

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

**ВІД РИМСЬКОГО ПРАВА
ДО ІНТЕГРАЦІЙНОГО ПРАВА ЄВРОПИ:
ЄВРООРІЄНТОВАНА ШКОЛА
ПОРІВНЯЛЬНОЇ ЦИВІЛІСТИКИ
НА ТЛІ ГІБРИДНОЇ ВІЙНИ**

Колективна монографія

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

Одеса
Фенікс
2025

УДК 323.22/.28:355.01] (477):342.7
В 42

*Рекомендовано рішенням вченої ради Національного університету
«Одеська юридична академія» 24 вересня 2025 року (протокол № 2)*

Рецензенти:

Булеца С. Б. – докторка юридичних наук, професорка, завідувачка кафедри цивільного права та процесу Ужгородського національного університету;

Гринько С. Д. – докторка юридичних наук, професорка, завідувачка кафедри приватного права Хмельницького університету управління та права імені Леоніда Юзькова;

Дудченко В. В. – докторка юридичних наук, професорка, професорка кафедри загальної теорії права та держави Національного університету «Одеська юридична академія».

В 42 **Від римського права до інтеграційного права Європи: євроорієнтована школа порівняльної цивілістики на тлі гібридної війни : кол. монографія / за заг. ред. проф.: Є. Харитонова, О. Харитонової, І. Давидової. – Одеса : Фенікс, 2025. – 660 с.**
ISBN 978-617-8763-01-5

Колективна монографія є комплексним дослідженням еволюції приватного права – від римської традиції до сучасних європейських моделей у контексті гібридної війни проти України.

У книзі поєднані: дослідження методологічних засад порівняльної цивілістики; аналіз римського приватного права як основи європейської правової цивілізації; вивчення впливу гібридної війни на приватноправові інститути; компаративістські студії у сфері сімейного, договірної, спадкового, банківського та цифрового права; розгляд нових викликів, пов'язаних із цифровізацією та трансформацією правосвідомості.

Монографія адресована науковцям, викладачам, юристам-практикам, студентам юридичних факультетів і всім, хто цікавиться розвитком приватного права в умовах європейської інтеграції та гібридної війни.

УДК 323.22/.28:355.01] (477):342.7

ISBN 978-617-8763-01-5

© Колектив авторів, 2025

ЗМІСТ

Авторський колектив	5
ВСТУП.	7

МЕТОДОЛОГІЯ ТА ІСТОРИЧНІ ПІДВАЛИНИ

Розділ 1. Від вивчення рецепції Римського приватного права до теорії адаптації європейських правових систем: Одеська школа порівняльної цивілістики (Євген Харитонов, Олена Харитонova)	9
Розділ 2. Методологічні імперативи порівняльної цивілістики під час гібридної війни (Євген Харитонов, Олена Харитонova)	39
Розділ 3. Римське приватне право як підґрунтя права ЄС (Євген Харитонов, Олена Харитонova)	77
Розділ 4. Глобалізація, глокалізація і дихотомія «приватне право-публічне право» через призму гібридної війни (Євген Харитонов, Олена Харитонova)	119
Розділ 5. Приватне право у відкритому суспільстві в аномальних умовах (Євген Харитонов, Олена Харитонova, Ірина Давидова)	150
Розділ 6. Еволюція суб'єктів права та розвиток представництва: від часів римського приватного права до сьогодення (Ірина Бабич)	179

ГІБРИДНА ВІЙНА ЯК ПРАВОВИЙ КОНТЕКСТ

Розділ 7. Російсько-українська гібридна війна: юридичний фронт (Євген Харитонов, Олена Харитонova)	210
Розділ 8. Розвиток цивільного законодавства в умовах гібридної війни: модернізація, рецепція, трансплантація. Досвід і перспективи (Богдан Фасій)	239
Розділ 9. Волонтерська діяльність в умовах гібридної війни (Юлія Кривенко)	272
Розділ 10. Цивільні правовідносини, що виникають у сфері цивільно-військового співробітництва Збройних сил України (Микола Павленко)	288
Розділ 11. Проблеми, що виникають у зв'язку зі смертю військовослужбовця ЗСУ, під час дії воєнного стану (Валерій Герсак)	309
Розділ 12. Проблеми інституту встановлення фактів, що мають юридичне значення в умовах гібридної війни (Юлія Цал-Цалко)	327

Розділ 8

РОЗВИТОК ЦИВІЛЬНОГО ЗАКОНОДАВСТВА В УМОВАХ ГІБРИДНОЇ ВІЙНИ: МОДЕРНІЗАЦІЯ, РЕЦЕПЦІЯ, ТРАНСПЛАНТАЦІЯ. ДОСВІД І ПЕРСПЕКТИВИ DOI

Богдан Фасій
кандидат юридичних наук, доцент

Методологічні підходи до регулювання права на інформацію в умовах гібридної війни

У сучасному світі інформація стала не лише важливим ресурсом для розвитку суспільства, але й потужним інструментом у міжнародних відносинах, політиці та навіть у військових конфліктах. Гібридні війни створюють нові виклики для правового регулювання інформаційного простору, адже маніпуляція інформацією, дезінформація, кібератаки та пропаганда стали невід'ємною частиною сучасних конфліктів. Ці загрози ставлять перед суспільством завдання ефективно захищати право на інформацію, пристосовуючи механізми правового захисту до нових реалій глобальних викликів.

Забезпечення права на інформацію в умовах гібридної війни є складним і делікатним процесом, який потребує балансування між свободою слова і необхідністю гарантування інформаційної безпеки. З одного боку, демократичні суспільства базуються на принципах відкритості, доступу до інформації та вільного обміну думками, що є основою розвитку прав людини і функціонування правової держави. З іншого боку, протистояння ворожим інформаційним атакам, спрямованим на дестабілізацію суспільства, маніпулювання громадською думкою та підрив національних інститутів, вимагає впровадження ефективних заходів для захисту. Водночас важливо не втратити з уваги, що надмірне обмеження доступу до інформації може спричинити зловживання, обмеження свободи

вираження думок та цензуру, що суперечить основам демократичного суспільства.

Гібридна війна впливає на всі сфери функціонування інформаційного простору, змушуючи держави адаптувати національні законодавства відповідно до нових викликів. У контексті України, яка тривалий час протистоїть гібридній агресії, особливо актуальним є питання вдосконалення нормативно-правового регулювання інформаційної сфери. Зокрема, важливим є узгодження національного законодавства із міжнародними стандартами у сфері свободи інформації та інформаційної безпеки, що дозволить не лише ефективно захищати громадян від дезінформації, а й забезпечувати належний рівень правового захисту журналістів, медіа та суспільства загалом.

Дослідження права на інформацію в умовах гібридної війни також має важливе значення з точки зору розвитку міжнародно-правових підходів до боротьби з дезінформацією та інформаційними маніпуляціями. У сучасних умовах міжнародні організації, такі як ООН, ЄС, Рада Європи та ОБСЄ, розробляють рекомендації та правові механізми щодо захисту інформаційного простору від гібридних загроз¹. Проте єдиної, універсальної правової моделі, яка б ефективно забезпечувала баланс між правом на інформацію та інформаційною безпекою, поки що не існує. Це вимагає активізації наукових досліджень виокремленої проблематики.

Крім того, врахування технологічного чинника є невід'ємною складовою сучасного правового регулювання інформаційного простору. Швидкий розвиток цифрових технологій, соціальних мереж та штучного інтелекту відкриває нові можливості для поширення інформації, водночас збільшуючи ризики маніпуляцій і втручання у внутрішні справи держав. Відтак, правові механізми регулювання інформаційної сфери повинні враховувати особливості цифрового середовища та бути адаптованими до умов, у яких інформаційні загрози можуть мати транснаціональний характер.

Таким чином, актуальність дослідження права на інформацію в умовах гібридної війни зумовлена необхідністю пошуку оптимального правового балансу між забезпеченням інформаційної відкритості

¹ Смотрич Д., Іванов Н. Правові аспекти боротьби з дезінформацією в Європейському Союзі: уроки для України. *Вісник Національного університету «Львівська політехніка»*. 2023. №4 (40). С. 155-161.

та захистом від деструктивних інформаційних впливів. Це питання є надзвичайно важливим не лише для України, а й для всього демократичного світу, оскільки інформаційні загрози є глобальним викликом, що вимагає комплексного правового реагування.

Сучасний глобалізований світ стикається з безпрецедентними викликами у сфері інформаційного регулювання, зумовленими швидкою цифровізацією, транснаціональним характером медіа та посиленням інформаційних загроз. Традиційні правові підходи, розроблені в епоху друкованих та аналогових медіа, вже не відповідають сучасним реаліям, коли інформаційні потоки перетинають державні кордони, а цифрові платформи відіграють ключову роль у формуванні суспільної думки. Це породжує проблему адаптації правових механізмів до умов, у яких національні інструменти регулювання стають недостатніми для забезпечення ефективного контролю над інформаційним середовищем.

