Інформаційний тероризм у російсько-українській війні: сутність, ознаки та інструменти реалізації

Information Terrorism in the Russian–Ukrainian War: The Essence, Features and Instruments of Realization

Вікторія Наместнік

Corresponding author: кандидат наук з державного управління, доцент, доцент кафедри інформаційної боротьби інституту стратегічних комунікацій, e-mail: namestnikviktoria@gmail.com, ORCID ID: https://orcid.org/0000-0002-9385-7905

Павлов Микола

доктор філософії в галузі публічного управління, e-mail: polaxn@gmail.com, ORCID ID: https://orcid.org/0000-0002-6363-9616

Національний університет оборони України, Київ, Україна

Viktoria Namestnik

Corresponding author: Candidate of Sciences in Public Administration, Associate Professor, Associate Professor of the Information Warfare Department, e-mail: namestnikviktoria@gmail.com, ORCID ID: https://orcid.org/0000-0002-9385-7905

Mykola Pavlov

Doctor of Philosophy in Public Administration, e-mail: polaxn@gmail.com, ORCID ID: https://orcid.org/0000-0002-6363-9616

National Defence University of Ukraine, Kyiv, Ukraine

Received: August 30, 2026 | Revised: September 30, 2026 | Accepted: October 31, 2026

УДК 316.485.26:316.776 + 327.88:007

DOI: https://doi.org/10.33445/sds.2026.16.5.13

Мета дослідження. Комплексне дослідження інформаційного тероризму як інструменту гібридної війни, уточненні його визначення, а також у визначенні основних рис та інструментів його реалізації в сучасному інформаційному середовищі.

Методи дослідження. Дослідження має теоретико-аналітичний характер. Застосовано концептуальний, порівняльний та дискурс-аналітичний підходи, а також кейс-орієнтований аналіз емпіричних матеріалів. Проаналізовано наукові публікації, нормативно-правові документи, офіційні заяви, медійні матеріали та аналітичні джерела.

Результати дослідження. Запропоновано авторське визначення інформаційного тероризму як цілеспрямованого систематичного використання інформації та цифрових технологій для деструктивного когнітивного впливу на волю, сприйняття і ставлення суспільства з метою залякування, примусу, підриву довіри до інституцій та впливу на управлінські й політичні рішення. Систематизовано основні ознаки та інструменти інформаційного тероризму. Обґрунтовано його відмінність від пропаганди, дезінформації та маніпулятивного втручання в інформаційне середовище через домінування ефекту страху і примусу.

Практична цінність дослідження. Запропоновані підходи можуть використовуватися для ідентифікації інформаційного тероризму, удосконалення стратегічних комунікацій, кризового реагування та підвищення інформаційної стійкості держави і суспільства.

Оригінальність дослідження. Функціональний розгляд інформаційного тероризму через характер цільового психологічного та поведінкового ефекту, авторське визначення поняття, систематизацію його ознак і інструментів з урахуванням досвіду російсько-української війни.

Обмеження результатів дослідження. Використання переважно відкритих джерел, кейс-орієнтований характер аналізу та складність безпосереднього вимірювання реального психологічного і поведінкового ефекту інформаційних впливів. Запропонований підхід потребує подальшої емпіричної перевірки на більших наборах даних.

Тип дослідження: дослідницька стаття.

Purpose. To conduct a comprehensive analysis of information terrorism as a tool of hybrid warfare, refine its definition, and identify the key characteristics and instruments of its implementation in the modern information environment.

Method. The study is theoretical and analytical. It employs conceptual, comparative, and discourse-analysis approaches, alongside a case-based analysis of empirical data. The research draws on scholarly publications, legal and regulatory documents, official statements, media materials, and analytical sources.

Results. The study proposes an original definition of information terrorism as the purposeful, systematic use of information and digital technologies to exert a destructive cognitive impact on society's will, perceptions, and attitudes, aiming to intimidate, coerce, undermine trust in institutions, and influence managerial and political decisions. The study systematizes the key features and instruments of information terrorism. The study distinguishes information terrorism from propaganda, disinformation, and manipulative interference in the information environment, highlighting fear and coercion as defining elements.

Practical implications. The proposed approaches can be utilized to identify instances of information terrorism, improve strategic communications and crisis response, and enhance the information resilience of the state and society.

Originality / value. A functional examination of information terrorism through the lens of its intended psychological and behavioral effects, an original definition of the concept, and a systematization of its characteristics and instruments, informed by the experience of the Russian–Ukrainian war.

Research limitations. The study relies primarily on open sources, employs a case-oriented approach, and is constrained by the difficulty of directly measuring the actual psychological and behavioral effects of information influence. The proposed approach requires further empirical validation using larger datasets.

Article type. Research article.

Ключові слова:. інформаційний тероризм; інформаційний простір; інформаційна безпека; інформаційно-психологічний вплив; російсько-українська війна; гібридна війна; когнітивний вплив.

Key words: Information Terrorism; Information Space; Information Security; Information-Psychological Influence; Russo-Ukrainian War; Hybrid Warfare; Cognitive Influence.

Вступ

Повномасштабна війна актуалізувала потребу розглядати інформаційний вплив не лише як сферу "переконання", а й як простір примусу: коли залякувальні повідомлення, наративи про "неминучість поразки", "невідворотні удари" чи "каральні санкції" системно масштабуються й узгоджуються з подіями на землі, вони стають інструментом психологічного тиску на населення та політичні інститути. У термінах сучасних рамок іноземного інформаційного втручання такі практики поєднують маніпуляцію, дезінформацію і сигнали ескалації, цільовим ефектом яких стає зниження стійкості суспільства і схильність до самообмеження поведінки під страхом наслідків. Саме тому операціоналізація інформаційного тероризму як окремого феномену є необхідною для точнішої діагностики загроз і вибору контрзаходів у кризових комунікаціях і безпековій політиці [9, 13, 7].

Однією з визначальних характеристик російсько-української війни є системне застосування Російською Федерацією інформаційно-психологічних операцій як складової гібридної агресії. Такий вплив Росія здійснювала задовго до початку війни з метою підготовки соціально-політичного та ідеологічного підґрунтя для майбутньої агресії. У 2022 році, з початком повномасштабного вторгнення, стратегія інформаційної війни РФ трансформувалася, набувши ознак комплексної деструктивної діяльності, спрямованої на підрив стійкості українського суспільства, деморалізацію населення, посилення панічних настроїв і дискредитацію України на міжнародній арені. Характерними рисами таких дій є надмірна агресивність, масовість і цілеспрямованість інформаційних атак, що дозволяє розглядати їх у контексті феномену інформаційного тероризму. Це поняття, хоч і не є новим, проте у науковому дискурсі все ще формується з огляду на стрімкий розвиток цифрового суспільства.

Досвід російсько-української війни засвідчує системну еволюцію методів і засобів ведення інформаційно-психологічного впливу з боку країни-агресора, що зумовлює необхідність ґрунтовного наукового аналізу феномену інформаційного тероризму. Отже, проблема дослідження інформаційного тероризму як детермінанти сучасної російсько-української війни набуває особливої актуальності та потребує подальшого теоретико-методологічного осмислення з огляду на особливості деструктивного когнітивного впливу в умовах цієї війни.

Огляд літератури

Стаття базується на попередніх наукових розвідках із кількох напрямів. Першу групу становлять напрацювання щодо інформаційної складової війни. Наприклад, П.Секеріс переосмислює роль пропаганди у сучасному конфлікті. Науковець підкреслює, що пропаганда ведеться не лише під час війни. Уряди та управлінські еліти так само намагаються впливати на думки та переконання громадян і в мирний час. Однак саме під час конфлікту інформація, яку отримує населення, зазвичай формує упереджене уявлення про кровожерливого ворога, який становить загрозу для власної системи цінностей, водночас перебільшуючи військові можливості й доблесть власного війська [25]. Варто зазначити, що саме так діє російська пропаганда, поширюючи міфи про "другу армію світу" та "Київ за три дні", "нацизм в Україні" та "необхідність захисту російськомовного населення".

Дж.Розенбік у праці "Пропаганда та ідеологія в російсько-українській війні" здійснив всебічний аналіз ролі пропаганди, ідеології та ідентичності в російсько-українській війні. Автор висловлює думку, що, незважаючи на зусилля Росії створити потужну медіа-машину вдома та за кордоном, протягом років пропаганди, яка легітимізувала присутність Росії на сході України, Росія так і не змогла озвучити переконливу альтернативу українській державності. Натомість російська пропаганда дала зворотний ефект: Україна зараз є більш єдиною, ніж будь-коли раніше [24]. Цю думку підтверджують результати соціологічного опитування у липні–серпні

2026 року – 60% респондентів вважають категорично неприйнятним передати під контроль Росії весь Донбас в обмін на гарантії безпеки. Попри нещадну кампанію бомбардувань м. Київ балістичними ракетами та іншими засобами, готовність мешканців міста схвалити таку пропозицію навіть знизилася – з 34 % до 26 %. Натомість частка тих, хто категорично проти, зросла із 62 % до 69 % [17].

