УДК / UDC: 34:004.8:004.056:351.86(477)
DOI: https://doi.org/10.37750/2616-6798.2026.2(57).364493

Юрій Петрович Калайда
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України
Київ, Україна
ORCID: https://orcid.org/0000-0002-1408-2145

ЮРИДИЧНІ МЕХАНІЗМИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЙНИМ КАМПАНІЯМ У МЕСЕНДЖЕРАХ ІЗ НАСКРІЗНИМ ШИФРУВАННЯМ: ПРАВО НА ПРИВАТНІСТЬ ТА НАЦІОНАЛЬНА БЕЗПЕКА

Анотація. *У статті здійснено комплексний теоретико-правовий аналіз юридичних механізмів протидії дезінформаційним кампаніям у месенджерах із наскрізним шифруванням. Досліджено специфіку зашифрованого трафіку як лакуни для класичних інструментів негласних слідчих (розшукових) дій та тимчасового доступу до речей і документів. Окрему увагу приділено аналізу європейських стандартів регулювання цифрового простору, зокрема Акта про цифрові послуги (DSA), та досвіду країн G7 щодо впровадження моделі "підзвітності алгоритмів". Визначено місце та роль вітчизняних правоохоронних органів у процесі верифікації та правового обмеження деструктивного контенту. З метою заповнення нормативних прогалин запропоновано доповнення КУпАП статтею 148-6 про адміністративну відповідальність за скоординовану неавтентичну поведінку (створення та функціонування бот-мереж) під час дії воєнного стану. Доведено, що захист інформаційного суверенітету держави в умовах гібридної агресії має реалізовуватися через баланс превентивної кіберпильності та суворого дотримання права громадян на доступ до достовірної публічної інформації про діяльність органів влади.*

***Ключові слова*:** *кібербезпека, дезінформація, наскрізне шифрування (E2EE), право на приватність, національна безпека, бот-мережі, скоординована неавтентична поведінка.*

Yurii P. Kalaida
Ukrainian Scientific and research Institute of special equipment and forensic expertise of the Security Service of Ukraine
Kyiv Ukraine
ORCID: https://orcid.org/0000-0002-1408-2145

LEGAL MECHANISMS FOR COUNTERING DISINFORMATION CAMPAIGNS IN END-TO-END ENCRYPTED MESSENGERS: THE RIGHT TO PRIVACY VS NATIONAL SECURITY

Summary: *The article provides a comprehensive theoretical and legal analysis of the legal mechanisms for countering disinformation campaigns in messengers with end-to-end encryption. The specificity of encrypted traffic is investigated as a loophole for classic tools of covert investigative actions and temporary access to things and documents. Particular attention is paid to the analysis of European standards for regulating the digital space, including the Digital Services Act (DSA), and the experience of G7 countries in implementing the "algorithmic accountability" model. The place and role of domestic law enforcement agencies in the process of verification and legal restriction of destructive content are determined. In order to fill regulatory gaps, the author proposes supplementing*

the Code of Administrative Offenses with Article 148-6, which introduces administrative liability for coordinated inauthentic behavior (creation and operation of botnets) during martial law. It is proved that the protection of the state's informational sovereignty under the conditions of hybrid aggression should be implemented through a balance of preventive cyber vigilance and strict adherence to the right of citizens to access reliable public information about the activities of authorities.

Keywords: *cybersecurity, disinformation, end-to-end encryption (E2EE), right to privacy, national security, botnets, coordinated inauthentic behavior.*

Постановка проблеми. Сучасна архітектура глобального інформаційного простору характеризується стрімким домінуванням месенджерів, що використовують технологію наскрізного шифрування (End-to-End Encryption — E2EE). Сьогодні такі платформи, як Signal, WhatsApp та окремі сегменти Telegram, стали основним інструментом не лише приватної комунікації, а й проведення масштабних дезінформаційних операцій (ІПСО), спрямованих на дестабілізацію конституційного ладу та підрив національної безпеки України. В контексті забезпечення інформаційної безпеки України однією з проблем є технічні труднощі провайдерів та правоохоронних органів здійснювати моніторинг контенту без доступу до кінцевих пристроїв користувачів, що створює “безпечну гавань” для кіберзлочинців.

