Міністерство освіти і науки України
Національний університет «Острозька академія»
Навчально-науковий інститут міжнародних відноси та національної безпеки
Кафедра міжнародних відносин

Кваліфікаційна робота
на здобуття освітнього ступеня магістра
«**Інформаційний тероризм як загроза міжнародній безпеці**»

Виконала студентка 2 курсу, групи Ммв - 1
спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»,
освітньо-професійної програми
«Міжнародні відносини»
Бебко Євгенії Юріївни

Керівник: кандидат історичних наук,
старший викладач кафедри міжнародних
відносин, Матвійчук Наталя Володимирівна,

Рецензент _____
_____

Робота допущена до захисту
(протокол № ____ засідання кафедри
міжнародних відносин від
_____20___року

Завідувач кафедри міжнародних відносин:
_____ Сидорук Тетяна Віталіївна

Острог – 2025

ЗМІСТ

ВСТУП

Актуальність теми визначається декількома взаємопов'язаними чинниками фундаментального характеру. По-перше, сучасний етап розвитку міжнародних відносин демонструє безпрецедентне зростання ролі

інформаційного простору як арени геополітичного протистояння, що особливо яскраво проявилося під час російської агресії проти України, яка супроводжується масштабною інформаційною кампанією, спрямованою на дискредитацію української державності, поширення дезінформації про хід бойових дій та маніпулювання міжнародною громадською думкою.

Документальні свідчення демонструють, що Російська Федерація систематично використовує методи інформаційного тероризму для досягнення стратегічних цілей, зокрема через поширення фейкових новин про нібито здійснені українськими військовими злочини, створення паніки серед цивільного населення через повідомлення про загрозу ядерної катастрофи та підрив довіри до західних партнерів України шляхом маніпулятивних наративів про зменшення підтримки. По-друге, традиційні механізми міжнародної безпеки, створені в епоху двополярного протистояння, виявляються малоефективними у протидії інформаційним загрозам, оскільки міжнародне право досі не містить чіткого визначення інформаційного тероризму, а наявні конвенції про боротьбу з тероризмом не повною мірою враховують специфіку інформаційно комунікаційного середовища. По-третє, гібридний характер сучасних конфліктів передбачає тісне переплетення кінетичних та некінетичних засобів ведення війни, де інформаційні операції стають невід'ємною складовою військових кампаній, що вимагає переосмислення базових концепцій національної та міжнародної безпеки. По-четверте, зростаюча складність та взаємозалежність глобальних інформаційних систем створює ситуацію, коли успішна атака на інформаційну інфраструктуру однієї держави може спричинити каскадний ефект та завдати шкоди безпеці цілого регіону або навіть міжнародній системі загалом.

Ступінь наукової розробки проблеми інформаційного тероризму як загрози міжнародній безпеці характеризується певною неоднорідністю та

фрагментарністю, що пояснюється відносною новизною феномену та міждисциплінарним характером дослідження. Теоретичні основи вивчення інформаційних загроз закладені у працях провідних західних дослідників, серед

яких варто виділити роботи: Мартіна Лібіцького, який одним із перших сформулював концепцію кібервійни та проаналізував вразливості сучасних інформаційних систем, Дороті Денінг, яка детально дослідила феномен кібертероризму та розробила типологію інформаційних загроз, а також Джона Аркілли та Девіда Ронфельдта, які запропонували концепцію мережевих війн та проаналізували трансформацію характеру збройних конфліктів в інформаційну епоху. Значний внесок у розуміння механізмів інформаційного впливу зробили дослідники психологічних операцій та стратегічних комунікацій, зокрема Герберт Фрідман, який систематизував досвід використання пропаганди у збройних конфліктах, та Френк Хоффман, який розробив концепцію гібридної війни, що поєднує традиційні та нетрадиційні методи ведення бойових дій.

У вітчизняній науковій думці проблематика інформаційних загроз активно розробляється з початку російської агресії проти України, коли гостро постала потреба осмислення нових форм ведення війни та вироблення ефективних механізмів протидії інформаційним атакам. Фундаментальні дослідження у цій галузі провели такі українські вчені: Володимир Горбулін, який у своїх працях проаналізував феномен світової гібридної війни та місце України у цьому протистоянні, Віктор Петров, який систематизував російський досвід ведення інформаційних війн та розробив рекомендації щодо підвищення інформаційної безпеки України, Георгій Почепцов, який дослідив механізми функціонування сучасних систем стратегічних комунікацій та їхню роль у забезпеченні національної безпеки. Окремо варто відзначити дослідження Євгена Магди, присвячені аналізу російської пропагандистської машини та методів поширення дезінформації, роботи Дмитра Дубова, який вивчав інформаційні та кіберзагрози у контексті національної безпеки України, а також праці Ольги Литвиненко, яка проаналізувала російську інформаційну агресію на окупованих територіях.

Мета дослідження полягає у комплексному висвітлені феномену інформаційного тероризму як сучасної загрози міжнародній безпеці шляхом визначення його характеристик, форм прояву та впливу на стабільність міжнародної системи, а також у розробці науково обґрунтованих рекомендацій

щодо підвищення ефективності протидії інформаційно-терористичним загрозам на національному та міжнародному рівнях.

Для досягнення мети необхідно вирішити такі **дослідницькі завдання**: 1. здійснити теоретичну концептуалізацію інформаційного тероризму як явища міжнародних відносин через критичний аналіз наявних підходів до його визначення, виявлення ознак та відмежування від суміжних понять; 2. проаналізувати еволюцію інформаційного тероризму у контексті трансформації глобального безпекового середовища та визначити основні етапи його становлення як інструменту впливу на міжнародні процеси; 3. систематизувати форми і методи здійснення інформаційно-терористичних актів через вивчення конкретних кейсів та виявлення типових патернів використання інформаційних технологій з терористичною метою; 4. оцінити масштаби впливу інформаційного тероризму на міжнародну безпеку, включаючи політичну, економічну, соціальну складові; 5. дослідити наявні міжнародно-правові механізми протидії інформаційному тероризму та виявити прогалини у правовому регулюванні цієї сфери; 6. проаналізувати міжнародні стратегії та практики боротьби з інформаційними загрозами у провідних державах світу та визначити ефективні підходи, які можуть бути адаптовані до потреб інших країн; 7. розробити рекомендації щодо вдосконалення системи міжнародної та національної безпеки у контексті протидії інформаційному тероризму. **Об'єктом дослідження** виступає інформаційний тероризм як феномен сучасних міжнародних відносин та форма загрози міжнародній безпеці. **Предметом дослідження** є особливості впливу інформаційного тероризму на систему міжнародної безпеки, механізми його здійснення, наслідки для

стабільності міжнародного порядку та ефективність існуючих механізмів протидії цій загрозі на національному та глобальному рівнях.

Теоретико-методологічну основу дослідження становить сукупність загальнонаукових та спеціальних методів, застосування яких у комплексі дозволяє забезпечити науковість та об'єктивність результатів аналізу. Системний підхід використовується для розгляду інформаційного тероризму як складного

багатокомпонентного явища, що функціонує у системі міжнародних відносин та впливає на різні її елементи, дозволяючи виявити взаємозв'язки між окремими проявами інформаційних загроз та їхнім інтегральним впливом на міжнародну безпеку. Структурно-функціональний метод застосовується для аналізу структури інформаційно-терористичної діяльності, виявлення основних її елементів та функцій, які вони виконують у досягненні цілей терористичних організацій або держав-агресорів. Компаративний метод використовується для порівняльного аналізу національних стратегій протидії інформаційним загрозам, визначення спільних та відмінних рис у підходах різних держав до забезпечення інформаційної безпеки, а також для співставлення інформаційного тероризму з традиційними формами терористичної діяльності. Історичний метод дозволяє простежити еволюцію інформаційного тероризму від ранніх форм використання інформації в терористичних цілях до сучасних високотехнологічних методів ведення інформаційних операцій. Івент-аналіз застосовується для систематизації та обробки даних про конкретні випадки інформаційно-терористичних актів, виявлення закономірностей у їхньому здійсненні та оцінки масштабів поширення цього явища. Контент-аналіз використовується для вивчення змісту інформаційних повідомлень, що поширюються терористичними організаціями або у рамках державних інформаційних кампаній з ознаками тероризму, визначення ключових наративів та маніпулятивних прийомів. **Хронологічні рамки дослідження** охоплюють період від початку XXI століття до сьогодення, що пояснюється кількома принципово важливими обставинами. Саме на початку нового тисячоліття відбувається якісний стрибок у розвитку інформаційно-комунікаційних технологій, пов'язаний із масовим

поширенням широкосмугового доступу до Інтернету, виникненням соціальних мереж та переходом значної частини суспільних процесів у цифровий простір, що створило принципово нові можливості для використання інформації як зброї.

Географічні рамки дослідження мають глобальний характер, оскільки інформаційний тероризм за своєю природою не обмежується кордонами окремих держав, а інформаційний простір є транснаціональним середовищем, де загрози,

що виникають в одному регіоні, можуть поширитися на інші частини світу.

Джерельна база дослідження є комплексною та забезпечує всебічність і об’єктивність аналізу. До першої групи віднесено офіційні документи міжнародних організацій у сфері безпеки й протидії тероризму: резолюції та доповіді ООН, матеріали Контртерористичного комітету, ITU та UNODC, а також документи НАТО зі стратегічних комунікацій і кіберзахисту та акти ЄС щодо боротьби з дезінформацією і гібридними загрозами. Друга група охоплює національні стратегії провідних держав, зокрема стратегії нацбезпеки й кібербезпеки США, доктрини РФ, а також британські та німецькі підходи; особливе місце займають українські стратегічні документи та концепції протидії російській пропаганді. Третю групу становлять аналітичні напрацювання провідних дослідницьких центрів і НУО (CSIS, Chatham House, SIPRI, ISW, Atlantic Council, Carnegie) та спеціалізованих проєктів з фактчекінгу і моніторингу дезінформації (EU East StratCom, DFRLab, Bellingcat, StopFake). Четверта група включає статистичні масиви та звіти про кіберінциденти від ENISA, урядових CERT і приватних компаній, а також Глобальний індекс тероризму Інституту економіки та миру. П’ята група містить емпіричні матеріали щодо конкретних інформаційних операцій, передусім російської агресії проти України, документи державних органів і think tanks, а також кейси втручання у виборчі процеси у США, Великій Британії та країнах Європи.

Практичне значення роботи полягає у можливості використання сформульованих рекомендацій органами державної влади України при розробці та вдосконаленні національної стратегії інформаційної безпеки, створенні ефективних механізмів протидії дезінформації та координації діяльності різних

державних інституцій у сфері стратегічних комунікацій. Висновки дослідження можуть бути корисними для міжнародних організацій, у процесі вдосконалення міжнародних та правових механізмів протидії інформаційному тероризму та вироблення скоординованих підходів до забезпечення інформаційної безпеки на глобальному рівні. Окремі положення роботи можуть знайти застосування у

діяльності недержавних організацій та медіа, які займаються фактчекінгом та боротьбою з дезінформацією, надаючи їм теоретичне підґрунтя для розуміння природи інформаційних загроз.

Апробація результатів дослідження здійснювалася через оприлюднення основних положень і висновків у двох наукових публікаціях, що відображають ключові аналітичні напрями роботи та забезпечують їхнє фахове обговорення у професійному середовищі. У статті «Соціальні наслідки інформаційного тероризму: дезінформація та маніпуляція суспільною думкою» було представлено концептуальні положення щодо психологічних механізмів інформаційного впливу, розкрито характер формування стану масової тривожності, недовіри та соціальної дезорієнтації унаслідок деструктивних інформаційних кампаній. Другий напрям апробації представлено у статті «Вплив інформаційного тероризму та кіберзлочинності на стабільність держави: практичний досвід України в умовах російської агресії», де основні положення дослідження було використано для аналізу національної безпекової політики та операційного досвіду протидії інформаційно-терористичним загрозам. У статті розкрито специфіку взаємодії кібератак, інформаційних операцій та маніпулятивних наративів у контексті російської агресії проти України, а також окреслено інституційні й правові проблеми реагування держави. Таким чином, апробація результатів засвідчила їхню наукову обґрунтованість, методологічну цілісність та практичну релевантність, а також забезпечила інтеграцію здобутих знань у сучасний науковий дискурс з проблематики інформаційного тероризму.

Структура роботи відповідає логіці дослідження та послідовності розв’язання завдань і включає вступ, три розділи, висновки та список використаних джерел та літератури.

РОЗДІЛ І. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ

1.1. Поняття та сутність інформаційного тероризму

Трансформація глобального інформаційного простору у першій чверті 21

століття радикально змінила характер безпекових загроз і породила якісно нові форми терористичної активності, що експлуатують цифрові технології та масові комунікації для досягнення деструктивних цілей. Сучасний етап цифровізації суспільних відносин характеризується переходом від традиційних силових методів тероризму до гібридних стратегій, де інформаційний компонент набуває стратегічного значення і часто перевершує за своїм деструктивним потенціалом фізичні акти насильства. Концептуалізація інформаційного тероризму як самостійного феномену вимагає критичного переосмислення класичних дефініцій тероризму та виокремлення специфічних характеристик, що відрізняють інформаційні загрози від традиційних форм терористичної діяльності. Дефініційна невизначеність залишається ключовою методологічною проблемою у дослідженнях цього відносно нового явища, оскільки відсутність загальноприйнятого визначення ускладнює розробку ефективних контрзаходів та міжнародної правової бази. [1] Теоретичне осмислення сутності інформаційного тероризму вимагає інтеграції концептуального апарату з різних дисциплінарних полів, включаючи теорію інформаційної безпеки, кримінологію, політичну психологію та дослідження масових комунікацій. Андрусишин Ю. І. та Баранник В. В. обстоюють тезу про те, що інформаційний тероризм являє собою цілеспрямоване маніпулювання суспільною свідомістю з метою створення напруженості, нестабільності та хаосу для реалізації політичних або економічних цілей терористів, що принципово відрізняється від кінетичних атак своєю невидимістю та тривалістю впливу. Автори розмежовують широке розуміння феномену як маніпулювання громадською свідомістю та вузьке тлумачення як

[1] Леонов Б. Д., Лихова С. Я. Інформаційний тероризм як загроза національній безпеці України. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник Повітряне і космічне право*. 2021. Т. 2, № 59. С. 110–116. URL: https://er.nau.edu.ua/items/a62f2dd2-8f1a-4346-9706-e6568f39cf55 (дата звернення: 16.10.2025).