Гіларі Аппел (Hilary Appel) досліджує наративи, що супроводжували початок повномасштабного вторгнення РФ в Україну у 2022 році та його наслідки. Авторка акцентує увагу на тому, який вплив мали наративи російської пропаганди на лідерів зарубіжних держав і наскільки вони формували позицію світових лідерів щодо Росії та війни в Україні [2]. Аналізу впливу російської пропаганди на іноземні держави також присвячене дослідження Д. Іррери та А. Білгіка (Irrera Daniella, Bilgic Ali). Автори розглядають дискурс і контекст повідомлень про Україну в іноземних медіа [19].

Другу групу становлять дослідження, присвячені інформаційному тероризму. Питання інформаційного тероризму здебільшого досліджується у контексті гібридної війни та забезпечення національної безпеки. Наприклад, саме в цьому контексті Р.Банк досліджував нормативно-правове закріплення інформаційного тероризму та окреслив прогалини в законодавстві України щодо регулювання цього явища [30]. Частину рекомендацій, розроблених науковцем, досі не виконано. Зокрема, не внесено змін до вітчизняного законодавства з метою закріплення термінів “інформаційний тероризм” та “інформаційний терористичний акт”.

Інформаційний тероризм як явище, що набуло нових рис у XXI ст. через глобалізацію й інформаційні технології розглядає Д. Харамурза. Зокрема, науковиця наводить принципові, на її думку, відмінності між інформаційним, медіа- та кібертероризмом [37]. Нормативно-правові колізії в частині регулювання інформаційного простору та закріплення інформаційного тероризму також досліджували Т. Лисько, О. Клімук, Д. Лисянська. Автори охарактеризували форми та класифікацію видів інформаційного тероризму в сучасному глобальному кіберпросторі [35]. Аналогічно, Г.Петришина пропонує розрізняти такі різновиди інформаційного тероризму: інформаційно-психологічний тероризм (медіатероризм) та інформаційно-технічний – кібертероризм [11]. К. Ветров та Є. Вознюк розглядають інформаційний тероризм як сучасну загрозу інформаційній безпеці європейських країн у контексті зростання кіберзагроз та поширення кіберзлочинності. Автори зазначають, що ефективна та активна боротьба європейських країн з інформаційним тероризмом відбувається в межах Європейського Союзу, усіма його країнами-членами, а також державами-сусідами й претендентами на вступ [28]. На нашу думку, кібертероризм є окремим видом злочинів, що потребують наукового обґрунтування та нормативно-правового закріплення, оскільки кіберпростір, на рівні з інформаційним (когнітивним) простором, є окремим доменом ведення війни. Разом з тим, кібератаки можуть розглядатися як додаткова складова інформаційного тероризму, але не обов’язкова.

У науковій статті [24] проведено аналіз тенденцій розвитку заходів протидії інформаційним терористичним атакам, що здійснювалися проти цілей у сфері глобальної політики у XXI столітті. Автори звертають увагу на необхідність протидії інформаційному тероризму через формування та вдосконалення нормативно-правової бази, що базується на глобальній співпраці, відкритості, прозорості, підвищенні відповідальності та проактивній державній політиці щодо протидії інформаційним терористичним атакам.

Підсумовуючи результати огляду наукових джерел, у таблиці 1 наведено порівняння найпоширеніших визначень інформаційного тероризму, що є необхідним з огляду на мету статті.

Таблиця 1. Порівняльний аналіз визначень інформаційного тероризму

Автор	Визначення	Ключова ознака
К. Герасименко	Інформаційний тероризм характеризується як множина інформаційних війн та спецоперацій, пов'язаних із національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав [31]	Комплекс інформаційних війн і спецоперацій; акцент на суб'єктах їх організації — кримінальних структурах та іноземних спецслужбах.
Р. Банк	Інформаційний терористичний акт – дії інформаційно-психологічного та інформаційно-технічного впливу, спрямовані на розв'язання суспільно-політичних, ідеологічних, національних, територіальних конфліктних ситуацій з метою маніпуляції та зомбіювання свідомості особи чи широкого кола осіб шляхом реалізації способів і методів інформаційного насильства, застосування інформаційної зброї [30]	Інформаційно-психологічне та інформаційно-технічне насильство, спрямоване на маніпулювання свідомістю.
М. Джеррод	Інформаційний тероризм – злиття фізичного насильства зі злочинним використанням інформаційних систем, а також умисне зловживання цифровими інформаційними системами, мережами або їх компонентами з метою сприяння здійсненню терористичних операцій або акцій [20]	Поєднання фізичного тероризму з кримінальним використанням цифрових інформаційних систем.
Л. Лабенко	Інформаційний тероризм — це здійснення або погроза здійснення за допомогою інформаційних технологій і/або інформаційної зброї вибуху, підпалу чи інших загально небезпечних діянь, що можуть спричинити загибель людей або інші тяжкі наслідки й спрямовані на залякування населення з метою спонукання держави, міжнародної організації, фізичної чи юридичної особи або групи осіб до здійснення чи відмови від здійснення якої-небудь дії [10]	Залякування та примушування через інформаційні технології, потенційно із заподіянням тяжкої фізичної шкоди.
В. Коршунов	Новий вид терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів, а також за допомогою протиправного використання інформаційної структури для створення умов, що тягнуть за собою тяжкі наслідки для різних сторін життєдіяльності особистості, суспільства і держави [33]	Виведення з ладу інформаційної інфраструктури та використання її для спричинення тяжких наслідків
Г. Петришин	Використання інформації та інформаційної інфраструктури задля насильства над свідомістю людей, маніпулювання їх поведінкою за допомогою певних методів і способів впливу, що дає змогу суб'єктам впливу чинити тиск на прийняття вигідних для них рішень з боку держав, груп людей або окремих осіб шляхом створення умов для хаосу, панічних настроїв тощо [11]	Маніпулювання поведінкою та рішеннями через індукцію хаосу і панічних настроїв.

Автор	Визначення	Ключова ознака
Т. Яцик	Множина інформаційних війн та спецоперацій, пов'язаних із національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав. Доступність інформаційних технологій значно підвищує ризики інформаційного тероризму [16]	Інформаційні війни та спецоперації як основна форма реалізації, посилена доступністю інформаційних технологій.

Джерело: складено авторами.

Наведені визначення демонструють відсутність єдиного усталеного підходу до розуміння інформаційного тероризму. Водночас у них повторюються три компоненти: інформаційний/технологічний інструментарій → цілеспрямований вплив → суспільно значущий результат. Відмінність полягає передусім у тому, який саме елемент автор вважає визначальним: технологію, інформаційно-психологічний вплив, терористичну мету, інфраструктурну шкоду чи поведінковий результат.

У науковій праці [29] запропоновано концепцію інформаційного тероризму та семантичне поле дезінформації. До ключових понять тероризму віднесено пропаганду, дезінформаційний наратив (як сукупність взаємопов'язаних викривлених і неправдивих фактів, подій та вражень, упорядкованих для маніпулювання свідомістю), дезінформацію (неправдиву, упереджену, викривлену інформацію маніпулятивного характеру) та фейк (імітацію новини або викривлене подання інформації з метою маніпулювання свідомістю). На нашу думку, поняття дезінформаційного наративу, дезінформації та фейку є дуже близькими, якщо не синонімічними, оскільки вони передбачають використання навмисно створеної інформації для введення в оману.

Отже, попри наявність наукових розвідок, що досліджують сутність і складові інформаційного тероризму, це поняття досі залишається недостатньо розкритим у вітчизняному науковому дискурсі. Також, на нашу думку, варто переглянути підходи до визначення інформаційного тероризму з урахуванням досвіду російсько-української війни. На сьогодні інформаційний тероризм розвивається й трансформується, стаючи однією з ключових складових сучасної когнітивної війни.

Мета даної роботи полягає в комплексному дослідженні інформаційного тероризму як інструменту гібридної війни, уточненні його визначення, а також у визначенні основних рис та інструментів його реалізації в сучасному інформаційному середовищі.

Для досягнення поставленої мети необхідно: (1) проаналізувати наукові підходи до поняття "інформаційний тероризм"; (2) відмежувати його від суміжних феноменів (пропаганда, психологічні операції, дезінформація); (3) запропонувати систему ознак і індикаторів; (4) систематизувати інструменти реалізації; (5) проаналізувати міжнародний вимір залякувально-примусових комунікацій та їхню роль у стримуванні підтримки України.

Методологія дослідження

Методологічну основу дослідження становить поєднання концептуального, порівняльного та дискурс-аналітичного підходів із кейс-орієнтованим аналізом емпіричних матеріалів. Така комбінація зумовлена комплексним характером інформаційного тероризму, який одночасно може проявлятися як форма інформаційно-психологічного впливу, комунікативна практика залякування, технологічний вплив на інформаційну інфраструктуру та інструмент політичного примусу.