Одним із важливих викликів є врівноваження свободи вираження поглядів та інформаційної безпеки. Свобода слова є фундаментальним правом, закріпленим у міжнародних актах, таких як Загальна декларація прав людини (ст. 19) та Європейська конвенція з прав людини (ст. 10). Проте в умовах інформаційних загроз, включаючи дезінформацію, пропаганду ненависті та втручання у виборчі процеси, держави вимушені запроваджувати обмеження, які можуть порушувати демократичні стандарти. Відсутність універсальних критеріїв щодо допустимості таких обмежень призводить до правової невизначеності та зловживань з боку окремих урядів, що використовують боротьбу з дезінформацією як привід для цензури та переслідування інакодумців.

Ще однією гострою проблемою є регулювання діяльності глобальних цифрових платформ, таких як Google, Meta (Facebook), X (Twitter) та TikTok. Ці корпорації мають величезний вплив на інформаційний простір, фактично виконуючи функції неформальних «регуляторів» контенту. Проте їх діяльність часто суперечить національним правовим нормам, а політика модерації контенту залишається непрозорою та піддається політичному впливу. До прикладу, ЄС намагається встановити єдині правила через прийняття Акту про цифрові послуги (Digital Services Act, DSA)¹ та Акту про цифрові ринки (Digital Markets

¹ The Digital Services Act. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

Act, DMA)¹, які покликані підвищити відповідальність платформ за поширення шкідливого контенту та забезпечити більшу прозорість їхніх алгоритмів.

Окремий аспект проблематики становить питання захисту персональних даних та приватності в умовах масового збору та аналізу інформації. Впровадження технологій штучного інтелекту, великих даних (big data) та алгоритмічного моделювання призводить до потенційних порушень права на приватність та незаконного використання особистої інформації. Водночас різні правові режими, такі як Загальний регламент ЄС про захист даних (GDPR) та менш суворі американські підходи, демонструють розбіжності в глобальному регулюванні, що ускладнює міжнародну співпрацю у сфері захисту даних.

Отже, проблематика регулювання інформаційної сфери в сучасному глобальному контексті зумовлена багатогранністю інформаційних загроз, складністю балансування між свободою слова та інформаційною безпекою, недостатньою ефективністю національних правових механізмів та впливом цифрових платформ на суспільні процеси. Це вимагає вироблення нових підходів до міжнародно-правового регулювання, гармонізації правових стандартів та створення ефективних механізмів співпраці між державами, корпораціями та громадянським суспільством.

Концепція права на інформацію має тривалу історію розвитку, яка відображає еволюцію суспільних та правових підходів до забезпечення свободи вираження поглядів, доступу до інформації та її поширення. Витоки цього права можна знайти ще у працях класичних філософів, таких як Джон Лок² та Джон Міль³, які обґрунтовували необхідність вільного обміну ідеями для розвитку демократичного суспільства. Проте у сучасному розумінні право на інформацію сформулося лише у XX столітті внаслідок розвитку міжнародних стандартів прав людини та національного законодавства демократичних держав.

На міжнародному рівні першим нормативним актом, що закріпив право на інформацію, стала Загальна декларація прав людини 1948

¹ Digital Markets Act. URL: <https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng>

² Подковенко Т. Концепція лібералізму Джона. *Актуальні проблеми правознавства*. 2022. № 1 (29). С. 12-17.

³ Міл Джон Стюарт. Про свободу: Есе / Пер. з англ. К: Основи, 2001. С. 7-24.

року. Стаття 19 цього документа гарантує кожному свободу дотримуватися своїх переконань і вільно поширювати інформацію, «шукати, отримувати і передавати її будь-якими засобами та незалежно від державних кордонів»¹. Це положення лягло в основу подальших міжнародних договорів, зокрема Міжнародного пакту про громадянські та політичні права (1966), який у ст.19 передбачає не лише право особи на свободу вираження, але й зобов'язання держав гарантувати доступ до інформації².

Значний внесок у розвиток права на інформацію зробили регіональні міжнародні організації. Європейська конвенція з прав людини (1950) у ст. 10 закріплює свободу вираження, включаючи право отримувати та передавати інформацію без втручання органів влади³. Однак судова практика Європейського суду з прав людини значно розширила тлумачення цього права, визнавши, що воно включає й позитивні зобов'язання держави щодо забезпечення доступу до інформації⁴.

На національному рівні окремих країн світу право на інформацію спочатку розглядалося переважно в контексті свободи преси. У США Перша поправка до Конституції (1791) гарантувала свободу слова та друку, що стало основою для подальшого розвитку законодавства щодо доступу до інформації. Пізніше, у 1966 році, був прийнятий Акт про свободу інформації (FOIA), який вперше закріпив механізм доступу громадян до інформації, що зберігається урядовими структурами⁵.

Європейські держави також поступово запроваджували законодавство про доступ до інформації. Одним із перших був Швецький акт про свободу друку (1766), який гарантував право громадян на доступ до державних документів⁶. В Україні розвиток цього права

¹ Universal Declaration of Human Rights. URL: <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

² International Covenant on Civil and Political Rights. URL: <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

³ European Convention on Human Rights. URL: https://www.echr.coe.int/documents/convention_eng.pdf

⁴ Magyar Helsinki Bizottság v. Hungary. URL: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-167828%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-167828%22]})

⁵ The Freedom of Information Act, 5 U. S. C. § 552. URL: <https://www.justice.gov/oip/freedom-information-act-5-usc-552>

⁶ Акт про свободу друку (Швеція). URL: [https://uk.wikipedia.org/wiki/Акт_про_свободу_друку_\(Швеція\)](https://uk.wikipedia.org/wiki/Акт_про_свободу_друку_(Швеція))

розпочався після здобуття незалежності. Прийняття Закону України «Про доступ до публічної інформації» (2011) стало важливим кроком у забезпеченні прозорості державного управління та реалізації принципу відкритого урядування¹.

В умовах цифровізації право на інформацію набуває нових аспектів. З одного боку, розвиток інтернету та соціальних мереж значно розширив можливості доступу до інформації, з іншого – породив нові виклики, пов'язані з фейковими новинами, маніпуляціями та загрозами приватності. У відповідь на це ЄС ухвалив Акт про цифрові послуги (2022), який встановлює вимоги щодо прозорості алгоритмів цифрових платформ та боротьби з дезінформацією².

Таким чином, еволюція концепції права на інформацію демонструє поступовий перехід від традиційного розуміння свободи слова до більш складної системи правового регулювання, яка враховує сучасні виклики інформаційного суспільства. Сучасні міжнародні стандарти базуються на балансі між свободою інформації та необхідністю захисту національної безпеки, персональних даних і протидії дезінформації. Це підкреслює важливість подальшого розвитку правових механізмів, здатних адаптуватися до динамічних змін інформаційного середовища.

У сучасному правовому дискурсі право на інформацію є складним і багатогранним явищем, що охоплює різні аспекти отримання, поширення та захисту інформації. Його визначення та регулювання ґрунтуються на поєднанні міжнародних, регіональних та національних правових підходів, які враховують як демократичні цінності, так і потреби забезпечення інформаційної безпеки.

Перший підхід – ліберально-демократичний, що базується на фундаментальних правах людини. Він закріплений у ключових міжнародно-правових актах, таких як Загальна декларація прав людини (1948) (ст. 19) та Міжнародний пакт про громадянські та політичні права (1966) (ст. 19). Цей підхід передбачає, що право на інформацію є невід'ємною складовою свободи вираження поглядів, яка включає право шукати, отримувати та поширювати інформацію незалежно

¹ Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>

² Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>

від державних кордонів. У рішеннях ЄСПЛ, зокрема у справі *Sunday Times v. United Kingdom* (1979), наголошується на важливості доступу до інформації для функціонування демократичного суспільства¹.

Другий підхід – функціонально-інформаційний, який розглядає право на інформацію як інструмент забезпечення прозорості діяльності органів державної влади та контролю з боку громадянського суспільства. Його реалізація передбачає встановлення обов'язку державних органів надавати доступ до публічної інформації, як це закріплено в Конвенції Ради Європи про доступ до офіційних документів (2009). На національному рівні цей підхід реалізований у законодавстві низки країн, зокрема через Закон України «Про доступ до публічної інформації» (2011).

Третій підхід – безпеково-регуляторний, який набув особливого значення в умовах сучасних викликів, зокрема гібридних війн, тероризму та дезінформації. Він передбачає можливість обмеження права на інформацію в інтересах національної безпеки, громадського порядку або захисту прав інших осіб. Цей підхід закріплений у ст. 10 Європейської конвенції з прав людини, яка допускає обмеження свободи вираження поглядів, якщо це необхідно у демократичному суспільстві. Проте практика ЄСПЛ, наприклад у справі *Handyside v. United Kingdom* (1976), вимагає, щоб такі обмеження були пропорційними та виправданими².

Четвертий підхід – технологічно-правовий, який враховує розвиток цифрового середовища та інформаційних технологій. Він орієнтований на регулювання доступу до інформації в інтернеті, захист персональних даних та протидію дезінформації. Прикладом такого підходу є Акт про цифрові послуги (2022) ЄС, що встановлює вимоги до цифрових платформ щодо видалення шкідливого контенту та забезпечення прозорості алгоритмів.

