

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Кафедра цивільного права

ІТ-ПРАВО ТА КІБЕРБЕЗПЕКА В УМОВАХ ГІБРИДНОЇ ВІЙНИ

**МАТЕРІАЛИ
Всеукраїнського круглого столу**

Одеса,
12 квітня 2025 року

Одеса
Фенікс
2025

УДК 342.95 : 343.32 (477): 351.863
I-52

За загальною редакцією

доктора юридичних наук, професора **Є. Харитонova**,
кандидатки юридичних наук, доцентки **Ю. Кривенко**.

Упорядники-укладачі:

Кривенко Юлія – к.ю.н., доцентка кафедри цивільного права Національного університету «Одеська юридична академія», доцентка;

Лешкова Єлизавета – лаборантка кафедри цивільного права Національного університету «Одеська юридична академія».

ІТ-право та кібербезпека в умовах гібридної війни :
I-52 матеріали Всеукр. круглого столу (м. Одеса, 12 квіт. 2025 р.) / за заг. ред.: Є. О. Харитонova, Ю. Кривенко ; кафедра цив. права НУ «Одес. юрид. академія». – Одеса : Фенікс, 2025. – 138 с. – Режим доступу:

ISBN 978-617-8430-57-3

Збірник містить матеріали доповідей з теоретичних, історичних і методологічних проблем ІТ-права та кібербезпеки, які були оприлюднені на Всеукраїнському круглому столі «ІТ-право та кібербезпека в умовах гібридної війни» 12 квітня 2025 у Національному університеті «Одеська юридична академія».

Збірник спрямований на ознайомлення громадськості з дослідженнями науковців у сфері ІТ-права та кібербезпеки і може бути корисний як у навчальному процесі, так і в практичній діяльності.

УДК 342.95 : 343.32 (477): 351.863

*Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть
учасники конференції, їхні наукові керівники, рецензенти,
які рекомендували ці матеріали до друку.*

ISBN 978-617-8430-57-3

© Колектив авторів, 2025

© НУ «Одеська юридична академія»,
2025

Калітенко Оксана Михайлівна,
*кандидатка юридичних наук, доцентка, професорка кафедри цивільного
права Національного університету «Одеська юридична академія»*

ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ, ЯК СТРАТЕГІЧНИЙ РЕСУРС У ГІБРИДНИХ КОНФЛІКТАХ

Сучасні міжнародні конфлікти людства дедалі частіше набувають гібридного характеру, у межах якого інформаційне середовище стає не лише каналом комунікації, але й потужним інструментом впливу, знищення авторитету інституцій, маніпулювання масовою свідомістю, підризу легітимності державної влади. У цьому контексті наукове осмислення правових, політичних і технологічних аспектів функціонування інформаційного середовища як одного з головних інструментів гібридної війни набуває особливої актуальності для формування ефективних заходів правового реагування.

Інформаційне середовище останнім часом трансформувалося у визначальний фактор гібридної війни. Воно охоплює цифрові канали комунікації, соціальні мережі, штучний інтелект, алгоритми поширення контенту та віртуальні платформи. У рамках гібридної агресії інформаційне середовище виступає не лише як інструмент поширення пропаганди, але й як спосіб здійснення психологічного тиску, провокування панічних настроїв, делегітимації державної влади та створення ілюзії політичної кризи. Інформаційна агресія охоплює елементи кібертероризму, інформаційних атак, дезінформації та маніпулювання громадською думкою.

Гібридна війна – це поєднання традиційних військових дій із невійськовими засобами: політичним тиском, економічними санкціями, інформаційними та психологічними операціями. Основною метою є досягнення політичних і стратегічних результатів без оголошення повномасштабної війни. Інформаційна складова передбачає використання фейкових новин, інформаційних вкидів, атак на медіаінститути, поширення панічного або роз'єднувального контенту. Згідно з дослідженнями НАТО, у сучасних конфліктах понад 70% успіху залежить від ефективності інформаційної кампанії (NATO Strategic Communications Centre of Excellence, 2021).