Джерела дослідження формувалися за принципом тематичної та функціональної релевантності. До списку включалися: 1) наукові публікації, у яких безпосередньо

визначається або концептуалізується поняття інформаційного тероризму; 2) наукові праці щодо пропаганди, дезінформації, психологічних операцій, FIMI, когнітивного та інформаційно-психологічного впливу, використані для теоретичного розмежування суміжних явищ; 3) нормативно-правові та міжнародно-правові документи, що визначають критерії терористичного залякування, примусу та впливу на цивільне населення; 4) офіційні повідомлення державних органів та інституцій; 5) публічні заяви, медіаматеріали та комунікативні продукти, що відображають інформаційні кампанії у контексті російсько-української війни; 6) аналітичні матеріали щодо інформаційних операцій Російської Федерації та їх впливу на українську і міжнародну аудиторію.

Основний емпіричний період дослідження охоплює 2022–2026 роки, тобто період повномасштабного вторгнення РФ в Україну, протягом якого особливо виразно проявилися поєднання інформаційних, кібернетичних та кінетичних засобів впливу. Окремі матеріали, що стосуються попереднього періоду, використовувалися як теоретичний і історико-контекстуальний матеріал для встановлення генези явища, порівняння підходів та визначення трансформації інструментів інформаційного впливу.

Віднесення комунікативної практики до інформаційного тероризму здійснювалося за сукупністю функціональних критеріїв. Базовим критерієм була наявність цілеспрямованого формування страху, тривоги або відчуття неконтрольованості ситуації як проміжного психологічного механізму впливу. Другим критерієм була наявність залякувально-примусової логіки, тобто використання загрози для спонукання аудиторії до певної поведінки, самообмеження, відмови від певних дій або зміни позиції. Додатковими критеріями були: системність і повторюваність повідомлень; персоналізація загрози; використання декількох каналів поширення; прив’язка комунікації до реальних кризових або насильницьких подій; демонстрація здатності суб’єкта завдати шкоди; спрямованість на дезорганізацію соціальних зв’язків або підрив довіри до інституцій; а також наявність політичної, управлінської чи стратегічної мети. При цьому неправдивість інформації не визначалася як необхідна умова для віднесення повідомлення до інформаційного тероризму. Це обумовлено тим, що страх і примус можуть формуватися як за допомогою дезінформації, так і через реальні погрози, демонстрацію реальної спроможності завдати шкоди або інформаційний супровід фактичних насильницьких дій. Відповідно, визначальним критерієм була не істинність чи хибність повідомлення, а його функціональне призначення та очікуваний психологічний і поведінковий ефект.

Дискурс-аналіз здійснювався шляхом виявлення стійких наративних рамок, повторюваних сюжетів і способів конструювання загрози. Аналізувалися, зокрема, способи репрезентації суб’єкта загрози, адресата, передбачуваної шкоди, відповідальності за її виникнення та можливих наслідків для аудиторії. Особлива увага приділялася бінарним опозиціям “жертва/агресор”, “порядок/хаос”, “захист/знищення”, а також конструкціям неминучості, умовності та невідворотності наслідків. Окремо аналізувався зв’язок між комунікативним повідомленням і подіями «на землі»: чи передує повідомлення фізичній атаці як погроза або попередження, чи супроводжує її, чи використовується після події для пояснення, легітимації або посилення страху. Це дозволило врахувати характерну для досліджуваного феномену синхронізацію інформаційного та кінетичного впливу.

Кейс-аналіз застосовувався не як статистично репрезентативна вибірка, а як цілеспрямований відбір інформаційно-комунікативних ситуацій, що дають змогу простежити різні механізми інформаційного тероризму. Критеріями включення кейсу були: наявність чітко ідентифікованої загрози; можливість встановити її цільову аудиторію; наявність залякувального або примусового компонента; можливість простежити зв’язок між комунікацією та кризовою/насильницькою подією або політичним процесом; а також наявність достатнього масиву відкритих матеріалів для реконструкції комунікативної послідовності. Відібрані кейси охоплювали різні рівні впливу: внутрішньодержавний,

локальний і міжнародний. Зокрема, аналізувалися кібератаки на українську цифрову інфраструктуру напередодні та на початку повномасштабного вторгнення, інформаційний супровід ударів по критичній інфраструктурі України, погрози подальших ударів, комунікації щодо наслідків українських ударів по об'єктах на території Російської Федерації, а також ядерні та інші ескалаційні сигнали, адресовані міжнародній аудиторії. Такий відбір забезпечив варіативність за типом загрози, аудиторією, каналом і зв'язком із фізичними подіями.

Ознаки інформаційного тероризму сформовані шляхом послідовного узагальнення повторюваних характеристик, виявлених під час концептуального, порівняльного та дискурс-аналізу наукових джерел і емпіричних кейсів. На першому етапі фіксувалися окремі характеристики комунікативних актів: характер психологічного ефекту, форма примусу, тип наративної конструкції, часовий контекст, повторюваність, канали поширення, персоналізація та зв'язок із фізичними подіями. На другому етапі близькі характеристики об'єднувалися у концептуальні категорії. На третьому етапі кожну категорію перевіряли на наявність у кількох незалежних випадках.

Формування системи з інструментів відображає конкретні канали, технології та комунікативні практики її реалізації. У процесі аналізу емпіричного матеріалу споріднені засоби групувалися за їхнім функціональним призначенням і способом залучення до створення залякувального ефекту.

Результати дослідження

Нормативно-етичний вимір проблеми інформаційного тероризму полягає у тому, що міжнародне гуманітарне право прямо забороняє акти або погрози насильства, головною метою яких є поширення терору серед цивільного населення. Отже, залякувально-примусові комунікації у війні слід розглядати не лише як "інформаційну політику", а й як потенційно заборонену практику, якщо вони прямо спрямовані на терор цивільних [18]. Для національної правозастосовної практики важливим є узгодження запропонованої дефініції з кримінально-правовими підходами до тероризму, які фіксують умисел залякування населення та вплив на рішення органів влади. Таке узгодження дозволяє формувати доказову базу та кваліфікувати окремі інформаційні дії у сукупності з іншими злочинами (наприклад, із кібернападами або підбурюванням до насильства) [34].

Враховуючи множину наукових трактувань та поглядів, наведемо власне визначення інформаційного тероризму: інформаційний тероризм – це цілеспрямоване, системне використання інформації та цифрових технологій: для деструктивного когнітивного впливу на волю, сприйняття і ставлення суспільства, що призводить до порушення громадської безпеки, залякування населення, провокації конфліктів (у тому числі збройних конфліктів та повномасштабної війни) чи їх інформаційного супроводу; з метою впливу на прийняття (чи не прийняття) управлінських рішень органами влади всіх рівнів, державну та міжнародну політику, підриву довіри до державних та міжнародних інституцій. Акти інформаційного тероризму можуть вчинятися на міжнародному, національному (в межах конкретної держави) чи локальному (в межах певних областей або районів) рівнях.

Таке формулювання безперечно узгоджується із висновком про системний характер інформаційного тероризму як інструменту гібридної війни: його функція полягає у виснаженні, підриві довіри та деморалізації [37, 35, 38]. Разом з тим, це корелює із напрацюваннями Е. Талішинського (Elvin Talişinski), який зазначає, що інформаційний тероризм зачіпає три основні сфери: а) особистісну – коли шкода має локальний характер і стосується окремої особи; б) наукову – коли руйнуються об'єктивно закономірні логічні зв'язки перевірених наукових істин; в) суспільно-політичну – коли на національно-державному (або й глобальному) рівні вводиться в оману все населення: людство, суспільство чи спільнота численних народів і цивілізацій [12].

На рівні суспільної стійкості вирішальним є розуміння того, що інформаційний тероризм діє через короткі “вікна вразливості” після кризових подій. Саме тоді ефективними є доказово орієнтовані кризові повідомлення, попередньо підготовлені сценарії спростування, сегментована комунікація для груп ризику та обмеження вірусності панічного контенту на платформах [5, 6].

Аналітичні джерела, присвячені воєнним наративам і зовнішнім аудиторіям, показують, що російські інформаційні кампанії націлені не лише на українське суспільство, а й на країни, які підтримують Україну: формуються сюжети про “марність допомоги”, “неминучу ескалацію”, “загрозу ядерної війни” тощо [2, 3, 4, 19, 9].

З погляду інструментів, ключовим є поєднання залякування з технологічними можливостями сучасного медіасередовища: алгоритмічна вірусність, боти, цільове таргетування, синтетичний контент. Поява дипфейків ускладнює перевірку джерел і підсилює ризики панічних реакцій, а тому потребує як правових, так і комунікаційних контрзаходів [14, 15].