кібератаки на критичну інфраструктуру, підкреслюючи багатовимірність явища та необхідність комплексного підходу до його вивчення.[2]

Центр протидії дезінформації при РНБО України пропонує розглядати

інформаційний тероризм як деструктивний феномен цифрової епохи, що потребує закріплення у міжнародному праві як окремий склад злочину з власними кваліфікуючими ознаками. Представники установи наголошують, як приклад, на координованому характері російсько-білоруських інформаційних кампаній під час міграційної кризи, що супроводжувалися цілеспрямованим розповсюдженням дезінформації для дестабілізації країн ЄС.[3]Ініціатива затвердження поняття інформаційного тероризму у міжнародній практиці відображає прагнення створити єдину правову систему для кваліфікації та переслідування таких діянь на глобальному рівні. Складність чіткого розмежування інформаційного тероризму від звичайних комп'ютерних злочинів та побутового маніпулювання у засобах масової інформації зумовлює термінологічну плутанину та методологічні труднощі у дослідженнях.

Леонов Б. Д. та Лихова С. Я. вказують на технічну подібність застосовуваних методів та інструментів при істотній відмінності у мотивації та цілях правопорушників, що ускладнює кваліфікацію діянь та розробку адекватних правових механізмів протидії. Автори підкреслюють, що доступність інформаційних технологій значно підвищує ризики інформаційного тероризму, а розвиненість інформаційної інфраструктури суспільства сприяє створенню додаткових вразливостей, які експлуатуються терористичними групами у сучасних умовах глобалізації та інтернаціоналізації.[4] Міжнародна наукова спільнота демонструє відсутність консенсусу щодо сутнісних характеристик інформаційного тероризму, що відображається у множинності визначень та

[2] Андрусишин Ю. І., Баранник В. В. Інформаційний тероризм як сучасна загроза інформаційній безпеці людини, суспільства, держави. *Інформаційна безпека людини, суспільства, держави*. 2022. № 1-3 (31-33). С. 6–15. URL: https://journals.uran.ua/ispss/article/view/260199 (дата звернення: 16.10.2025).

[3] Центр протидії дезінформації РНБО. Інформаційний тероризм. URL: https://cpd.gov.ua/reports/informaczijnyj teroryzm/ (дата звернення: 17.10.2025).

[4] Леонов Б. Д., Лихова С. Я. Інформаційний тероризм як загроза національній безпеці України. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник Повітряне і космічне право*. 2021. Т. 2, № 59. С. 110–116. URL: https://er.nau.edu.ua/items/a62f2dd2-8f1a-4346-9706-e6568f39cf55 (дата звернення: 16.10.2025).

підходів до його концептуалізації. Марсилі М. демонструє, що гібридна війна використовує кібероперації, дезінформаційні кампанії та когнітивну

маніпуляцію для дестабілізації противника без переходу порогу конвенційної війни, що розмиває традиційні межі між станом миру та збройного конфлікту. Автор наголошує на складності прийняття рішень у такому середовищі та необхідності нових правових і стратегічних відповідей для протистояння викликам, що залишаються нижче порогу відкритої війни.[5] Каузальний зв'язок між розповсюдженням дезінформації у соціальних мережах та зростанням внутрішнього тероризму став предметом емпіричних досліджень останніх років. П’яцца Дж. А. обґрунтовує статистично значущу кореляцію у вибірці понад 150 країн за період 2000 до 2017, теоретизуючи що дезінформація, розповсюджувана політичними діячами онлайн, посилює політичну поляризацію всередині країн, що створює середовище де внутрішній тероризм стає більш імовірним. Дослідник доводить, що пропаганда фейкових новин через соціальні медіа безпосередньо сприяє зростанню терористичної активності, функціонуючи як медіатор між інформаційним впливом та насильницькими діями.[6]

Концептуальна рамка аналізу інформаційного тероризму передбачає розгляд явища як форми психологічної війни, що експлуатує інформаційне середовище для досягнення стратегічних цілей без застосування фізичної сили. Митко А. М. та Кольцова І. І. концептуалізують інформаційний тероризм як інструмент впливу на інформаційний конформізм у глобальному середовищі, виділяючи дві основні форми його прояву через кібертероризм та медіа тероризм, які функціонують за різними механізмами але мають спільну мету дестабілізації соціальної системи. Автори підкреслюють, що сучасний інформаційний тероризм використовує як технічні засоби впливу на інформаційні системи, так і психологічні методи маніпулювання громадською

[5] Marsili M. Navigating the Risks of Hybrid Warfare: Cyber, Cognitive, and Information Threats at the Brink of Conflict. 2024.URL: https://www.researchgate.net/publication/385751572_Navigating_the_Risks_of_Hybrid_Warfare_Cyber_Cognitive_and_Information_Threats_at_the_Brink_of_Conflict (date of access: 21.10.2025).

[6] Piazza J. A. Fake news: the effects of social media disinformation on domestic terrorism. *Dynamics of Asymmetric Conflict: Pathways toward Terrorism and Genocide*. 2022. Vol. 15, no. 1. P. 55–77. URL: https://doi.org/10.1080/17467586.2021.1895263 (date of access: 21.10.2025).

думкою через засоби масової інформації.[7] Онлайн-радикалізація як механізм

формування терористичної мотивації через інформаційний простір потребує критичного переосмислення з огляду на суперечливість емпіричних даних. Біндер Дж. Ф. та Кеньон Дж. критично переосмислюють загрозу онлайн радикалізації, стверджуючи що емпіричні дані не підтверджують панічних оцінок щодо масштабів інтернет-радикалізації, яка хоча і є реальною загрозою, проте не може розглядатися як головний драйвер терористичних актів та супутніх правопорушень. Дослідники визначають онлайн-радикалізацію як процес, під час якого індивіди піддаються впливу, імітують та інтерналізують екстремістські переконання і настанови за допомогою інтернету, зокрема соціальних медіа та інших форм онлайн-комунікації.[8]

Бібліометричний аналіз наукової літератури демонструє зростаючий інтерес дослідників до проблематики інформаційного тероризму та його цифрових проявів. Юмітро Г., Фебріані Р. та Розікін А. провели аналіз міжнародних публікацій у базі даних Scopus за період 2009 до 2022 років, виявивши пік досліджень соціальних мереж та тероризму у 2018 році зі 103 публікаціями, що свідчить про зростаючу наукову увагу до цифрових аспектів терористичної активності. Дослідники застосували візуалізацію даних через Microsoft Excel та VOSviewer для ідентифікації провідних тем, країн, авторів та джерел публікацій.[9] Психологічні механізми впливу інформаційного тероризму базуються на експлуатації когнітивних упереджень, емоційних вразливостей та соціальної ідентичності для формування бажаних поведінкових патернів у цільових аудиторій. Лабенко Л. В. показує, що інформація відіграє визначальну роль у сучасному суспільстві, породжуючи актуальність висловів про володіння інформацією як володіння світом та про інформаційну війну як зіткнення

[7] Митко А. М., Кольцова І. І. Інформаційний тероризм як інструмент впливу на інформаційний конформізм у глобальному середовищі. *Політичне життя*. 2018. № 2. С. 135–139. URL: https://doi.org/10.31558/2519-2949.2018.2.22 (дата звернення: 21.10.2025).

[8] Binder J. F., Kenyon J. Terrorism and the internet: How dangerous is online radicalization?. *Frontiers in Psychology*. 2022. Vol. 13. URL: https://doi.org/10.3389/fpsyg.2022.997390 (date of access: 21.10.2025).

[9] Yumitro G., Febriani R., Roziqin A. Bibliometric analysis of international publication trends on social media and terrorism by using the Scopus database. *Frontiers in Communication*. 2023. Vol. 8. URL: https://doi.org/10.3389/fcomm.2023.1140461 (date of access: 21.10.2025).

цивілізацій з різними базовими цілями, знаннями та теоріями. Автор підкреслює, що за допомогою інформації можна досягти як позитивних так і негативних результатів, що робить такий вид тероризму ще більш небезпечним.[10]

Комплексність інформаційного тероризму як виклику сучасності полягає у відсутності географічних та національних кордонів, складності ідентифікації особи терориста в інформаційному просторі та встановлення місця його перебування. Андрусишин Ю. І. та Баранник В. В. констатують, що віртуальний простір та масмедіа широко використовуються різними угрупованнями терористичного спрямування для досягнення власних цілей, оскільки доступність, відсутність цензури, наявність величезної потенційної аудиторії користувачів, висока швидкість розповсюдження інформації та комплексність її подачі і сприйняття сприяють розширенню інформаційного тероризму у сучасному світі.[11] Міждисциплінарність дослідження інформаційного тероризму вимагає синтезу методологічних підходів з різних галузей знання для формування цілісного розуміння явища. П'ятдесятирічний огляд наукових досліджень тероризму демонструє експоненційне зростання публікацій, при цьому понад 18651 наукових праць станом на вересень 2020 року присвячені цій тематиці. Найбільша концентрація досліджень спостерігається у дисциплінах політичних наук з 4177 публікаціями та міжнародних відносин з 3558 публікаціями, що відображає переважно політологічне та міжнароднознавче трактування тероризму.[12] Еволюція концептуальних підходів до інформаційного тероризму відображає зміни у технологічному ландшафті та геополітичній ситуації. Данік Ю., Маліарчук Т. та Бріггс С. доводять, що гібридна війна у Східній Європі демонструє безпрецедентне застосування високотехнологічних інформаційних та кіберконфліктів, де традиційні військові операції поєднуються

[10] Лабенко Л. В. Інформаційний тероризм: поняття та ознаки. *Міжнародні читання пам'яті професора П. Є. Казанського*. Одеса, 2010. С. 195–198. URL: https://dspace.onua.edu.ua/items/2f48fe7c-3290-4b25-b9aeee96a5222c6e (дата звернення: 21.10.2025).

[11] Андрусишин Ю. І., Баранник В. В. Інформаційний тероризм як сучасна загроза інформаційній безпеці людини, суспільства, держави. *Інформаційна безпека людини, суспільства, держави*. 2022. № 1-3 (31-33). С. 6–15. URL: https://journals.uran.ua/ispss/article/view/260199 (дата звернення: 16.10.2025).

[12] Haghani M. Fifty years of scholarly research on terrorism: Intellectual progression, structural composition, trends and knowledge gaps of the field. *International Journal of Disaster Risk Reduction*. 2021. URL: https://www.sciencedirect.com/science/article/abs/pii/S2212420921006750 (date of access: 21.10.2025).

з психологічними операціями та кібератаками у єдину стратегію. Автори підкреслюють, що концепції гібридної війни на Заході часто фокусуються на так званій доктрині Герасимова та діями нижче порогу відкритої конвенційної війни при збереженні правдоподібного заперечення участі.[13]

Методологічні труднощі вивчення інформаційного тероризму пов'язані з латентністю явища, анонімністю терористів, швидкоплинністю цифрового середовища та відсутністю усталених метрик для вимірювання впливу. Леонов Б. Д. та Лихова С. Я. наголошують на необхідності уніфікації та гармонізації національного законодавства та міжнародних актів, проведення наукових розробок у сфері створення сучасних технологій виявлення та запобігання кримінальним і терористичним впливам на інформаційні ресурси, створення спеціалізованих підрозділів у сфері боротьби з комп'ютерними злочинами та комп'ютерним тероризмом.[14] Теоретична новизна досліджень інформаційного тероризму полягає у спробах інтеграції традиційних теорій тероризму з концепціями інформаційної безпеки та кібервійни. Марсилі М. аргументує, що навігація ризиків гібридної війни вимагає врахування когнітивних та інформаційних загроз на межі конфлікту, де традиційні парадигми воєнного права та міжнародних відносин виявляються недостатніми для адекватної відповіді на нові виклики. Автор підкреслює складність прийняття рішень у цьому середовищі та необхідність еволюції правових і стратегічних відповідей. [15] Прогностичний потенціал досліджень інформаційного тероризму залежить від здатності науковців передбачити еволюцію технологій та адаптацію терористичних організацій до нових можливостей. Центр протидії дезінформації підкреслює, що у зв'язку з дальшим розвитком технологій та масмедіа питання протидії інформаційному тероризму буде особливо актуальним, оскільки

[13] Danyk Y., Maliarchuk T., Briggs C. Hybrid War: High-tech, Information and Cyber Conflicts. *Connections: The Quarterly Journal*. 2017. Vol. 16, no. 2. P. 5–24. URL: https://doi.org/10.11610/Connections.16.2.01 (date of access: 21.10.2025).

[14] Леонов Б. Д., Лихова С. Я. Інформаційний тероризм як загроза національній безпеці України. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник Повітряне і космічне право*. 2021. Т. 2, № 59. С. 110–116. URL: https://er.nau.edu.ua/items/a62f2dd2-8f1a-4346-9706-e6568f39cf55 (дата звернення: 16.10.2025).