У юридичній площині існує колізія між статтею 8 Конвенції про захист прав людини і основоположних свобод, яка гарантує право на повагу до приватного і сімейного життя, та інтересами національної безпеки, які вимагають превентивного виявлення загроз, у т.ч. інформаційного характеру. В умовах гібридної агресії дезінформаційні кампанії в зашифрованих середовищах стають каталізатором реальних кінетичних загроз, що змушує державу шукати нові правові інструменти, які б не порушували саму сутність демократичних свобод.

Аналіз останніх досліджень. Питання правового регулювання цифрового простору та протидії дезінформаційним кампаніям є предметом поглибленого аналізу у працях провідних українських та іноземних вчених. Різні аспекти цієї правової проблеми, зокрема в контексті використання зашифрованих месенджерів та оптимізації процесуального інструментарію під час дії воєнного стану, досліджували В. Пилипчук [1], В. Гурковський [2], О. Дзьобань[1], Д. Дубов[3], Ю. Когут[4], І. Кост [5], І. Корж [6] та ін.

Значний внесок у дослідження когнітивних та комунікативних закономірностей інформаційного протиборства, а також сутності деструктивних операцій інформаційного впливу (ІПСО) у закритих соціальних мережах зробив Г. Почепцов [7]. Його концептуальний аналіз механізмів конструювання емоцій та смислів у закритих цифрових середовищах став базовим для розуміння природи сучасного маніпулятивного контенту в месенджерах із наскрізним шифруванням [7].

Серед зарубіжних дослідників фундаментального значення набули праці Д. Кея (D. Kaye), який по-новому розкрив роль шифрування та анонімності як невід’ємних технологічних елементів забезпечення права на свободу вираження поглядів та приватність у цифрову епоху [8].

Міжнародно-правовий вимір реагування на кіберзагрози, питання атрибуції транскордонних операцій впливу та юридичні межі державного втручання в зашифровані мережі детально досліджували М. Шмітт (M. Schmitt), Р. Дейберт (R. Deibert) та Н. Цагуріас (N. Tsagourias) [9]. У свою чергу, у зарубіжній доктрині інформаційної безпеки комп’ютерних систем вагоме місце посідають роботи Б. Шнаєра

(B. Schneier), присвячені аналізу ризиків системного впровадження бекдорів для правоохоронних органів [10].

Методологію дотримання балансу інтересів безпеки та конфіденційності, зокрема крізь призму аналізу метаданих та впровадження стандартів алгоритмічної підзвітності цифрових платформ, висвітлювали у своїх працях зарубіжні експерти з питань інформаційного права – К. Кастберг (K. Kastberg) та Л. Ортолані (L. Ortolani) [11]. Дослідження цих авторів спрямовані на формування єдиних правових протоколів взаємодії між спецслужбами та провайдерами зашифрованих сервісів з метою протидії транскордонній кіберзлочинності та координованій неавтентичній поведінці без компрометації сутності права на приватність [11].

Метою цієї статті є удосконалення юридичних механізмів протидії дезінформаційним кампаніям у месенджерах із наскрізним шифруванням в умовах правового режиму воєнного стану в контексті забезпечення балансу прав людини на приватність та інтересів національної безпеки.

Виклад основного матеріалу. Наскрізне шифрування (E2EE) за своєю юридичною природою є цифровим засобом реалізації права на таємницю листування. Технологічно воно передбачає, що лише відправник та отримувач володіють ключами дешифрування, а будь-яка третя сторона, включаючи власника платформи, не має технічної можливості ознайомитися зі змістом повідомлень [12]. Це створює ситуацію, коли правоохоронні органи, навіть маючи ухвалу суду на проведення негласних слідчих розшукових дій (НСРД), отримують лише зашифрований трафік, який неможливо використати у процесі доказування [12]. Злочинці використовують цю особливість для поширення дезінформації через так звані “канали” та “закриті групи”, де контент маскується під приватну переписку. Відсутність механізмів автоматизованої модерації вмісту в E2EE-середовищах унеможливлює швидке блокування фейків, що в умовах воєнного стану може призвести до паніки серед населення або зриву мобілізаційних заходів. Організатори таких кампаній часто використовують анонімність, яку надають цифрові сервіси, зареєстровані в офшорних юрисдикціях [13].

Трансформація національного законодавства України у сфері протидії дезінформації відображає складний баланс між захистом суверенного інформаційного простору та дотриманням конституційних гарантій на приватність. В умовах гібридної агресії правовий режим забезпечення безпеки в месенджерах перейшов із площини загального нагляду в площину реагування у кіберпросторі.

