Концептуальні та нормативні основи боротьби з інформаційним тероризмом під час великомасштабної агресії російської федерації проти України: проблематика, теоретичні аспекти та практичне застосування

Костянтин Перепадін
аспірант юридичного факультету,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: perepadinkv@krok.edu.ua,
ORCID: 0009-0009-5205-5824

Повномасштабна агресія росії проти України, розпочата двадцять четвертого лютого дві тисячі двадцять другого року, актуалізувала проблематику інформаційного протиборства як невід'ємного елемента сучасної війни. Поруч із традиційними збройними засобами агресор системно застосовує інформаційно-психологічні операції, спрямовані на дезорганізацію суспільства, деморалізацію населення та підрив обороноздатності держави. Саме такі дії дослідники визначають як інформаційний тероризм – явище, яке потребує окремого правового регулювання та комплексної стратегії протидії.

Інформаційний тероризм являє собою систематичний насильницький вплив на психіку населення через інформаційні канали з метою викликати страх, паніку та дезорієнтацію. На відміну від класичної пропаганди, що прагне переконати аудиторію у певних ідеях, інформаційний терор спрямований на паралізацію волі та руйнування здатності до критичного мислення [3]. Центр протидії дезінформації при РНБО України визнає необхідність затвердження терміну "інформаційний тероризм" у міжнародній практиці.

Характерним прикладом інформаційного тероризму стало поширення у березні дві тисячі двадцять другого року маніпулятивного відео, створеного за технологією deepfake, де використовувалося зображення Президента України [5] [7]. Фальшиве відео демонструвало українського лідера, який нібито закликав військових скласти зброю та капітулювати. Подібні дії мають на меті не стільки переконати, скільки спровокувати емоційну реакцію та хаотичні дії.

Теоретичне осмислення інформаційного тероризму залишається фрагментованим. Дослідники розглядають це явище через призму різних правових категорій – від кіберзлочинності до психологічної війни. Дослідниця Дар'я Харамурза зазначає, що інформаційний тероризм руйнує медіасистему через поєднання дезінформаційних кампаній, поширення фейків і діпфейків, застосування маніпулятивних технологій та психологічного тиску [4].

Чинне українське законодавство не містить спеціалізованої норми щодо інформаційного тероризму. Кримінальний кодекс України передбачає відповідальність за терористичний акт у статтях двісті п'ятдесят вісім – двісті п'ятдесят вісім дефіс п'ять [1, 164-68], проте ці норми орієнтовані передусім на фізичні дії та матеріальні наслідки. Відповідно до статті двісті п'ятдесят вісім КК України, тероризм визначається як свідоме застосування насильства шляхом вбивств, тортур або інших посягань на життя та здоров'я людей із метою

залякування населення.

Відсутність окремої кваліфікації інформаційного тероризму створює правову невизначеність. Слідчі органи змушені кваліфікувати такі дії за суміжними статтями – про пропаганду війни (стаття чотириста тридцять шість дефіс один), посягання на територіальну цілісність (стаття сто десять) або поширення завідомо неправдивої інформації. Така ситуація ускладнює як процесуальне реагування, так і міжнародну правову співпрацю у притягненні винних до відповідальності.

На міжнародному рівні ситуація є не менш проблемною. Будапештська конвенція про кіберзлочинність дві тисячі першого року регулює технічні аспекти комп'ютерних злочинів, але не охоплює інформаційно-психологічний вплив. Жодна універсальна конвенція не визнає інформаційний тероризм окремим видом злочину, що дозволяє державам-агресорам здійснювати такі операції практично безкарно.

Російська Федерація побудувала розгалужену інфраструктуру інформаційного впливу. Європейські держави висловили стурбованість діями російської влади та активно блокували діяльність організацій, що координували фейкові акаунти у соціальних мережах. Серед інструментів впливу – організовані мережі тролів, анонімні месенджер-канали, автоматизовані бот-ферми та технології штучного інтелекту для створення синтетичного контенту.

