для аналізу воєнної ситуації, позицій противника, громадських настроїв. Наприклад, OSINTгрупи (Bellingcat, InformNapalm), аналіз геолокацій з соцмереж, фото з TikTok/Telegram. Сьогодня вона використовується як державними структурами, так і волонтерами; дозволяє коригувати дії в реальному часі.

Рекрутингова та мобілізаційна функція агресора полягає у вербуванні через інформаційні кампанії, створення наративу участі у «святій справі», «боротьбі з фашизмом» тощо. Наприклад, використання TikTok у РФ для вербування молоді до ПВК «Вагнер», розміщення

роликів про «героїзм добровольців». Агресор щодо України активно використовує сучасні візуальні платформи для залучення «мобілізаційного ресурсу» через образи.

Інформаційне середовище в гібридних конфліктах виконує водночас інформаційні, правові, політичні, емоційно-психологічні та стратегічні функції. Його значення не обмежується медійною сферою – воно впливає на правовий статус територій, юридичну оцінку подій, міжнародну підтримку, здатність держави до самоорганізації. Саме тому в науковому дискурсі та правовому аналізі інформаційне середовище дедалі частіше розглядається як глобально-стратегічний ресурс, що визначає хід і наслідки гібридного конфлікту.

Окремо варто зробити акцент на тому, що інформаційне середовище цифрового світу є важливим інструментом збереження та передачі культурних цінностей. З допомогою сучасних інформаційних технологій здійснюється демонстрація та поширення культурних, наукових та освітніх матеріалів, що є основою для розвитку національних культур і взаємодії між культурами різних країн та різних людських формувань. І саме в цих напрямках проявляється культурологічна функція інформаційного середовища.

У сучасному цифровому середовищі користувачі не лише споживають інформацію, але й активно її створюють і поширюють. Це веде до зміни традиційної моделі «один до багатьох», замінюючи її на «багато до багатьох». І саме цей підхід відображає інтерактивність сучасного інформаційного середовища. Як зазначалось раніше, інформаційне середовище в сучасному світі вже давно не обмежується національними кордонами. Взаємодія між країнами та культурами через цифрові платформи стає безперешкодною, що збільшує можливості для транснаціональних інформаційних кампаній і глобальних інформаційних війн та свідчить про міжнародний, а більш правильно говорити сьогодні – планетарний, характер інформаційного середовища.

Окремо слід звернути увагу на зміну призначення інформаційних ресурсів в цифровому світі. Так, якщо раніше інформація в основному виконувала функцію повідомлення один одному про життєві обставини, то в сучасних умовах вона виконує скоріше функцію **боротьби за увагу і довіру людини** тим чи іншим конкретним інформаційним ресурсам.

Водночас із життєво важливими, позитивними та особливими моментами, інформаційне середовище несе в собі й значні ризики, про які останнім часом вголос сповіщають всі навколо. Такими ризиками є – кіберзагроза, зловживання даними, маніпуляція інформацією або навіть фальсифікація фактів, що призводить до серйозних наслідків для безпеки суспільства.

З огляду на значні ризики, які несе в собі інформаційне середовище, важливо зазначити, що ці загрози стають особливо критичними в умовах гібридних конфліктів. Саме в такому контексті інформаційне середовище перетворюється на поле битви, де використання інформаційних технологій, маніпуляція даними та цілеспрямований вплив на суспільну свідомість є інструментами інформаційної війни. Це підкреслює не лише потенціал інформаційного середовища, але й його вразливість, що робить інформаційне середовище полем інформаційної війни та ключовим елементом сучасних гібридних стратегій.

Інформаційна війна є невід'ємною складовою гібридних конфліктів, які в сучасних умовах набули глобального масштабу та багатовимірного характеру. Вона може визначатися як систематичний, цілеспрямований вплив на інформаційне середовище з метою досягнення політичних, економічних або військових цілей, часто навіть без застосування прямої військової сили. Її сутність полягає в маніпулюванні інформаційними потоками, створенні та поширенні певних наративів, дезінформації та пропагандистських матеріалів, які впливають на сприйняття реальності, поведінку та рішення суспільства. У рамках гібридних конфліктів інформаційна війна набуває особливого значення, адже її інструменти дозволяють ефективно досягати стратегічних цілей, мінімізуючи фізичні втрати, а також формувати умови для посилення інших компонентів конфлікту, таких як економічний тиск чи військові дії.

