ISSN (Print) 2708-339X ISSN (Online) 2786-7498
Legal Bulletin № 3 (17), 2025

УДК 341.232:327(477.63)
DOI 10.31732/2708-339X-2025-17-C12

ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ ПРОТИДІЇ ІНФОРМАЦІЙНОМУ ТЕРОРИЗМУ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ РОСІЇ ПРОТИ УКРАЇНИ

Сидор В.Д.,
доктор юридичних наук, професор,
професор кафедри державно-правових дисциплін
Університет економіки та права «КРОК»
м. Київ, вул. Табірна, 30-32, Україна, 03113
e-mail: victoriasd@krok.edu.ua
ORCID: https://orcid.org/0000-0002-1794-2577

Перепадін К.В.,
аспірант ВНЗ «Університет економіки та права «КРОК»
м. Київ, вул. Табірна, 30-32, Україна, 03113
e-mail: perepadinkv@krok.edu.ua
ORCID: https://orcid.org/0009-0009-5205-5824

THEORETICAL AND LEGAL FOUNDATIONS OF COUNTERING INFORMATION TERRORISM IN THE CONTEXT OF MILITARY AGGRESSION BY RUSSIA AGAINST UKRAINE

Sydor V.D.,
Doctor of Legal Sciences, Professor,
Professor of the Department of State and Legal Disciplines
«KROK» University
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail: victoriasd@krok.edu.ua
ORCID: https://orcid.org/0000-0002-1794-2577

Perepadin K.V.,
Postgraduate student of the «KROK» University
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail: perepadinkv@krok.edu.ua
ORCID: https://orcid.org/0009-0009-5205-5824

Анотація*. Стаття присвячена теоретико-правовому аналізу інформаційного тероризму як ключового інструмента гібридної війни в умовах повномасштабної збройної агресії російської федерації проти України. Автор розглядає інформаційний тероризм як системну загрозу, що реалізується через дезінформаційні кампанії, кібератаки, маніпулятивні технології, спрямовані на підрив національної безпеки, створення паніки, недовіри до органів влади, а також дестабілізацію суспільства у період воєнного стану. Визначено, що чинне українське законодавство, попри наявність загальних положень про боротьбу з тероризмом і забезпечення інформаційної безпеки, не містить чіткого визначення поняття «інформаційний тероризм», що ускладнює ефективну протидію цьому явищу. У межах дослідження запропоновано концептуальну модель правового визначення інформаційного тероризму, здійснено порівняльно-правовий аналіз суміжних понять – інформаційна війна, кібертероризм, пропаганда. Проаналізовано існуючу нормативно-правову базу у сфері інформаційної безпеки, кіберзахисту та боротьби з тероризмом, зокрема Конституцію України, Закон України «Про національну безпеку», аналітичні документи РНБОУ, Стратегію інформаційної безпеки.*

Автори обґрунтовують необхідність комплексного підходу до протидії інформаційному тероризму, який має включати законодавче врегулювання, інституційне посилення, розвиток державно-приватного партнерства, міжнародну співпрацю та підвищення медіаграмотності населення. У висновках підкреслюється, що вдосконалення теоретико-правових основ протидії інформаційному тероризму є важливою умовою захисту інформаційного простору України, забезпечення інформаційної безпеки та зміцнення національної безпеки в умовах гібридної війни.

Ключові слова*: інформаційна безпека, інформаційний тероризм, гібридна війна, дезінформація, кіберзахист, національна безпека, воєнний стан.*

***Формул**: 0, рис.: 0, табл.: 0, бібл.: 9.*

***Abstract**: The article is dedicated to the theoretical and legal analysis of information terrorism as a key tool of hybrid warfare in the context of the full-scale military aggression of the Russian Federation against Ukraine. The author considers information terrorism as a systemic threat, realized through disinformation campaigns, cyber attacks, manipulative technologies aimed at undermining national security, creating panic, distrust in government authorities, and destabilizing society during a state of war. It is determined that current Ukrainian legislation, despite having general provisions on combating terrorism and ensuring information security, does not contain a clear definition of the concept of 'information terrorism,' which complicates effective counteraction against this phenomenon. Within the framework of the study, a conceptual model for the legal definition of information terrorism is proposed, and a comparative legal analysis of related concepts – information warfare, cyberterrorism, and propaganda – is carried out.*

An analysis has been conducted of the existing legal framework in the field of information security, cyber defense, and counter-terrorism, in particular the Constitution of Ukraine, the Law of Ukraine «On National Security», analytical documents of the National Security and Defense Council of Ukraine, and the Information Security Strategy.The authors argue for the necessity of a comprehensive approach to countering information terrorism, which must include legislative regulation, institutional strengthening, the development of public-private partnerships, international cooperation, and the enhancement of media literacy among the population. The conclusions emphasize that improving the theoretical and legal foundations for countering information terrorism is an important condition for protecting Ukraine's information space, ensuring information security, and strengthening national security in the context of hybrid warfare.Keywords: information security, information terrorism, hybrid warfare, disinformation, cyber defense, national security, martial law.