За прогнозами Центру протидії дезінформації на червень дві тисячі двадцять п'ятого року [2], російська пропаганда продовжить кампанію з дискредитації української влади та активізує наратив про український тероризм. Такі операції спрямовані як на внутрішню аудиторію в Україні, так і на міжнародну спільноту з метою підриву довіри до української держави.

Особливу небезпеку становлять масові інформаційні атаки на цивільне населення. Сюди належать телефонні обдзвони із повідомленнями про загибель близьких, координоване поширення паніки щодо техногенних катастроф, фальсифікація офіційних повідомлень державних органів. Інформаційні ресурси, підконтрольні агресору, спрямовують свою підривну діяльність на громадянське населення з єдиною метою – посіяти страх та паніку.

Ефективне реагування на інформаційний тероризм вимагає комплексного підходу на кількох рівнях одночасно. Превентивний напрямок охоплює підвищення медіаграмотності населення, розвиток стратегічних комунікацій держави, оперативне спростування дезінформації. Україна досягла значних результатів через проекти верифікації інформації та державні комунікаційні платформи, які забезпечують швидку реакцію на інформаційні загрози.

Оперативний рівень включає моніторинг інформаційного простору, блокування ворожих ресурсів, кіберрозвідку та OCINT-дослідження. Служба безпеки України та кіберполіція напрацювали механізми швидкого виявлення та нейтралізації каналів поширення дезінформації. Втім, адміністративні процедури блокування досі потребують оптимізації та спрощення в умовах воєнного стану.

Репресивний компонент передбачає кримінальне переслідування осіб, причетних до інформаційного тероризму, застосування санкцій та міжнародні механізми притягнення до відповідальності. Дієва стратегія протидії має містити забезпечення конструктивного міфодизайну всередині України та продукування власних атак на інформаційний простір ворога [6].

Найактуальнішим завданням є створення спеціалізованого законодавства про протидію інформаційному тероризму. Такий нормативний акт має чітко визначити поняття інформаційного тероризму, встановити відповідальність через внесення нової статті до Кримінального кодексу, спростити процедури блокування загрозливого контенту під час воєнного стану. Необхідно також створити міжвідомчий координаційний центр із реальними повноваженнями та передбачити можливість екстериторіальної юрисдикції щодо іноземних громадян, які здійснюють інформаційні атаки проти України.

Без комплексної правової бази держава продовжуватиме боротьбу з інформаційним тероризмом наявними засобами, що не відповідають масштабу та специфіці загрози. Сучасна війна визначається не лише військовою потужністю, а й спроможністю контролювати інформаційний простір та захищати психологічну стійкість населення. Визнання інформаційного тероризму повноцінним видом терористичної діяльності та створення адекватної правової відповіді є критично важливими для національної безпеки України.

Ключові слова: інформаційний тероризм; боротьба з тероризмом.

Список використаних джерел

1. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 02.11.2025).

2. Прогноз Центру щодо інформаційних загроз на другу половину червня 2025 року. Центр протидії дезінформації. URL: https://cpd.gov.ua/international-direction/yevropa/prognoz-czen-tru-shhodo-informaczijnyh-zagroz-na-drugu-polovynu-chervnya-2025-roku/ (дата звернення: 02.11.2025).

3. Інформаційний тероризм. Центр протидії дезінформації. 18 серпня 2023. URL: https://cpd.gov.ua/en/report/information-terrorism-2/ (дата звернення: 02.11.2025).

4. Харамурза Д. Інформаційний тероризм як інструмент гібридної війни та фактор руйнації медіапростору. Інтегровані комунікації. 2023. № 2(16). С. 29–37. URL: https://intcom.kubg.edu.ua/index.php/journal/article/view/272 (дата звернення: 02.11.2025).

5. Ovide T. A deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn. NPR. March 17, 2022. URL: https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia

6. Інформаційний тероризм Кремля і відповідь України: потрібно діяти у двох напрямках. Радіо Свобода. 11 грудня 2018. URL: https://www.radiosvoboda.org/a/29649171.html

7. Landi M., Duffy C. Facebook, YouTube, and Twitter remove Zelensky deepfake. CNN Business. March 16, 2022. URL: https://www.cnn.com/2022/03/16/tech/deepfake-zelensky-facebook-meta/index.html