Як свідчить практика життя сучасної України, інформаційна війна виконує кілька ключових завдань у гібридних конфліктах. По-перше, вона спрямована на формування стратегічних наративів, які виправдовують дії сторони-агресора та дискредитують супротивника. Такі наративи створюються з урахуванням історичних, культурних чи ідеологічних контекстів, що дозволяє зробити їх максимально переконливими для певних аудиторій. По-друге, інформаційна війна

агресора спрямована на підрив довіри до сучасних державних інституцій. Це досягається шляхом поширення компрометуючих матеріалів, викривлення офіційної позиції уряду та створення ілюзії його неспроможності забезпечувати ефективне управління. По-третє, інформаційна війна використовується для деморалізації українців. Через масове поширення негативної інформації, візуалізацію жахів війни та маніпулятивні повідомлення створюється атмосфера безвиході та зневіри. Окрім цього, інформаційна війна сприяє загостренню внутрішніх конфліктів в українському суспільстві. Вона використовує наявні суперечності – політичні, етнічні, релігійні, психологічні – для посилення соціальної напруги, що ускладнює консолідацію суспільства перед зовнішніми викликами.

Методи та інструменти інформаційної війни надзвичайно різноманітні. Вона включає дезінформацію, пропаганду, кібератаки, маніпулювання засобами масової інформації та використання соціальних мереж з такою ж метою. Дезінформація як метод передбачає поширення неправдивих чи викривлених фактів, що вводять аудиторію в оману. Вона може бути спрямована як на дискредитацію супротивника, так і на створення помилкового позитивного іміджу агресора.

Пропаганда, в свою чергу, зосереджується на нав'язуванні ідеологічних установок, які виправдовують дії ініціатора конфлікту. В умовах сучасного цифрового світу соціальні мережі стали основним інструментом інформаційної війни. Завдяки їхній інтерактивності, широкому охопленню аудиторії та можливості таргетованого впливу соціальні платформи використовуються для розповсюдження фейкових новин, маніпулятивного контенту, організації інформаційних кампаній через ботів та тролів. Ще одним важливим методом інформаційної війни є кібератаки, які спрямовані на підрив інформаційної інфраструктури супротивника, викрадення конфіденційних даних, руйнування баз даних чи саботаж у критично важливих галузях, таких як енергетика чи транспорт. Сучасні технології, включаючи штучний інтелект, дозволяють автоматизувати процеси створення та поширення інформаційних продуктів, зокрема deepfake-відео чи фейкових новин, що ускладнює їх виявлення та нейтралізацію.

Наслідки будь-якої інформаційної війни є масштабними та довготривалими. По-перше, вона призводить до деградації або, як мінімум, суттєвої трансформації інформаційного середовища та людського

суспільства в цілому, створюючи атмосферу недовіри до будь-яких джерел інформації. Це **ускладнює формування об'єктивної картини реальності та сприяє розповсюдженню інформаційного хаосу.** По-друге, інформаційна війна спричиняє соціальну поляризацію, загострюючи внутрішні конфлікти у суспільстві. Це знижує рівень соціальної єдності та послаблює здатність держави до ефективної реакції на зовнішні загрози. По-третє, вона створює ризики для міжнародної стабільності, оскільки інформаційні кампанії можуть виходити за межі локального конфлікту та провокувати ескалацію напруженості на глобальному рівні.

В наявних обставинах російсько-українського воєнного конфлікту можна із впевненістю зробити висновок, що інформаційна війна в інформаційному середовищі є одним із найефективніших інструментів протистояння, який дозволяє сторонам досягати стратегічних цілей з мінімальними матеріальними витратами та фізичними втратами. Її багатофункціональність, інтеграція в цифрове середовище та використання сучасних технологій щодня роблять цей інструмент дедалі потужнішим та небезпечнішим. У контексті глобальних викликів, спричинених інформаційною війною, держави мають удосконалювати механізми її запобігання, розробляти новітні інструменти інформаційної безпеки та забезпечувати медіаграмотність населення. Лише комплексний підхід, що охоплює технічні, правові, освітні та організаційні заходи, може стати ефективною відповіддю на виклики, які створює війна в інформаційному середовищі.