Останній підхід – комплексний, що поєднує аспекти свободи слова, доступу до інформації, інформаційної безпеки та технологічного регулювання. Він передбачає гармонізацію різних правових механізмів для досягнення балансу між відкритістю інформаційного простору та захистом від загроз. Такий підхід реалізується у політиці ЄС та

¹ *Sunday Times v. United Kingdom*. URL: <https://hudoc.echr.coe.int/eng?i=001-57584>

² *Case of Handyside v. The United Kingdom*. URL: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-57499%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57499%22]})

низки національних законодавств, спрямованих на створення безпечного та прозорого інформаційного середовища.

Таким чином, правові підходи до визначення права на інформацію відображають поступову еволюцію від забезпечення свободи вираження до комплексного регулювання інформаційного простору з урахуванням сучасних технологічних, безпекових та демократичних викликів.

Вітчизняні науковці розглядають право на інформацію як фундаментальне право людини, що забезпечує можливість вільно отримувати, використовувати, поширювати та зберігати інформацію. Це право є невід'ємною складовою демократичного суспільства та гарантується Конституцією України.

Так, В. В. Фурман зазначає, що право на інформацію є багатоаспектною правовою категорією, що охоплює систему правових можливостей, пов'язаних із пошуком, отриманням, збереженням, створенням, використанням, передачею, поширенням та охороною інформації. Це право забезпечує широкий спектр дій, не заборонених законом, за умови дотримання балансу між свободою інформації та вимогами інформаційної безпеки держави, суспільства й особи. При цьому, науковцем доречно вказано, що характерною особливістю права на інформацію є його багатоаспектність не лише з погляду видів дозволеної поведінки, а й щодо суб'єктного складу. Суб'єктами цього права виступають фізичні особи, юридичні особи, організації, що не мають статусу юридичної особи, а також держава. При цьому кожній категорії суб'єктів притаманні специфічні правомочності. Зокрема, доступ до інформації, що має статус державної таємниці, належить виключно державі, тоді як право на комерційну таємницю реалізують юридичні особи та підприємці. Водночас особиста інформація, що охороняється правом на приватність, є виключним правом фізичних осіб¹.

Право на інформацію розглядається як ключова передумова для усвідомлення особистістю свого становища в суспільстві, забезпечення її гармонійного розвитку та вільного існування. Це одне з фундаментальних прав людини, оскільки її здатність діяти вільно та усвідомлено безпосередньо залежить від можливості отримувати й

¹ Фурман В. В. Право на інформацію в системі конституційних прав людини і громадянина. *Правничий часопис Донецького національного університету імені Василя Стуса*. 2024. С. 100-110.

аналізувати інформацію про події та процеси, що відбуваються у на-вколишньому світі¹.

Як влучно зазначають О. П. Дзьобань та С. Б. Жданенко, право на інформацію стало рівнозначним природним правам людини, оскільки без здатності отримувати, обробляти чи виробляти інформацію людина не може повноцінно існувати в сучасному світі. Лише за умо-ви, що особа отримує інформацію, аналізує її та створює нову, вона здатна до розвитку і, відповідно, бути активним і рівноправним чле-ном суспільства².

Структуру права на інформацію детально аналізують провідні науковці Інституту держави і права ім. В. М. Корецького, які під-креслюють його складний характер. Вони виокремлюють ключові елементи цього права, зокрема: право на вільний збір, збереження, використання та поширення інформації у будь-якій формі за власним вибором, а також право на охорону та захист інформації³.

Варто зазначити, що реалізація кожного з наведених елементів неможлива без забезпечення права на доступ до інформації. Саме отримання інформації є передумовою її подальшого використання, збереження чи поширення, що дозволяє розглядати право на доступ до інформації як фундаментальну складову комплексного права на інформацію.

Баланс між правом на інформацію та національною безпекою є однією з найбільш складних і актуальних проблем у сучасному пра-ві, особливо в умовах, коли суспільства зазнають нових викликів, пов'язаних із інформаційними війнами, тероризмом, кіберзагрозами та гібридними конфліктами. Право на інформацію є основоположним правом людини, що забезпечує доступ до відомостей, необхідних для прийняття обґрунтованих рішень, а також для свободи думки та вираження. Однак його реалізація не може бути абсолютною, оскільки існують певні обмеження, необхідні для захисту національної без-пеки, територіальної цілісності та суверенітету держави.

¹ Політанський В. С. Право на інформацію як фундаментальне право людини: автореферат дис. ... канд. юрид. наук. Харків, 2017. С. 9.

² Дзьобань О. П., Жданенко С. Б. Право на інформацію: філософсько-правовий аспект проблеми. *Вісник Національного університету Юридична академія України імені Ярослава Мудрого*. 2013. 4. С. 56-64.

³ Правове забезпечення інформаційної діяльності в Україні / Ю. С. Шемшученко та ін.; Заг. ред. Ю. С. Шемшученко, І. С. Чиж. К.: Юридична думка, 2006. 384 с.

Перш за все, важливо розуміти, що право на інформацію і національна безпека не завжди взаємно сумісні. У ситуаціях, коли розголошення певної інформації може завдати шкоди безпеці держави, її обороноздатності чи інтересам суспільства, виникає необхідність встановлення певних обмежень на доступ до такої інформації. Це стосується, зокрема, відомостей, що становлять державну таємницю, військові плани, інші стратегічні дані, які можуть бути використані ворожими силами для завдання шкоди країні.

З одного боку, право на інформацію забезпечує прозорість влади, дозволяючи громадянам здійснювати контроль за діями державних органів, що є важливим аспектом демократичного управління. Однак з іншого боку, розголошення інформації, що може поставити під загрозу безпеку держави, може призвести до серйозних наслідків для національної стабільності. Тому завжди виникає дилема між прозорістю і необхідністю приховування певних відомостей для забезпечення безпеки.

Важливим аспектом є розмежування між інформацією, яку необхідно приховувати з міркувань національної безпеки, і інформацією, яка не повинна підпадати під обмеження навіть в умовах воєнного або кризового стану. Одним із таких критеріїв є застосування принципу «необхідності» для обмеження доступу до інформації, який передбачає, що обмеження можуть бути введені лише в тих випадках, коли вони є необхідними для досягнення певної мети, наприклад, для запобігання загрозам національній безпеці.

Проблема балансу між цими двома сферами піднімає питання, яким чином держава має визначати, що є надмірними обмеженнями, а що є необхідним для захисту інтересів держави. Оскільки ці питання можуть мати різні трактування, важливим є наявність чітких нормативних актів і критеріїв, що дозволяють чітко відокремити інформацію, яка підлягає публікації, від тієї, що повинна залишатися конфіденційною.

У світовій практиці цей баланс також є предметом ретельного правового регулювання. У більшості розвинених країн право на інформацію обмежується в ситуаціях, коли розголошення може завдати шкоди національній безпеці, зовнішній політиці чи міжнародним відносинам. Одним із найбільш відомих прикладів є Закон про свободу інформації (Freedom of Information Act) у Сполучених

Штатах¹, який встановлює правила доступу до державної інформації, однак в ньому також передбачені чіткі виключення для захисту національної безпеки.

У контексті гібридних війн та сучасних інформаційних технологій ситуація ускладнюється. Інформаційна війна, яка проводиться за допомогою фальшивих новин, пропаганди та маніпуляцій, здатна завдати серйозної шкоди безпеці країни. Тому, у випадках збройних конфліктів чи гібридних воєн, країни змушені вдаватися до заходів із блокування дезінформації та пропаганди, що є прямим обмеженням на право на вільний доступ до інформації. Тут знову постає питання, де знаходиться межа між необхідністю захисту держави та дотриманням прав громадян. Якщо спробувати дати відповідь на це питання з точки зору цивільного права, то головний принцип – держава не може втручатися в приватні права громадян, якщо немає законних підстав. Але навіть якщо такі підстави є, держава зобов'язана діяти пропорційно, не порушуючи основоположні права, і забезпечувати компенсацію в разі обмежень. Наприклад, якщо держава конфіскує майно в інтересах національної безпеки, то власник має право на справедливе відшкодування. Це ж стосується будь-яких інших ситуацій, де громадянин стикається з втручанням держави у його приватні сфери: від обмеження підприємницької діяльності до контролю за персональними даними.

У цивільному праві також важливе питання приватності. Наприклад, держава може мотивувати збір інформації про громадян потребами безпеки, але це не означає, що вона може безконтрольно збирати та використовувати персональні дані. Для цього потрібні чіткі юридичні механізми, а громадянин має право знати, хто і як використовує його інформацію.

Окремо варто згадати, що громадяни мають можливість оскаржити дії держави, якщо вони вважають, що їхні права порушені. Це реалізується в судовому порядку. У цьому сенсі цивільне право виконує роль такого собі балансу між інтересами держави та правами особи.

Зрештою, все зводиться до того, що межа між захистом держави та правами громадян у цивільному праві визначається через законність, пропорційність, можливість судового захисту та обов'язкову

¹ Freedom of Information Act Resources. URL: <https://www.ilsdc.org/freedom-of-information-act-resources>

компенсацію в разі втручання. Тобто, якщо з боку держави вжито заходи обмеження прав особи, то державні інституції мають роз'яснити з якою метою здійснюються обмеження, надати механізми захисту та, якщо потрібно, компенсувати втрати.