[15] Marsili M. Guerre à la Carte: Cyber, Information, Cognitive Warfare and the Metaverse. *Applied*

цифровізація створює нові вразливості та можливості для зловмисників використовувати інформаційний простір для досягнення деструктивних цілей.[16] Інформаційний тероризм у сучасних умовах набуває особливого значення як складова гібридних загроз, що поєднують у собі елементи інформаційної війни, пропаганди, психологічного впливу та маніпулювання суспільною свідомістю. Аналіз положень Закону України «Про боротьбу з тероризмом» від 20 березня 2003 року № 638-IV [17] та Указу Президента України «Про Концепцію боротьби з тероризмом в Україні» від 5 березня 2019 року № 53/2019 [18] дає підстави розглядати інформаційний тероризм як специфічний різновид терористичної діяльності, що реалізується в інформаційному просторі через цілеспрямоване поширення деструктивних повідомлень, фейкових новин, панічних настроїв, закликів до насильства або недовіри до державних інституцій. У Законі № 638-IV тероризм визначено як суспільно небезпечну діяльність, яка полягає у свідомому застосуванні насильства або погрозі його застосування з метою порушення громадської безпеки, залякування населення, впливу на рішення органів влади чи міжнародних організацій. У цьому контексті насильство може мати не лише фізичний, а також й психологічний чи інформаційний характер, коли засоби масової інформації, соціальні мережі чи електронні комунікації стають інструментом терористичного впливу. Концепція боротьби з тероризмом 2019 року, ухвалена Указом Президента № 53/2019, розширює сферу національної безпеки, включаючи інформаційний простір до переліку потенційних об’єктів терористичних посягань. У документі зазначено, що терористична діяльність може реалізовуватись шляхом використання інформаційних технологій, комунікаційних мереж і засобів масової інформації для дестабілізації ситуації в державі, підриву авторитету влади, посилення панічних настроїв чи маніпулювання громадською думкою.

[16] Центр протидії дезінформації РНБО. Інформаційний тероризм. URL: https://cpd.gov.ua/reports/informaczijnyj teroryzm/ (дата звернення: 17.10.2025).

[17] Про боротьбу з тероризмом : Закон України від 20.03.2003 № 638-IV : станом на 9 січ. 2025 р. URL:

https://zakon.rada.gov.ua/laws/show/638-15#Text (дата звернення: 21.10.2025).
[18] Про Концепцію боротьби з тероризмом в Україні : Указ Президента України від 05.03.2019 № 53/2019. URL: https://zakon.rada.gov.ua/laws/show/53/2019#Text (дата звернення: 21.10.2025).

Такий підхід відображає розуміння інформації як ресурсу, що може бути інструментом розвитку, та зброєю деструкції, здатною завдати шкоди без застосування фізичного насильства. Концепція також наголошує на необхідності удосконалення механізмів інформаційної безпеки, захисту населення від деструктивних психологічних впливів та формування стійкості суспільства до маніпуляцій. Інформаційний тероризм можна визначити як цілеспрямовану діяльність фізичних чи юридичних осіб, державних або недержавних сторін, спрямовану на створення стану страху, хаосу, недовіри чи дезорієнтації у суспільстві через системне використання інформаційних технологій. Його основною метою є вплив на політичні рішення, дестабілізація соціально політичного життя, підрив довіри до державних інституцій або створення умов для прийняття вигідних для агресора рішень. На відміну від традиційних форм тероризму, інформаційний не потребує фізичних атак, адже інформаційні операції здатні досягати масштабного впливу через поширення панічних повідомлень, фейкових новин, відеоконтенту або маніпуляцій у цифровому середовищі. Його характерною рисою є прихований, системний характер впливу, який ускладнює ідентифікацію джерела загрози та правову кваліфікацію дій.

Попри наявність концептуальних положень у Концепції 2019 року, українське законодавство наразі не містить чіткого юридичного визначення поняття «інформаційний тероризм». Закон «Про боротьбу з тероризмом» формулює загальні засади протидії терористичній діяльності, проте не деталізує інформаційні форми реалізації терористичних намірів, що створює нормативну прогалину. У зв’язку з розвитком цифрових технологій, соціальних мереж та платформ миттєвого обміну даними, така невизначеність обмежує ефективність правозастосовної практики у сфері інформаційної безпеки. Водночас Концепція вказує на необхідність створення системи моніторингу, аналізу контенту, виявлення джерел деструктивної інформації та формування відповідного законодавчого підґрунтя для реагування на інформаційні загрози. Отож,

інформаційний тероризм постає як нова форма терористичної діяльності, що використовує інформаційний простір як поле протистояння. Він охоплює

широкий спектр дій, від поширення дезінформації та кібератак до психологічного впливу на суспільство через маніпулювання фактами й емоціями. В умовах збройної агресії проти України цей феномен набуває особливої актуальності, адже спрямований на руйнування інформаційного середовища та на послаблення морально-психологічного потенціалу громадян, роз'єднання суспільства та підрив довіри до державних інституцій. Боротися з інформаційним тероризмом можливо лише через комплексний підхід, що поєднує правове регулювання, технологічні інструменти моніторингу, міжнародну співпрацю та розвиток інформаційної грамотності населення. У цьому сенсі аналіз зазначених нормативних актів засвідчує необхідність деталізацію поняття інформаційного тероризму в українському законодавстві як окремого явища, що має потенціал спричиняти масштабні наслідки для національної безпеки без застосування фізичного насильства.

Порівняльний аналіз концепцій (Додаток А), засвідчує, що інформаційний тероризм еволюціонує від вузько технічного до комплексного соціально психологічного та політико-комунікаційного явища. Його розуміння у сучасному науковому і правовому дискурсі виходить за межі традиційного трактування тероризму як фізичного насильства і акцентує на інформації як головному інструменті дестабілізації. Наукові підходи зосереджуються на когнітивних, комунікаційних і технологічних аспектах, тоді як нормативні документи України визнають інформаційний простір сферою терористичних ризиків, але потребують подальшого розвитку правового визначення та інституційних механізмів реагування. Інформаційний тероризм у сучасній науковій і правовій традиції формується як окремий феномен гібридних загроз, що поєднує інформаційно-психологічний, комунікаційний і технологічний впливи, спрямовані на підрив безпеки суспільства, держави чи міжнародної спільноти. Його сутність полягає у свідомому використанні інформації, цифрових технологій і медіаінструментів як засобу досягнення деструктивних політичних,

ідеологічних чи соціальних цілей через формування стану страху, хаосу, недовіри, паніки або дезорієнтації населення. На відміну від класичних

форм тероризму, інформаційний тероризм не потребує фізичного насильства, а його головною зброєю є маніпуляція свідомістю, викривлення фактів, поширення фейкових повідомлень і дезінформаційних кампаній, що дестабілізують суспільну систему. У широкому розумінні це будь-яка системна діяльність, спрямована на дестабілізацію політичних процесів, руйнування соціальної єдності чи підрив довіри до владних інституцій шляхом використання інформаційного впливу як інструменту терору.

З урахуванням наукових підходів і положень українського законодавства, інформаційний тероризм можна визначити як системну діяльність фізичних чи юридичних осіб, державних або недержавних сторін, спрямовану на навмисне порушення інформаційної, психологічної та політичної стабільності суспільства через цілеспрямоване використання інформаційних технологій, засобів масової комунікації, мережевих ресурсів і маніпулятивних методів впливу з метою досягнення політичних, ідеологічних або воєнних цілей. Його мета полягає у створенні атмосфери страху, недовіри чи хаосу, впливі на процеси прийняття рішень, зниженні стійкості держави до зовнішнього чи внутрішнього тиску. Такий тероризм характеризується відсутністю фізичного насильства, але високим рівнем психологічної, політичної та когнітивної деструктивності, що ускладнює його ідентифікацію і правову кваліфікацію. У практичному вимірі це може проявлятися через кібератаки на державні інформаційні системи, створення панічних наративів у соціальних мережах, поширення фейкових новин чи маніпулятивних меседжів, які впливають на політичну поведінку або масову свідомість. Проблема визначення інформаційного тероризму полягає у відсутності міжнародного консенсусу та чіткого нормативного закріплення, що створює труднощі у кваліфікації таких діянь у правовій площині. Міжнародна наукова спільнота розглядає його крізь призму кібербезпеки, когнітивних воєн, інформаційних маніпуляцій і психологічних операцій, що розмиває межу між

злочином, пропагандою та політичним впливом. Водночас український контекст актуалізує цю проблему через системну інформаційну агресію з боку зовнішніх сторін, спрямовану на підрив внутрішньої єдності, деморалізацію населення та

делегітимацію державних інституцій. Це вимагає як нормативного уточнення поняття, так і створення механізмів оперативного виявлення, нейтралізації та превенції таких загроз. Узагальнюючи, інформаційний тероризм є складовим елементом гібридних війн і новітніх форм терористичної активності, у яких інформація стає основним ресурсом і зброєю. Його ефективність зумовлюється масовістю доступу до цифрових комунікацій, швидкістю поширення контенту, глобальною природою мережевих взаємодій і слабкістю механізмів міжнародного контролю. Тому протидія інформаційному тероризму потребує комплексного підходу, що поєднує правову кодифікацію, розвиток технологічних засобів моніторингу, міжнародну координацію, зміцнення інформаційної безпеки держави та підвищення рівня медіаграмотності населення. Лише синтез цих заходів здатен забезпечити адекватну відповідь на інформаційні загрози, які, не маючи фізичного прояву, становлять не меншу небезпеку для стабільності держав і безпеки громадян у XXI столітті.

1.2. Основні види та форми інформаційного тероризму

В сучасній науковій літературі немає єдиної класифікації інформаційного тероризму, проте більшість дослідників виділяють дві основні його форми: кібертероризм та медіа-інформаційний тероризм. Кібертероризм охоплює техногенні атаки на інформаційну інфраструктуру (наприклад, злам комп’ютерних систем, виведення з ладу мереж, викрадення або знищення даних), тобто застосування високих технологій для завдання шкоди або створення загрози. Натомість медіа-інформаційний тероризм – це психологічний терор через інформаційний простір: цілеспрямовані маніпуляції інформацією, масове поширення дезінформації, фейків і пропаганди з метою впливу на свідомість людей та посіяти паніку або ненависть. Ці два різновиди часто переплітаються, адже технічні кібератаки можуть слугувати засобом доставки

пропагандистських повідомлень (наприклад, злам телеканалу для трансляції фейкових новин), а інформаційно-психологічні атаки можуть використовувати кіберінструменти (соціальні мережі, ботоферми) для масштабування свого

впливу.[19] Основні форми й прояви інформаційного тероризму охоплюють низку взаємопов’язаних явищ, що зазвичай реалізуються комплексно та взаємно підсилюють одне одного. Ключовим виміром є дезінформація і фейкові новини, тобто навмисне поширення неправдивої або спотвореної інформації для введення аудиторії в оману; вона може постати як повністю вигадані «новини», як конспіративні теорії чи як цілеспрямоване перекручення фактів. Показовим є системне тиражування російськими державними медіа під час війни проти України відомих фальсифікацій, зокрема сюжету про «розіп’ятого хлопчика» у Слов’янську 2014 року, коли вигадану історію про розп’яття дитини українськими військовими продемонстрували у федеральному ефірі; цей випадок став хрестоматійним прикладом логіки «постправди», коли шок використовується для розпалювання ненависті й легітимації агресії.

Дезінформаційний компонент лежить в основі більшості інших форм інформаційного терору, формуючи паралельну реальність для маніпуляції масовою свідомістю. Тісно пов’язана з цим пропаганда як практика систематичного поширення тенденційної інформації, не обов’язково цілком хибної, з метою сформувати потрібні погляди, у контексті інформаційного тероризму набуває примусового, насильницького характеру через інформаційне перевантаження і емоційний тиск, що позбавляють аудиторію змоги критично оцінювати повідомлення. Перед повномасштабним вторгненням 2022 року в Україні така пропаганда створила тло «суцільної загрози» через постійні сюжети про нібито «злочини українців» і «геноцид російськомовних», покликані виправдати агресію і залякати населення.=пні 2022-го з вкиданням фейку про «реанімацію Президента Зеленського», яку організували російські хакери. Нарешті, інформаційний терор реалізується через соціальні маніпуляції та психологічні операції, що охоплюють псевдосоціологічні вкиди, перекручення

новин і цілеспрямоване поширення панічних чуток із експлуатацією наявних соціальних розколів, етнічних, релігійних, політичних. Типовою є стратегія

[19] Lysko T. D., Klimuk O. O., Lysianska D. V. Information terrorism as a threat to national security and a method of information warfare. *Juridical scientific and electronic journal*. 2022. No. 10. P. 574–576. URL: https://doi.org/10.32782/2524-0374/2022-10/143 (date of access: 22.10.2025).

нагнітання наративів «неминучої загрози» та змовницьких версій у соціальних мережах для індукції страху й ірраціональної реакції; у 2020–2022 роках це проявлялося, зокрема, через поширення тез про «біолабораторії США в Україні» чи «радіаційні провокації», що мали відвернути увагу від реальних дій РФ, підірвати довіру до української влади та союзників і психологічно дестабілізувати населення.[20] Такі операції здійснюються і на мікрорівні за допомогою масових SMS із закликами складати зброю або повідомленнями про «зраду керівництва» для деморалізації військ і цивільних, чим досягається головний ефект інформаційного терору, індукований страх, дезорієнтація та руйнування суспільної суб'єктності.

Отже, інформаційний тероризм проявляється як комбінування технічних (кібер) атак із контентними (інформаційно-пропагандистськими). Його відмінна риса – створення атмосфери страху та дестабілізації через інформаційні засоби, на відміну від класичного тероризму, що використовує фізичне насильство. Важливо розуміти конкретні канали та інструменти, якими користуються інформаційні терористи для досягнення своїх цілей. Традиційні засоби масової інформації (телебачення, радіо, преса) залишаються потужним каналом для інформаційного терору. Держави-агресори та терористичні організації нерідко використовують підконтрольні телеканали або радіостанції для трансляції пропаганди. Телебачення впливове завдяки візуальному контенту, який легко сприймається усіма віковими групами і долає мовні бар'єри. Наприклад, у розпал конфліктів пропагандистські телеканали показують шокуючі постановочні кадри насильства або жертви серед мирного населення, щоб викликати страх чи ненависть. Такі сюжети часто не дають глядачу часу на осмислення – емоційний ефект досягається обсягом та частотою показу. Важливо зазначити, що й

міжнародні мережі можуть ставати ретрансляторами дезінформації – зокрема, російські канали RT, Sputnik в минулі роки були впіймані на систематичному

[20] Котляров В. Кібертероризм як загроза міжнародній безпеці. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2023. № 5(71). С. 46–54. URL: https://doi.org/10.32689/2523-4625-2023-5(71)-6 (дата звернення: 22.10.2025).