Вразливість інформаційного середовища в умовах гібридних конфліктів обумовлена низкою причин, серед яких можна виділити як технічні, так і соціальні та правові аспекти. Так однією з головних проблем є юрисдикційні обмеження на конкретних територіях і в конкретних країнах. Інформаційне середовище є глобальним (загальнопланетарним) явищем, тоді як правове регулювання інформаційного середовища здебільшого обмежується національними рамками. Це ускладнює протидію транскордонним інформаційним атакам, зокрема тим, що здійснюються недержавними авторами, такими як хакерські групи або комерційні організації, які співпрацюють з державами-агресорами. У багатьох випадках відповідальні за деструктивні дії особи залишаються поза межами досяжності національної юрисдикції.

Міжнародне право відіграє важливу роль у регулюванні інформаційного середовища, особливо в умовах гібридних конфліктів. Зокрема, міжнародні конвенції, резолюції та договори встановлюють загальні принципи, які сприяють захисту інформаційного середовища. Наприклад, Європейська конвенція про права людини гарантує свободу вираження поглядів, але допускає її обмеження з метою захисту національної безпеки. Такі інструменти створюють рамкові умови для формування національних стратегій у сфері інформаційної безпеки.

Проте міжнародно-правове регулювання інформаційного середовища так само стикається з низкою проблем. Однією з них є відсутність чітких і універсальних норм, які б регламентували поведінку всіх, або хоча б більшості держав у кіберпросторі. Спроби розробити такі правила, зокрема в рамках ООН, часто наштовхуються на політичні суперечності між країнами. Водночас регіональні ініціативи, такі як діяльність Європейського Союзу у сфері боротьби з дезінформацією, є ефективнішими, але їхній вплив обмежується територіальними рамками.

На національному рівні відповідальність за інформаційні загрози може бути передбачена в адміністративній, кримінальній чи цивільно-правовій формах. Наприклад, законодавство України передбачає кримінальну відповідальність за кібератаки на державні інформаційні ресурси, що є важливим елементом забезпечення інформаційної безпеки. Однак проблема ефективності правозастосування таких законодавчих норм залишається актуальною, оскільки багато авторів діють не на території України, а у міжнародному просторі, знаходячись у постійному русі (IT-кочевники, хакери-мандрівники, тощо).

Без сумніву сьогодні інформаційне середовище відіграє ключову роль у забезпеченні національної стійкості України, особливо в умовах тривалої гібридної агресії, яка націлена на підрив її суверенітету, територіальної цілісності та політичної стабільності. У цій ситуації інформаційне середовище виконує подвійну функцію: з одного боку, воно є полем битви, на якому розгортаються інформаційні операції агресора, а з іншого – стратегічним ресурсом для мобілізації суспільства, захисту державних інтересів та забезпечення національної безпеки. Успіх України у протистоянні інформаційним загрозам значною мірою залежить від її здатності розвивати та адаптувати інформацій-

ну політику, законодавчу базу, залучати медіа та громадські ініціативи, а також формувати довгострокову стратегію побудови стійкого інформаційного простору.

Інформаційна політика України у період гібридної агресії зазнала значних трансформацій, спрямованих на зміцнення здатності держави протистояти інформаційним загрозам. Після початку агресії у 2014 році основним викликом стало реагування на масовані дезінформаційні кампанії, спрямовані на підрив довіри до державних інституцій, дестабілізацію громадської думки та міжнародну ізоляцію України. У відповідь були запроваджені заходи, спрямовані на моніторинг інформаційного середовища, боротьбу з фейковими новинами, блокування деструктивних медіаресурсів і підвищення прозорості діяльності державних органів. Уряд України ініціював створення системи стратегічних комунікацій, яка має забезпечити ефективну координацію інформаційної діяльності державних структур. Одночасно відбувалася активна співпраця з міжнародними партнерами для адаптації передового досвіду у сфері інформаційної безпеки.