З урахуванням усіх цих факторів, важливим є створення механізмів, які дозволяють здійснювати контроль за інформацією, що може бути використана для шкоди державним інтересам, з одночасним забезпеченням прав громадян на доступ до інформації, що не має стратегічного значення для безпеки. Це передбачає створення правових інститутів, що будуть сприяти чіткій і прозорій оцінці інформаційних загроз та визначенню обмежень на доступ до певних видів інформації.

Враховуючи сучасні виклики в інформаційній сфері, критично важливо, щоб держави мали чітко визначені механізми для забезпечення балансу між правом на інформацію та національною безпекою. Це потребує розвитку законодавства, яке б передбачало ефективні інструменти для захисту інформаційної безпеки без порушення основоположних прав людини. Створення таких механізмів має бути зосереджено на забезпеченні безпеки національних інтересів, одночасно не перешкоджаючи основним принципам демократії та свободи вираження.

Оскільки проблема балансу між правом на інформацію та національною безпекою є складною та багатогранною, для її вирішення необхідне не лише чітке правове регулювання, але й розвиток сучасних механізмів моніторингу та адаптації законодавства до нових інформаційних реалій.

Гібридна війна, яка поєднує традиційні військові дії з новітніми інформаційними маніпуляціями, значно змінює баланс між національною безпекою та правом на інформацію. У зв'язку з цим виникає потреба у перегляді існуючих міжнародних стандартів, що визначають свободу інформації, а також механізмів її захисту в умовах зростаючих загроз національній безпеці, які постають внаслідок зовнішнього втручання в інформаційний простір. У такій ситуації, на нашу думку, варто діяти в двох напрямках: оновлення міжнародних стандартів щодо свободи інформації та створення ефективних механізмів захисту інформаційного простору без надмірного обмеження прав громадян.

Перегляд міжнародних стандартів має бути реалізований за допомогою:

- розширення визначення інформаційних загроз, включаючи нові форми кібер- та інформаційних атак (дезінформація, гібридні війни, маніпулятивні алгоритми соцмереж);
- вдосконалення балансу між свободою інформації та необхідністю її обмеження в інтересах національної безпеки, з чіткими критеріями, коли втручання держави є допустимим;
- посилення міжнародної відповідальності технологічних платформ та держав за використання інформації як зброї (наприклад, через санкції чи правові механізми ООН).

Механізми захисту інформаційного простору доречно здійснювати через:

- розвиток системи раннього виявлення інформаційних загроз та міжнародного співробітництва у сфері кібербезпеки;
- вдосконалення юридичних механізмів протидії дезінформації без загрози цензури (наприклад, через незалежні міжнародні органи з перевірки фактів);
- підвищення цифрової грамотності населення та прозорість алгоритмів поширення інформації у соцмережах.

Таким чином, оновлені міжнародні стандарти мають створювати механізми для стримування зовнішніх інформаційних загроз, водночас не даючи державам зловживати ними для обмеження свободи слова.

В умовах гібридної війни, коли інформаційні атаки стають однією з основних форм впливу на держави, концепція свободи інформації зазнає значних змін. Зокрема, держава має балансувати між захистом від маніпуляцій та забезпеченням права на інформацію. Наслідки гібридної війни для міжнародних стандартів свободи інформації також відображаються в рамках діяльності ЄС. Зокрема, в межах Регламенту ЄС 2018 року про вільний обіг даних була введена низка обмежень, спрямованих на захист інформації від маніпуляцій з боку держав, які можуть намагатися використовувати інформаційні потоки для військових цілей або підриву демократичних інститутів¹.

¹ Regulation (EU) 2018/1807 of The European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807>

Нині свобода медіа є одним з основних принципів демократичного суспільства, що гарантує право громадян на доступ до інформації та вираження своїх поглядів. Однак, в умовах гібридних війн, що характеризуються активним використанням інформаційних технологій, пропаганди, фальсифікації новин та дезінформації, необхідний контроль за медіа, щоб захистити національну безпеку. Інформаційні атаки можуть послабити соціальну згуртованість, підривати довіру до урядових інститутів і сприяти політичній дестабілізації. Тому держави змушені застосовувати обмеження, щоб запобігти розповсюдженню шкідливої або маніпулятивної інформації, не порушуючи при цьому основні принципи свободи вираження.

Проте, важливо дотримуватися балансу між свободою медіа і необхідністю забезпечення національної безпеки. Контроль за медіа не має переростати у цензуру чи політичну репресію, а повинен бути спрямований на захист суспільства від зовнішніх загроз, які можуть бути приховані під виглядом свободи інформації. У цьому контексті важливу роль відіграють чіткі регуляторні механізми, які дозволяють державі впливати на інформаційний простір, не порушуючи фундаментальних прав людини, таких як свобода слова та доступ до правдивої інформації.

Не менш важливою є роль національних правових систем, що повинні забезпечувати належний захист прав на інформацію, навіть коли національна безпека перебуває під загрозою. Так, боротьба з інформаційними атаками вимагає від урядів не лише зміцнення власних засобів інформаційної безпеки, але й вироблення чітких стратегій щодо протидії дезінформації.

Таким чином, гібридна війна суттєво трансформує міжнародні стандарти свободи інформації, що вимагає адаптації міжнародного права до нових викликів у сфері інформаційної безпеки. Це вимагає розробки нових механізмів правового регулювання та ефективних способів боротьби з інформаційними загрозами на глобальному рівні. Відповідні стратегії повинні враховувати баланс між захистом національних інтересів і забезпеченням прав людини, зокрема права на доступ до інформації.

Дослідження методологічних основ права на інформацію в умовах гібридної війни є критично важливим через трансформацію інформаційного простору та зміну підходів до забезпечення інформаційної

безпеки. Гібридна війна поєднує традиційні воєнні методи з інформаційними маніпуляціями, кібернетичними атаками та пропагандою, що створює нові виклики для правового регулювання. У такому контексті розробка ефективних методологічних підходів до дослідження права на інформацію дозволяє визначити межі допустимого державного контролю за інформаційними потоками, гарантувати реалізацію свободи слова та доступу до інформації, а також створити механізми протидії інформаційним загрозам.

Методологічний аналіз цього питання також сприяє розробці адаптивних правових механізмів, які враховують динаміку інформаційного середовища та сучасні технологічні виклики. Гібридна війна змушує науковців переосмислювати традиційні підходи до інформаційних прав і створювати нові концептуальні моделі їх захисту. Зокрема, необхідно інтегрувати міждисциплінарні методи дослідження, такі як правовий аналіз, кібербезпекові стратегії, соціологічні підходи до інформаційних процесів і теорії комунікації. Без чіткого методологічного обґрунтування неможливо ефективно оцінити правові ризики, розробити дієві механізми регулювання інформаційної сфери та забезпечити баланс між свободою інформації та національною безпекою.

Застосування порівняльно-правового аналізу у дослідженні регулювання права на інформацію в країнах, що зазнали інформаційних атак, дає можливість виявити ефективні законодавчі механізми захисту інформаційного простору та адаптувати їх до національних умов. Цей метод дозволяє не лише оцінити правові підходи різних держав, а й виявити тенденції розвитку міжнародних стандартів у сфері інформаційної безпеки.

Порівняльно-правовий аналіз також дає змогу оцінити баланс між забезпеченням права на інформацію як особистого немайнового права та необхідністю запровадження обмежень в умовах інформаційної війни. Дослідження законодавства різних країн дозволяє зрозуміти, які правові механізми найкраще забезпечують цей баланс, а також які заходи держави можуть вважатися надмірними та такими, що порушують основоположні права людини. Завдяки цьому методу можна розробити рекомендації щодо вдосконалення національного законодавства з урахуванням світового досвіду та міжнародних стандартів.

Право на інформацію є фундаментальним особистим немайновим правом, яке забезпечує можливість вільного отримання, використання, поширення та зберігання інформації¹. В умовах сучасних інформаційних загроз, зокрема інформаційних атак, держави стикаються з необхідністю адаптувати своє законодавство для забезпечення інформаційної безпеки, не порушуючи при цьому основоположних прав людини.

Україна, яка зазнала численних інформаційних атак, зокрема під час гібридної війни, внесла зміни до свого законодавства для посилення інформаційної безпеки. Так, було прийнято Закон України «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи захисту національних інтересів у кіберпросторі. Цей закон спрямований на захист критичної інформаційної інфраструктури та забезпечення стійкості інформаційних систем від кібератак.

Литва, яка також зазнала інформаційних атак, зокрема кібератак на державні установи, впровадила стратегію кібербезпеки, яка передбачає тісну співпрацю між державним та приватним секторами для захисту інформаційного простору. Крім того, Литва активно працює над підвищенням обізнаності громадян щодо інформаційних загроз та методів їхнього запобігання.

Естонія, відома своїм розвиненим електронним урядуванням, після масштабної кібератаки у 2007 році створила Центр кібербезпеки НАТО в Таллінні та впровадила комплексну стратегію кібербезпеки. Ця стратегія включає як технічні заходи захисту, так і правові механізми реагування на інформаційні загрози.

Польща, враховуючи зростаючі інформаційні загрози, прийняла Закон «Про національну кібербезпеку», який встановлює обов'язки державних органів та приватних компаній щодо захисту інформаційних систем. Цей закон також передбачає створення спеціальних підрозділів для реагування на кіберінциденти та координацію дій у разі інформаційних атак.