Зарубіжні науковці М. Девост, Б. Хоутон та Н. Поллард (Devost, M. G., Houghton, B. K., Pollard, N. A.) розглядають два ключові напрямки інформаційного тероризму: 1) коли ціллю є власне інформаційні (цифрові) технології і 2) коли інформаційні (цифрові) технології є інструментом [8]. Перший метод передбачає фізичне знищення інформаційних систем або виведення їх з ладу шляхом безпосереднього втручання (наприклад, через кібератаку). Другий метод передбачає маніпулювання публічною інформацією, поширення дезінформації, крадіжку персональних даних або іншої чутливої інформації тощо. На нашу думку, протягом російсько-української війни спостерігається використання Росією інформаційного тероризму в обох зазначених вимірах. Наприклад, у січні-лютому 2022 року, безпосередньо напередодні повномасштабного вторгнення РФ на територію України, Державна служба спеціального зв’язку та захисту інформації зафіксувала кілька кібератак на цифрову інфраструктуру України. Так, 23 лютого 2022 року масованої DDoS-атаки зазнали сайти низки державних і банківських установ, серед яких — сайти Верховної Ради, Кабінету Міністрів України, Служби безпеки України та Міністерства закордонних справ. Міністерство освіти і науки [32]. Атаки на цифрову інфраструктуру України тривали й 24 лютого 2022 року. Метою таких дій є посилення негативного емоційного ефекту, поширення паніки та хаосу, які супроводжували збройну агресію. Це один із прикладів поєднання кінетичних і некінетичних дій, що є характерною ознакою інформаційного тероризму РФ проти України.

Також протягом 2022–2026 років Росія неодноразово вдавалася до актів інформаційного тероризму як проти України загалом, так і на окремих, зокрема тимчасово окупованих, територіях. Особливістю такого інформаційного тероризму є поєднання кінетичних і некінетичних дій: масовані ракетно-дронові атаки, у тому числі на цивільну критичну інфраструктуру, – із потужним інформаційним супроводом через найдоступніші канали комунікації – соцмережі та месенджери. До прикладу, напередодні початку опалювального сезону РФ активно погрожує нанесенням ударів по об’єктах енергетичної, газової та нафтовидобувної інфраструктури України, що спричинить масове відключення електро- та теплопостачання в найхолодніший період року, зупинить роботу інших галузей промисловості та виробництва. Інформаційні повідомлення супроводжуються фізичними атаками на інфраструктуру з різною ефективністю ураження [27, 41]. Такі удари, серед іншого, мають на меті змусити цивільне населення вимагати від військово-політичного керівництва України припинення війни на вигідних для Росії умовах під тиском критичної небезпеки для життя та здоров’я.

Ще один приклад систематичного інформаційного тероризму РФ – заяви про те, що будь-які удари Збройних Сил України по інфраструктурі Росії “матимуть серйозні наслідки” та “спричинять потужні удари у відповідь” [13, 26]. Поширення цього наративу має подвійне призначення: залякати цивільне населення можливими майбутніми ударами та змістити

акценти, мовляв, Росія “не атакує, а лише відповідає на атаку”. У контексті протидії цьому наративу варто пам’ятати, що саме РФ здійснила акт агресії та розпочала повномасштабне вторгнення на територію незалежної суверенної держави. Відтак будь-яка діяльність Збройних Сил України є виключно відповіддю на агресію та захистом державного суверенітету й територіальної цілісності України.

Варто також звернути увагу на результати 40-денної операції зі спонукання РФ до завершення війни [39]. Регулярні удари по об'єктах у глибині території Російської Федерації сприяли формуванню в російського населення відчуття вразливості внутрішнього простору держави, що суперечило образу повної безпеки тилових регіонів, сформованому офіційною пропагандою. Однак після кожного успішного удару українських сил по стратегічних об'єктах інформаційний простір Росії наповнюється повідомленнями про масштабні удари по території України. При цьому інформаційний акцент зміщується з причин ударів на їхні наслідки, що дозволяє формувати в уявленнях внутрішньої аудиторії уявлення про здатність Росії повністю контролювати ескалацію конфлікту. Російські офіційні особи та пропагандистські ресурси намагаються представити власні масовані удари як “вимушену відповідь” на українські атаки. Така комунікаційна модель має на меті легітимізувати застосування сили та перекласти відповідальність за ескалацію на Україну. Водночас з позиції міжнародного гуманітарного права сам факт попереднього удару не створює правових підстав для невибіркових або непропорційних атак на цивільну інфраструктуру [18]. Російські інформаційні ресурси активно використовують окремі випадки загибелі чи поранення цивільних осіб внаслідок українських ударів для формування емоційно насичених інформаційних кампаній. При цьому такі повідомлення часто подаються без належного контексту щодо характеру уражених об'єктів, їхнього військового призначення або особливостей розміщення військової інфраструктури поблизу цивільної забудови.

Прикладом інформаційного тероризму РФ на міжнародному рівні можуть слугувати численні погрози нанесення ядерних ударів по території іноземних держав, зокрема держав-членів НАТО та ЄС [42, 43]. Для підсилення “вагомості” цього наративу було підписано указ “Про затвердження основ державної політики Російської Федерації в галузі ядерного стримування”. У зазначеному документі, серед іншого, передбачено, що підставою для завдання ядерного удару може стати “агресія проти РФ та її союзників з боку будь-якої неядерної держави за підтримки ядерної держави”, а також масована повітряна атака неядерними засобами, зокрема безпілотниками [36]. На нашу думку, поширення цього наративу стало певним фактором стримування для іноземних держав, які дотримуються політики “недопущення ескалації”, однак не вплинуло на діяльність Сил оборони України. Так, станом на серпень 2026 року Сили оборони України неодноразово завдавали ударів по російських військових і енергетичних об'єктах. За попередніми оцінками, росіяни втратили майже 43% потенціалу нафтопереробки [40]. Удари поблизу великих промислових підприємств використовуються для поширення повідомлень про нібито загрозу масштабних екологічних катастроф або порушення роботи критично важливих об'єктів. Основною метою таких інформаційних кампаній є формування негативного ставлення міжнародної аудиторії до українських далекобійних операцій.

Отже, проведений аналіз дає підстави сформулювати ключові риси інформаційного тероризму:

1) Цільовий стан аудиторії: стабільно відтворюваний психологічний результат у вигляді індукованого страху, тривоги та відчуття неконтрольованості ситуації, який виступає проміжною ланкою між повідомленням і поведінковою реакцією. Комунікаційні повідомлення структуруються як “сигнали загрози”, що поєднують опис шкоди, вказівку на суб’єкта-“винуватця” та демонстрацію безсилля інститутів захисту; таким чином забезпечується зниження готовності до спротиву й підвищення схильності до самообмеження.

2) Ефект залякування та примусу: переважання логіки “залякати, щоб змусити” над логікою “переконати, щоб залучити”. Використовується риторика умовності (“якщо… то…”), персоналізація відповідальності та демонстративне приписування собі здатності завдати шкоди; ефект підкріплюється посиланнями на реальні (кінетичні) події, що підвищує правдоподібність погроз.

3) Наративна рамка: стійка система сюжетів і категорій, що задає інтерпретацію подій через бінарні опозиції (жертва/агресор, “порядок”/”хаос”, “захист”/”знищення”), легітимізуючи примус і насильство. Наративи конструюють “моральну необхідність” дій суб’єкта інформаційного тероризму та водночас нормалізують шкоду цивільним як “неминучий побічний ефект” або “покарання”. Наративне підсилення підвищує стійкість повідомлень до спростування.

4) Часові “вікна”: підвищена ефективність впливу у короткі періоди після кризових/насильницьких подій, коли аудиторія перебуває у стані високої емоційної реактивності та інформаційного дефіциту. У ці моменти активізуються масові вкиди, “екстрені” повідомлення, псевдоінструкції та “прогнози”, спрямовані на негайні поведінкові рішення (евакуацію, відмову від участі у заходах, панічні закупівлі тощо).

5) Повторюваність та кумулятивність: систематичне повторення загроз і демонстрацій сили, яке накопичує тривожність, формує стійкі очікування небезпеки та знижує поріг прийнятності насильства. Ефект досягається циклічним відтворенням однакових меседжів через різні канали та їх узгодженням із ритмом бойових дій; повторюваність виконує роль “психологічного тиску на виснаження”.

6) Мультиканальність і екосистемність: одночасне використання традиційних медіа, соціальних платформ, месенджерів, “офіційних” комунікацій та мереж підсилення для створення ефекту всюдисущості й “очевидності”. Повідомлення циркулюють як у відкритих, так і в напівзакритих середовищах; при цьому одна й та сама теза подається у форматах новини, “експертного коментаря”, меметичного контенту й “свідчень очевидців”.

7) Персоналізація загроз: спрямування залякування на конкретні групи або категорії (мешканці певного регіону, військовослужбовці та їхні сім’ї, волонтери, лідери думок) із метою дезорганізації соціальних мереж підтримки. Механізм включає погрози, доксинг, адресні інформаційні атаки, підроблені повідомлення “від імені” знайомих/держорганів; персоналізація підвищує суб’єктивну значущість загрози.