Медіа та громадські ініціативи відіграють невід'ємну роль у зміцненні інформаційного середовища України. Незалежні засоби масової інформації стали важливим інструментом для протидії пропаганді та донесення правдивої інформації до української та міжнародної аудиторії. Вони забезпечують оперативне реагування на дезінформаційні атаки, підвищують обізнаність громадян про реальні події та сприяють формуванню критичного мислення. Громадські ініціативи, такі як фактчекінгові платформи, медіаосвітні проєкти та волонтерські рухи, значно посилюють здатність суспільства протидіяти інформаційним загрозам. Ці ініціативи сприяють поширенню культури інформаційної безпеки, формуванню стійкості до маніпулятивних наративів і залученню громадян до захисту національних інтересів в інформаційному просторі.

Перспективи розбудови національної інформаційної стійкості України тісно пов'язані з необхідністю подальшого розвитку стратегічних комунікацій, інноваційних технологій та партнерства між державою, бізнесом і громадянським суспільством. Україна має адаптувати свої стратегії до швидких змін у технологічному середовищі, зокрема використовувати штучний інтелект для моніторингу та аналізу інформаційних загроз, підвищувати рівень захищеності

цифрових платформ і розвивати національні медіа для популяризації української культури та ідентичності. Важливим є також впровадження комплексних програм медіаграмотності, які спрямовані на підвищення обізнаності громадян щодо інформаційних загроз та розвиток критичного мислення.

Таким чином, роль інформаційного середовища у забезпеченні стійкості України є визначальною у протистоянні гібридній агресії. Вона вимагає інтегрованого підходу, який включає ефективну інформаційну політику, вдосконалене законодавче регулювання, активну участь медіа та громадянського суспільства, а також впровадження довгострокових стратегій для формування захищеного та стійкого інформаційного простору. Тільки спільними зусиллями можна забезпечити належний рівень національної інформаційної безпеки та протидії сучасним викликам у цифрову епоху.

Інноваційні технології відіграють вирішальну роль у сучасних стратегіях протидії інформаційним загрозам, які є одним із ключових викликів цифрової епохи. Гібридні конфлікти та ескалація інформаційних атак вимагають застосування технологічно розвинених рішень, здатних ефективно моніторити інформаційне середовище, ідентифікувати джерела загроз, нейтралізувати їхній вплив та підвищувати стійкість суспільства до маніпулятивних наративів. Серед таких технологій особливу увагу заслуговують штучний інтелект, блокчейн, інструменти для підвищення медіаграмотності та кібербезпекові рішення. Їхнє застосування дозволяє значно підвищити ефективність стратегій захисту інформаційного простору та забезпечити комплексний підхід до вирішення проблем сучасних інформаційних загроз.

Штучний інтелект (ШІ) є одним із найпотужніших інструментів у протидії дезінформації та маніпуляціям. Його використання дозволяє автоматизувати процеси моніторингу інформаційних потоків, аналізувати великі масиви даних та ідентифікувати підозрілий або маніпулятивний контент. Завдяки алгоритмам машинного навчання ШІ здатен визначати фейкові новини, оцінювати їхній вплив на аудиторію та прогнозувати реакції суспільства. Наприклад, спеціалізовані алгоритми аналізують лінгвістичні особливості текстів, виявляють невідповідності або штучно створені елементи, а також ідентифікують мережі, задіяні у поширенні дезінформації. Водночас ШІ вико-

ристовується для розробки інформаційних платформ, які надають користувачам доступ до перевіреної інформації, забезпечуючи альтернативу маніпулятивним джерелам. Такі рішення не лише нейтралізують вплив дезінформації, але й сприяють формуванню довіри до офіційних джерел інформації.

Блокчейн та інші технології захисту даних відкривають нові можливості для забезпечення прозорості інформаційних потоків і гарантування автентичності джерел інформації. Використання блокчейну дозволяє створювати незмінні реєстри даних, які можуть використовуватися для підтвердження джерел походження контенту та ідентифікації тих, хто відповідальний за його створення. Це особливо актуально в умовах поширення фейкових новин та deepfake-матеріалів, які важко відрізнити від реальної інформації. Технології розподіленого реєстру також можуть бути використані для створення захищених платформ обміну інформацією, де неможливо змінити або видалити дані без відповідного підтвердження. Це підвищує довіру до інформаційних ресурсів і знижує ризик маніпуляцій.