Велика Британія, зіткнувшись з інформаційними загрозами, розробила Національну стратегію кібербезпеки, яка акцентує увагу на захисті критичної інфраструктури та підвищенні стійкості суспіль-

¹ Мартюк А. С. Право на інформацію як особисте немайнове право фізичних осіб. URL: <https://df.duit.in.ua/index.php/dictum/article/view/14/8>

ства до інформаційних впливів. Стратегія передбачає інвестиції в кібербезпеку, розвиток навичок у цій сфері та міжнародну співпрацю для протидії глобальним інформаційним загрозам.

Франція, реагуючи на зростаючі кіберзагрози, створила Агентство національної безпеки інформаційних систем (ANSSI), яке відповідає за координацію заходів з кібербезпеки та захисту державних інформаційних систем. Крім того, Франція впровадила законодавчі акти, які зобов'язують операторів критичної інфраструктури дотримуватися високих стандартів кібербезпеки.

Німеччина, враховуючи зростаючі інформаційні загрози, прийняла Закон «Про безпеку інформаційних технологій», який встановлює вимоги до операторів критичної інфраструктури щодо забезпечення кібербезпеки. Цей закон також передбачає обов'язкове повідомлення про кіберінциденти та співпрацю з федеральними органами для забезпечення національної безпеки¹.

Сполучені Штати Америки, зіткнувшись з масштабними інформаційними атаками, розробили стратегію кібербезпеки, яка включає як захист державних інформаційних систем, так і співпрацю з приватним сектором для забезпечення стійкості національної інфраструктури. Крім того, США активно працюють над підвищенням обізнаності громадян щодо кіберзагроз та методів їхнього запобігання².

Таким чином, аналіз досвіду країн, що зазнали інформаційних атак, демонструє важливість комплексного підходу до регулювання інформаційної сфери, який поєднує технічні, організаційні та правові заходи. Забезпечення інформаційної безпеки вимагає не лише впровадження сучасних технологій захисту, але й розробки відповідного законодавства, яке враховує специфіку інформаційних загроз та гарантує захист особистих немайнових прав громадян.

Функціонально-системний підхід є важливим методологічним інструментом для дослідження права на інформацію в цивільному праві. Цей підхід передбачає аналіз інформаційних правовідносин як складної системи, де взаємодіють різні елементи: суб'єкти (фізичні

¹ Міжнародне інформаційне право: теорія і практика: монографія. Київський національний університет імені Тараса Шевченка. Дніпропетровськ.: «Середняк Т. К.», 2015. С. 148.

² США представили нову стратегію кібербезпеки на тлі зростання хакерських атак, головними загрозами вважають Китай і Росію. URL: <https://forbes.ua/news/ssha-predstavili-novu-strategiyu-kiberbezpeki-na-tli-zrostannya-khakerskikh-atak-golovnimi-zagrozami-vvazhayut-kitay-i-rosiyu-02032023-12093>

та юридичні особи, держава), об'єкти (інформація як нематеріальне благо), правові норми та механізми захисту. В умовах гібридної війни застосування цього підходу дозволяє встановити ефективні механізми балансу між забезпеченням доступу до інформації та захистом національної безпеки¹.

З точки зору цивільного права, право на інформацію є особистим немайновим правом, що забезпечує можливість особи отримувати, використовувати, поширювати та захищати інформацію. Воно належить до категорії абсолютних прав і не може бути відібране чи обмежене без належних юридичних підстав. Функціонально – системний підхід дозволяє оцінити, як це право співвідноситься з іншими особистими немайними правами, наприклад, правом на приватне життя або правом на свободу вираження поглядів, та як забезпечується його реалізація в умовах зростаючих інформаційних загроз.

Особливість цього підходу полягає в тому, що він розглядає право на інформацію не ізольовано, а як систему правових норм, що функціонують у межах загального методу цивільно-правового регулювання. Визначення інформації як нематеріального об'єкта цивільних правовідносин дозволяє розглядати її у взаємозв'язку з іншими нематеріальними благами, такими як честь, гідність, ділова репутація². Водночас система правового захисту інформації має враховувати потенційні загрози її викривлення чи маніпуляції в умовах гібридної війни.

У функціональному аспекті дослідження права на інформацію охоплює аналіз його ролі у регулюванні суспільних відносин. Право на інформацію забезпечує не лише доступ до відомостей, а й можливість їх використання у цивільному обороті, наприклад, у сфері договірних зобов'язань або захисту прав споживачів. Системний підхід дозволяє простежити взаємозв'язок між правом на інформацію та інформаційною безпекою, оскільки без належного правового регулювання це право може бути використане як інструмент інформаційних атак та дезінформації³.

¹ Скакун О. Ф. Теорія держави і права. Харків: Консум, 2020. С. 112.

² Борисова А. «Інформація» та «правова інформація» як об'єкти правовідносин у сфері інформаційних комунікацій. *Юридичний вісник*. 2020. № 4. С. 180-188.

³ Пашковський В. Ф. Інституційний механізм інформаційної безпеки України в умовах гібридної війни: характер та перспективи трансформації. *Політикус*. С. 69-78. URL: http://politicus.od.ua/1_2021/11.pdf

Сучасні виклики, пов'язані з гібридною війною, вимагають комплексного переосмислення правових механізмів захисту інформації. Використання функціонально-системного підходу дозволяє виявити слабкі місця у чинному цивільному законодавстві та запропонувати шляхи вдосконалення правового регулювання. Зокрема, важливим напрямом є розробка ефективних механізмів судового захисту права на інформацію та його балансування з іншими правами, включно з правом на приватність та правом на інтелектуальну власність.

Однією з ключових проблем у цьому контексті є розмежування легітимного обмеження права на інформацію з метою захисту національної безпеки та неправомірного цензурування. Функціонально – системний підхід дозволяє проаналізувати міжнародні стандарти у цій сфері, зокрема практику Європейського суду з прав людини, який неодноразово наголошував, що будь-яке обмеження інформаційних прав має бути пропорційним і необхідним у демократичному суспільстві¹.

Таким чином, застосування функціонально-системного підходу у дослідженні права на інформацію в цивільному праві дозволяє забезпечити комплексний аналіз правових норм, механізмів їх реалізації та впливу на суспільні відносини. У контексті гібридної війни цей підхід є необхідним для розробки ефективних заходів правового регулювання, що сприятимуть як захисту інформаційного простору держави, так і збереженню основоположних прав людини.

Діалектичний метод є одним із ключових методологічних підходів у дослідженні права на інформацію, оскільки він дозволяє розглядати його як динамічне, змінне явище, що перебуває у взаємодії з іншими правами та соціальними процесами. З позиції цивільного права право на інформацію не є статичним утворенням, а трансформується під впливом технологічного розвитку, правового регулювання та загроз, пов'язаних із гібридною війною. Це відповідає загальному діалектичному принципу єдності і боротьби протилежностей, адже право на інформацію має балансувати між свободою вираження поглядів і необхідністю захисту інтересів осіб та держави від дезінформації².

¹ Збірник Рішення Європейського Суду з прав людини щодо доступу до публічної інформації. URL: https://cedem.org.ua/wp-content/uploads/2017/07/FMU_Access_2017_web-1.pdf

² Даценко А. Ю. Шляхи забезпечення балансу між свободою слова та її цензурними обмеженнями в умовах гібридної війни. *Політикус*. 2021. Вип. 1. С. 26-32.

Застосування діалектичного методу дає змогу розглядати право на інформацію як цивільне немайнове право, що кореспондує з іншими правами: правом на честь, гідність і ділову репутацію, правом на приватність, правом інтелектуальної власності тощо. У сучасних умовах гібридної війни виникає конфлікт між правом на вільний доступ до інформації та необхідністю контролю за її змістом з метою захисту громадян від маніпуляцій та інформаційного впливу з боку ворожих суб'єктів.

Діалектичний метод також дозволяє оцінити взаємозв'язок між правовими нормами та соціальними процесами. Наприклад, з одного боку, свобода інформації сприяє розвитку громадянського суспільства, забезпечуючи прозорість діяльності державних органів та можливість участі громадян у суспільних процесах. З іншого боку, у кризові періоди, такі як збройний конфлікт чи гібридна війна, свобода інформації може використовуватися для дестабілізації суспільства через поширення фейкових новин та інформаційно-психологічний вплив.

Окремим аспектом діалектичного методу є розгляд еволюції правового регулювання інформаційної сфери. Цивільне право в цьому контексті змінюється відповідно до викликів часу: від класичних норм про захист немайнових прав особи до сучасних механізмів боротьби з дезінформацією, що можуть включати цивільно-правову відповідальність за поширення неправдивої інформації, судові механізми її спростування та захисту репутації¹.

Крім того, діалектичний метод дозволяє простежити взаємозалежність між національним та міжнародним правом у сфері інформації. Так, Європейський суд з прав людини неодноразово наголошував на необхідності забезпечення свободи вираження поглядів відповідно до ст. 10 Європейської конвенції з прав людини, однак при цьому визнавав, що в умовах кризових ситуацій можуть бути обґрунтовані певні обмеження.