У межах дослідження правових засад протидії дезінформаційним загрозам критичного значення набуває аналіз того, наскільки релевантним є інституційний інструментарій Служби безпеки України та розвідувальних органів України для забезпечення протидії сучасним викликам у сегменті месенджерів із наскрізним шифруванням (E2EE). Питання кореляції положень профільних законів України “Про Службу безпеки України” та “Про розвідку” [14] із динамікою поширення деструктивного контенту в зашифрованих середовищах визначає спроможність держави забезпечити сталий правовий режим інформаційного суверенітету.

Закон України “Про Службу безпеки України”, виступаючи фундаментом правового статусу спеціальної служби, детермінує її обов’язок щодо захисту державного суверенітету та інформаційного простору від підривної діяльності. Відповідно до статті 2 цього Закону на СБУ покладається у межах визначеної законодавством компетенції захист державного суверенітету, конституційного ладу, територіальної цілісності, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб,

посягань з боку окремих організацій, груп та осіб [15]. Однак стрімка експансія платформ із технологією E2EE виявила певну консервативність наявних процесуальних алгоритмів. Традиційна модель доступу до змісту комунікацій, заснована на співпраці з провайдерами, втрачає свою ефективність через криптографічну ізоляцію даних [12]. Це обумовлює необхідність перегляду концептуальних підходів: від прямого моніторингу трафіку до вдосконалення методик атрибуції на основі метаданих та ідентифікації мережевої активності бот-структур, що вимагає гнучкішого нормативного регулювання оперативно-розшукових заходів [12].

Важливим доповненням до архітектури національної безпеки став Закон України "Про розвідку", який трансформував підходи до виявлення загроз у цифровому середовищі [14]. Законодавча легалізація активних заходів та розвідувально-інформаційної діяльності створює передумови для нейтралізації дезінформаційних центрів за межами національного юрисдикційного периметра. Водночас практична імплементація цих повноважень стикається із процесуальною колізією в межах статті 163 КПК України, яка передбачає розгляд клопотання про тимчасовий доступ до речей і документів. За змістом цієї норми слідчий суддя постановляє ухвалу про надання тимчасового доступу до речей і документів, якщо сторона кримінального провадження у своєму клопотанні доведе наявність достатніх підстав вважати, що ці речі або документи: 1) перебувають або можуть перебувати у володінні відповідної фізичної або юридичної особи; 2) самі по собі або в сукупності з іншими речами і документами кримінального провадження, у зв'язку з яким подається клопотання, мають суттєве значення для встановлення важливих обставин у кримінальному провадженні[16]. Необхідність отримання тимчасового доступу до цифрових носіїв у зашифрованих мережах часто супроводжується надмірним процедурним обтяженням, що в умовах блискавичних дезінформаційних операцій призводить до втрати оперативності реагування. Така ситуація зумовлює потребу впровадження моделі "превентивної кіберпильності", де право на втручання в цифрову приватність чітко збалансоване з нагальними інтересами національної оборони.

Вельми важливим в даному контексті є обґрунтування доктринального переходу від парадигми "контролю вмісту" (Content Monitoring) до парадигми "структурного аналізу трафіку" (Traffic Architecture Analysis) [11]. Оскільки подолання E2EE без компрометації загальної безпеки криптосистеми неможливе, юридичні зусилля правоохоронних органів мають бути зосереджені на легітимізації методів цифрової деградації інфраструктури ворога. Це вимагає розширення правових меж щодо реалізації активної кібероборони (Active Cyber Defence). Сучасна правозастосовна практика свідчить про те, що суто оборонна стратегія захисту цифрового периметра є анахронізмом у протидії таргетованим кампаніям впливу. Відтак, пріоритетним стає питання законодавчого закріплення інструментів, спрямованих на превентивну деградацію технічної інфраструктури країни-агресора, блокування криптогаманців фінансування ботоферм та примусове видалення неавтентичних облікових записів через міжнародно-правові механізми. Таким чином, пріоритет правової охорони зміщується до захисту інформаційного суверенітету, що є безальтернативною умовою виживання держави в епоху тотальних кіберзагроз.