***Keywords**: information security, information terrorism, hybrid warfare, disinformation, cyber defense, national security, martial law.*

***Formulas**: 0, fig.: 0, tabl.: 0, bibl.: 9.*

Постановка проблеми. 24 лютого 2022 року розпочалася повномасштабна збройна агресія російської федерації проти України, яка супроводжується не лише воєнними діями, а й масштабними інформаційними атаками, що мають характер системної гібридної війни. Інформаційний тероризм виступає одним із головних інструментів агресора, спрямованим на послаблення внутрішньої стабільності України, підрив морального духу громадян, дискредитацію органів влади та створення хаосу в суспільстві. У таких умовах протидія інформаційному тероризму стає надзвичайно актуальним завданням для української держави, що потребує розробки комплексних теоретико-правових підходів і посилення законодавчого регулювання.

Аналіз останніх досліджень і публікацій. Дослідження питань інформаційної безпеки та протидії інформаційним загрозам активно розвиваються в українській і міжнародній правовій науці. Зокрема, значну увагу приділено аналізу інформаційної політики держави у сфері національної безпеки, інформаційної безпеки, права, стратегічних досліджень у працях таких науковців: В.А. Ліпкана, Б.І. Леонова, С.П. Лихової, В.П. Горбуліна, А.Б. Качинського, Д.С. Мельника, М.В. Гончарова та ін. Разом із тим, актуальними залишаються питання адаптації українського законодавства до умов ведення гібридної війни, розвитку стратегії інформаційної безпеки, підвищення ефективності протидії дезінформації та кіберзагрозам.

Не вирішені раніше частини загальної проблеми. Незважаючи на наявність ґрунтовних теоретичних напрацювань і численні публікації, недостатньо уваги приділено саме комплексному теоретико-правовому обґрунтуванню протидії інформаційному тероризму в умовах активної збройної агресії. Переважна більшість досліджень акцентує увагу на окремих аспектах медіаграмотності, боротьбі з фейками чи кібербезпеці, однак бракує цілісної концепції, що об'єднувала б правові, інформаційні та безпекові заходи в єдину стратегію. Крім того, потребують уточнення та посилення нормативно-правові механізми, здатні забезпечити ефективну протидію інформаційному тероризму на всіх рівнях: державному, регіональному та локальному.

Метою статті слід вважати комплексне визначення теоретико-правових основ протидії інформаційному тероризму в Україні під час збройної агресії росії, розкриття сутності та особливостей цього явища, аналіз чинної нормативно-правової бази, а також вироблення науково обґрунтованих пропозицій щодо удосконалення державної політики та законодавства у сфері інформаційної безпеки.

Виклад основного матеріалу. Повномасштабна збройна агресія російської федерації проти України, розпочата 24 лютого 2022 року, стала каталізатором безпрецедентних змін у всіх сферах суспільного та

державного життя. Однією з ключових особливостей цієї війни є її гібридний характер, де конвенційні бойові дії нерозривно пов'язані з масштабною інформаційно-психологічною війною. У цьому контексті феномен інформаційного тероризму набуває особливої актуальності, перетворюючись із теоретичної загрози на щоденну реальність, що вимагає глибокого наукового осмислення та вдосконалення національних теоретико-правових механізмів протидії.