Таким чином, застосування діалектичного методу у дослідженні права на інформацію дозволяє: аналізувати його розвиток у взаємозв'язку з іншими правами, виявляти закономірності його трансформації під впливом сучасних загроз, оцінювати ефективність право-

¹ Відповідальність за розповсюдження недостовірної інформації. URL: <https://legalaid.gov.ua/publikatsiyi/vidpovidalnist-za-rozpovsyudzhennya-nedostovirnoyi-informacziyi/>

вого регулювання в умовах гібридної війни та пропонувати шляхи вдосконалення механізмів захисту інформаційних прав.

Інституціональний метод є важливим інструментом у дослідженні права на інформацію, особливо в умовах гібридної війни, коли право на інформацію стикається з питаннями безпеки та державного контролю. Цей метод фокусується на аналізі інституційних структур та органів, що відповідають за регулювання інформаційної сфери, а також на їхньому впливі на забезпечення прав людини в умовах кризових ситуацій. З точки зору цивільного права, інституціональний метод дозволяє вивчити роль держави та інших інститутів у реалізації та обмеженні права на інформацію, а також визначити функціонування правових органів у цьому контексті.

У межах цього методу досліджуються нормативно-правові акти, механізми правового регулювання, судові інституції та інші органи, які мають відношення до інформаційної діяльності. Наприклад, в умовах гібридної війни, роль держави стає подвійне значення: з одного боку, вона повинна забезпечити свободу доступу до інформації для громадян, а з іншого – забезпечити контроль за інформаційними потоками для попередження загроз національній безпеці. В Україні цей процес регулюється через законодавчі акти, які обмежують доступ до певних видів інформації, пов'язаних з державними таємницями або інформацією, що може загрожувати суспільному порядку¹. Таким чином, інституціональний підхід дозволяє з'ясувати, як державні органи, суди, органи контролю за медіа використовують свої повноваження для регулювання інформаційних прав та свободи слова.

В умовах гібридних війн інституціональний підхід дозволяє також дослідити роль інститутів, які відповідають за боротьбу з інформаційними загрозами, таких як системи кібервійни, національні органи, що спеціалізуються на контрінформаційних операціях, а також засоби масової інформації, які виконують функцію надання інформації громадянам. Зрозуміло, що в умовах гібридної війни, контроль за медіа та іншими джерелами інформації є важливим аспектом забезпечення національної безпеки, оскільки країна повинна бути здатною відбивати інформаційні атаки та маніпуляції. Водночас важливо, щоб цей контроль не порушував основоположні права на свободу інфор-

¹ Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал*. 2020. № 2. С. 200-203.

мації, оскільки це може спричинити порушення прав людини, зокрема у сфері цивільних немайнових прав, таких як право на свободу вираження поглядів.

Інституціональний метод дозволяє також вивчити міжнародні організації та інститути, які здійснюють контроль за правами людини та інформаційною діяльністю в умовах міжнародних конфліктів, зокрема такі органи, як ООН, ЄС, Ради Європи, а також різноманітні міжнародні судові інституції, які можуть мати вплив на забезпечення інформаційної безпеки та прав на інформацію у війнах і конфліктах. Таким чином, аналіз інституціональних механізмів, їхньої діяльності та ефективності дозволяє дійти висновку про важливість взаємодії між національними і міжнародними органами в межах правового регулювання права на інформацію.

Застосування інституціонального методу дозволяє також оцінити практичні аспекти реалізації права на інформацію, зокрема через діяльність медіа та громадських організацій, що працюють у сфері прав людини. Враховуючи важливість незалежних медіа як механізму боротьби з пропагандою в умовах гібридної війни, інституціональний підхід дозволяє розглянути роль регуляторів медіа-простору (наприклад, національних агентств з контролю за медіа) у забезпеченні балансованості між безпекою та свободою інформації.

Таким чином, застосування інституціонального методу дає змогу дослідити механізми і структури, які впливають на регулювання права на інформацію в умовах гібридної війни. Це дозволяє краще зрозуміти, як органи державної влади та інші інституції взаємодіють для забезпечення балансу між правом на свободу інформації та необхідністю контролю за інформаційними потоками.

Використання кібернетичних та комунікаційних теорій у правовому аналізі відкриває нові горизонти для розуміння та вдосконалення правових систем. Кібернетика, як наука про управління та зв'язок у складних системах, надає інструменти для моделювання правових процесів, що дозволяє підвищити їх ефективність та передбачуваність. Застосування кібернетичного підходу в праві сприяє системному аналізу правових явищ, що дозволяє виявляти закономірності та оптимізувати процеси правозастосування.

Комунікаційні теорії, зокрема ті, що стосуються інформаційних потоків та обміну даними, є фундаментальними для розуміння функ-

ціювання правових систем. Право можна розглядати як систему комунікації, де закони та нормативні акти є засобами передачі інформації від держави до громадян. Ефективність цієї комунікації впливає на рівень правосвідомості та дотримання законодавства. Дослідження в галузі інформаційно-комунікаційної діяльності підкреслюють необхідність адаптації правових норм до сучасних реалій цифрового суспільства¹.

Інтеграція кібернетичних та комунікаційних підходів у правовий аналіз дозволяє створювати моделі, які відображають динаміку правових відносин у цифровому середовищі. Це особливо актуально в контексті розвитку інформаційного суспільства, де виникають нові правові виклики, пов'язані з використанням глобальних інформаційно-комунікаційних систем. Аналіз правових проблем, пов'язаних з інформацією, стає все більш актуальним у зв'язку з підвищенням соціальної ролі інформації та розвитком глобальних мереж².

Кібернетичний підхід також сприяє розробці автоматизованих систем підтримки прийняття рішень у правовій сфері. Використання методів штучного інтелекту та експертних систем дозволяє підвищити точність і об'єктивність правозастосування, зменшуючи вплив людського фактора та можливість помилок. Це відкриває перспективи для розвитку цифрової юриспруденції, яка базується на використанні сучасних інформаційних технологій.

Комунікаційні теорії, зокрема ті, що стосуються стратегічних комунікацій, є важливими для формування правової політики та забезпечення інформаційної безпеки. Розвиток системи стратегічних комунікацій вимагає адекватних правових механізмів, що забезпечують ефективну взаємодію між державою та суспільством. Це вимагає переосмислення ролі комунікації в державному управлінні та розробки нових підходів до правового регулювання інформаційної сфери³.

¹ Інформаційно-комунікаційна діяльність: правові проблеми розвитку. URL: <https://lexinform.com.ua/dumka-eksperta/informatsijno-komunikatsijna-diyalnist-pravovi-problemy-rozvytku/>

² Демкова М., Фігель М. Інформація, як основа інформаційного суспільства: поняття та правове регулювання. URL: <https://lexinform.com.ua/dumka-eksperta/informatsijno-komunikatsijna-diyalnist-pravovi-problemy-rozvytku/>

³ Ситник Г. П., Заворітня Г. П., Марутян Р. Р. Інформаційно-комунікаційні технології у сфері національної безпеки: навчальний посібник. За заг. ред. Г. П. Ситника; ТОВ «Академпрес». Київ, 2024. 176 с.

Загалом, інтеграція кібернетичних та комунікаційних теорій у правовий аналіз сприяє більш глибокому розумінню функціонування правових систем у сучасному світі. Це дозволяє адаптувати правові норми до швидких змін інформаційного середовища, забезпечуючи ефективне регулювання та захист прав громадян у цифрову епоху.

Регулювання інформаційної політики в Україні здійснюється через комплекс нормативно-правових актів, які визначають засади інформаційної діяльності, забезпечують інформаційну безпеку та захищають права громадян у цій сфері. Основним документом, що закладає фундамент інформаційної політики, є Закон України «Про інформацію»¹. Цей закон встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного життя.

Для захисту інформації в інформаційно-телекомунікаційних системах діє Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»². Цей закон визначає правові та організаційні засади захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, встановлює обов'язки суб'єктів відносин у цій сфері та відповідальність за порушення законодавства про захист інформації.

Питання державної таємниці регулюються Законом України «Про державну таємницю»³. Цей закон визначає порядок віднесення інформації до державної таємниці, її охорони та захисту, а також встановлює відповідальність за розголошення державної таємниці.

З метою захисту персональних даних громадян прийнято Закон України «Про захист персональних даних»⁴. Цей закон регулює відносини, пов'язані із захистом персональних даних під час їх обробки, та спрямований на захист основних прав і свобод людини, зокрема права на недоторканність приватного життя у зв'язку з обробкою персональних даних.

¹ Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12> – Text

² Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр> – Text

³ Про державну таємницю: Закон України від 21 січня 1994 року № 3855-XII. URL: <https://zakon.rada.gov.ua/laws/show/3855-12> – Text

⁴ Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI URL: <https://zakon.rada.gov.ua/laws/show/2297-17> – Text

Указом Президента України № 47/2017 від 25 лютого 2017 року затверджено Доктрину інформаційної безпеки України¹, яка визначає актуальні загрози національній безпеці в інформаційній сфері та механізми протидії цим загрозам. Доктрина спрямована на забезпечення інформаційного суверенітету України, розвиток національного інформаційного простору та інтеграцію України у світовий інформаційний простір.

Основними положеннями Доктрини є визнання інформаційної агресії з боку Російської Федерації та необхідність захисту національного інформаційного простору від деструктивного впливу. Документ підкреслює важливість забезпечення інформаційного суверенітету, розвитку національних інформаційних ресурсів та інтеграції України у світовий інформаційний простір.