У контексті відсічі повномасштабній військовій агресії Російської Федерації в інформаційній сфері, Україна здійснює форсоване розгортання та модернізацію спеціального законодавства, спрямованого на превенцію та нейтралізацію ворожих пропагандистських кампаній. Особливістю сучасного етапу цієї законотворчої діяльності є її чітка євроінтеграційна векторність: вітчизняні нормативні ініціативи

системно наближаються до жорстких стандартів європейського Регламенту про цифрові послуги (Digital Services Act – DSA), що створює уніфікований правовий підхід до підзвітності цифрових платформ та модерації протиправного контенту.

У цій правовій архітектоніці ключова роль відведена спеціально уповноваженим державним органам та інституціям забезпечення інформаційної безпеки. Зокрема, стратегічною координацією заходів із протидії гібридним загрозам займається Центр протидії дезінформації (ЦПД), який у синергії з Національною радою України з питань телебачення і радіомовлення здійснює безперервний моніторинг медійного та мережевого простору. Функціональне навантаження цих структур полягає не лише у верифікації та деконструкції ворожих інформаційно-психологічних операцій (ІПСО), а й у формуванні належного юридичного та фактологічного підґрунтя для подальшого правового блокування деструктивних цифрових ресурсів і каналів комунікації.

Водночас, реалізація функції держави із забезпечення інформаційної безпеки не може відбуватися за рахунок безпідставного звуження фундаментальних прав і свобод, передбачених міжнародними договорами України. Прагнучи зберегти хиткий баланс між імперативами національної безпеки та принципами демократії, українська держава паралельно зміцнює правові гарантії прозорості й відкритості. Це знаходить своє відображення у суворому забезпеченні права на доступ до публічної інформації та закріпленні невід'ємного права громадян на отримання достовірних даних про діяльність органів державної влади, що виступає головним інституційним запобіжником проти поширення маніпулятивних наративів у суспільстві.

В даному контексті заслуговує на увагу сучасний міжнародний досвід протидії дезінформації та деструктивній пропаганді. Сучасна архітектура глобальної цифрової безпеки у 2024–2026 роках формується під впливом посилення регуляторного тиску на технологічні гіганти. Європейський Союз виступає лідером у цьому процесі, впроваджуючи механізми, що поєднують захист фундаментальних прав людини із жорстким контролем за деструктивним контентом [17]. Ключовим інструментом став Акт про цифрові послуги (DSA), який детермінує статус "дуже великих онлайн-платформ" (VLOPs) та зобов'язує їх проводити щорічний аудит системних ризиків, зокрема щодо поширення дезінформації та маніпуляцій громадською думкою. Важливо, що DSA не вимагає відмови від наскрізного шифрування, проте впроваджує принцип "підзвітної прозорості", згідно з яким провайдери мають доводити ефективність своїх алгоритмів модерації [17].

Еволюція міжнародних стандартів у 2025–2026 роках призвела до підписання країнами G7 Меморандуму про "підзвітність алгоритмів" [18]. Цей документ закріпив компромісну модель, за якої конфіденційність змісту повідомлень залишається недоторканною, проте провайдери месенджерів зобов'язуються надавати доступ до розширених метаданих (часові мітки, геолокаційні вектори, ідентифікатори пристроїв). Такий підхід дозволяє суб'єктам національної безпеки здійснювати точну атрибуцію кібератак та нейтралізувати бот-мережі шляхом трафік-аналізу, не порушуючи при цьому сутнісного змісту права на приватність. Вказана модель стає глобальним орієнтиром для демократичних держав, що прагнуть протидіяти гібридним загрозам без переходу до авторитарних методів цифрового контролю [18].

Важливим правовим прецедентом у сфері дотримання балансу інтересів стала практика Суду ЄС та ЄСПЛ, які послідовно вказують, що будь-яке втручання в приватність повинно бути "передбаченим законом", "пропорційним" та "необхідним у демократичному суспільстві" [19]. Особливої уваги заслуговує міжнародна дискусія щодо впровадження "клієнтського сканування" (Client-Side Scanning — CSS), яке

передбачає перевірку контенту на пристрої користувача до його зашифрування. Правозахисні організації та Венеціанська комісія застерігають, що впровадження таких інструментів де-факто означає знищення приватності та створення інфраструктури для тотального стеження [8]. Європейський суд з прав людини у справі "Big Brother Watch v. UK" наголосив, що масове перехоплення даних можливе лише за умови наявності незалежного нагляду та чітких законодавчих запобіжників, що виключає можливість свавільного використання CSS державними органами [19].