Україна з 2014 року перебуває під системним впливом інформаційної агресії з боку РФ. Російські інформаційні кампанії мають на меті підрив довіри до української державності, армії, міжнародних союзників, а також маніпулювання історичною пам'яттю, етнічною ідентичністю, мовними й релігійними маркерами. Інструментами агресії виступають бот-мережі, автоматизовані платформи поширення контенту, кіберфлуди, фейкові експертні коментарі. Міністерство цифрової трансформації України у 2022–2023 роках зафіксувало понад 4 тис. випадків цілеспрямованих інформаційних атак на державні інституції та стратегічні об'єкти інфраструктури.

Сучасна міжнародна правова система наразі не містить ефективного механізму боротьби з інформаційною агресією. Наявні правові інструменти кіберзахисту, інформаційного суверенітету та відповідальності за поширення фейків є розпорошеними, а механізми юрисдикційного переслідування – складними і не гарантованими у реалізації. Водночас в Україні триває активний процес нормативного забезпечення інформаційної безпеки, зокрема ухвалено Закон України «Про національну безпеку України» (2018), «Про основи національного спротиву» (2021), а також розробляється Концепція інформаційної стійкості. Потребує вдосконалення судова практика в частині боротьби з фейками, мови ворожнечі, деструктивного контенту, що порушує національну безпеку країни.

Глобальне посилення сучасної інформаційної безпеки має здійснюватися на основі міждисциплінарного, комплексного підходу: поєднання правових, технологічних, освітніх, філософських та культурологічних стратегій. Як свідчить практика, необхідно розширювати правову експертизу щодо категорій «інформаційна атака», «цифрова суверенність», «штучна дезінформація», а також удосконалювати систему державного реагування на правопорушення в медіапросторі. Медіаосвіта, формування критичного мислення, фактчекінг, розробка національних цифрових платформ з прозорими алгоритмами – є фундаментальними інструментами формування інформаційної стійкості нації. Додатково, застосування технологій ШІ для ідентифікації фейків, бот-активності, коорди-

нованих дезінформаційних кампаній може стати елементом національної інформаційної політики.

Правова протидія інформаційним атакам в умовах гібридної війни потребує комплексного підходу, що має поєднувати як національні законодавчі ініціативи, так і участь у міжнародному правотворенні. Одним із першочергових напрямів є запровадження спеціального законодавства, яке б комплексно регулювало питання інформаційної безпеки та протидії дезінформації. Йдеться, зокрема, про нормативне закріплення таких категорій, як «інформаційна атака», «координована інформаційна операція», «деструктивний контент» тощо. Таке законодавство має визначити чіткі підстави правової відповідальності для організацій та осіб, що беруть участь в інформаційній агресії, зокрема в межах цифрових платформ і соціальних мереж. Аналогічні механізми уже успішно застосовуються у правових системах країн ЄС, наприклад у Франції (закон 2018 року про протидію інформаційним маніпуляціям) та Німеччині (NetzDG).

Наступним кроком має стати розширення кримінально-правових заходів реагування на інформаційні загрози. Йдеться про кодифікацію окремих складів злочинів, таких як умисне поширення фейкових повідомлень у період воєнного стану, публічне виправдання колабораціонізму через цифрові платформи, участь в інформаційних диверсійних структурах. Особливої актуальності набуває кваліфікуюча ознака участі в діяльності організованих груп або в координації з державою-агресором. В умовах війни такі дії мають прирівнюватися до інформаційного тероризму й розглядатися як загроза національній безпеці.

Окрему увагу слід приділити врегулюванню діяльності цифрових платформ у межах національної юрисдикції. Це передбачає запровадження правових механізмів державної взаємодії з глобальними соціальними мережами та пошуковими системами. Йдеться про обов'язок реагувати на запити держави щодо блокування інформаційного контенту, що має ознаки дезінформації, пропаганди чи мови ворожнечі, а також про вимогу прозорості алгоритмів ранжування новин. Подібні підходи уже запроваджено в Європей-

ському Союзі у межах Digital Services Act (2022), який встановлює правила відповідальності для цифрових посередників.

Важливим інструментом протидії є також розвиток національної інфраструктури стратегічних комунікацій. Йдеться не лише про оперативне спростування фейків, але й про формування стійкої інформаційної парадигми, орієнтованої на демократичні цінності, прозорість державного управління та збереження національної ідентичності. Центри стратегічних комунікацій, які об'єднують ресурси держави, медіа, академічної спільноти та громадських організацій, мають діяти на постійній основі та в координації з міжнародними партнерами. Яскравим прикладом є Центр стратегічних комунікацій та інформаційної безпеки, створений в Україні у 2021 році.