поширенні викривлених наративів про Україну, США, ЄС (за що їх діяльність згодом обмежили в Європі через порушення стандартів об'єктивності. [21] Соціальні мережі Facebook, Twitter (X), YouTube, Instagram, TikTok та інші платформи стали головним полем бою інформаційних війн у сучасному світі. Через соцмережі дезінформація розходиться вірусно, її важко контролювати, а аудиторія вимірюється сотнями мільйонів. Інформаційні терористи активно застосовують бот-акаунти, «ботферми» і фейкові профілі для масового тиражування своїх меседжів. Наприклад, під час виборів у США 2016 року російські агенти впливу через тисячі фальшивих акаунтів та таргетовану рекламу охопили аудиторію до 126 мільйонів американців на Facebook, просуваючи роз'єднувальні та екстремістські повідомлення. У Twitter було виявлено не менш як 2752 облікові записи, пов'язані з російськими операціями впливу. [22] Подібні величезні масштаби охоплення роблять соцмережі дуже привабливим інструментом інформаційного тероризму – через них можна точково націлювати пропаганду на окремі групи (за інтересами, регіоном, політичними вподобаннями), створюючи ефект інформаційних «бульбашок». Алгоритми соцмереж нерідко підсилюють резонанс скандального або емоційного контенту, що грає на руку дезінформаторам. Окрім публічних соцмереж, велика частка шкідливої інформації шириться через відносно закриті канали: Telegram, WhatsApp, Viber, Signal та інші месенджери, а також тематичні форуми і чати. Telegram-канали в умовах війни стали одними з основних джерел новин для населення, і цією довірою зловживає противник – створюються фейкові канали «під місцевих жителів» чи від імені чиновників, які в критичний момент можуть поширити панічний фейк. Месенджери небезпечні тим, що інформація там часто

подається як «інсайдерська» або від знайомих, що підвищує довіру. До того ж, у закритих чатах складніше відслідковувати і спростовувати фейки. Терористичні

[21] Bentzen N., Russell M. Russia's disinformation on Ukraine and the EU's response. Brussels : European Parliament, 2015. 7 p. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/571339/EPRS_BRI(2015)571339_EN.pdf (date of access: 20.10.2025).

[22] Solon O., Levin S. Divisive Russian-backed Facebook ads released to the public. *the Guardian*. URL: https://www.theguardian.com/technology/2017/nov/01/facebook-ads-russia-us-election-fake-news-released public (date of access: 01.10.2025).

організації на Близькому Сході (ІДІЛ тощо) теж широко використовували Telegram для пропаганди та координації, оскільки він забезпечує відносну анонімність і розповсюдження без цензури.

Також важливими є й інші канали, коли можна віднести платформи обміну відео (наприклад, TikTok, де короткі вірусні відео можуть формувати викривлену картину подій), стрімінгові сервіси, блогохостинги, а також традиційні методи на кшталт друкованих листівок чи «сарафанного радіо». Хоча основний акцент нині на цифрових медіа, традиційні методи не зникли: у зоні конфлікту можуть поширюватися чутки через агентів впливу в місцевих громадах, або ж за допомогою «телефонного терору» (масових анонімних дзвінків з фальшивими повідомленнями про мінування тощо). Отже, будь-який засіб комунікації може стати каналом інформаційного тероризму, якщо його використовувати для масового залякування та обману.[23]

Інструментарій інформаційних терористів характеризується високим ступенем диференціації та технологічної складності. У науковій літературі прийнято класифікувати засоби інформаційно-терористичної діяльності на дві основні категорії: технічні та контентні, хоча в операційній практиці ці компоненти функціонують як взаємопов'язана система. Технічні інструменти забезпечують дистрибуцію та ампліфікацію шкідливого контенту, тоді як контентні методи реалізують безпосередній психологічний вплив на цільову аудиторію. Серед технічних засобів провідне місце посідають боти та ботнети, що являють собою автоматизовані акаунти або скомпрометовані пристрої, інтегровані у координовані мережеві структури. Ботоферми здатні генерувати

масові потоки однорідних повідомлень, штучно формуючи уявлення про домінуючу суспільну думку або актуальність певної тематики. Механізм їхнього функціонування передбачає синхронізоване коментування публікацій у соціальних мережах із використанням уніфікованих тез, що дозволяє маніпулювати наративним простором. Ботнети застосовуються для штучного

[23] В'ячеслав Юренко. Короткі формати відео та мікроінфлюенсери: революція контенту на YouTube, TikTok та Reels. *CASES*. URL: https://cases.media/article/korotki-formati-video-ta-mikroinflyuenseri-revolyuciya-kontentu-na youtube-tiktok-ta-reels (дата звернення: 01.10.2025).

розгону хештегів, координованих атак на сторінки опонентів через механізми скарг та спаму, а також для маніпулювання трендовими алгоритмами платформ. Масштабність, яку забезпечують ботнети, створює у реальних користувачів ілюзію всеохопної підтримки певної позиції, що суттєво впливає на формування індивідуальних і колективних переконань.[24] Фішингові технології та методи кібершпигунства становлять критичний елемент інструментарію інформаційного тероризму. Фішингові розсилки реалізуються через імітацію легітимних електронних комунікацій з метою отримання автентифікаційних даних або інсталяції шпигунського програмного забезпечення на пристрої потенційних жертв. Після успішної компрометації системи доступу зловмисники отримують можливість вилучення конфіденційної інформації, зокрема приватного листування посадових осіб, із подальшою публікацією цих даних супроводжуваною маніпулятивним трактуванням. Емпіричним підтвердженням ефективності таких методів слугує інцидент 2016 року, коли через фішингову атаку було скомпрометовано електронне листування штабу Гіларі Клінтон, що згодом було оприлюднено через платформу WikiLeaks і спричинило значний інформаційний скандал у період виборчої кампанії. Компрометація акаунтів авторитетних осіб або інформаційних ресурсів уможливлює розміщення дезінформації від їхнього імені, що підвищує довіру аудиторії до фальсифікованого контенту. Техніки соціальної інженерії, мережеве шпигунство та кейлогери функціонують як комплементарні інструменти, що посилюють ефективність психологічних операцій через інтеграцію викрадених даних або

встановлення контролю над комунікаційними каналами.[25]

Стрімка еволюція технологій штучного інтелекту уможливила появу якісно нового інструменту інформаційного тероризму – діпфейк-технологій. Діпфейк являє собою синтезований засобами машинного навчання аудіовізуальний контент, у якому реальна публічна особа демонструє дії або висловлює позиції,

[24] Що таке ботнет? | CyberCalm. *CyberCalm | Кіберзахист та кібербезпека простою мовою*. URL: https://cybercalm.org/shho-take-botnet/ (дата звернення: 01.10.2025).
[25] Що таке фішинг? | Захисний комплекс Microsoft. *Your request has been blocked. This could be due to several reasons.* URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-phishing (дата звернення: 01.10.2025).

які фактично не мали місця. Технологічна досконалість сучасних діпфейків забезпечує високий рівень переконливості імітації зовнішності та голосових характеристик. Показовим є випадок березня 2022 року, коли було створено діпфейк-відео Президента України Володимира Зеленського, у якому він нібито закликав українські Збройні сили до капітуляції. Цей фальсифікат короткочасно транслювався через скомпрометований телеканал, проте був оперативно ідентифікований як підробка.[26] Діпфейк-технології дозволяють генерувати дезорієнтацію серед військовослужбовців та цивільного населення, систематично підриваючи довіру до офіційних комунікацій керівництва держави. Додатково ці технології застосовуються для фабрикації псевдодоказів у пропагандистських наративах або дискредитації публічних осіб через створення компрометуючого контенту. Протидія діпфейкам вимагає розробки спеціалізованих технологічних рішень для верифікації автентичності контенту та підвищення медіаграмотності населення щодо можливостей сучасних фальсифікаційних технологій.[27] Комерційні рекламні інструменти соціальних мереж, зокрема Facebook Ads та Google Ads, уможливлюють таргетування повідомлень на чітко визначені демографічні та психографічні сегменти аудиторії. Інформаційні операції експлуатують ці механізми через запуск таргетованої реклами з дезінформаційним змістом, що демонструється виключно обраним групам користувачів. Така сегментація суттєво ускладнює виявлення фейкового контенту, оскільки різні аудиторні групи експонуються до

диференційованих меседжів. Іноземні агенти впливу використовують мікротаргетинг у виборчих кампаніях, демонструючи консервативним виборцям одні наративи, а лібералам – кардинально протилежні, що поглиблює суспільну поляризацію. У 2016 році російські структури систематично купували рекламу на платформі Facebook з провокативним змістом стосовно зброї, расових проблем та релігійних питань, адресуючи диференційовані меседжі різним

[26] Catalina Marchant de Abreu. Truth or Fake - Debunking a deepfake video of Zelensky telling Ukrainians to surrender. *France 24*. URL: https://www.france24.com/en/tv-shows/truth-or-fake/20220317-deepfake-video-of zelensky-telling-ukrainians-to-surrender-debunked (date of access: 01.10.2025).
[27] Deepfakes and international conflict | Brookings. *Brookings*. URL: https://www.brookings.edu/articles/deepfakes-and international-conflict/ (date of access: 01.10.2025).

сегментам населення Сполучених Штатів з метою стимулювання міжгрупових конфліктів. Таким чином легітимні маркетингові інструменти трансформуються у засоби здійснення інформаційно-терористичних операцій.[28]

Психологічні операції становлять комплексну систему інформаційно психологічного впливу, що плануються спеціалізованими фахівцями, часто у структурі спецслужб. Ці операції інтегрують поширення чуток, інсценування медійних подій, рекрутування лідерів думок та ініціювання хештег-кампаній. Стратегічна мета полягає у модифікації поведінкових патернів цільової аудиторії через маніпулювання емоційними станами, мотиваційними структурами та ціннісними орієнтирами. Емпіричною ілюстрацією служать кампанії на Донбасі у 2014 році, коли проукраїнськи налаштованих мешканців переконували у зраді Києвом їхніх інтересів та неминучості переслідувань, що фасилітувало підтримку сепаратистських рухів. Психологічні операції можуть спрямовуватися на деморалізацію військових формувань через поширення інформації про значні втрати або зрадництво командування, або, альтернативно, на радикалізацію протестних рухів через провокаторську діяльність у соціальних мережах. Сучасні психологічні операції характеризуються інтенсивним використанням даних соціальних мереж для ідентифікації суспільних настроїв та вразливих точок, а також застосуванням елементів нейролінгвістичного програмування в контенті для латентного впливу на підсвідомі процеси.[29] Додатковий

інструментарій інформаційного тероризму включає широкий спектр методів різної природи. Фальсифікація документів та візуальних матеріалів через фотомонтаж або створення псевдоофіційних листів дозволяє конструювати псевдодокументальну базу для дезінформаційних наративів. Шантаж та викрадення даних з вимогою викупу під загрозою публічного оприлюднення конфіденційної інформації функціонують як форма інформаційного тероризму з

[28] Петришин Г. Р. Інформаційний тероризм: джерела формування та активізації в Україні. *Габітус : науковий журнал*. 2021. Т. 21. С. 44–50. URL: http://dspace.tnpu.edu.ua/handle/123456789/19054 (дата звернення: 01.10.2025).

[29] Kharamurza D. Information terrorism as a tool of hybrid warfare and a destructive factor of the media space. *Integrated communications*. 2023. Vol. 16, no. 2. P. 29–37. URL: https://doi.org/10.28925/2524-2644.2023.163 (date of access: 01.10.2025).

економічною мотивацією. SEO-спам реалізується через створення фейкових веб сайтів або масове продукування низькоякісного контенту з метою витіснення достовірної інформації з пошукової видачі. Мережі професійних тролів, що являють собою оплачуваних осіб для систематичного коментування публікацій із заданим наративом, провокують конфлікти та відволікають увагу від релевантних тем. Незважаючи на гетерогенність цих методів, їх об'єднує спільна стратегічна мета – досягнення інформаційного ефекту терору через придушення волі до опору, генерування хаосу, маніпулювання аудиторією на користь агресора або паралізацію її здатності до цілеспрямованих дій.[30]

Систематизація форм, каналів та інструментарію інформаційного тероризму демонструє його фундаментальну трансформацію від одновимірного феномену до складної багаторівневої системи гібридного впливу на масову свідомість. Додаток Б ілюструє конвергенцію технічного та контентного компонентів інформаційно-терористичних операцій, де технологічна інфраструктура функціонує як мультиплікатор психологічного ефекту, а змістовні маніпуляції набувають безпрецедентної масштабності через цифрові канали дистрибуції. Критичною особливістю сучасного інформаційного тероризму є його здатність до адаптивної диференціації інструментарію залежно від специфіки цільової аудиторії та операційного контексту. Кібертехнічні атаки на інфраструктурному

рівні забезпечують початкову дестабілізацію та несанкціонований доступ до каналів комунікації, створюючи технологічну основу для подальшого впровадження дезінформаційних наративів. Емпіричні дані засвідчують системну кореляцію між множинністю використовуваних каналів та ефективністю досягнення цільових психологічних ефектів. Операції з максимальним резонансом характеризуються одночасним задіянням принаймні трьох-чотирьох різнотипових каналів із синхронізованим контентним наповненням, що створює ефект інформаційного оточення та унеможливлює критичну дистанцію реципієнта від маніпулятивного повідомлення. Показовим

[30] Бадер А. Тероризм як інструмент інформаційної агресії. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2025. № 1(77). С. 11–16. URL: https://doi.org/10.32689/2523- 4625-2025-1(77)-2 (дата звернення: 01.10.2025).