Підвищення медіаграмотності населення є одним із найважливіших напрямів протидії інформаційним загрозам, і в цьому процесі інноваційні технології також відіграють ключову роль. Розробка інтерактивних платформ для навчання, мобільних додатків та симуляційних ігор дозволяє навчати громадян навичкам критичного мислення, розпізнавання фейкових новин та аналізу джерел інформації. Наприклад, освітні програми можуть використовувати віртуальну реальність або гейміфікацію, щоб моделювати ситуації, у яких користувачі стикаються з дезінформацією, та вчити їх правильно реагувати. Сучасні інноваційні технології також сприяють розвитку платформ для фактчекінгу, де користувачі можуть швидко перевіряти достовірність інформації за допомогою спеціалізованих інструментів і баз даних. Фактчекінг (англ. fact-checking) – це процес перевірки достовірності фактів, тверджень, повідомлень чи публікацій, що поширюються в медіа, соціальних мережах, публічному дискурсі або політичному житті. Його мета – встановлення істинності або хибності інформації на основі доступних об'єктивних джерел, офіційних документів, наукових даних або логічного аналізу. Фактчекінг сьогодні є одним з головних інструментів протидії дезінформації, маніпуляціям та фейковим новинам у публічному просторі.

Фактчекінг в сучасних обставинах є інструментом не лише журналістики або масової комунікації, але й важливим елементом забезпечення інформаційної безпеки держави. В умовах гібридної війни, інформаційної агресії та когнітивних операцій фактчекінг виконує функцію фільтрації та нейтралізації маніпулятивного впливу. У цьому сенсі, його варто розглядати як превентивний механізм у сфері захисту інформаційного суверенітету.

У правовому аспекті, фактчекінг не є чітко кодифікованою категорією в українському законодавстві, однак він тісно пов'язаний із такими поняттями, як: право громадян на достовірну інформацію (ст. 34 Конституції України); право на доступ до публічної інформації (Закон України «Про доступ до публічної інформації»); обов'язок ЗМІ надавати перевірену інформацію (Закон України «Про медіа»).

Основні етапи роботи фактчекінга можуть виглядати наступним чином.

1. Ідентифікація твердження, що перевіряється. Фактчекери відбирають суспільно важливі заяви, які викликають сумніви, є резонансними або потенційно маніпулятивними. Це можуть бути: політичні промови, пости в соціальних мережах, журналістські матеріали, відео/фото з сумнівним контекстом, тощо.

2. Контекстуалізація. Фактчекери визначають контекст заяви: коли, ким і з якою метою вона була зроблена, на який сегмент аудиторії спрямована, і які наслідки може мати її поширення.

3. Пошук джерел. Наступний етап – ретельна перевірка твердження через: офіційні бази даних (законодавство, судові реєстри, статистика); наукові джерела (академічні публікації, звіти, експертні дослідження); першоджерела (відео, протоколи, стенограми, прямі цитати); міжнародні бази даних (Eurostat, WHO, UN, NATO тощо).

4. Аналіз доказової бази. Фактчекером здійснюється критичний аналіз знайденої інформації, виявляються розбіжності, логічні невідповідності, відсутність доказів, маніпуляції емоційним тоном чи статистикою. Особливу увагу приділяють використанню вирваних з контексту фраз, модифікації зображень, використанню бот-мереж тощо.

5. Встановлення вердикту. Після завершення аналізу, автори фактчекінгу дають висновок про істинність/хибність заяви за шкалою: «Правда» / «Факт підтверджено»; «Маніпуляція»; «Неповна правда» / «Позбавлено контексту»; «Фейк» / «Брехня».

6. Публікація та поширення результату перевірки. Результати фактчекінгу оформлюються у вигляді доступного матеріалу (текст, інфографіка, відео) й публікуються на спеціалізованих платформах.

Результати фактчекінгу часто використовуються у журналістських розслідуваннях, які мають юридичні наслідки (викриття корупції, подання до суду, ініціювання перевірок), в судових процесах як докази маніпулятивності або недостовірності тверджень, як підстави для звернення до регуляторів (Національна рада з питань телебачення і радіомовлення, Кіберполіція, Центр стратегічних комунікацій при РНБО). Таким чином, фактчекінг сприяє реалізації механізмів юридичної відповідальності – зокрема, за поширення фейкових новин, наклеп, порушення етичних стандартів медіа, сприяння інформаційній агресії.