Для України, яка перебуває у стані повномасштабної війни, імплементація цих європейських та інших стандартів є критично важливою не лише з погляду євроінтеграції (acquis communautaire), а й як засіб підвищення легітимності дій власних спецслужб у цифровому просторі. З огляду на це, заслуговує на увагу запровадження концепції "криптографічного дуалізму" в національне інформаційне право.

Дана концепція передбачає абсолютну недоторканність змісту приватних повідомлень громадян за відсутності вироку суду, але запроваджує імперативний обов'язок для іноземних цифрових платформ (зокрема Telegram), які діють на території України, здійснювати алгоритмічне маркування автоматизованого контенту та надавати доступ до метаданих у разі верифікації координованої неавтентичної поведінки (CIB) з боку бот-мереж країни-агресора. Це дозволяє локалізувати дезінформаційні впливи на етапі їхнього зародження, не порушуючи конституційного права на таємницю комунікації. Вважаємо, що одним з шляхів протидії дезінформаційним кампаніям є встановлення адміністративної відповідальності неавтентичну поведінку із використанням бот-мереж.

На основі вищевикладеного, у порядку наукової дискусії пропонується доповнити Главу 14 КУпАП "Адміністративні правопорушення в галузі зв'язку та інформації" статтею 173-6 такого змісту:

"Стаття 173-6. Поширення дезінформації з використанням автоматизованих програмних засобів (бот-мереж)

1. Поширення через електронні комунікаційні мережі завідомо неправдивих відомостей, що можуть завдати шкоди національній безпеці, громадському порядку, здоров'ю населення або правам і свободам громадян, вчинене з використанням автоматизованих програмних засобів (бот-мереж), облікових записів, що містять неправдиві дані про особу (ботів), або шляхом скоординованої неавтентичної поведінки, — тягне накладення штрафу на громадян від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян і на посадових осіб — від тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян з конфіскацією програмних та технічних засобів, використаних для поширення зазначених відомостей.

2. Дії, передбачені частиною першою цієї статті, вчинені особою, яку протягом року було піддано адміністративному стягненню за таке саме правопорушення, —

тягнуть накладення штрафу на громадян від трьох тисяч до п'яти тисяч неоподатковуваних мінімумів доходов громадян і на посадових осіб — від п'яти тисяч до десяти тисяч неоподатковуваних мінімумів доходів громадян з конфіскацією програмних та технічних засобів.

Примітка. 1. Під дезінформацією у цій статті слід розуміти завідомо неправдиву інформацію з питань, що становлять суспільний інтерес, зокрема, щодо національної безпеки, територіальної цілісності, здоров'я та безпеки громадян.

2. Під автоматизованими програмними засобами (бот-мережами) слід розуміти сукупність облікових записів у мережах електронних комунікацій (месенджерах,

соціальних мережах), управління якими здійснюється за допомогою програмного забезпечення для масового автоматичного розповсюдження інформації".

Висновки. На підставі проведеного аналізу можна дійти висновку, що традиційні методи моніторингу вмісту є неефективними в E2EE-середовищах. Забезпечення національної безпеки зумовлює потребу переходу правоохоронних органів та спецслужб від контролю контенту до структурного аналізу метаданих та ідентифікації неавтентичних мережевих зв'язків.

На нашу думку, існуючий порядок отримання тимчасового доступу до цифрових носіїв у порядку, передбаченому ст. 163 КПК України, не відповідає швидкості поширення ІПСО. Необхідно легітимізувати інструменти активної кібероборони для превентивної технічної деградації інфраструктури дезінформаційних центрів держави-агресора.

Запровадження статті 173-6 КУпАП створює чіткий правовий механізм відповідальності за скоординовану неавтентичну поведінку із використанням бот-мереж, що дозволяє притягати винних осіб до відповідальності не за вираження поглядів (що гарантовано ст. 10 Конвенцією про захист прав людини і основоположних свобод), а за штучну автоматизовану ампліфікацію деструктивного контенту.

ПОДЯКИ: Немає

КОНФЛІКТ ІНТЕРЕСІВ: Немає

Список використаних джерел

1. Пилипчук В., Дзьобань О. Глобальні виклики й загрози національній безпеці в інформаційній сфері. *Вісник Національної академії правових наук України*. 2014. № 3 (78). С. 43-52.