є приклад втручання у виборчий процес США 2016 року, де російські структури експлуатували соціальні мережі через ботнети, таргетовану рекламу, викрадену через фішинг конфіденційну інформацію та мікросегментоване психографічне профілювання, досягаючи ефекту через багатоканальну синхронізацію впливу.

Технологічна еволюція штучного інтелекту радикально розширила операційні можливості інформаційних терористів, надаючи їм інструментарій для створення синтетичного контенту з високим рівнем переконливості, що фундаментально підриває традиційні механізми верифікації інформації. Діпфейк-технології та алгоритмічна генерація тексту трансформують інформаційний простір у середовище епістемологічної невизначеності, де розмежування автентичного та фабрикованого контенту вимагає спеціалізованих технічних засобів і високого рівня медіаграмотності. Це створює структурну асиметрію між виробництвом дезінформації та її спростуванням, оскільки генерація фальсифікованого контенту потребує значно менших ресурсів і часу порівняно з процедурами його верифікації та публічного спростування. Аналіз цільових психологічних ефектів виявляє стратегічну орієнтацію інформаційного тероризму на досягнення трьох взаємопов'язаних цілей. По-перше, індукція масового страху та паніки через створення атмосфери перманентної загрози та непередбачуваності, що паралізує раціональне прийняття рішень як на

індивідуальному, так і на колективному рівнях. По друге, дезінтеграція соціальної суб'єктності через поглиблення наявних розколів та конструювання нових ліній конфлікту, що унеможливлює консолідовану відповідь суспільства на зовнішню загрозу. По-третє, підрив довіри до легітимних інститутів та авторитетних джерел інформації, що створює вакуум достовірності, який заповнюється маніпулятивними наративами агресора. Критичним викликом для систем національної безпеки стає необхідність розробки комплексної стратегії протидії, яка інтегрує технологічні рішення для детекції фальсифікацій, законодавче регулювання цифрового простору, підвищення медіаграмотності населення та міжнародну координацію у сфері інформаційної безпеки. Фрагментарність поточних підходів до боротьби з

інформаційним тероризмом залишає вразливості у захисті інформаційного суверенітету держав, що підтверджується прогресуючою інтенсифікацією інформаційних атак у геополітичних конфліктах останнього десятиліття.

1.3. Інформаційний тероризм як сучасна загроза міжнародній безпеці

Сучасна архітектура міжнародної безпеки зазнає фундаментальної трансформації під впливом якісно нових загроз, серед яких інформаційний тероризм посідає провідне місце в ієрархії глобальних викликів. За даними Всесвітнього економічного форуму 2024 року, дезінформація та відсутність кібербезпеки посіли відповідно перше та четверте місця серед найбільших ризиків для людства [31], що засвідчує безпрецедентну актуалізацію інформаційно технологічних загроз у глобальному дискурсі безпеки. Трансформація традиційних форм тероризму у цифровий простір створює нову парадигму асиметричних конфліктів, де психологічний вплив на масову свідомість через інформаційні канали набуває стратегічного значення, порівнянного з класичними формами військової агресії. Масштаби терористичних операцій у 2024-2025 роках демонструють експоненціальну динаміку зростання як за кількісними, так і за якісними параметрами. Згідно з даними Центру

стратегічних та міжнародних досліджень, кількість значущих кібератак зросла утричі порівняно з попереднім роком, причому 89 інцидентів були класифіковані як загрози національного значення. Китайські структури здійснили понад 1300 цілеспрямованих атак на 14 ключових секторів економіки, що свідчить про системний характер інформаційної агресії.[32] Європейське агентство з кібербезпеки зафіксувало, що між липнем 2023 та червнем 2024 років найбільше постраждали сектори державного управління, охорони здоров'я та цифрової інфраструктури, де атаки мали комплексний характер із одночасним

[31] World Economic Forum. Spotlight on cybersecurity: 10 things you need to know in 2024. URL: https://www.weforum.org/stories/2024/10/cybersecurity-threats-in-2024/ (date of access: 01.10.2025). [32] Significant Cyber Incidents. *Center for Strategic & International Studies*. 2025. URL: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (date of access: 01.10.2025).

застосуванням технічних та контентних компонентів впливу.[33] За оцінками дослідницької компанії DeepMedia, у 2023 році було зафіксовано понад 500 000 відео- та аудіодіпфейків у цифровому просторі, тоді як прогнозні моделі передбачають зростання до 8 000 000 одиниць синтетичного контенту до 2025 року.[34] [35] Статистика Insikt Group документує вісімдесят два випадки використання діпфейків проти публічних осіб у 38 країнах протягом дванадцяти місячного періоду липень 2023 - липень 2024, причому 30 країн проводили або планували проводити вибори в цей період, що підкреслює цілеспрямований характер інформаційних атак на демократичні процеси.[36] Надзвичайно тривожним є той факт, що 6.5 % всіх зафіксованих випадків шахрайства вже включають діпфейк-компонент, а спроби фінансового шахрайства з використанням синтетичних медіа зросли на 2 137 % протягом трьох років.[37]

Технологічна досконаліть сучасних діпфейків створює безпрецедентні виклики для систем верифікації інформації. Дослідження засвідчують, що точність ідентифікації високоякісних відеодіпфейків людиною становить лише 24.5 %??, тоді як для зображень цей показник підвищується до 62 %. [38] Критично важливим є те, що лише 0.01 % учасників експериментів демонстрували

стабільну здатність розпізнавати фальсифікації в змішаних тестах. Ця епістемологічна невизначеність підриває фундаментальні основи суспільної довіри до інформаційних потоків та створює структурну асиметрію між виробництвом дезінформації та її спростуванням, оскільки створення переконливого діпфейку коштує приблизно 100 доларів і не вимагає

[33] European Parliament. Cybersecurity: Main and Emerging Threats. URL: https://www.europarl.europa.eu/topics/en/article/20220120STO21428/cybersecurity-main-and-emerging threats (date of access: 02.10.2024).
[34] SQ Magazine. Deepfake Statistics 2025: The Hidden Cyber Threat. URL: https://sqmagazine.co.uk/deepfake statistics/ (date of access: 01.10.2023).
[35] Romanishyn A., Malytska O., Goncharuk V. AI-driven disinformation: policy recommendations for democratic resilience. *Frontiers in Artificial Intelligence*. 2025. Vol. 8. URL: https://doi.org/10.3389/frai.2025.1569115 (date of access: 01.10.2025).
[36] Recorded Future. 2024 Deepfakes and Election Disinformation Report. 2024. URL: https://www.recordedfuture.com/research/targets-objectives-emerging-tactics-political-deepfakes (date of access: 01.10.2025).
[37] SQ Magazine. Deepfake Statistics 2025: The Hidden Cyber Threat. URL: https://sqmagazine.co.uk/deepfake statistics/ (date of access: 01.10.2025).
[38] SQ Magazine. Deepfake Statistics 2025: The Hidden Cyber Threat. URL: https://sqmagazine.co.uk/deepfake statistics/ (date of access: 01.10.2025).

спеціалізованих технічних навичок, тоді як його детекція потребує складних алгоритмічних систем та експертного аналізу.[39] Емпіричні свідчення демонструють глибоку інтеграцію інформаційно-терористичних тактик у геополітичні конфлікти. Російська Федерація здійснила майже 70% збільшення кількості кібератак проти України протягом 2024 року, зафіксувавши 4 315, що цільово спрямовувалися на критичну інфраструктуру, включаючи урядові сервіси, енергетичний сектор та оборонні установи. Кібероперації супроводжувалися систематичними кампаніями дезінформації, де діпфейк технології використовувалися для створення фальшивих заяв від імені українського керівництва. Тактики діпфейків застосовувалися в контексті президентських виборів на Тайвані 2024 року, де хвиля дезінформаційних кампаній включала фабриковані відео та аудіозаписи з метою дискредитації політичних фігур Демократичної прогресивної партії.[40]

Китайські кіберструктури демонструють системний підхід до інформаційного тероризму з акцентом на довготривале проникнення у критичну інфраструктуру. Операція Salt Typhoon, атрибутована китайським державним

акторам, призвела до компрометації щонайменше восьми американських телекомунікаційних провайдерів та операторів у понад 20 країнах як частину масштабної шпигунсько-розвідувальної кампанії. Атака, яка тривала приблизно два роки, забезпечила доступ до метаданих телефонних дзвінків клієнтів та даних запитів правоохоронних органів, а також компрометувала приватні комунікації осіб, залучених до урядової або політичної діяльності. У грудні 2024 року китайські хакери скомпрометували сторонній сервіс Міністерства фінансів США, отримавши доступ до понад 3 000 некласифікованих файлів, включаючи документи, пов'язані з ключовими посадовими особами та Комітетом з іноземних інвестицій. Кількість щоденних спроб кібератак на Тайвань

[39] Cybersecurity and the Deepfake, Disinformation and Misinformation Challenge. *Cybersecurity Certifications and Continuing Education | ISC2*. URL: https://www.isc2.org/Insights/2025/02/Deepfakes-Disinformation_Misinformation (date of access: 01.10.2025).

[40] The Malicious Exploitation of Deepfake Technology: Political Manipulation, Disinformation, and Privacy Violations in Taiwan | Global Taiwan Institute. *Global Taiwan Institute*. URL: https://globaltaiwan.org/2025/05/the-malicious exploitation-of-deepfake-technology/ (date of access: 01.10.2025).

подвоїлася до 2 400 000 у 2024 році, при цьому успішні атаки зросли на двадцять % порівняно з 2023 роком.[41] Іранські та північнокорейські структури також активно експлуатують інформаційно-терористичні методології. Іран інтенсифікував шпигунські зусилля проти урядових агентств Об'єднаних Арабських Еміратів, розгортаючи спеціалізоване шкідливе програмне забезпечення для ексфільтрації конфіденційних автентифікаційних даних.

Північнокорейські хакери здійснили найбільшу в історії криптовалютну крадіжку, викравши півтора мільярда доларів в ефіріумі з дубайської біржі ByBit у лютому 2025 року, експлуатуючи вразливість у програмному забезпеченні третьої сторони та відмивши щонайменше сто шістдесят мільйонів доларів протягом перших сорока восьми годин після атаки. Ці операції фінансують подальші інформаційно-терористичні кампанії та розробку технологічних засобів дестабілізації. Вплив інформаційного тероризму на виборчі процеси демонструє його потенціал до системної дестабілізації демократичних інститутів. Під час виборів у Сполучених Штатах 2016 року російські структури

через тисячі фальшивих акаунтів та таргетовану рекламу охопили аудиторію до 26 000 000 американців на платформі Facebook, просуваючи роз'єднувальні та екстремістські повідомлення. У Twitter було ідентифіковано 2 752 облікових записи, пов'язані з російськими операціями впливу. Китайські актори здійснили координовану дезінформаційну кампанію в месенджері WeChat проти канадського кандидата на лідерство Ліберальної партії Христі Фріленд у лютому 2025 року. У Словаччині напередодні виборів з'явилося діпфейк-аудіо про нібито виборче шахрайство, що спричинило значний резонанс у політичному дискурсі. У Туреччині президент Ердоган використав діпфейк для зв'язування лідера опозиції з терористичними групами під час виборчої кампанії.[42]

[41] Hacıoğlu S. Ö. The Major Cyber Breaches and Attack Campaigns of 2024. *Automated Security Validation Platform | Picus*. URL: https://www.picussecurity.com/resource/blog/the-major-cyber-breaches-and-attack-campaigns-of 2024 (date of access: 01.10.2025).

[42] Significant Cyber Incidents. *Center for Strategic & International Studies*. 2025. URL: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (date of access: 01.10.2025).

Таблиця 1.1 Кількісні показники інформаційно-терористичної діяльності у глобальному вимірі (2023-2025 рр.)

Категорія загрози	Географічний охоплення	Кількісні показники	Динаміка зростання	Цільові сектори/об'єкти
Кібератаки національного значення	Глобальний	89 інцидентів (2024)	Зростання утричі порівняно з 2023	Критична інфраструктура, державне управління
Китайські цілеспрямовані атаки	Міжнародний	1 300 атак	Системний характер	14 ключових економічних секторів
Діпфейк контент (відео/аудіо)	Глобальний цифровий простір	500 000 одиниць (2023), прогноз 8 000 000 (2025)	Зростання у 16 разів за 2 роки	Публічні особи, виборчі процеси
Діпфейки проти політичних	38 країн	82 зафіксовані випадки (липень 2023 -	30 країн з виборами у цей період	Демократичні інститути,

фігур		липень 2024)		лідери держав
Шахрайство з діпфейк компонентом	Міжнародний фінансовий сектор	6,5% від усіх випадків шахрайства	Зростання на 2 137% за 3 роки	Фінансові установи, корпорації
Точність виявлення діпфейків людиною	Експериментальні дослідження	24,5% (відео), 62% (зображення), 0,1% (стабільні учасники)	Прогресуюче зниження ефективності	Системи верифікації інформації
Російські кібератаки на Україну	Україна	4 315 інцидентів (2024)	Зростання на 70% порівняно з 2023	Урядові сервіси, енергетика, оборона
Операція Salt Typhoon (Китай)	США та 20+ країн	8 телекомунікацій них провайдерів скомпрометован о	Тривалість операції ~2 роки	Телекомуніка ції , метадані дзвінків, приватні комунікації
Компрометація Міністерства фінансів США	США	3 000+ некласифіков ан их файлів	Грудень 2024	Ключові посадові особи, CFIUS
Кібератаки на Тайвань	Тайвань	2 400 000 спроб щодня (2024)	Подвоєння кількості, успішні атаки +20%	Урядові системи, телекомунікації
Північнокорейська криптовалютна крадіжка	ОАЕ (біржа ByBit)	1,5 млрд доларів (лютий 2025)	Найбільша в історії	Криптовалютні біржі, відмито 160 млн за 48 годин
Російський вплив на вибори США	США	126 млн користувачів Facebook, 2 752 акаунти Twitter	Вибори 2016 року	Виборчі процеси, суспільна думка