У межах сучасної правової науки в Україні та Європейському Союзі зростає тенденція до визнання фактчекінгу частиною правових стратегій протидії дезінформації, інтеграції інструментів перевірки фактів до систем саморегулювання медіа (media co-regulation), розробки етичних кодексів, які зобов'язують журналістів і публічних осіб перевіряти інформацію перед публікацією, підтримки незалежних фактчекінгових інституцій як елементів публічного контролю за правдою. У деяких юрисдикціях (наприклад, у Франції, Німеччині) результати фактчекінгу навіть впливають на алгоритмічні рішення цифрових платформ, зокрема – на модерацію контенту, маркування повідомлень, тимчасове блокування акаунтів.

Фактчекінг у структурі демократичної правової держави корелює з такими базовими принципами, як: доступ до правдивої інформації як умова реалізації основоположних прав і свобод; публічна відповідальність політиків і інституцій; розвиток критичного мислення як частини правової культури громадян. Відтак, функціонування незалежних фактчекінгових організацій є індикатором зрілості інформаційної демократії та складовою правової інфраструктури відкритого суспільства.

Таким чином, хоча фактчекінг на сучасному етапі і не кодифіковано як окремий правовий механізм, він фактично виконує функції, тотожні превентивним, контрольним і регулятивним інструментам права. У межах сучасної правової доктрини, фактчекінг доцільно трактувати як структурний компонент механізму інформаційної без-

пеки, що працює на перетині права, етики та публічного управління. Думається, що його подальша інституціоналізація, нормативне закріплення та інтеграція в національну систему правового захисту інформаційного простору мають стати одним з актуальних завдань сучасної правової науки.

Приклади інституцій, які сьогодні здійснюють фактчекінг в Україні StopFake.org[1] – один із перших проєктів в Україні, який з 2014 року фокусується на викритті російської дезінформації; Verify (Радіо Свобода) – мультимедійна платформа перевірки фактів, зокрема візуального контенту; Львівський медіафорум[2] -здійснює моніторинг регіональної преси на предмет фейків; Центр стратегічних комунікацій та інформаційної безпеки при МКІП[3] – виконує функції державного реагування на дезінформацію.

Фактчекінг сьогодні є не просто технологією перевірки повідомлень, а одним із механізмів інформаційної гігієни суспільства, важливою складовою цифрової освіти та компонентом правової культури. Він сприяє підвищенню медійної грамотності населення, зменшенню впливу інформаційних атак і маніпуляцій, підвищенню довіри до медіа, посиленню інституційної стійкості держави в умовах гібридної війни. Таким чином, фактчекінг в сучасних умовах це не лише інструмент журналістського контролю, а й соціально-правовий механізм демократичного захисту істини в інформаційному середовищі.

Кібербезпекові технології є невід'ємною складовою стратегій захисту інформаційного середовища. Інструменти кібербезпеки забезпечують захист критичної інформаційної інфраструктури, попередження кібератак і зниження ризиків витоку даних. Сучасні рішення включають системи виявлення та запобігання вторгненням, криптографічні технології, а також платформи моніторингу та аналізу кіберзагроз у реальному часі. Інтеграція таких рішень у державну та приватну інформаційну інфраструктуру дозволяє не лише захищати інформаційне середовище від атак, але й швидко реагувати на інциденти, мінімізуючи їхні наслідки. Особливо важливою є розробка технологій прогнозування загроз, які базуються на аналізі даних та використанні алгоритмів штучного інтелекту.

---

[1] Про діяльність організації дивись за посиланням https://www.stopfake.org/ru/o-nas/

[2] Про діяльність організації дивись за посиланням https://lvivmediaforum.com/

[3] Про діяльність організації дивись за посиланням https://spravdi.gov.ua/

Отже, інноваційні технології відкривають нові можливості для протидії інформаційним загрозам у сучасному світі. Вони дозволяють ефективно моніторити та аналізувати інформаційні потоки, забезпечувати захист даних, підвищувати рівень медіаграмотності населення та зміцнювати кібербезпекову інфраструктуру. Усе це сприяє формуванню стійкого інформаційного середовища, здатного протистояти сучасним викликам та забезпечувати національну і міжнародну інформаційну безпеку. Успішна інтеграція цих технологій потребує активної співпраці між державою, бізнесом і громадянським суспільством, що стане запорукою стійкості до інформаційних загроз у майбутньому.