8) Прив’язка до подій “на землі”: постійне підкріплення інформаційних погроз реальними епізодами фізичного насильства або демонстрацією здатності завдати шкоди, що підвищує довіру до меседжів. Інформаційний тероризм синхронізується з кінетичними операціями, а повідомлення формуються як “пояснення” та “попередження” до/після ударів, унаслідок чого виникає ефект причинно-наслідкового зв’язку.

Варто також додати ще один аспект – цілеспрямоване висвітлення надмірного рівня жорстокості російської армії. З одного боку, це дає нам підстави для юридичного доведення фактів вчинення воєнних злочинів. З іншого – це свідоме залякування українського суспільства шляхом постійного підсвічування жорстокості ворога. При цьому на “внутрішньому” просторі, російському, така жорстокість подається як певна “доблесть”, “героїзм”, “патріотизм” або як відповідь на нашу “жорстокість”.

Разом з тим, заслуговують уваги й інструменти реалізації інформаційного тероризму. На сьогодні такими є:

1) Традиційні медіа та мовлення. Інституціоналізовані канали легітимізації загроз через “новинний” формат і повторення. Створюється ефект офіційності й масовості; наративи підкріплюються синхронними сюжетами та “експертними включеннями.

2) Соціальні мережі. Платформи швидкого масштабування емоційного контенту, здатного формувати панічні хвилі. Використовуються алгоритмічні механізми розповсюдження, вірусність і таргетинг; контент адаптується до локальних аудиторій.

3) Месенджери та телеграм-екосистеми. Напівзакриті канали швидкого доведення погроз і псевдоінструкцій до груп ризику. Через канали/чати поширюються “зливи”, фальшиві повідомлення “від влади”, а також контент, який важко модерувати.

4) “Офіційні” заяви державних інституцій агресора. Комунікації, що підсилюють сприйняття загрози як політичної позиції та сигналу ескалації. Заяви транслюються як попередження для інших держав чи населення, формуючи міжнародний ефект стримування/примусу.

5) Псевдоекспертні мережі. Імітація наукового або аналітичного консенсусу для нормалізації загроз і легітимації насильства. Залучаються коментатори зі статусом “експертів”, які повторюють потрібні тези, посилаючись на нібито “дані” та “прогнози”.

6) Ботоферми та координовані мережі підсилення. Штучне збільшення видимості та створення ілюзії масової підтримки залякувальних меседжів. Автоматизовані акаунти продукують коментарі, репости, “свідчення очевидців”, підвищуючи охоплення і тиск на дискусію.

7) Маніпулятивні відео та дипфейки. Використання синтетичного або змонтованого контенту для підвищення емоційної переконливості й “доказовості” погроз. Дипфейки та змонтовані відео імітують “офіційні” звернення або “свідчення”, що може провокувати паніку та підривати довіру.

8) Інформаційні атаки на інфраструктуру комунікацій. Поєднання кібервпливів із комунікативним супроводом для демонстрації вразливості та підриву довіри. Технічний інцидент подається як “втрата контролю державою”, а паралельно поширюються чутки про “витоки даних” та “хаос”.

9) Спрямовані інформаційні операції проти гуманітарних практик. Делегітимація волонтерства, евакуації, допомоги як “небезпечних” або “марних”, щоб посилити відчуття безпорадності. Формуються наративи про “зраду”, “розкрадання”, “пастки” під час отримання допомоги, що зменшують готовність до взаємодії.

10) Персоналізовані погрози та доксинг. Використання розкриття персональних даних і загроз для залякування активних груп. Публікація даних супроводжується демонстративними погрозами, що створює “ефект навчання” для ширшої аудиторії.

11) Нормативно-правова риторика та квазіюридичні повідомлення. Спроба надати погрозам форму “законності” через посилання на “право” та “відповідальність”. Залякування подається як “законні наслідки”, що ускладнює його спростування та підвищує сприйняття невідворотності.

12) Зовнішньополітичні сигнали-ультиматуми. Публічні заяви, адресовані іншим державам, що спрямовані на стримування їхньої підтримки України. Сигнали супроводжуються демонстрацією ескалаційних можливостей і формують у зовнішній аудиторії відчуття зростання ризиків.

Наведені риси та інструменти реалізації інформаційного тероризму формують відносно цілісну модель примусового впливу, що поєднує наративні та технологічні засоби з “підкріпленням” у вигляді фізичного насильства. Це дозволяє розглядати інформаційний тероризм як структурний компонент гібридної війни, у якому комунікація виступає не лише супроводом дій, а й самостійним засобом виробництва страху та керованого впливу на поведінку.

Обговорення

Авторське визначення є комплексним, інтегрує кілька підходів одночасно та визначає низку принципових ознак. Безпосереднім об’єктом впливу є воля, сприйняття і ставлення суспільства, що дозволяє відмежувати інформаційний тероризм від підходів, у яких об’єктом

є інформаційна система чи інфраструктура. Також йдеться не просто про поширення інформації чи маніпуляцію, а про цілеспрямоване формування такого когнітивного стану, що спричиняє суспільно значущі наслідки. Положення про інформаційний супровід збройного конфлікту/війни дозволяє розглядати інформаційний тероризм не лише як засіб безпосереднього впливу на населення, а й як компонент ширшої конфліктної діяльності. Також передбачено перехід від індивідуального/масового психологічного ефекту до політико-управлінського результату.

Сукупність запропонованих нами рис інформаційного тероризму дозволяє відмежувати це поняття від пропаганди, яка переважно орієнтована на довгострокове переконання та мобілізацію, та від психологічних операцій у вузькому доктринальному сенсі, які можуть поєднувати переконання і примус, але не обов'язково ставлять за домінантну мету поширення страху. Водночас у практиці сучасних конфліктів ці феномени взаємодіють у межах ширших комплексів іноземного інформаційного втручання та маніпуляції, які в сучасних рамкових документах Європейського Союзу описуються як іноземні інформаційні маніпуляції та втручання (foreign information manipulation and interference, FIMI) [6]. Порівняльний аналіз інформаційного тероризму, дезінформації, пропаганди та FIMI наведено у таблиці 2.

Таблиця 2. Порівняльний аналіз за критеріями

Критерій	Інформаційний тероризм	Дезінформація	Пропаганда	FIMI
Головна мета	Залякування, примус, дезорганізація та зміна поведінки через страх	Навмисне введення в оману, формування хибного сприйняття	Формування (закріплення) певних поглядів, цінностей, ставлень	Маніпулювання інформаційним середовищем, втручання у суспільні політичні процеси
Ключовий психологічний механізм	Страх → відчуття загрози → примус → поведінкова реакція	Обман → хибне сприйняття → помилкові висновки/дії	Переконання, навіювання	Маніпуляція інформацією, поляризація, підрив довіри
Неправдивість інформації	Не обов'язково	Так	Не обов'язково	Не обов'язково
Страх як обов'язковий елемент	Так	Ні	Ні	Можливо
Примус як обов'язковий елемент	Так	Ні	Ні	Ні
Часовий фактор	Критичний: особливо важливі короткі «вікна» після атак/криз	Може бути важливим, але не визначає явище	Не обов'язково	Важливий для операцій, але не обов'язково прив'язаний до фізичної атаки
Повторюваність	Кумулятивний психологічний тиск	Посилює охоплення та ефект	Формує сталі установки	Типова для кампаній та операцій
Мультиканальність	Характерна й функціонально важлива	Може бути	Дуже характерна	Одна з центральних рис

Критерій	Інформаційний тероризм	Дезінформація	Пропаганда	FIMI
Організованість	Висока, особливо у системному застосуванні	Може бути як організованою, так і децентралізованою	Зазвичай системна, але не обов'язково	Координованість та навмисність – ключові характеристики

Джерело: складено авторами.

Наведене порівняння дає підстави стверджувати, що інформаційний тероризм не доцільно ототожнювати з дезінформацією, пропагандою або FIMI. Зазначені явища мають спільні інструменти реалізації – маніпулятивний контент, емоційне навантаження, повторення повідомлень, використання різних каналів комунікації та цільове сегментування аудиторії, – однак відрізняються домінуючою функцією інформаційного впливу.

Для дезінформації визначальною є навмисна передача неправдивої або оманливої інформації з метою введення аудиторії в оману. Водночас інформаційний тероризм може ґрунтуватися не лише на неправдивих повідомленнях: реальна загроза, реальний факт застосування насильства або демонстрація реальної спроможності завдати шкоди можуть бути використані для формування страху і примусу. Отже, критерій істинності повідомлення не може бути основним критерієм для ідентифікації інформаційного тероризму.

Пропаганда передбачає систематичне поширення ідей, оцінок та інтерпретацій з метою формування або зміни суспільних установок, переконань і поведінки. Інформаційний тероризм також може використовувати пропагандистські наративи, однак їхнє функціональне призначення в цьому випадку змінюється: вони не лише формують певну картину світу, а й конструюють і легітимують загрозу, визначають її джерело та підсилюють очікування неминучості негативних наслідків.