Сучасна наукова доктрина не має єдиного, уніфікованого підходу до визначення поняття «інформаційний тероризм». Ця проблема ускладнюється його тісним зв'язком із суміжними категоріями, такими як «інформаційна війна», «кібертероризм», «психологічні операції» та «пропаганда». Проте, для цілей правового регулювання та ефективної протидії, необхідно чітко розмежувати ці поняття. Якщо інформаційна війна є ширшим поняттям, що охоплює комплекс заходів держави проти держави з метою завдання шкоди інформаційним ресурсам та інфраструктурі супротивника, то інформаційний тероризм має специфічні риси, що зближують його з тероризмом у класичному розумінні. На думку провідного українського науковця Ліпкана В.А., ключовою ознакою тероризму є створення обстановки страху, паніки та суспільної напруги шляхом застосування або погрози застосування насильства для впливу на прийняття рішень органами державної влади, місцевого самоврядування чи міжнародними організаціями [4, с. 58]. Інформаційний тероризм використовує ті ж самі цілі, але досягає їх специфічними методами – шляхом цілеспрямованого руйнівного впливу на інформаційну сферу. Таким чином, інформаційний тероризм можна визначити як протиправну, цілеспрямовану діяльність окремих осіб, груп чи державних акторів, що полягає у використанні інформаційної зброї (дезінформації, маніпулятивних технологій, кібератак) для створення в суспільстві стану страху, хаосу, недовіри до державних інституцій, провокування соціальних конфліктів та/або завдання шкоди критичній інфраструктурі з метою примусу держави до прийняття певних рішень або відмови від них. Об'єктом інформаційного тероризму є інформаційна безпека держави, суспільства та особистості, а також суспільні відносини, що забезпечують стабільне функціонування держави. Предметом виступає інформація, інформаційні ресурси, інформаційна інфраструктура, а також свідомість і психіка людей. Суб'єктами можуть бути як державні спецслужби (що є характерним для агресії рф), так і недержавні терористичні організації, окремі хакерські угруповання чи особи.

Нормативно-правова база України, що регулює питання протидії інформаційним загрозам, є досить розгалуженою, проте не завжди повною мірою відповідає викликам сьогодення. Основоположні принципи закладені в Конституції України, яка гарантує кожному право на свободу думки і слова, на вільне вираження своїх поглядів і переконань (ст. 34), але водночас наголошує, що здійснення цих прав може бути обмежене законом в інтересах національної безпеки [3]. Саме на цьому балансі між свободою та безпекою будується вся система протидії інформаційним загрозам. Ключовим документом у цій сфері є Закон України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII. Цей закон визначає національні інтереси, серед яких є забезпечення інформаційної безпеки, та встановлює загрози національній безпеці, зокрема «здійснення іноземними державами, недержавними структурами інформаційно-психологічного впливу» [1]. Закон закладає інституційну основу для діяльності сектору безпеки і оборони, до якого належать Служба безпеки України, Збройні Сили України, розвідувальні органи та інші структури, що безпосередньо залучені до протидії інформаційній агресії. Спеціальним нормативно-правовим актом є Закон України «Про боротьбу з тероризмом» від 20 березня 2003 року № 638-IV. Він визначає тероризм як «суспільно небезпечну діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей» [2]. Важливо, що закон у статті 1 згадує таку форму тероризму, як технологічний тероризм, що полягає у застосуванні або погрозі

застосування ядерної, хімічної, біологічної та іншої зброї масового ураження, в тому числі з використанням комп'ютерних мереж. Однак дослідники Леонов Б.І та Лихова С.П. зазначають, що поняття «інформаційний тероризм» у законі прямо не закріплене, що створює певні правові лакуни [5, с. 238]. На практиці дії, що мають ознаки інформаційного тероризму, кваліфікуються за іншими статтями Кримінального кодексу України. Кримінальний кодекс України (КК України) є основним інструментом кримінально-правової реакції на відповідні діяння. Стаття 258 «Терористичний акт» визначає відповідальність за застосування зброї, вчинення вибуху, підпалу чи інших дій, які створювали небезпеку для життя чи здоров'я людини, але прямо не охоплює суто інформаційні атаки, які не призводять до фізичних наслідків, але спричиняють паніку чи дестабілізацію. Водночас інші статті КК України можуть застосовуватися для кваліфікації окремих проявів інформаційного тероризму: стаття 109 «Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади», стаття 110 «Посягання на територіальну цілісність і недоторканність України», стаття 111 «Державна зрада», стаття 114-1 «Перешкоджання законній діяльності Збройних Сил України та інших військових формувань», а також злочини з Розділу XVI, що стосуються використання комп'ютерних мереж. Окремої уваги заслуговують стратегічні документи. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021, прямо визначає інформаційну агресію російської федерації як одну з головних загроз. Метою стратегії є «формування загальнонаціональної системи протидії дезінформації та маніпулятивній інформації, підвищення рівня медіаграмотності суспільства та забезпечення захисту інформаційного простору» [6]. Цей документ є дороговказом для всіх державних органів, проте його положення мають переважно декларативний характер і потребують конкретної імплементації на рівні законів та підзаконних актів.