У сучасному світі, коли гібридні конфлікти стали однією з головних загроз міжнародній безпеці, захист інформаційного середовища набув глобального значення. Країни та міжнародні організації розробляють стратегії, спрямовані на підвищення стійкості інформаційного простору, протидію дезінформації, забезпечення кібербезпеки та створення механізмів міжнародної співпраці. Досвід країн НАТО, Європейського Союзу та інших міжнародних організацій є цінним прикладом для адаптації в умовах гібридної агресії проти України. Цей підрозділ присвячений аналізу міжнародної практики у сфері інформаційної безпеки, ефективності міждержавної співпраці та можливостям використання цього досвіду для зміцнення інформаційного середовища України.

Практика країн НАТО у забезпеченні стійкості інформаційного простору базується на комплексному підході, який поєднує політичні, військові, технічні та інформаційні заходи. Одним із ключових елементів стратегії НАТО є розробка концепції стратегічних комунікацій (StratCom), яка спрямована на координацію інформаційної діяльності членів Альянсу для захисту їхніх національних інтересів і протидії ворожим інформаційним кампаніям. Створення Центру стратегічних комунікацій НАТО у Ризі стало важливим кроком у розвитку інституційної спроможності Альянсу у сфері інформаційної безпеки. Цей центр займається дослідженням методів дезінформації, розробкою інструментів для її виявлення та аналізу, а також навчанням експертів, які працюють у цій сфері. Важливим аспектом діяльності НАТО є акцент на підвищенні кібербезпеки, адже кіберпростір розглядається як окремий домен операцій, нарівні з сушею, морем, повітрям і

космосом. Альянс активно впроваджує технології для моніторингу кіберзагроз, розробляє стандарти для захисту критичної інфраструктури та організовує спільні навчання для підвищення готовності до кіберінцидентів.

Європейський підхід до протидії інформаційним загрозам базується на принципах демократії, прав людини та верховенства права. Європейський Союз активно працює над розробкою законодавчих ініціатив та інструментів для боротьби з дезінформацією і маніпуляціями в інформаційному середовищі. Однією з ключових ініціатив ЄС є створення Плану дій з боротьби проти дезінформації, який передбачає комплекс заходів для виявлення, аналізу та нейтралізації дезінформаційних кампаній. У цьому контексті важливу роль відіграє діяльність Спеціальної групи зі стратегічних комунікацій Східного партнерства (East StratCom Task Force), яка займається моніторингом інформаційного простору, аналізом фейкових новин та розробкою стратегій для їхнього спростування. Крім того, ЄС розвиває ініціативи у сфері медіаграмотності, спрямовані на підвищення обізнаності громадян щодо інформаційних загроз і розвиток їхніх навичок критичного мислення. Важливим напрямом є також співпраця між країнами-членами у сфері кібербезпеки, зокрема через Агентство Європейського Союзу з кібербезпеки (ENISA), яке надає технічну підтримку, проводить навчання та розробляє стандарти для забезпечення безпеки цифрового простору.

Механізми співпраці у сфері інформаційної безпеки на міжнародному рівні відіграють ключову роль у протидії глобальним викликам, пов'язаним із гібридними загрозами. Одним із найважливіших інструментів є спільні навчання та симуляції, які організовуються міжнародними організаціями, такими як НАТО, ЄС та ООН. Ці заходи дозволяють країнам обмінюватися досвідом, відпрацьовувати спільні дії у випадку кіберінцидентів та удосконалювати свої механізми реагування. Важливою є також міжнародна співпраця у сфері розробки стандартів кібербезпеки, які сприяють уніфікації підходів до захисту критичної інфраструктури та мінімізації ризиків у цифровому середовищі. Окремо слід відзначити роль міжнародних партнерств у сфері розслідування дезінформаційних кампаній, адже ці кампанії часто мають транснаціональний характер і вимагають координації зусиль між державами.