Відмінність від FIMI полягає насамперед у рівні аналізу. FIMI характеризує організовану та навмисну поведінку суб'єкта, спрямовану на маніпулювання інформаційним середовищем і втручання у суспільні або політичні процеси. Тому FIMI може виступати операційною рамкою, у межах якої реалізуються різні форми інформаційного впливу. Інформаційний тероризм, натомість, доцільно визначати передусім через специфічний психологічний і поведінковий результат – залякування та примус.

Таким чином, запропоновані категорії можна розмежувати за домінуючим функціональним критерієм: дезінформація спрямована на введення в оману, пропаганда – на формування переконань і установок, FIMI – на маніпулятивне втручання в інформаційне середовище, тоді як інформаційний тероризм – на формування страху та використання цього стану для залякування, примусу або дезорганізації цільової аудиторії.

Водночас зазначені явища не є взаємовиключними. Одна інформаційна операція може одночасно містити дезінформаційні повідомлення, використовувати пропагандистські наративи, реалізовуватися в межах FIMI та мати ознаки інформаційного тероризму. Тому інформаційний тероризм доцільно розглядати не як альтернативу цим явищам, а як окремий функціональний вимір інформаційного впливу, який визначається передусім характером цільового психологічного та поведінкового ефекту.

Висновки

Проведене дослідження дозволило уточнити зміст поняття інформаційного тероризму та обґрунтувати доцільність його розгляду як самостійного інструменту гібридної війни, спрямованого на досягнення політичних і військових цілей шляхом системного залякування населення, підриву довіри до державних інституцій та примусу до прийняття агресору вигідних рішень. На відміну від суміжних форм інформаційного впливу, визначальною

ознакою інформаційного тероризму є домінування примусового механізму впливу, в основі якого лежить цілеспрямоване формування страху як інструменту керування поведінкою окремих осіб, соціальних груп і держав.

У результаті дослідження запропоновано авторське визначення інформаційного тероризму, систематизовано його основні ознаки та інструменти реалізації. Встановлено, що ефективність інформаційного тероризму забезпечується комплексним використанням традиційних і цифрових медіа, соціальних мереж, месенджерів, кібератак, ботомереж, синтетичного контенту, офіційної політичної риторики та інших взаємопов'язаних засобів впливу. Їхня синхронізація з кінетичними діями створює кумулятивний психологічний ефект, який істотно посилює вплив інформаційних кампаній на суспільство.

Досвід російсько-української війни підтверджує, що Російська Федерація системно застосовує інформаційний тероризм як складову комплексної воєнної стратегії. Інформаційний супровід ракетних ударів, кібератак, ядерного шантажу, погроз ескалації та інших примусових комунікацій спрямований не лише на українське суспільство, а й на міжнародну аудиторію з метою зниження рівня підтримки України, стримування партнерів і формування вигідного для агресора інформаційного середовища.

Практична цінність одержаних результатів полягає у можливості використання запропонованих підходів для ідентифікації ознак інформаційного тероризму, удосконалення механізмів стратегічних комунікацій, кризового реагування та розроблення заходів із підвищення стійкості держави й суспільства до інформаційно-психологічних впливів.

Перспективи подальших досліджень доцільно пов'язати з розробленням методик оцінювання інформаційного тероризму, створенням систем раннього виявлення відповідних інформаційних кампаній, дослідженням впливу штучного інтелекту й синтетичних медіа на еволюцію інформаційного тероризму, а також удосконаленням міжнародних і національних правових механізмів протидії йому.

Обмеження дослідження. Проведене дослідження має низку обмежень, які необхідно враховувати під час інтерпретації отриманих результатів. По-перше, інформаційний тероризм залишається концептуально та термінологічно дискусійним явищем, щодо якого у науковій літературі відсутнє єдине загальновизнане визначення. Запропонована в роботі дефініція та система критеріїв ґрунтуються на функціональному підході, у межах якого визначальними є залякування, формування страху та використання цього стану для примусу. Тому результати дослідження відображають авторську концептуалізацію явища та потребують подальшої теоретичної й емпіричної верифікації.

По-друге, емпіричний матеріал охоплює переважно публічно доступні джерела та кейси російсько-української війни 2022–2026 років. Це обмежує можливість аналізу закритих інформаційних операцій, внутрішніх комунікацій організаторів впливу, алгоритмів таргетування та інших компонентів, недоступних для зовнішнього спостереження. Відповідно, висновки щодо намірів суб’єктів інформаційного впливу в окремих випадках ґрунтуються на реконструкції комунікативного контексту та сукупності доступних індикаторів, а не на безпосередньому доступі до планів або внутрішніх документів відповідних суб’єктів.

По-третє, кейс-аналіз у дослідженні не має на меті забезпечення статистичної репрезентативності. Відібрані випадки використовувалися для виявлення та порівняння механізмів, ознак і способів реалізації інформаційного тероризму. Тому отримані результати не можна автоматично екстраполювати на всі інформаційні кампанії Російської Федерації або на всі сучасні збройні конфлікти. Для перевірки універсальності запропонованої моделі необхідні ширші корпуси даних та порівняльні дослідження інших конфліктів і суб’єктів.

По-четверте, визначення психологічного та поведінкового ефекту інформаційного тероризму залишається методологічно складним. Аналіз публічних повідомлень дає змогу встановити наявність залякувальних конструкцій, повторюваність загроз, їхню персоналізацію,

мультиканальність та зв'язок із подіями, однак не завжди дозволяє безпосередньо виміряти реальний рівень страху аудиторії або довести причинно-наслідковий зв'язок між конкретним інформаційним повідомленням і подальшою поведінкою населення чи політичних інституцій. Відтак поняття "очікуваного" або "цільового" психологічного ефекту в окремих кейсах не слід ототожнювати з емпірично доведеним фактичним ефектом.

По-п'яте, динамічний характер інформаційного середовища створює часові обмеження для запропонованої моделі. Нові технології генерації синтетичного контенту, зміни алгоритмів платформ, розвиток автоматизованих мереж поширення інформації та трансформація тактик інформаційно-психологічного впливу можуть змінювати форми реалізації інформаційного тероризму швидше, ніж встановлюються відповідні наукові критерії для його ідентифікації. Тому запропонована система ознак та інструментів має розглядатися як така, що може потребувати подальшого уточнення відповідно до розвитку інформаційного середовища.

Нарешті, дослідження зосереджене передусім на концептуалізації, ідентифікації та описі механізмів інформаційного тероризму і не передбачає кількісного вимірювання його ефективності або порівняльного оцінювання результативності різних способів протидії. Це визначає перспективу подальшої перевірки запропонованих критеріїв на більших масивах даних, розроблення кількісних індикаторів інтенсивності та результативності інформаційного тероризму, а також проведення порівняльних досліджень у різних конфліктах і інформаційних середовищах.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Використання штучного інтелекту

Автори заявляють, що використовували ШІ для перевірки правопису.

Список використаних джерел

1. Leonov B., Lykhova S. (2021) Information Terrorism as a Threat to the National Security of Ukraine. *Air and Space Law*. 2(59), 170–176. DOI: https://doi.org/10.18372/2307-9061.59.15615
2. Appel Hillary (2024) "Competing narratives of the Russia–Ukraine war: Why the West hasn't convinced the rest," Global Policy, London School of Economics and Political Science, vol. 15(4), pages 559-569, September. DOI: https://doi.org/10.1111/1758-5899.13431
3. Aspriadis, N. (2023). Preparing for War: Strategic Narratives and Disinformation in Leadership Rhetoric during the Ukraine War. *ESSACHESS – Journal for Communication Studies*, *16*(1(31), 21-41. https://doi.org/10.21409/9037-1Y61
4. Bradshaw, S., Elswah, M., Haque, M., & Quelle, D. (2024). Strategic storytelling: Russian state-backed media coverage of the Ukraine war. International Journal of Public Opinion Research, 36(3), edae028. DOI: https://doi.org/10.1093/ijpor/edae028
5. Center for Civilians in Conflict. (2023). When words become weapons: A human-centered approach to understanding and countering hate speech and incitement in conflict. https://www.civiliansinconflict.org/wp-content/uploads/2023/11/CIVIC_Disinformation_Report.pdf
6. Council conclusions on Foreign Information Manipulation and Interference (FIMI) https://data.consilium.europa.eu/doc/document/ST-11429-2022-INIT/en/pdf