Китайська дезінформація в Канаді	Канада	Кампанія проти Х. Фріленд	Лютий 2025	Виборчі кампанії, лідери партій

Джерело: сформовано самостійно автором на основі власного дослідження

Систематизація емпіричних даних щодо інформаційно-терористичної діяльності у 2023–2025 роках засвідчує фундаментальну трансформацію архітектури глобальних загроз, де інформаційний простір набуває статусу повноцінного театру військових дій. Кількісні показники демонструють експоненціальну динаміку зростання із потроєнням кібератак національного значення та прогнозованим 16-кратним збільшенням обсягу діпфейк-контенту протягом двох років, що свідчить про перехід від спорадичних інцидентів до системної інструменталізації інформаційних технологій у геополітичних конфліктах. Географічна концентрація активності навколо стратегічно значущих держав виявляє чітку координацію держав, зокрема 1 300 китайських атак на 14 економічних секторів, 70 % збільшення російських кібератак проти України до 4 315 інцидентів та подвоєння щоденних спроб на Тайвань до 2 400 000. Багаторічні операції на кшталт Salt Typhoon з компрометацією 8 американських телекомунікаційних провайдерів у понад 20 країнах демонструють якісно новий рівень складності стратегічного проникнення у критичну інфраструктуру. Діпфейк-феномен створює епістемологічну кризу верифікації інформації, де точність людської ідентифікації відеофальсифікацій становить лише 24.5%, а стабільну здатність розпізнавання демонструють лише 0.01 % учасників експериментів. Структурна асиметрія між тривіальністю виробництва дезінформації за сто доларів і складністю її детекції генерує сприятливе середовище для масштабної експлуатації технологічної вразливості, що підтверджується зростанням фінансового шахрайства з діпфейк-компонентом на 2137% за три роки. Виборчі процеси стають пріоритетними цілями для інформаційно-терористичних операцій, що засвідчується 82 зафіксованими випадками використання діпфейків проти публічних осіб у 32 країнах, причому тридцять країн проводили вибори в цей період. Російське охоплення 126 000

проти канадського кандидата Фріленд та використання діпфейків у Словаччині і Туреччині ілюструють глобальне поширення практик втручання незалежно від рівня технологічного розвитку держав. Фінансово-економічний вимір набуває системної значущості через північнокорейську операцію з викрадення півтора мільярда доларів із дубайської біржі ByBit, що стала найбільшою криптовалютною крадіжкою в історії та генерує ресурси для подальших інформаційно-терористичних кампаній, створюючи самопідтримувану екосистему гібридних загроз з власною економічною базою.

Узагальнюючи, можна констатувати досягнення критичного порогу, за яким фрагментарні інциденти трансформуються у системний виклик міжнародній безпеці. Конвергенція державних та недержавних акторів, синергія кібертехнічних і психологічних методологій, експоненціальне зростання можливостей синтетичних медіа та прогресуюче зниження когнітивної здатності суспільства до верифікації інформації створюють умови для масштабної дестабілізації демократичних систем. Відсутність скоординованої міжнародної відповіді та фрагментарність національних підходів залишають критичні вразливості, які систематично експлуатуються для руйнування довіри до інститутів, дезінтеграції соціальної суб'єктності та паралізації здатності до колективного прийняття рішень у демократичних суспільствах.

Висновки до розділу І

Узагальнюючи результати розділу, можна констатувати, що інформаційний тероризм вийшов за межі вузько технічного чи пропагандистського явища і формує окремий, якісно відмінний тип терористичної діяльності. Проаналізовані дефініції й концепції показують поступовий перехід від редукції цього феномену до кіберзлочинів або медіа-маніпуляцій до його розуміння як системної практики цілеспрямованого руйнування інформаційної, психологічної та політичної стабільності суспільства. Водночас зберігається дефініційна й методологічна

невизначеність: немає єдиного підходу до розмежування інформаційного тероризму з інформаційною війною, кібербезпековими інцидентами та

політичною комунікацією, що безпосередньо обмежує можливості його правової кваліфікації та вироблення уніфікованих механізмів протидії. Розгляд інформаційного тероризму в контексті міжнародної безпеки та емпіричний аналіз динаміки кібератак, використання діпфейків і втручання у виборчі процеси показують, що інформаційний простір перетворився на повноцінний театр асиметричних конфліктів. Зростання масштабів і складності операцій, конвергенція інтересів державних і недержавних акторів, а також структурна асиметрія між простотою виробництва дезінформації та складністю її виявлення означають перехід від окремих інцидентів до стійкого системного виклику. Український контекст демонструє особливу гостроту проблеми: при формальному визнанні інформаційного виміру у базових актах протидії тероризму відсутнє спеціалізоване нормативне визначення інформаційного тероризму та чітко окреслені механізми притягнення до відповідальності за інформаційно-психологічні операції. У результаті розділ фіксує ключові методологічні та практичні розриви: між швидкістю еволюції інформаційно терористичних тактик і повільністю правових та інституційних відповідей; між міждисциплінарним характером явища й фрагментарністю існуючих дослідницьких підходів; між глобальною природою загроз і національно обмеженими рамками регулювання. Подальші дослідження та політика мають бути спрямовані на формування інтегрованої концептуальної моделі інформаційного тероризму, уточнення його правового статусу, розвиток технологічних інструментів детекції та зміцнення суспільної стійкості до маніпуляцій як необхідної умови збереження демократичних інститутів в умовах гібридних загроз.

РОЗДІЛ ІІ. ВПЛИВ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ НА МІЖНАРОДНУ БЕЗПЕКУ

2.1. Вплив інформаційного тероризму на політичну стабільність держав

Інформаційний тероризм чинить багатоаспектний вплив на політичну стабільність держави, зачіпаючи інтереси особистості, суспільства та держави на всіх рівнях їхньої взаємодії. Глазов О.В. наголошує, що «інформаційна безпека стає невід'ємною складовою кожної зі сфер національної безпеки» і водночас є важливою самостійною сферою забезпечення національної безпеки. [43] Ця теза підкреслює комплексний характер впливу інформаційних загроз на всі аспекти життєдіяльності держави. На індивідуальному рівні інформаційний тероризм спрямований на формування у громадян почуття страху, невпевненості та безпорадності. Масовий страх, породжений інформаційними атаками, «не просто засліплює суспільство. Він сіє розбрат: ми починаємо боятися не тільки завтрашнього дня й подальшого шокуючого розвитку подій – ми починаємо боятися один одного»[44]. Це призводить до атомізації суспільства, руйнування соціальних зв'язків та зниження спроможності громадян до колективної дії та опору. Такий страх розколює суспільство, змушує одних його членів побоюватися інших, змушуючи їх діяти наперекір один одному, створюючи справді некеровані й неконтрольовані ситуації.

На загальнодержавному рівні, рівні суспільства інформаційний тероризм спрямований на дестабілізацію соціально-політичної ситуації, підрив легітимності влади та провокування конфліктів. Ломака І.І., Липчук О.І. та Кобець Ю.В. визначають головні загрози інформаційній безпеці на суспільному рівні, включаючи розповсюдження ідей, що провокують конфлікти на національному, релігійному та міжетнічному ґрунті, а також розпалювання ідей

[43] Глазов О. В. Міжнародний інформаційний тероризм у контексті загроз національній безпеці України. Наукові праці. Політологія. 2012. Випуск 185. Том 197. С. 78-82.

[44] Жайворонок О. І. Сучасні загрози інформаційного тероризму в умовах гібридної війни проти України. Державне управління: удосконалення та розвиток. 2018. № 4. С. 1-5. URL: http://www.dy.nayka.com.ua/pdf/4_2018/103.pdf (дата звернення: 01.10.2025).

сепаратизму.[45] Формування якісного інформаційно-аналітичного простору,

плюралізм, багатоканальність отримання інформації, незалежні потужні ЗМІ є необхідними елементами забезпечення інформаційної безпеки на суспільному рівні. Особливу небезпеку становить використання інформаційного тероризму для маніпуляції суспільною свідомістю під час виборчих кампаній. Втручання у вибори через соціальні мережі, поширення фейкових новин та використання фабрик тролів стали звичним явищем у сучасному політичному процесі.

Це підриває основи демократії та довіру громадян до виборчих процедур. Намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації є однією з основних загроз інформаційній безпеці держави. Інформаційний тероризм також сприяє поглибленню соціальної поляризації. Алгоритми соціальних мереж створюють «інформаційні бульбашки», в яких користувачі отримують лише ту інформацію, яка підтверджує їхні існуючі переконання. Це призводить до радикалізації поглядів, зниження толерантності та готовності до діалогу між різними суспільними групами. Поширення засобами масової інформації культу насильства, жорстокості, порнографії є додатковим фактором деструктивного впливу на суспільну свідомість. Дестабілізація суспільства через інформаційний тероризм може викликати масові заворушення, протести та навіть революційні потрясіння. Складовою політичної функції сучасного тероризму є дискредитація органів державного управління в суспільній свідомості, підрив їхнього авторитету, прагнення продемонструвати політичну недієздатність владних інститутів у встановленні законності та правопорядку, руйнування базових основ демократичного світоустрою.[46] Значні зусилля терористичних структур спрямовуються на створення в соціумі атмосфери страху, панічних настроїв, тривожних очікувань. Подібний стан масової свідомості розглядається терористами як найважливіша складова для досягнення заявлених політичних

[45] Ломака І. І., Липчук О. І., Кобець Ю. В. Інформаційна безпека держави: теоретико-методологічні засади та особливості в умовах збройного конфлікту. *Регіональні студії*. 2022. № 31. С. 113-118. DOI: https://doi.org/10.32782/2663-6170/2022.31.21

[46] Глазов О. В. Міжнародний інформаційний тероризм у контексті загроз національній безпеці України. Наукові праці. Політологія. 2012. Випуск 185. Том 197. С. 78-82.

цілей. Одним з аспектів даної функції є прагнення (на тлі домінуючих негативних переживань) впровадити в суспільну свідомість ідею певної моральної переваги терористів над суспільством та його владою. [47]

На рівні держави інформаційний тероризм становить пряму загрозу національній безпеці, територіальній цілісності та суверенітету. Глазов О.В. зазначає, що серед загроз інформаційній безпеці на державному рівні особливе місце посідають «спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив». Інформаційна безпека держави означає стан її захищеності, за якої спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдають суттєвої шкоди національним інтересам. Інформаційний тероризм здатен паралізувати критичну інфраструктуру держави, порушити функціонування органів державної влади та підірвати обороноздатність країни. Жайворонок О.І. наголошує, що «доступність інформаційних технологій значно підвищує ризики інформаційного тероризму. Розвиненість інформаційної інфраструктури суспільства сприяє створенню додаткових ризиків інформаційного тероризму». Чим вище рівні інтелектуалізації та інформатизації суспільства, тим важливішою стає його інформаційна безпека, оскільки реалізація інтересів, цілей держав і народів дедалі більше здійснюється за допомогою інформаційних, а не матеріально енергетичних впливів. Особливої актуальності набуває проблема інформаційного тероризму в умовах гібридних війн. Бадер А. підкреслює, що «тероризм як суспільно-політичне явище виник наприкінці XIX ст., а протягом першої XX ст. набув своїх основних сутнісних характеристик, серед яких

[47] Гончар М. В. Вплив соціальних мереж на політичні системи у контексті суперництва демократичних та авторитарних режимів. Науковий журнал «Політикус». 2024. Випуск 5. С. 11-18. DOI: https://doi.org/10.24195/2414-9616.2024-5.2 (дата звернення: 01.10.2025).

ключовою є інформаційний резонанс».[48] В епоху глобалізації завдяки сучасним медіа та телекомунікаційним технологіям цей інформаційний ефект лише посилився, перетворивши інформаційний простір на арену міждержавного протистояння. Терористичні акти передусім спрямовані на психологічний тиск – залякування, створення масової паніки та підрив довіри до державних інститутів.

Важливим аспектом впливу на державному рівні є небезпека для економічної незалежності держави, пов'язана з нерозвиненістю внутрішнього ринку високотехнологічної продукції та відсутністю його ефективного захисту від іноземної технічної і технологічної експансії. Науково-технологічне відставання держави від розвинутих країн, еміграція висококваліфікованих працівників за межі країни також створюють додаткові ризики для інформаційної безпеки та посилюють вразливість до інформаційного тероризму.

Інформаційний тероризм як явище перетинається з такими поняттями, як інформаційна війна, пропаганда та кібервійна. Хоча між ними є багато спільного (пов’язані з використанням інформації), важливо розуміти ключові відмінності, особливо в контексті політичного впливу на загальнодержавному рівні.

Таблиця 2.1. Опис концептуальних понять

Поняття	Ключові риси та відмінності
Інформаційний тероризм	Це форма тероризму, де головна зброя – інформація. Мета – залякати або дестабілізувати суспільство, примусити до потрібних дій через паніку чи маніпуляцію свідомістю. Інформаційний тероризм фокусується на створенні атмосфери страху та безвиході методами інформаційного впливу (фейки, погрози, шок-контент). Наприклад, масове поширення неправдивих повідомлень про «неминучі теракти» або демонстрація наджорстоких відео страт – щоб паралізувати волю людей. Від звичайної пропаганди відрізняється інтенсивністю і насильницьким характером впливу (психологічне насильство). Від кібер-війни відрізняється тим, що головна ціль – психіка, а не інфраструктура (хоч може бути засобом).
Інформаційна війна	Ширше поняття, яке означає комплекс заходів інформаційного протиборства між державами чи групами. Мета інформаційної війни – отримати стратегічну перевагу, впливаючи на думки і переконання мас або дезорганізуючи супротивника. Вона включає і пропаганду, і дезінформацію, і захист власних комунікацій. Інформаційна війна може вестися і в мирний час (наприклад, інформаційний тиск однієї країни на іншу), і під час воєн як складова гібридної війни. На

	відміну від інформаційного тероризму, інформаційна війна не обов'язково

[48] Бадер А. Тероризм як інструмент інформаційної агресії. Наукові праці Міжрегіональної академії управління персоналом. Політичні науки та публічне управління. 2025. Випуск 1 (77). С. 11-16. DOI: https://doi.org/10.32689/2523-4625-2025-1(77)-2 (дата звернення: 01.10.2025).