Інформаційний тероризм, що здійснюється російською федерацією, має системний, добре скоординований та багатовекторний характер. Його основні цілі полягають у делегітимізації української влади через поширення наративів про «неонацистський режим», «зовнішнє управління» та «державу, що не відбулася», аби підірвати довіру населення до військово-політичного керівництва. Також ключовим завданням є деморалізація суспільства та війська шляхом розповсюдження фейків про величезні втрати, зраду командування, безперспективність спротиву, що реалізується через масовані розсилки в месенджерах та соціальних мережах для створення панічних настроїв. Крім того, агресор прагне розколоти українське суспільство, штучно розпалюючи мовні, регіональні, релігійні конфлікти та протиставляючи цивільних військовим чи біженців мешканцям приймаючих громад. Не менш важливою метою є підрив міжнародної підтримки України через дискредитацію нашої держави на міжнародній арені, поширення дезінформації про «нецільове використання» західної допомоги або «контрабанду зброї». Невід'ємною складовою цих зусиль є атаки на критичну інформаційну інфраструктуру: здійснення DDoS-атак на сайти державних органів, банків, медіа, спроби втручання в роботу енергетичних об'єктів та систем зв'язку. Як зазначається у звітах Держспецзв'язку, кількість кібератак на державні ресурси України з початку повномасштабного вторгнення зросла в кілька разів [7].

В умовах такої тотальної інформаційної війни існуюча система протидії, незважаючи на її значну стійкість та ефективність, продемонстровану з 2022 року, потребує подальшого вдосконалення. Першочерговим напрямом має стати удосконалення нормативно-правової бази, що включає законодавче закріплення чіткого визначення поняття «інформаційний тероризм». Це дозволить адекватно кваліфікувати відповідні діяння та встановити за них пропорційну юридичну відповідальність, зокрема через внесення змін до статті 258 КК України, яка має прямо передбачати відповідальність за інформаційні атаки, що мають на меті тероризування населення. Поряд із цим, нагальною є потреба в посиленні інституційної спроможності відповідальних органів. Діяльність Центру

протидії дезінформації при РНБОУ, Держспецзв'язку, кіберполіції та відповідних підрозділів СБУ має бути ще тісніше скоординованою, забезпеченою належним фінансуванням, сучасними технічними засобами моніторингу та висококваліфікованими кадрами. Це має доповнюватися активним розвитком державно-приватного партнерства, оскільки боротьба неможлива без залучення громадянського суспільства, незалежних медіа, фактчекінгових організацій та ІТ-сектору. Водночас критично важливою залишається активна міжнародна співпраця. Україна повинна ініціювати на міжнародному рівні розробку та ухвалення міжнародної конвенції про боротьбу з інформаційним тероризмом і посилювати обмін даними з розвідками країн-партнерів. Однак найефективнішим довгостроковим захистом від дезінформації є підвищення медіаграмотності населення. Запровадження системних освітніх програм на всіх рівнях та широкі інформаційні кампанії є стратегічним завданням для забезпечення стійкості суспільства до ворожих впливів.

Протидія інформаційному тероризму в умовах збройної агресії є комплексним завданням, що лежить на перетині правової, безпекової, технологічної та освітньої сфер. Ефективна відповідь на цей виклик вимагає системного підходу, політичної волі та консолідації зусиль держави, громадянського суспільства і міжнародних партнерів. Вдосконалення теоретико-правових основ є фундаментом, на якому має будуватися стійка та проактивна система захисту українського інформаційного простору від агресивних посягань ворога.

Висновки. Проведений аналіз засвідчив, що інформаційний тероризм у сучасних умовах повномасштабної збройної агресії російської федерації проти України є однією з ключових форм гібридної війни, спрямованої на підрив національної безпеки, дестабілізацію суспільства та делегітимізацію державної влади. Ця загроза має системний і багаторівневий характер, реалізується через дезінформаційні кампанії, кібератаки, маніпулятивні технології та психологічний тиск на населення.

Науковий дискурс вказує на відсутність чіткого законодавчого визначення поняття «інформаційний тероризм» у національному праві України, що створює прогалини в його правовому регулюванні та ускладнює притягнення винних до відповідальності. Наявна нормативно-правова база, хоча й передбачає загальні механізми протидії тероризму та інформаційним загрозам, потребує вдосконалення та адаптації до сучасних викликів.