Доктрина також визначає основні напрями державної політики у сфері інформаційної безпеки, серед яких:

- захист інформаційного простору від зовнішніх і внутрішніх загроз;
- забезпечення кібербезпеки;
- протидія інформаційним впливам, що спрямовані на дестабілізацію суспільно-політичної ситуації в Україні;
- розвиток системи стратегічних комунікацій та підвищення рівня медіаграмотності населення.

Водночас, експерти відзначають, що Доктрина має декларативний характер і потребує конкретизації та впровадження через відповідні нормативно-правові акти та практичні заходи. Зокрема, Центр демократії та верховенства права зазначає, що документ окреслює загрози та пропонує певні дії для протидії агресії, але багато з цих положень вже були відображені в інших нормативних актах².

Загалом, Доктрина інформаційної безпеки України є важливим кроком у формуванні державної політики у сфері інформаційної безпеки, проте її ефективність залежить від конкретних дій та механізмів реалізації, спрямованих на захист національного інформаційного простору та забезпечення прав і свобод громадян.

¹ Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України №47/2017. URL: <https://www.president.gov.ua/documents/472017-21374>

² Як вплине доктрина інформаційної безпеки України на свободу слова? URL: <https://cedem.org.ua/analytics/yak-vplyne-doktryna-informatsijnoyi-bezpeky-ukrayiny-na-svobodu-slova/>

Гармонізація законодавства України з європейськими стандартами є ключовим етапом на шляху інтеграції країни до ЄС. Цей процес передбачає адаптацію національних нормативно-правових актів до *acquis communautaire* – сукупності правових норм та принципів, що діють у ЄС. Гармонізація сприяє зміцненню верховенства права в Україні та забезпечує однакове застосування норм права, що є фундаментом для ефективного функціонування правової системи.

У рамках Угоди про асоціацію між Україною та ЄС, підписаної у 2014 році, передбачено поступове наближення українського законодавства до *acquis* ЄС у сфері інформаційної політики. Зокрема, ст. 51 цієї Угоди зазначає, що сторони визнають важливою умовою для зміцнення зв'язків між Україною та Співтовариством зближення існуючого та майбутнього законодавства України з законодавством Співтовариства. Україна вживатиме заходів для забезпечення того, щоб її законодавство поступово було приведене у відповідність до законодавства Співтовариства¹.

Незважаючи на досягнутий прогрес, Україна продовжує працювати над удосконаленням законодавства у сфері права на інформацію для забезпечення повної відповідності європейським стандартам. Це включає адаптацію національних норм до нових директив та регламентів ЄС, а також впровадження найкращих практик держав-членів ЄС у сфері інформаційної політики.

В умовах гібридної війни право на інформацію, як одне з фундаментальних немайнових прав людини, зазнає певних обмежень, що ґрунтуються на необхідності забезпечення національної безпеки, громадського порядку та захисту прав інших осіб. З точки зору цивільного права, баланс між правом на доступ до інформації та державними інтересами набуває особливої важливості, оскільки неправомірні обмеження можуть призводити до порушення принципу правової визначеності, який є ключовим у регулюванні немайнових відносин.

Законодавча база України передбачає можливість запровадження інформаційних обмежень в умовах воєнного стану відповідно до Закону України «Про правовий режим воєнного стану». Стаття 8 цього закону дозволяє запроваджувати спеціальні заходи, зокрема контроль за діяльністю засобів масової інформації, обмеження доступу

¹ Дорошев А. О. Гармонізація інформаційного законодавства України та ЄС. *Наукові праці МАУП*. 2011. Вип. 1 (28). С. 175-180.

до окремих інформаційних ресурсів та заборону поширення певних відомостей. Водночас, такі обмеження мають відповідати Конституції України, яка в ст. 64 зазначає, що деякі права та свободи можуть бути обмежені лише в межах, необхідних для захисту держави. Таким чином, будь-яке обмеження інформації повинно відповідати принципу пропорційності, що закріплений у практиці Європейського суду з прав людини.

З точки зору цивільного права, інформаційні обмеження можуть впливати на право фізичних та юридичних осіб на захист ділової репутації, приватності та комерційної таємниці. Наприклад, заборона на поширення критичних матеріалів або блокування ЗМІ може призводити до зловживань та порушень прав громадян. У міжнародній практиці відомі випадки, коли держави використовували воєнний стан як привід для запровадження необґрунтованої цензури, що суперечить стандартам Європейської конвенції з прав людини (ст. 10).

В умовах сьогодення, право на інформацію передбачає низку обмежень, зокрема щодо розголошення відомостей про розташування військових об'єктів або даних, що можуть бути використані противником. Проте ці обмеження мають бути конкретизовані та піддаватися юридичній оцінці, щоб уникнути надмірного втручання у свободу інформації.

Ризики запровадження обмежень включають можливі зловживання з боку органів влади, відсутність чітких критеріїв для блокування інформації та складність у забезпеченні ефективного судового контролю. Крім того, обмеження інформації можуть негативно впливати на економічні процеси, оскільки відсутність доступу до достовірних даних створює невизначеність для бізнесу та громадянського суспільства.

Отже, регулювання інформаційної політики в умовах воєнного стану має базуватися на принципах правової визначеності, пропорційності та відповідності міжнародним стандартам. Незаконне або надмірне обмеження інформації може спричинити порушення цивільних прав громадян та юридичних осіб, тому необхідно розробити ефективні механізми контролю за діяльністю державних органів у цій сфері.

Основним завданням державної інформаційної політики в умовах гібридної війни є забезпечення інформаційного суверенітету та протидія інформаційним загрозам, що спрямовані на підри夫 довіри

до державних інституцій, дестабілізацію суспільства та маніпуляцію суспільною свідомістю.

Одним із ключових аспектів інформаційної політики є стратегічна комунікація держави. Вона передбачає узгоджену взаємодію урядових структур у сфері поширення офіційної інформації, оперативне реагування на ворожі інформаційні атаки та формування національного нарративу. Наприклад, Україна активно використовує офіційні канали комунікації, зокрема соціальні мережі, офіційні сайти державних установ та міжнародні медіа-платформи для розповсюдження перевірених даних про ситуацію в країні.

Важливим компонентом інформаційної політики є розвиток механізмів боротьби з дезінформацією. В умовах гібридної війни інформаційні атаки спрямовані на дискредитацію державних органів, маніпуляцію суспільною думкою та створення панічних настроїв. Для протидії таким загрозам застосовуються методи фактчекінгу, блокування ресурсів, які систематично поширюють неправдиву інформацію, а також підвищення рівня медіаграмотності населення. Зокрема, в Україні діють незалежні організації, такі як StopFake, що займаються перевіркою фактів та викриттям фейкових новин¹.

Окрему роль у реалізації інформаційної політики відіграє міжнародне співробітництво. Україна активно співпрацює з ЄС, НАТО та міжнародними організаціями у сфері інформаційної безпеки, беручи участь у спільних програмах із протидії пропаганді та дезінформації. Такі ініціативи сприяють обміну досвідом, зміцненню кібербезпеки та покращенню стратегічних комунікацій.

Крім того, значну увагу приділяють інформаційній реінтеграції тимчасово окупованих територій. Ворожа пропаганда на цих територіях формує викривлене уявлення про реальність та створює штучні розбіжності в суспільстві. Для подолання цих наслідків Україна здійснює мовлення на тимчасово окуповані території, підтримує локальні ініціативи, спрямовані на поширення достовірної інформації, та розвиває культурні та освітні програми, що сприяють відновленню національної ідентичності.

Таким чином, інформаційна політика України в умовах гібридної війни є багатовекторною та охоплює як заходи з протидії дезінформації, так і формування ефективної комунікації з населенням. Для під-

¹ StopFake. URL: <https://uk.wikipedia.org/wiki/StopFake>

вищення її ефективності необхідно розвивати інституційні механізми інформаційної безпеки, зміцнювати міжнародне співробітництво та розширювати можливості для медіаосвіти громадян.

Гібридна війна та введення воєнного стану істотно змінили підходи до регулювання права на інформацію в Україні. Ці умови змусили державу переглянути баланс між свободою інформації та національною безпекою, що призвело до запровадження нових обмежень, посилення контролю за інформаційними потоками та зміни в законодавстві. Одним із ключових наслідків гібридної війни стало посилення боротьби з дезінформацією та інформаційними операціями противника. У цьому контексті Україна розширила повноваження державних органів щодо блокування інформаційних ресурсів, які поширюють пропаганду та фейки. Наприклад, було ухвалено низку законодавчих актів, які дозволяють Національній раді з питань телебачення і радіомовлення та Раді національної безпеки і оборони блокувати ворожі інформаційні ресурси, забороняти діяльність про-російських медіа та вживати заходів щодо осіб, які сприяють поширенню маніпулятивної інформації.

Воєнний стан також призвів до тимчасових обмежень у сфері журналістики та свободи преси. Було введено заборони на розголошення певної інформації, що може становити загрозу для військових операцій або дати перевагу противнику. Це стосується, зокрема, даних про переміщення військ, місцезнаходження критичної інфраструктури та плани оборонних заходів. Водночас законодавство передбачає відповідальність за поширення фейкової інформації, що вводить громадян в оману та може підірвати суспільну довіру до державних органів.