7. Namestnik V., Klunnyk M. (2024) Russian information operations against Ukraine in 2022–2023: conclusions, recommendations, lessons learned. Science and Defence, №2 (2024). С. 58-64. DOI: https://doi.org/10.33099/2618-1614-2024-25-2-58-64
8. Devost, M. G., Houghton, B. K., & Pollard, N. A. (1997). Information terrorism: Political violence in the information age. Terrorism and Political Violence, 9(1), 72–83. DOI: https://doi.org/10.1080/09546559708427387
9. Digital Forensic Research Lab. (2024) Undermining Ukraine: How Russia widened its global information war in 2023. Atlantic Council. https://surl.li/hbcjmb
10. Mytko A. M., Koltsova I. I. (2018) Information terrorism as a tool of influence on information conformism in the global environment. *Political Life*. 2. DOI: https://doi.org/10.31558/2519-2949.2018.2.22
11. Петришин Г. Р. Інформаційний тероризм: джерела формування та активізації в Україні // Габітус : науковий журнал. Одеса : Гельветика, 2021. Вип. 21. С. 44–50. DOI: https://doi.org/10.32843/2663- 5208.2021.21.7
12. Talişinski E. Information Terrorism As a Form of International Terrorism. *Dünya İnsan Bilimleri Dergisi*. 2023(2), 127–134 DOI: https://doi.org/10.55543/insan.1244109
13. Путин назвал удары РФ по энергетической инфраструктуре Украины ответом на действия Киева. *Інтерфакс* https://www.interfax.ru/russia/875984.com
14. Мельник Б., Леонов Д. Інформаційний тероризм як загроза національній інформаційній інфраструктурі. *Інформація і право*. 3(50). DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311667
15. European Parliament & Council of the European Union. (2024). Artificial Intelligence Act (Regulation (EU) 2024/1689). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689
16. Яцик Т.П. Особливості інформаційного тероризму як одного із способів інформаційної війни // Науковий вісник Національного університету ДПС України (економіка, право). – 2014. – № 2 (65) – С. 55-60.
17. Думки і погляди українців з питань війни і миру: результати опитування, проведеного 20 липня — 3 серпня 2026 року. *Київський міжнародний інститут соціології.* https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1626&page=1
18. International Committee of the Red Cross. (1977). Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Article 51.
19. Irrera D, Bilgic A. Perceptions of the war in Ukraine: how the Russian propaganda works outside the west. *European Political Science*. 2025;24(1):66-73. DOI: https://doi.org/10.1057/s41304-024-00477-6
20. Post, Jerrold & Ruby, Keven & Shaw, Eric. (2000). From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism. Terrorism and Political Violence - TERROR POLIT VIOLENCE. 12. 97-122. DOI: https://doi.org/10.1080/09546550008427563.
21. Kobet Y., Pogrebytskyi M., Berezovska-Chmil O., Kharchenko S., Pravdiuk A. Information terrorism as a threat to the global security system of the 21st century. Cuestiones Políticas. Vol. 40. № 75. P. 274-284. DOI: https://doi.org/10.46398/cuestpol.4075.18
22. Kuzmenko, H. (2025). Conceptualization of Russia's strategic narratives in the full-scale Russo-Ukrainian war. Scientific Notes of the Institute of Journalism, 86, 3. DOI: https://doi.org/10.17721/2522-1272.2025.86.3
23. Mandić, J., & Klarić, D. (2023). Case study of the Russian disinformation campaign during the war in Ukraine – propaganda narratives, goals and impacts. (Review paper). DOI: https://doi.org/10.37458/nstf.24.2.5

24. Roozenbeek, J. (2024). Propaganda and ideology in the Russian–Ukrainian War. Cambridge University Press. DOI: https://doi.org/10.1017/9781009244039
25. Sekeris, P. (2025). Propaganda and conflict. Games and Economic Behavior, 153, 569–585. DOI: https://doi.org/10.1016/j.geb.2025.08.006
26. Военные назвали удар по энергетике Украины ответом на атаку в Таганроге. Радио РБК. https://surl.li/hbnjpg
27. Тарасовський Ю. Міноборони Росії заявило про підготовку до масованих ударів по енергетиці України. Forbes. https://surl.li/iddchn
28. Voznyuk Y., Vetrov K. Information Terrorism as a Modern Threat for Information Security of European States. *International Relations, Public Communications and Regional Studies*. 1(5), 34–41. DOI: https://doi.org/10.29038/2524-2679-2019-01-34-41
29. Vnuchko S., Teremko V., Polovko O., Stychynska A. (2024) Information Terrorism And Its Prevention In The Global Political Environment In The 21st Century. Journal of Interdisciplinary Research, № 1, p. 63-68. DOI: https://doi.org/10.33543/1401396368
30. Банк Р.О. (2016) Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект. *Інформація і право*. 1(16). с. 110-116 DOI: https://doi.org/10.37750/2616-6798.2016.1(16).272856
31. Герасименко К. С. Сучасні ознаки загроз "інформаційного тероризму". Форум права. 2009. № 3. С. 162-166.
32. Державна служба спеціального зв'язку та захисту інформації. Сьогоднішні атаки – продовження атак 15 лютого. Офіційний сайт https://cip.gov.ua/ua/news/23-lyutogo-2022-roku-stavsya-chergovii-akt-kiberagresiyi-proti-ukrayini
33. Коршунов В. О. Політичний тероризм: інформаційні методи боротьби : автореф. дис. …канд. політ. наук : спец. 23.00.02 «Політич на інститути та процеси». Дніпропетровськ, 2008. – 18 с.
34. Кримінальний кодекс України. Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131 (зі змінами) https://zakon.rada.gov.ua/laws/show/2341-14#Text
35. Лисько, Т. Д., Клімук, О. О., & Лисянська, Д. В. (2022). Інформаційний тероризм як загроза національній безпеці та спосіб інформаційної війни *Юридичний науковий електронний журнал*. 10. DOI: https://doi.org/10.32782/2524-0374/2022-10/143
36. Михайлов Д. Путін затвердив оновлену «ядерну доктрину» Росії. Суспільне. Новини, 19.11.2024, https://suspilne.media/883111-putin-zatverdiv-onovlenu-adernu-doktrinu-rosii/
37. Харамурза, Д. (2023). Інформаційний тероризм як інструмент гібридної війни та фактор руйнації медіапростору. *Інтегровані комунікації*, (2 (16), 29–37. DOI: https://doi.org/10.28925/2524-2644.2023.16
38. Інформаційний тероризм: злочин проти людяності, скоєний за допомогою інструментів впливу на свідомість. Центр протидії дезінформації при РНБО України. (2022). https://cpd.gov.ua/reports/informaczijnyj-teroryzm/
39. Шабранська В. (2026) СБУ назвала свою 40-денну операцію дієвим механізмом впливу на РФ і підбила підсумки досягнутих цілей. Українська правда. https://www.pravda.com.ua/news/2026/08/04/8047254/
40. Сили оборони вивели з ладу майже 43% загальної проєктної потужності нафтопереробки Росії. *Укрінформ* https://www.ukrinform.ua/rubric-ato/4140661-sili-oboroni-viveli-z-ladu-majze-43-zagalnoi-proektnoi-potuznosti-naftopererobki-rosii-genstab.html
41. Погорілов С. Медведєв пропонує виконати "вимоги" Росії, щоб в українців з'явилося світло, в ОП відповіли. Українська правда, 28.10.2022. https://www.pravda.com.ua/news/2022/10/28/7373946/

42. Костіна І., Погорілов С. Медведєв почав погрожувати новим членам НАТО ударами "відплати" та ядерною зброєю. Українська правда, 29.04.2025, https://www.pravda.com.ua/news/2025/04/29/7509679/
43. Костіна І. "Постраждають найпершими": в РФ пригрозили Польщі і країнам Балтії. Європейська правда, 15.04.2025. https://www.eurointegration.com.ua/news/2025/04/15/7209553/