41

	переслідує терористичну ціль залякування – вона може більш тонко формувати потрібні наративи, підривати авторитет влади, вербувати союзників тощо. Інформаційний тероризм можна вважати однією з тактик або екстремальних форм інформаційної війни, коли застосовується саме терористичний почерк (шок і страх як метод). Якщо образно: інформаційна війна – це спектр операцій, а інформаційний тероризм – найгостріші з них, націлені на психологічний шок.
Пропаганда	Інструмент і явище, що полягає у цілеспрямованому поширенні тенденційної, часто неправдивої інформації з метою впливу на масову свідомість. Пропаганда може бути частиною як інформаційної війни, так і інформаційного тероризму. Ключова відмінність: пропаганда сама по собі не обов'язково має на меті залякати – вона може переконувати, «промивати мізки», вихваляти потрібні ідеї. Пропаганда – поняття старіше і нейтральніше: існує навіть поняття «соціальна пропаганда» (не шкідлива). Але в контексті, що нас цікавить, це агресивна брехня або напівправда на службі політики. Наприклад, російські державні ЗМІ брехали про Україну системно – це пропаганда; коли ж ця брехня досягає крайнощів на кшталт фейків про розп'ятих дітей, що сіють жах, – пропаганда стає інфотерором. Отже, пропаганда – це радше зброя, тоді як інформаційний тероризм – режим її застосування (з наміром тероризувати). Пропаганда може тривати роками на низькому вогні, інформаційний тероризм – це завжди ескалація до емоційного терору.
Кібервійна / кібератаки	Це поняття стосується протиборства у кіберпросторі – атак на комп'ютерні системи, мережі, дані. Кібервійна часто є частиною інформаційної війни (наприклад, зламати сервер – щоб викрасти дані для подальшої дезінформації, або щоб позбавити супротивника зв'язку). Проте фокус кібервійни – технічний: завдати шкоди інфраструктурі противника, викрасти секрети, паралізувати системи управління. Інформаційний тероризм же зосереджений на психологічному ефекті. Втім, межі іноді розмиті: коли хакери зламують телевізійний ефір і передають фейк, це водночас і кіберінцидент, і інформаційна атака. Різниця в мотивації: кіберзлочинець може атакувати банк заради грошей – це кіберзлочин, але не інформаційний терор. А от якщо державні хакери вирубають електростанцію і паралельно через медіа роздмухують паніку від блекауту – це вже поєднання кібернетичного удару з інформаційним терором. Тобто, кібервійна – про комп'ютери, інформаційна війна – про людей. Інформаційний тероризм оперує людьми, їх емоціями, хоча часто й через комп'ютерні канали.

Джерело: сформовано самостійно автором на основі власного дослідження [49]На практиці всі ці явища переплітаються. Сучасна гібридна агресія включає і кібератаки, і пропаганду, і елементи тероризування населення через медіа. Проте, розрізнення важливе для правильної відповіді: якщо пропаганду можна нищити правдивою інформацією, то проти інформаційного терору однієї правди може бути замало – потрібні ще заходи психологічного захисту, іноді і

[49] Леонов Б., Лихова С. Інформаційний тероризм як загроза національній безпеці України. Scientific works of National Aviation University. Series: Law Journal "Air and Space Law". 2021. Т. 2, № 59. С. 170–176. URL: https://doi.org/10.18372/2307-9061.59.15615 (дата звернення: 01.10.2025).

правові механізми (як проти тероризму звичайного). Аналогічно, кібербезпека сама не вирішить проблеми, коли ворог б’є по серцях і умах – тут вступають в дію фахівці з комунікацій, психологи, медіаексперти.

Країни ЄС останніми роками також зазнали численних інформаційно психологічних атак, більшість з яких пов’язують з активністю Росії. Європейські уряди прямо говорять про російську дезінформацію як загрозу. Мета цих атак – посіяти розбрат всередині європейських суспільств, підірвати довіру до ЄС і НАТО, а також вплинути на політичні процеси (вибори, референдуми). Один із перших дзвіночків пролунав під час міграційної кризи 2015–2016 років. Тоді Кремль, за даними дослідників, активно маніпулював темою біженців: прокремлівські медіа звинувачували ЄС у неспроможності захистити громадян від «ісламських терористів», роздували окремі інциденти за участю мігрантів, поширювали фейки про злочини біженців. Метою було розпалити ксенофобію і підірвати європейську солідарність (і значною мірою це вдалося, підтримка крайньоправих партій зросла, в деяких країнах були інциденти насильства на ґрунті ненависті, що можна трактувати як опосередкований результат інформаційного терору). У Німеччині став відомим фейк «справа Лізи» (2016) – вигадана історія про російськомовну дівчинку, нібито зґвалтовану мігрантами в Берліні, яку підхопили російські ЗМІ; розслідування показало, що історія неправдива, але вона викликала масові протести російської діаспори і

напруження у німецькому суспільстві.[50]

Це класичний приклад інформаційної атаки на соціально чутливу тему, аби через страх і гнів впливати на політичний порядок денний. Європа також відчула на собі втручання у вибори і референдуми. У 2016 році під час референдуму щодо Brexit у Британії, за даними розслідувань, тисячі фейкових акаунтів з Росії агітували за вихід з ЄС, поширюючи дезінформацію про Євросоюз. Хоча важко оцінити їхній вплив, факт залишається, зовнішні гравці прагнули інформаційно тероризувати британський електорат страхами про мігрантів, «диктат Брюсселя»

[50] Nestoras A. How the Kremlin is manipulating the Refugee Crisis: Russian Disinformation as a Threat to European Security. *Institute of European Democrats*. 2019. P. 14. URL: https://www.iedonline.eu/download/2019/IED-Research Paper-Russia-as-a-security-provider_January2019.pdf (date of access: 01.10.2025).

тощо. У 2017 році у Франції перед другим туром виборів зламали пошту команди Еммануеля Макрона («MacronLeaks»), викрадені дані виклали в інтернет з метою зашкодити Макрону, паралельно у соцмережах фабрикувалися фейки проти нього. Французька кіберполіція заявляла про «іноземний слід», і хоч масштабної зміни громадської думки не сталося, цей кібервзлом був спробою дестабілізувати демократичний процес. У Німеччині спецслужби попереджали про кібератаки на Бундестаг (2015) і спроби проросійської пропаганди вплинути на вибори 2017 року, зокрема, поширювалися тези, що санкції проти Росії шкодять самій Німеччині, що кандидатку Ангелу Меркель «підтримують США» тощо. Частину цих наративів озвучували через російськомовні медіа для німецької аудиторії, частину – через соцмережі та маргінальні сайти.[51]

ЄС з часом виробив механізми відповіді. У 2015 році була створена команда East StratCom Task Force зі штаб-квартирою в Брюсселі, яка запустила проект EU vs Disinfo, моніторинг та викриття дезінформації, головно проросійської. За кілька років вони зібрали тисячі прикладів фейків і регулярно публікують спростування на офіційному сайті. Також деякі країни ухвалили закони проти дезінформації: у Франції ввели покарання за фейкові новини під час виборів, Німеччина зобов’язала соцмережі видаляти незаконний контент (включно з мовою ворожнечі) швидко під загрозою штрафів. Литва, Латвія,

Естонія як фронтові держави ще з 2014 року блокують ретрансляцію російських телеканалів, що ловлять на пропаганді війни і розпалюванні ненависті. Великобританія через регулятора Ofcom штрафувала RT за порушення стандартів, а після початку війни 2022 взагалі відкликала ліцензію RT на мовлення у Британії. Усі ці кроки перш за все спрямовані на спроба обеззброїти інформаційних терористів на їхніх каналах поширення.[52]

[51] Nestoras A. How the Kremlin is manipulating the Refugee Crisis: Russian Disinformation as a Threat to European Security. *Institute of European Democrats*. 2019. P. 14. URL: https://www.iedonline.eu/download/2019/IED-Research Paper-Russia-as-a-security-provider_January2019.pdf (date of access: 01.10.2025).

[52] Bentzen N., Russell M. Russia's disinformation on Ukraine and the EU's response. Brussels : European Parliament, 2015. 7 p. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/571339/EPRS_BRI(2015)571339_EN.pdf (date of access: 20.10.2025).

Однак Європа стикається і з новими формами: китайська пропаганда (наприклад, щодо COVID-19 було багато дезінформації з китайських джерел), антивакцинаторські рухи (які активно розпалювали російські тролі під час пандемії), і навіть проіранські кампанії (хоч менш масштабні). Міжнародний прецедент ЄС свідчить: інформаційний тероризм не знає кордонів. Кремль використовував відкритість європейських медіа для поширення своїх токсичних наративів, але Європа поступово вчиться давати відсіч – законодавчо, технічно і шляхом просвіти. Втім, виклики залишаються: треба знайти баланс між боротьбою з дезінформацією і свободою слова, а також встигати за технологічними змінами, адже противник не стоятиме на місці.

Близькосхідний регіон дав кілька сумнозвісних прикладів інформаційного тероризму, пов'язаного насамперед з діяльністю екстремістських угруповань. Найбільш показовий кейс, «Ісламська держава» (ІДІЛ), яка у період 2014–2017 років розгорнула безпрецедентну за масштабом і жорстокістю медіа-кампанію. ІДІЛ використовувала сучасні технології і соціальні платформи, щоб пропагувати свої ідеї, залякувати ворогів і вербувати прибічників по всьому світу. Їхня офіційна медіа-продукція включала високоякісні відеоролики страт заручників, бойових дій, а також псевдорелігійні послання. Ці відео мали

декілька цілей: інтернаціоналізувати страх (щоб ніхто у світі не почувався в безпеці), надихнути радикальних ісламістів приєднатися до «священної війни», і створити образ всемогутності халіфату. Фахівці відзначають, що ІДІЛ фактично продемонструвала новий вимір «цифрового тероризму», вміло маніпулюючи психологічними, риторичними та релігійними мотивами для впливу. [53] Їхня пропаганда була надзвичайно агресивною: сцени насильства спеціально постановочні, змонтовані як трейлери до фільмів жахів, супроводжувалися саундтреками, тобто все зроблено, щоб шокувати глядача і закарбуватися в пам'яті. Соціальні мережі та месенджери стали основним каналом для цієї жахаючої інформаційної кампанії. ІДІЛ освоїв Twitter (де автоматизовані боти

-[53] Propaganda in focus: decoding the media strategy of ISIS - Humanities and Social Sciences Communications. *Nature*. URL: https://www.nature.com/articles/s41599-024-03608-y (date of access: 01.10.2025).

поширювали їхні хештеги тисячами), Facebook, а згодом особливо Telegram – останній надавав змогу вести канали та чати з відносною безпекою від блокувань. Через інтернет ІДІЛ залучив до своїх лав тисячі іноземних бойовиків (у тому числі з Європи, Центральної Азії), багато з яких радикалізувалися повністю онлайн. Це продемонструвало, що пропаганда терору здатна перетинати географічні межі без фізичної присутності терористів – достатньо медіаконтенту. Відтак міжнародна коаліція проти ІДІЛ приділяла значну увагу протидії їхньому медіафронту: зусиллями хакерів і спецслужб закривалися сотні аккаунтів, блокувався доступ до сайту журналу "Dabiq" (офіційного друкованого органу ІДІЛ), проводились контрпропагандистські кампанії. Наприклад, урядові структури США та європейські НУО запускали відеоролики, де колишні бойовики ІДІЛ розповідали про реальний жах життя під їхньою владою – щоб нейтралізувати романтизований образ «халіфату», який ІДІЛ малювала у своїх відео. Це боротьба за розуми і серця на тлі терору.[54]

Іншим виміром інформаційного тероризму на Близькому Сході є пропаганда з боку державних діячів у ході воєн. Наприклад, під час громадянської війни в Сирії, режим Башара Асада та його союзники (РФ, Іран)

систематично використовували медіа для тероризування населення, яке підтримувало опозицію: показували жорстокі кадри розправ як «попередження», поширювали теорії змови про «терористів-сунітів», щоб мобілізувати свою базу. З іншого боку, антиурядові сили та екстремісти теж вдавалися до інформаційного терору, знімали показові страти солдатів режиму, обстрілів цивільних районів і виставляли це як помсту. Усе це створювало атмосферу взаємного страху.[55] В Ізраїльсько-Палестинському конфлікті також присутній компонент інформаційного тероризму: екстремістські угруповання на кшталт ХАМАС поширювали відео ракетних обстрілів із тріумфальними піснями, аби підняти бойовий дух своїх і вселити страх ізраїльтянам; у відповідь ізраїльські

[54] Syrinska O. A. Isil as a Hybrid Networked Organization: History, Ideology and Information Strategy. *The Oriental Studies*. 2015. Vol. 2015, no. 70. P. 114–133. URL: https://doi.org/10.15407/skhodoznavstvo2015.70.114 (date of access: 01.10.2025).

[55] Панфілов О. Сирійські немовлята російської пропаганди. *Крым.Реалии*. URL: https://ua.krymr.com/a/27293544.html (дата звернення: 01.10.2025).

військові акаунти публікують відео ліквідації лідерів бойовиків, щоб деморалізувати супротивника. Соцмережі в ці періоди заповнені шокуючими образами руйнувань, загиблих, і нерідко обидві сторони звинувачують одна одну у фейках (постановочних кадрах, старих фото з інших воєн тощо). [56] Це показує, яка тонка грань між інформуванням і залякуванням у воєнний час. У підсумку, досвід Близького Сходу демонструє, що терористичні та екстремістські сили давно зробили інформацію своєю зброєю нарівні з бомбами та кулями. ІДІЛ тільки найбільш відома з них, але й інші (Аль-Каїда, таліби в Афганістані, шиїтські воєнізовані формування) – всі мають свої «PR-відділи», які займаються інформаційним терором: погрожують, вербують, лякають, розпалюють ненависть. Не даремно кажуть, що «тероризм живе в телевізорі» сенс терористичної акції багато в чому в тому, щоб її показали якнайбільшій аудиторії і посіяли страх. Тепер, у цифрову епоху, терористи самі транслюють свої акції і досягають глобальної аудиторії без посередництва медіа.