З огляду на викладене, першочерговим завданням держави має стати закріплення на законодавчому рівні поняття «інформаційний тероризм», визначення його об'єктивних і суб'єктивних ознак та встановлення чіткої системи юридичної відповідальності. Не менш важливим є посилення інституційної спроможності спеціалізованих органів, розвиток державно-приватного партнерства, розширення міжнародної співпраці та створення механізмів швидкого обміну інформацією.

Ключову роль у протидії інформаційному тероризму відіграє також підвищення медіаграмотності населення та формування критичного мислення, що у довгостроковій перспективі здатне значно посилити стійкість українського суспільства до дезінформаційних атак. Отже, протидія інформаційному тероризму в умовах збройної агресії російської федерації є багатокомпонентним завданням, вирішення якого потребує комплексного підходу, злагоджених дій державних інституцій, активної участі громадянського суспільства та підтримки міжнародних партнерів. Тому вдосконалення теоретико-правових засад є фундаментальною передумовою для побудови ефективної системи захисту інформаційного простору України та забезпечення її суверенітету.

Література:

1.Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

2.Про боротьбу з тероризмом : Закон України від 20.03.2003 № 638-IV. *Відомості Верховної Ради України.* 2003. № 25. Ст. 180.

3.Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.

4.Ліпкан В. Тероризм і національна безпека України. К.: Знання, 2000. 184 с.

5.Леонов Б.І., Лихова С.П. Інформаційний тероризм як загроза національній безпеці України. *Наукові праці Київського авіаційного інституту. Серія: Юридичний вісник «Повітряне і космічне право»*. 2021, 2(59). С. 170-176. https://doi.org/10.18372/2307-9061.59.15615

6.З початку року Держспецзв'язку зафіксувала понад 1000 кіберінцидентів. *Укрінформ*. URL: https://www.ukrinform.ua/rubric-technology/3850123-z-pocatku-roku-derzspeczvazku-zafiksuvala-ponad-1000-kiberincidentiv.html (дата звернення: 10.07.2025).

7.Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41005 (дата звернення: 10.07.2025).

8.Горбулін В. П., Качинський А. Б. Гібридна війна як інструмент реалізації геостратегії реваншизму. *Стратегічні пріоритети*. 2021. № 2 (58). С. 5-12.

9.Мельник Д.С. Кібертероризм: поняття, форми прояву, перспективні заходи протидії. *Вісник Харківського національного університету внутрішніх справ.* Харків, 2023. № 3(102). С. 144-158.

References:

1.On National Security of Ukraine : Law of Ukraine dated 21.06.2018 № 2469-VIII. *Bulletin of the Verkhovna Rada of Ukraine*. 2018. № 31. 241 p.

2.On Combating Terrorism : Law of Ukraine dated 20.03.2003 № 638-IV. *Bulletin of the Verkhovna Rada of Ukraine*. 2003. № 25. 180 p.

3.Constitution of Ukraine : Law of Ukraine dated 28.06.1996 № 254k/96-VR. *Bulletin of the Verkhovna Rada of Ukraine*. 1996. № 30. 141 p.

4.Lipkan V. Terrorism and National Security of Ukraine. Kyiv: Znannya, 2000. 184 p.

5.Leonov B.I., Likhova S.P. Information Terrorism as a Threat to National Security of Ukraine. *Scientific Papers of Kyiv Aviation Institute. Series: Legal Bulletin "Air and Space Law"*. 2021. Vol. 2(59). P. 170-176. https://doi.org/10.18372/2307-9061.59.15615 (accessed: 10.07.2025).

6.From the Beginning of the Year, State Special Communications Service Recorded over 1000 Cyber Incidents. *Ukrinform*. URL: https://www.ukrinform.ua/rubric-technology/3850123-z-pocatku-roku-derzspeczvazku-zafiksuvala-ponad-1000-kiberincidentiv.html (accessed: 10.07.2025).

7.On the Decision of the National Security and Defense Council of Ukraine dated 15 October 2021 "On the Information Security Strategy" : Decree of the President of Ukraine dated 28.12.2021 № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41005 (accessed: 10.07.2025).

8.Horbulin V.P., Kachynsky A.B. Hybrid Warfare as an Instrument for Implementing the Geostrategy of Revanchism. *Strategic Priorities.* 2021. № 2(58). P. 5-12.

9.Melnyk D.S. Cyberterrorism: Concepts, Forms of Manifestation, Prospective Countermeasures. *Bulletin of Kharkiv National University of Internal Affairs*. Kharkiv, 2023. № 3(102). P. 144-158.

Стаття надійшла до друку 13 липня 2025 року