References

1. Leonov B., Lykhova S. (2021) Information Terrorism as a Threat to the National Security of Ukraine. *Air and Space Law*. 2(59), 170–176. https://doi.org/10.18372/2307-9061.59.15615
2. Appel Hillary (2024) "Competing narratives of the Russia–Ukraine war: Why the West hasn't convinced the rest," Global Policy, London School of Economics and Political Science, vol. 15(4), pages 559-569, September. https://doi.org/10.1111/1758-5899.13431
3. Aspriadis, N. (2023). Preparing for War: Strategic Narratives and Disinformation in Leadership Rhetoric during the Ukraine War. *ESSACHESS – Journal for Communication Studies*, *16*(1(31), 21-41. https://doi.org/10.21409/9037-1Y61
4. Bradshaw, S., Elswah, M., Haque, M., & Quelle, D. (2024). Strategic storytelling: Russian state-backed media coverage of the Ukraine war. International Journal of Public Opinion Research, 36(3), edae028. https://doi.org/10.1093/ijpor/edae028
5. Center for Civilians in Conflict. (2023). When words become weapons: A human-centered approach to understanding and countering hate speech and incitement in conflict. https://www.civiliansinconflict.org/wp-content/uploads/2023/11/CIVIC_Disinformation_Report.pdf
6. Council conclusions on Foreign Information Manipulation and Interference (FIMI) https://data.consilium.europa.eu/doc/document/ST-11429-2022-INIT/en/pdf
7. Namestnik V., Klunnyk M. (2024) Russian information operations against Ukraine in 2022–2023: conclusions, recommendations, lessons learned. Science and Defence, №2 (2024). С. 58-64. https://doi.org/10.33099/2618-1614-2024-25-2-58-64
8. Devost, M. G., Houghton, B. K., & Pollard, N. A. (1997). Information terrorism: Political violence in the information age. Terrorism and Political Violence, 9(1), 72–83. https://doi.org/10.1080/09546559708427387
9. Digital Forensic Research Lab. (2024) Undermining Ukraine: How Russia widened its global information war in 2023. Atlantic Council. https://surl.li/hbcjmb
10. Mytko A. M., Koltsova I. I. (2018) Information terrorism as a tool of influence on information conformism in the global environment. *Political Life*. 2. https://doi.org/10.31558/2519-2949.2018.2.22
11. Petryshyn H. R. Informatsiynyy teroryzm: dzherela formuvannya ta aktyvizatsiyi v Ukrayini // Habitus : naukovyy zhurnal. Odesa : Hel'vetyka, 2021. Vyp. 21. S. 44–50. https://doi.org/https://doi.org/10.32843/2663- 5208.2021.21.7
12. Talişinski E. Information Terrorism As a Form of International Terrorism. *Dünya İnsan Bilimleri Dergisi*. 2023(2), 127–134. https://doi.org/10.55543/insan.1244109
13. Putin nazvav udary RF po enerhetychniy infrastrukturi Ukrayiny vidpoviddyu na diyi Kyyeva. *Interfaks* https://www.interfax.ru/russia/875984.com
14. Melnyk D., Leonov B. Information terrorism as a threat to the national information infrastructure. *Information and Law*. 3(50). https://doi.org/10.37750/2616-6798.2024.3(50).311667
15. European Parliament & Council of the European Union. (2024). Artificial Intelligence Act (Regulation (EU) 2024/1689). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

16. Yatsyk T.P. Osoblyvosti informatsiynoho teroryzmu yak odnoho iz sposobiv informatsiynoyi viyny // Naukovyy visnyk Natsional'noho universytetu DPS Ukrayiny (ekonomika, pravo). – 2014. – № 2 (65) – S. 55-60
17. Dumky i pohlyady ukrayintsiv z pytan' viyny i svitu: rezul'taty opytuvannya, provedenoho 20 lypnya-3 serpnya 2026 roku. *Kyyivs'kyy mizhnarodnyy instytut sotsiolohiyi*. https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1626&page=1
18. International Committee of the Red Cross. (1977). Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Article 51.
19. Irrera D, Bilgic A. Perceptions of the war in Ukraine: how the Russian propaganda works outside the west. *European Political Science*. 2025;24(1):66-73. https://doi.org/10.1057/s41304-024-00477-6
20. Post, Jerrold & Ruby, Keven & Shaw, Eric. (2000). From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism. Terrorism and Political Violence - TERROR POLIT VIOLENCE. 12. 97-122. https://doi.org/10.1080/09546550008427563.
21. Kobet Y., Pogrebytskyi M., Berezovska-Chmil O., Kharchenko S., Pravdiuk A. Information terrorism as a threat to the global security system of the 21st century. Cuestiones Políticas. Vol. 40. № 75. P. 274-284. https://doi.org/10.46398/cuestpol.4075.18
22. Kuzmenko, H. (2025). Conceptualization of Russia's strategic narratives in the full-scale Russo-Ukrainian war. Scientific Notes of the Institute of Journalism, 86, 3. https://doi.org/10.17721/2522-1272.2025.86.3
23. Mandić, J., & Klarić, D. (2023). Case study of the Russian disinformation campaign during the war in Ukraine – propaganda narratives, goals and impacts. (Review paper). https://doi.org/10.37458/nstf.24.2.5
24. Roozenbeek, J. (2024). Propaganda and ideology in the Russian–Ukrainian War. Cambridge University Press. https://doi.org/10.1017/9781009244039
25. Sekeris, P. (2025). Propaganda and conflict. Games and Economic Behavior, 153, 569–585. https://doi.org/10.1016/j.geb.2025.08.006
26. Viys'kovi nazvaly udar po enerhetytsi Ukrayiny vidpoviddyu na ataku v Tahanrohe. *Radio RBK* https://surl.li/hbnjpg
27. Tarasovskyi Y.: The Russian Ministry of Defense has announced preparations for massive strikes on Ukraine's energy infrastructure. Forbes https://surl.li/iddchn
28. Voznyuk Y., Vetrov K. Information Terrorism as a Modern Threat for Information Security of European States. *International Relations, Public Communications and Regional Studies*. 1(5), 34–41. https://doi.org/10.29038/2524-2679-2019-01-34-41
29. Vnuchko S., Teremko V., Polovko O., Stychynska A. (2024) Information Terrorism And Its Prevention In The Global Political Environment In The 21st Century. Journal of Interdisciplinary Research, № 1, p. 63-68. https://doi.org/10.33543/1401396368
30. Bank R. O. (2016) Information terrorism as a threat to the national security of Ukraine: theoretical and legal aspect. *Information and Law*. 1(16). P. 110-116. https://doi.org/10.37750/2616-6798.2016.1(16).272856
31. Herasymenko K. S. Suchasni oznaky zahrozy "informatsiynoho teroryzmu". Forum prava. 2009. № 3. S. 162-166.
32. Derzhavna sluzhba spetsial'noho zv"yazku ta zakhystu informatsiyi. S'ohodnishni ataky – prodovzhennya ataky 15 lyutoho. Ofitsiynyy sayt https://cip.gov.ua/ua/news/23-lyutogo-2022-roku-stavsya-chergovii-akt-kiberagresiyi-proti-ukrayini
33. Korshunov V. O. Politychnyy teroryzm: informatsiyni metody borot'by : avtoref. dys. …kand. polit. nauk : spets. 23.00.02 «Politych na instytuty ta protsesy». Dnipropetrovs'k, 2008. – 18 s.

34. Kryminal'nyy kodeks Ukrayiny. Vidomosti Verkhovnoyi Rady Ukrayiny (VVR), 2001, № 25-26, st.131 (zi zminamy) https://zakon.rada.gov.ua/laws/show/2341-14#Text
35. Lys'ko, T. D., Klimuk, O. O., & Lysyans'ka, D. V. (2022). Informatsiynyy teroryzm yak zahroza natsional'noyi bezpetsi ta sposib informatsiynoyi viyny Yurydychnyy naukovyy elektronnyy zhurnal. 10. https://doi.org/10.32782/2524-0374/2022-10/143
36. Mykhaylov D. Putin zatverdyv onovlenu «yadernu doktrynu» Rosiyi. Suspil'ne. Novyny, 19.11.2024, https://suspilne.media/883111-putin-zatverdiv-onovlenu-adernu-doktrinu-rosii/
37. Kharamurza, D. (2023). Informatsiynyy teroryzm yak instrument hibrydnoyi viyny ta faktor ruynatsiyi mediaprostoru. *Intehrovani komunikatsiyi,* (2 (16), 29–37. https://doi.org/10.28925/2524-2644.2023.16
38. Informatsiynyy teroryzm: zlochyn proty lyudyanosti, skoyenyy za dopomohoyu instrumentiv vplyvu na svidomist'. Tsentr protydiyi dezinformatsiyi pry RNBO Ukrayiny. (2022). https://cpd.gov.ua/reports/informaczijnyj-teroryzm/
39. Shabrans'ka V . (2026) SBU nazvala svoyu 40-dennu operatsiyu diyevym mekhanizmom vplyvu na RF i pidbyla pidsumky dosyahnutykh tsiley. *Ukrayins'ka pravda*. https://www.pravda.com.ua/news/2026/08/04/8047254/
40. Syly oborony vyvely z ladu mayzhe 43% zahal'noyi proyektnoyi potuzhnosti naftopererobky Rosiyi. *Ukryinform* https://www.ukrinform.ua/rubric-ato/4140661-sili-oboroni-viveli-z-ladu-majze-43-zagalnoi-proektnoi-potuznosti-naftopererobki-rosii-genstab.html
41. Pohorilov S. Medvedyev proponuye vykonaty «vymohy» Rosiyi, shchob v ukrayintsiv z"yavylosya svitlo, v OP vidpovily. *Ukrayins'ka pravda*, 28.10.2022. https://www.pravda.com.ua/news/2022/10/28/7373946/
42. Kostina I., Pohorilov S. Medvedyev pochav pohrozhuvaty novym chlenam NATO udaramy "vidplaty" ta yadernoyu zbroyeyu. *Ukrayins'ka pravda*, 29.04.2025, https://www.pravda.com.ua/news/2025/04/29/7509679/
43. Kostina I. «Postrazhdayte naypershymy»: v RF zahrozyly Pol'shchi i krayinam Baltiyi. *Yevropeys'ka pravda,* 15.04.2025. https://www.eurointegration.com.ua/news/2025/04/15/7209553/

This is an open access journal and all published articles are licensed under a Creative Commons «Attribution» 4.0.