Ще одним важливим аспектом змін у регулюванні права на інформацію стало посилення державної комунікаційної політики. В умовах гібридної війни влада зобов'язана оперативно реагувати на інформаційні атаки, пояснювати суспільству ухвалені рішення та запобігати паніці. Тому державні установи значно активізували роботу у соціальних мережах, розширили співпрацю з міжнародними партнерами у сфері комунікаційної безпеки та впровадили нові канали інформування громадян¹.

¹ Черниш Р. Ф. Фейк як один із інструментів негативного впливу на національну безпеку України в умовах ведення гібридної війни. *Часопис Київського університету права*. 2019. № 2. С. 109-114.

Водночас існує ризик надмірного обмеження свободи інформації під приводом захисту національної безпеки. Зловживання такими обмеженнями може призвести до звуження демократичних прав і свобод, що суперечить міжнародним стандартам у сфері прав людини. Тому важливим завданням залишається збереження балансу між державним контролем та гарантіями свободи слова, що передбачає чітке регулювання таких обмежень, їхню обґрунтованість та тимчасовий характер.

Таким чином, гібридна війна та воєнний стан значно вплинули на регулювання права на інформацію, спричинивши посилення заходів щодо протидії дезінформації, контроль за медіапростором та зміни у комунікаційній політиці держави. Водночас ці зміни мають відповідати міжнародним стандартам та забезпечувати основні права громадян, не допускаючи зловживань і порушень принципів демократичного суспільства.

Гібридна війна та воєнний стан по-різному вплинули на фізичних і юридичних осіб у контексті регулювання права на інформацію. Для фізичних осіб основні зміни пов'язані з обмеженням доступу до певних категорій інформації, зростанням відповідальності за її поширення та необхідністю адаптації до нових норм інформаційної безпеки. Юридичні особи, особливо у сфері медіа, ІТ та комунікацій, зіткнулися з новими вимогами щодо контенту, зростанням регуляторного тиску та необхідністю дотримання посилених стандартів щодо боротьби з дезінформацією.

Воєнний стан призвів до блокування ворожих інформаційних ресурсів, що обмежило можливості громадян отримувати певні види інформації. Закриття пропагандистських ЗМІ та обмеження діяльності проросійських блогерів зменшило кількість дезінформації, але водночас викликало дискусії щодо меж свободи слова. Крім того, варто зазначити, що громадяни несуть підвищену відповідальність за розповсюдження чуток, фейків та даних, які можуть загрожувати національній безпеці. Наприклад, законодавство України передбачає кримінальну відповідальність за поширення неправдивої інформації про Збройні Сили України (ст. 436-2 КК України). В умовах воєнного стану державні органи отримали розширені повноваження щодо моніторингу соціальних мереж, месенджерів та онлайн-ресурсів, що вплинуло на рівень приватності громадян. Також, гібридна війна

спричинила зростання попиту на перевірену інформацію, що змусило громадян більше довіряти офіційним державним джерелам та міжнародним ЗМІ, а також ретельніше перевіряти факти перед їхнім поширенням.

Що стосується впливу на юридичних осіб, то варто зазначити, що юридичні особи, які працюють у сфері ЗМІ, стикаються з новими вимогами до контенту. Законодавчі ініціативи, такі як Закон України «Про медіа», запроваджують жорсткіші критерії щодо недопущення дезінформації, що впливає на редакційну політику телеканалів, онлайн-видань та блогерів. Платформи, що працюють в Україні, зобов'язані оперативно реагувати на контент, який порушує національне законодавство, включаючи блокування акаунтів, що поширюють фейки. Юридичні особи несуть відповідальність за поширення неправдивої або маніпулятивної інформації, особливо якщо це стосується національної безпеки або військових дій. Компанії, що працюють у сфері маркетингу та реклами, змушені адаптувати свої кампанії до умов воєнного стану, уникаючи тем, що можуть сприйматися як провокаційні або маніпулятивні¹.

Отже, гібридна війна та воєнний стан спричинили глибокі зміни у сфері регулювання права на інформацію як для фізичних осіб, так і для юридичних осіб. Це підвищило рівень відповідальності за поширення інформації, змінило інформаційні звички громадян та посилило контроль за діяльністю ЗМІ й онлайн-платформ.

В Україні право на інформацію є однією з основоположних гарантій, закріплених Конституцією України та міжнародними актами. Однак практична реалізація цього права часто стикається з різними правовими, організаційними та технічними труднощами. Розгляд справ, пов'язаних із порушенням права на інформацію, має свою специфіку, яка визначається як особливостями національного законодавства, так і вимогами до обґрунтованості та способів захисту цього права.

Згідно з українським законодавством, справи, пов'язані з порушенням права на інформацію, зазвичай розглядаються в адміністративних судах. Ці справи стосуються доступу до публічної інформації, оскарження відмов або ненадання інформації органами державної влади або місцевого самоврядування. Закон України «Про доступ

¹ Лисич Ю. Відповідальність за поширення недостовірної інформації. URL: <https://ukrainer.gov.ua/uk/articles/vidpovidalnist-za-poshirennya-nedostovirnoyi-infor/>

до публічної інформації» передбачає механізм оскарження у разі відмови від надання інформації чи ненадання її в установлені строки. За таких обставин суди приймають рішення щодо вимоги надання інформації, що підтверджує важливу роль судової системи у забезпеченні цього права.

У разі поширення неправдивої інформації, що може завдати шкоди репутації фізичної або юридичної особи, справа розглядається в контексті цивільного або кримінального законодавства. Однією з основних категорій таких справ є позови про захист честі, гідності та ділової репутації, коли заявник оскаржує публікації, що містять недостовірні або маніпулятивні дані. За таких умов суди застосовують принципи обмеження свободи вираження поглядів, якщо це необхідно для захисту прав та інтересів інших осіб. Водночас, у зв'язку з ескалацією гібридної війни, акцент робиться на боротьбі з інформаційними атаками та фальшивими новинами, що можуть завдати шкоди національній безпеці.

У разі порушення права на інформацію, заявники можуть вимагати не тільки відшкодування матеріальної шкоди, але й моральної шкоди, особливо у випадках, коли відмова у наданні інформації чи поширення неправдивих даних спричинили серйозні соціальні чи економічні наслідки. Суд може призначити штрафи, зобов'язати до публічних вибачень або виправлення поширених відомостей, що відповідає вимогам законодавства щодо репутації та прав на інформацію.

З огляду на нові виклики, пов'язані з гібридною війною, воєнним станом і постійною еволюцією інформаційних технологій, необхідним є вдосконалення правового механізму захисту права на інформацію. Це включає створення більш чітких стандартів та процедур для розгляду справ, а також визначення механізмів взаємодії між державними органами, судовою системою та правозахисниками для забезпечення ефективного захисту цього права в умовах нових загроз.

Узагальнюючи ключові положення дослідження, можна виділити кілька важливих аспектів, які підкреслюють актуальність і складність цієї теми. Гібридна війна значною мірою змінює традиційні підходи до регулювання інформаційної політики, оскільки вона супроводжується численними маніпуляціями з інформацією, психологічними операціями та іншими методами дезінформації. Це

створює необхідність адаптації методологічних підходів до нових реалій. Методологічні підходи до регулювання права на інформацію в умовах гібридної війни повинні бути гнучкими, багатоаспектними та спрямованими на збереження балансу між необхідністю захисту національної безпеки та правами громадян на свободу інформації. Це вимагає постійного удосконалення законодавства, що відповідає сучасним викликам, а також застосування новітніх правових підходів до регулювання інформаційного простору в умовах конфлікту.

Подальші наукові дослідження повинні бути спрямовані на детальне дослідження ефективності правових інструментів, що забезпечують захист права на інформацію в умовах гібридних воєн. Зокрема, аналіз механізмів боротьби з дезінформацією та маніпуляцією інформацією через цифрові платформи дозволить знайти оптимальний баланс між свободою слова і захистом національної безпеки. Розробка та вдосконалення правових норм, які регулюють інформаційні загрози в умовах воєнного стану, допоможе створити ефективну правову базу для реагування на нові виклики сучасного інформаційного простору.

Аналіз існуючих законодавчих актів та правових норм, а також їхнього співвідношення з міжнародними стандартами у сфері інформаційної безпеки є важливим етапом у вдосконаленні правової системи України. Зокрема, необхідно досліджувати і адаптувати норми, які регулюють обмеження інформації в умовах воєнного стану, щоб ці обмеження не порушували права громадян, але при цьому ефективно захищали національну безпеку.

Таким чином, подальші наукові дослідження в цій галузі мають ключове значення для створення гнучкої правової системи, яка зможе ефективно реагувати на інформаційні загрози, що виникають у контексті гібридних воєн, і забезпечить відповідний рівень захисту прав людини в умовах сучасних інформаційних викликів.

Ключові слова: право на інформацію, методологія, методи цивільно-правового регулювання, правове регулювання, національна безпека, кібербезпека, кіберзагроза, гібридна війна, інформаційна безпека, інформаційна політика, інформаційна війна, мас-медіа в умовах гібридної війни, баланс між свободою і безпекою.