Адаптація міжнародного досвіду в умовах гібридної агресії проти України є важливим завданням, адже вона дозволяє використовувати найкращі практики для зміцнення національного інформаційного середовища. Україна активно співпрацює з міжнародними організаціями та країнами-партнерами у сфері інформаційної безпеки. Одним із прикладів такої співпраці є участь у спільних навчаннях НАТО, які спрямовані на підвищення готовності до кіберзагроз і розвитку стратегічних комунікацій. Крім того, Україна адаптує законодавчі ініціативи ЄС у сфері боротьби з дезінформацією та кібербезпекою, що дозволяє підвищити ефективність національної політики. Важливим аспектом є інтеграція європейського досвіду у програми медіаграмотності, які допомагають населенню краще розуміти природу інформаційних загроз і ефективно їм протидіяти. Усе це сприяє формуванню стійкого інформаційного середовища, яке є важливим елементом національної безпеки України.

Таким чином, міжнародний досвід захисту інформаційного середовища у гібридних конфліктах є надзвичайно цінним для зміцнення національної інформаційної безпеки. Практика НАТО, ЄС та інших міжнародних організацій демонструє ефективність комплексного підходу, який поєднує розробку стратегічних комунікацій, підвищення кібербезпеки, боротьбу з дезінформацією та розвиток медіаграмотності. Адаптація цього досвіду до українського контексту є ключовим кроком на шляху до забезпечення стійкості інформаційного простору та протидії сучасним гібридним загрозам.

Проведене дослідження дозволяє виокремити наступні характерні риси інформаційного середовища як стратегічного ресурсу в гібридних конфліктах:

Глобальний характер. Інформаційне середовище виходить за межі національних кордонів, забезпечуючи миттєву комунікацію між учасниками конфліктів у різних частинах світу. Ця особливість дозволяє агресорам поширювати вплив далеко за межі регіону конфлікту.

Швидкість поширення інформації. Інформація в цифрову епоху поширюється практично миттєво, що дозволяє оперативно впливати на громадську думку, змінювати наративи і створювати паніку чи дезінформацію.

Маніпулятивний потенціал. Інформаційне середовище дає змогу створювати та поширювати маніпулятивний контент, такий як фей-

кові новини, пропагандистські матеріали та дезінформаційні кампанії, які впливають на сприйняття реальності.

Доступність для різних суб'єктів (всіх). У гібридних конфліктах інформаційне середовище використовується як державними, так і недержавними акторами, включаючи терористичні угруповання, хакерів, громадські організації та окремих осіб.

Асиметричність впливу. Інформаційне середовище дозволяє менш потужним сторонам конфлікту завдавати суттєвої шкоди більш сильним суперникам, використовуючи інноваційні технології та низькозатратні методи інформаційного впливу.

Інтерактивність. Сучасні цифрові платформи, особливо соціальні мережі, забезпечують зворотний зв'язок між творцями інформаційного контенту та його споживачами, що дозволяє оперативно коригувати стратегії впливу.

Високий рівень уразливості. Відкритість інформаційного середовища робить його вразливим до кібератак, дезінформаційних кампаній і пропаганди, що може дестабілізувати суспільство та послабити державні інституції.

Поляризація суспільства. Інформаційне середовище здатне посилювати соціальні розколи, використовуючи чутливі теми для створення конфліктів між різними групами населення.

Інтеграція з іншими сферами. Інформаційне середовище тісно пов'язане з політичними, економічними, військовими та соціальними процесами, що робить його важливим елементом комплексного впливу у гібридних конфліктах.

Технологічна залежність. Сучасне інформаційне середовище базується на цифрових технологіях, таких як штучний інтелект, великі дані та алгоритми, що підвищує ефективність його використання, але водночас створює нові виклики для захисту.

Ці риси підкреслюють багатогранність і стратегічне значення інформаційного середовища в умовах гібридних конфліктів, що робить його не лише ресурсом впливу, але й важливим об'єктом захисту.

Ключові слова: інформація, інформаційне середовище, гібридні конфлікти, інформаційна безпека, міждисциплінарний підхід, функції. інформаційного середовища, цифровізація, фактчекінг.