2. Гурковський В.І. Сучасні медіа та протидії російській пропаганді: державно-управлінський аспект. *Публічне урядування.* 2015. № 1. С. 70-84.

3. Дубов Д. В. Фейки, пропаганда, дезінформація та виборчий процес: як нам захистити демократичні практики? Київ: ТОВ «Видавництво Сталь», 2019. 254 с.

4. Когут Ю. Гібридна війна нового типу як загроза національній безпеці держав. Сідкон. 2024. 348 с.

5. Кост І. Російська пропаганда в Україні як інформаційна складова конфлікту. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3332/3010.

6. Корж І. Сутність деструктивної пропаганди в сучасних умовах. Деструктивна пропаганда: шляхи протидії та проблеми відповідальності: матеріали науково-практичної конференці (21 травня 2015 р., м. Київ). Упорядн.: Фурашев В.М., Поперечнюк В.М. Київ. ТОВ «ІВА». 2015. С.16-21.

7. Почепцов Г. Сучасні інформаційні війни. Київ: Києво-Могилян. акад., 2015. 496 с.

8. Kaye D. Speech Police: The Global Struggle to Govern the Internet : monograph. New York : Columbia Global Reports, 2019. 160 p.

9. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations : monograph / gen. ed. M. N. Schmitt. Cambridge : Cambridge University Press, 2017. 598 p.

10. Schneier B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World : monograph. New York : W. W. Norton & Company, 2015. 384 p.

11. Kastberg K., Ortolani L. Algorithmic Accountability and Metadata Analysis in Encrypted Networks. *European Journal of Information Law*. 2025. Vol. 14, No. 3. P. 204–218.

12. Дубов Д. В. Кіберпростір як новий об'єкт міжнародного та національного права: монографія. К. НІСД, 2014. 328 с.

13. Дробюк С. Пропаганда та її види. шляхи протидії пропаганді. *Електронне наукове видання «Аналітично-порівняльне правознавство».* С.153-157. URL: http://journal-app.uzhnu.edu.ua/article/view/258841/255602. DOI: https://doi.org/10.24144/2788-6018.2022.01.28.

14. Закон України «Про розвідку» від 17.09.2020 р. № 912-IX. *Відомості Верховної Ради України*. 2020. № 47. Ст. 408.

15. Закон України «Про Службу безпеки України» від 25.03.1992 р. № 2229-XII. *Відомості Верховної Ради України*. 1992. № 27. Ст. 382.

16. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/.

17. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act). *Official Journal of the European Union*. 2022. L 277. P. 1–102.

18. G7 Leaders' Communiqué: Unity of Purpose for a Digital Age. Luxembourg, 2025. 48 p.

19. Case of Big Brother Watch and Others v. the United Kingdom (Applications nos. 58170/13, 62322/14 and 24960/15). ECHR. 2021. URL: http://hudoc.echr.coe.int/eng?i=001-210077.

Юрій Петрович Калайда
провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
03113, вул. Миколи Василенко, 3, Київ, Україна
email: yurika@i.ua

Yurii P. Kalaida
Senior Researcher of the Ukrainian Scientific and research Institute of special equipment and forensic expertise of the Security Service of Ukraine
03113, Kyiv Ukraine, M. Vasylenka Str. 3
email: yurika@i.ua

Рекомендоване цитування: Калайда Ю.П. Юридичні механізми протидії дезінформаційним кампаніям у месенджерах із наскрізним шифруванням: право на приватність та національна безпека. *Інформація і право.* № 2(57)/2026. 2026. С. 263-270. https://doi.org/10.37750/2616-6798.2026.2(57).364493

Suggested Citation: Kalaida Y. (2026) Legal Mechanisms for Countering Disinformation Campaigns in End-To-End Encrypted Messengers: The Right to Privacy vs National Security. *Information and Law*. 2(57)/2026. 263-270. https://doi.org/10.37750/2616-6798.2026.2(57).364493

Дата надходження статті до редакції: 20.05.2026 р.
Дата прийняття статті до друку після рецензування: 25.05.2026 р.
Дата публікації (оприлюднення): 26.05.2026 р.

~~~~~~~~~~~~ * * * ~~~~~~~~~~~~
~~~~~~~~~~~~