Останнім, проте ключовим, напрямом є удосконалення міжнародного правового регулювання у сфері протидії інформаційній агресії. Необхідно ініціювати створення спеціального міжнародного правового інструменту – наприклад, конвенції про цифровий суверенітет або про відповідальність за інформаційні атаки як форму агресії. Також варто визначити чіткі критерії, за яких інформаційні дії держави можуть розглядатися як порушення міжнародного гуманітарного права або Статуту ООН. З огляду на глобальну природу інформаційних загроз, лише консолідована правова позиція всіх держав світу може забезпечити ефективний захист у гібридному вимірі сучасної війни.

Кривенко Юлія Василівна,

*кандидатка юридичних наук, доцентка, доцентка кафедри цивільного права
Національного університету «Одеська юридична академія»*

ДО ПИТАННЯ СПАДКУВАННЯ ЦИФРОВОЇ РЕЧІ

Питання, що виникають у процесі спадкування майна, займають одне із ключових місць у цивільному праві. Сучасна людина накопичує безліч цифрових об'єктів впродовж життя – від електронної пошти та облікових записів у соціальних мережах до файлів, фотографій та інших даних, що зберігаються в хмарних сервісах. Після смерті власника виникає потреба передачі цих об'єктів його

Зміст

ПЕРЕДМОВА	4
Харитонов Євген Олегович ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ: ПРАВОВІ ПРОБЛЕМИ	6
Булеца Сібілла Богданівна ЦИФРОВІ АВАТАРИ: ОБ'ЄКТИ ЧИ СУБ'ЄКТИ ПРИВАТНОГО ПРАВА	10
Голубєва Неллі Юрійвна РОЗВИТОК CROSS BORDER E-COMMERCE В УКРАЇНІ	16
Давидова Ірина Віталівна ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ УКЛАДАННЯ СМАРТ-КОНТРАКТІВ	20
Менджул Марія Василівна ЦИФРОВІЗАЦІЯ ЯК ІНСТРУМЕНТ РЕАЛІЗАЦІЇ ПРАВА НА ОСВІТУ ДІТЕЙ В УМОВАХ ВІЙНИ	24
Самойленко Георгій Валерійович ДО ПИТАННЯ ВИЗНАЧЕННЯ ПРАВОВОЇ ПРИРОДИ СТАРТАПУ	27
Сафончик Оксана Іванівна ДЕЯКІ ПИТАННЯ ШЛЯБНИХ ПРАВОВІДНОСИН В ЦИФРОВУ ДОБУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ	31
Харитонova Олена Іванівна БАГАТОАСПЕКТНІСТЬ РОЗУМІННЯ «ШТУЧНОГО ІНТЕЛЕКТУ»	35
Берназ-Лукавецька Олена Михайлівна ОСОБЛИВОСТІ СТРАХУВАННЯ ПРОФЕСІЙНОЇ ВІДПОВІДАЛЬНОСТІ ІТ КОМПАНІЙ	40
Василевська Надія Станіславівна ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В СИСТЕМІ ОХОРОНИ ЗДОРОВ'Я	43
Галупова Лариса Ігорівна КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ПРАВОВОЇ ОХОРОНИ РЕЗУЛЬТАТІВ ТВОРЧОЇ ДІЯЛЬНОСТІ, СТВОРЕНИХ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ	47
Калітенко Оксана Михайлівна ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ, ЯК СТРАТЕГІЧНИЙ РЕСУРС У ГІБРИДНИХ КОНФЛІКТАХ	52
Кривенко Юлія Василівна ДО ПИТАННЯ СПАДКУВАННЯ ЦИФРОВОЇ РЕЧІ	55
Маковій Віктор Петрович ПРАВОВИЙ СТАТУС СТАРТАПУ ЯК СУБ'ЄКТА ІТ-ВІДНОСИН	59
Омельчук Олександр Сергійович ПОТЕНЦІАЛ ТА ПРОБЛЕМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ НА ДЕЙТИНГ-ПЛАТФОРМАХ	64