В азійських країнах проблематика інформаційного тероризму теж проявилася різними гранями. Один із найтрагічніших прикладів – криза

рохінджа в М’янмі (Бірмі). У 2016–2017 роках світ став свідком етнічних чисток щодо мусульман-рохінджа у М’янмі, і розслідування показали, що значну роль у розпалюванні ненависті зіграли соціальні мережі, зокрема Facebook. В країні, де раніше інтернетом майже не користувались, стрімка поява смартфонів і Facebook без належної медіакультури призвела до того, що фейкові новини і мова ворожнечі ширились неконтрольовано. Бірманські націоналісти (в тому числі деякі буддійські монахи-екстремісти) через Facebook поширювали страшні чутки: ніби рохінджа готують джихад, ґвалтують жінок, підпалюють села буддистів. Ці дописи ставали вірусними, згідно з розслідуванням Reuters, було виявлено тисячі постів і коментарів з відвертою мовою ненависті до рохінджа. У результаті, коли м’янмарська армія почала каральні операції, значна частина населення сприймала це якщо не з схваленням, то принаймні без протесту,

[56] Супермаркет пропаганди: Ізраїль та Палестина | ADASTRA. *ADASTRA I Аналітичний центр*. URL: https://adastra.org.ua/blog/supermarket-propagandi-izrayil-ta-palestina (дата звернення: 01.10.2025).

вважаючи мусульман і «терористами». Наслідки жахливі: близько 700 тисяч рохінджа втекли з країни, рятуючись від насильства. ООН назвала цю кризу «найшвидшою у світі». Отож маємо приклад того, як інформаційний тероризм у формі розпалювання етнічної ненависті онлайн може призвести до геноциду. Згодом Facebook визнало свої помилки і посилило модерацію у М’янмі, але було пізно. Розглянутий кейс став наукою для всіх, великі платформи тепер уважніше стежать за «риторикою ненависті» у регіонах конфліктів.[57]

В інших країнах теж є феномени, що потрапляють під поняття інформаційного тероризму. Китай активно використовує інформаційні технології для контролю власного населення (тотальна цензура, пропаганда через державні медіа) і для впливу за кордоном. Китайська компартія інвестує в глобальні медіа (наприклад, CGTN, China Daily) і у бот-мережі, які просувають пробурантівські наративи або атакують критиків КНР (приклад – масовані кампанії дезінформації про походження COVID-19, де бот-акаунти поширювали теорії змови, або цькування онлайн активістів за права уйгурів). Китайська модель

дещо відрізняється: це більше «інформаційна війна» і пропаганда, але елементи терору присутні, погрози тайванцям військовим вторгненням через ролики, або коли через соцмережі розганяють паніку на фінансових ринках (фейкові новини від китайських хакерів викликали коливання акцій).[58]

Індія та Пакистан, тут інформаційне протистояння також триває десятиліттями, особливо щодо Кашміру. Пакистанські і про-пакистанські джерела поширюють інформацію про нібито «геноцид мусульман у Кашмірі», тоді як індійські, про «пакистанських терористів».[59] Обидві сторони використовують соцмережі для впливу на міжнародну думку, інколи вдаючись і до явних фейків. Внутрішньо в Індії був скандал з WhatsApp (2018–2019), коли

[57] NV.ua. Зайвий народ. Як мусульманську меншину рохінджа жорстоко витісняють з М'янми і не пускають в Бангладеш. URL: https://nv.ua/ukr/world/geopolitics/zajvij-narod-jak-musulmanska-menshina-rohindzha-zhorstoko vitisnjajut-z-m-janmi-i-ne-puskajut-v-bangladesh-1762375.html (дата звернення: 01.10.2025). [58] Кацімон О. AP: Китай використовує фейкові новини як інструмент впливу у глобальній грі. *detector.media*. URL: https://detector.media/infospace/article/232772/2024-09-28-ar-kytay-vykorystovuie-feykovi-novyny-yak instrument-vplyvu-u-globalniy-gri/ (дата звернення: 01.10.2025).

[59] Pakistan leader Imran Khan warns of "genocide" as is India accused of torture in Kashmir. *CBS News | Breaking news, top stories & today's latest headlines*. URL: https://www.cbsnews.com/news/kashmir-news-india-accused-torture pakistan-imran-khan-warns-genocide-muslims-today-2019-08-30/ (date of access: 01.10.2025).

через фейкові повідомлення про викрадення дітей натовпи лінчували невинних, можна сказати, що це стихійний інформаційний терор, коли чутки в месенджерах призвели до реального терору на вулицях.[60]

Південно-Східна Азія: окрім М'янми, вартий уваги приклад Філіппін, під час президентства Родріго Дутерте соцмережі заповнили «фабрики тролів», які тероризували опонентів президента онлайн (цькування журналістів, погрози активістам). Хоч це радше авторитарна пропаганда, але її метод – залякати критиків через інформаційний простір, що підпадає під нашу тему. Північна Корея використовує кібератаки як політичний інструмент: відомий випадок зламування студії Sony Pictures (2014) у відповідь на фільм «Інтерв'ю», що висміював Кім Чен Ина. Пхеньянські хакери викрали дані, розповсюдили їх та погрожували терактами в кінотеатрах, якщо фільм вийде. Це був приклад кібертерористичного залякування – і справді, Sony спершу скасувала покази через страх. Тут стирається грань між кібератакою і інформаційним терором, бо

кібератака стала каналом для поширення страхітливого меседжу (про можливі вибухи, якщо не послухаються вимог). Отже, азійський регіон дає зрозуміти, що інформаційний тероризм – універсальний феномен. Він може набувати різних форм залежно від контексту: етнічна ненависть (М'янма), екстремістська релігійна пропаганда від ІДІЛ, державна пропаганда і кіберзалякування, інформаційні війни між державами (Індія–Пакистан). В усіх випадках спільним є використання страху і дезінформації як зброї проти цілих груп людей.

2.2. Економічні наслідки інформаційного тероризму для глобальної безпеки

Інформаційний тероризм у сучасному розумінні являє собою комплексну загрозу, що поєднує технологічні атаки на цифрову інфраструктуру з маніпулятивними операціями впливу, спрямованими на дестабілізацію економічних систем, підрив довіри до інституцій та створення умов для масштабного перерозподілу фінансових ресурсів. За оцінками компанії

-[60] Curtis J. Kashmir: Renewed India-Pakistan tensions. URL: https://researchbriefings.files.parliament.uk/documents/CBP-10264/CBP-10264.pdf (date of access: 01.10.2025).

CompTIA, глобальні втрати від кіберзлочинності досягнуть 10,5 трильйонів доларів США щорічно до 2025 року, що становить зростання на 10 % порівняно з попереднім роком. [61] Якби кіберзлочинність розглядалася як окрема економіка, вона посідала б третє місце у світі після США та Китаю, перевершуючи сукупний валовий внутрішній продукт Франції, Італії та Іспанії.[62] Ця трансформація кіберзагроз у системний глобальний ризик відображає фундаментальні зміни в архітектурі міжнародної безпеки, де цифровий простір стає основною ареною економічного протистояння між державними та недержавними акторами. Прямі економічні збитки від кібератак демонструють експоненціальне зростання та диверсифікацію векторів впливу. Федеральне бюро розслідувань США зареєструвало понад 859 тисяч скарг на інтернет-злочини протягом 2024 року з загальними втратами, що перевищили 16 млн. дол. США, що становить зростання на 33 % порівняно з 2023 роком.[63]

Середня вартість однієї кібератаки в Сполучених Штатах становить приблизно 27,37 млн. дол. США що включає витрати на відновлення даних, юридичні процедури, регуляторні штрафи та репутаційні втрати. [64] Згідно з дослідженням IBM та Інституту Понемона, глобальна середня вартість витоку даних у 2024 році досягла історичного максимуму в 4,88 млн. дол. США Критично важливим аспектом є тривалість виявлення та локалізації інцидентів, яка в середньому становить 258 днів, що створює пролонгований період уразливості для постраждалих організацій та дозволяє зловмисникам здійснювати багаторівневу експлуатацію скомпрометованих систем. Організації,

[61] Cybercrime Statistics 2024–2025: Scale, Costs, Vectors. *DeepStrike*. URL: https://deepstrike.io/blog/cybercrime statistics-2025 (date of access: 01.10.2025).
[62] Vergara Cobos E., Cakir S. A Review of the Economic Costs of Cyber Incidents. Washington, DC : {World Bank}, 2024.
URL:
https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919ffee4079180e81701969ad0a 18.pdf (date of access: 01.10.2025).
[63] Cybercrime Statistics 2024–2025: Scale, Costs, Vectors. *DeepStrike*. URL: https://deepstrike.io/blog/cybercrime statistics-2025 (date of access: 01.10.2025).
[64] Ciphertex. The Cost of Cyber Theft to the U.S. Economy in 2024. URL:
https://ciphertex.com/2024/05/24/the-cost-of cyber-theft-to-the-u-s-economy-in-2024/ (date of access: 01.10.2025).

які використовують системи безпеки на основі ШІ, можуть виявляти та локалізувати витоки даних на 108 днів швидше порівняно з іншими.[65]

Секторальний аналіз економічних наслідків інформаційного тероризму виявляє нерівномірний розподіл ризиків з концентрацією загроз у галузях критичної інфраструктури. Фінансовий сектор зазнав безпрецедентного тиску, при цьому 65 % організацій фінансових послуг повідомили про атаки програм вимагачів у 2024 році порівняно з 64 % у 2023 році, що підтверджує стійку тенденцію до зростання. Експлуатовані вразливості становили 40% основних причин атак у фінансовому секторі, а скомпрометовані облікові дані - 23%.[66] Міжнародний валютний фонд у звіті про глобальну фінансову стабільність за квітень 2024 року зазначив, що розмір екстремальних збитків від кіберінцидентів зріс більш

ніж у чотири рази з 2017 року до 2,5 млн. дол. США, при цьому непрямі втрати, пов'язані з репутаційними ризиками та модернізацією систем безпеки, суттєво перевищують прямі фінансові збитки. Атаки на фінансові установи становлять майже п'яту частину від загальної кількості кіберінцидентів, причому банки залишаються найбільш уразливою категорією через обсяги конфіденційних даних та транзакцій, які вони обробляють.[67] Сектор охорони здоров'я демонструє найвищі питомі витрати на один інцидент, що пояснюється критичною природою медичних послуг та регуляторними вимогами щодо захисту персональних даних пацієнтів. Дві третини організацій охорони здоров'я зазнали атак програм-вимагачів, при цьому середня вартість витоку даних у медичній галузі становила 10,93 млн. дол. США. Протягом періоду з 2020 по 2025 роки сектор охорони здоров'я витратить 125 млн. дол. США на захист від витоків інформації.[68] У 2024 році було зареєстровано понад 630 інцидентів з програмами-вимагачами, що вплинули на

-[65] IBM, {Ponemon Institute}. Cost of a Data Breach Report 2024. URL: https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics (date of access: 01.10.2025). [66] Shulmistra D. Ransomware attacks in finance hit new high (Updated 2025). *Invenio IT*. URL: https://invenioit.com/continuity/ransomware-attacks-finance/ (date of access: 01.10.2025). [67] International Monetary Fund. Global Financial Stability Report, Chapter 3: Cyber Risk. URL: https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial stability (date of access: 01.10.2025).
[68] Chief Healthcare Executive. Healthcare Cybersecurity Investment Forecast 2020-2025. URL: https://www.varonis.com/blog/ransomware-statistics (date of access: 01.10.2025).

медичні заклади по всьому світу, причому кількість атак зросла на 50% порівняно з попереднім роком.[69] Атака на Change Healthcare у лютому 2024 року скомпрометувала дані 100 мільйонів записів і стала однією з найсерйозніших атак першої половини року з індексом ризику 9,46 балів з 10 [70]. Унікальність загрози для медичного сектору полягає в тому, що кіберінциденти безпосередньо впливають на можливість надання медичної допомоги, створюючи ризики для життя та здоров'я пацієнтів, що трансформує загрозу в гуманітарну кризу.

Виробничий сектор став найбільш атакованою галуззю за кількістю інцидентів, при цьому кількість атак зросла на 61 % порівняно з попереднім роком.[71] Між січнем та вереснем 2025 року було зареєстровано 4701 інцидент з

програмами-вимагачами, з яких 2332, або 50 %, були спрямовані на критичні сектори, включаючи виробництво, охорону здоров'я, енергетику, транспорт та фінансові послуги. Високопрофільні інциденти, такі як глобальне відключення виробництва Jaguar Land Rover та порушення виробничих процесів Bridgestone, ілюструють, як програми-вимагачі можуть паралізувати ланцюги постачання та національні економіки. Сполучені Штати залишаються епіцентром активності програм-вимагачів проти критичної інфраструктури, становлячи приблизно 21% від глобальних атак у 2025 році з близько 1000 інцидентами, за якими слідують Канада, Німеччина, Великобританія та Італія.[72]

Атаки на ланцюги постачання представляють особливо небезпечний вектор економічних загроз через каскадний ефект впливу на взаємопов'язані бізнес-екосистеми. Атака програми-вимагача на CDK Global призвела до збитків, що перевищили 1 мільярд доларів, порушивши роботу автомобільних дилерських центрів у США та Канаді. Інцидент з оновленням CrowdStrike

[69] Fortinet. Ransomware Statistics Report 2024. URL: https://www.fortinet.com/resources/cyberglossary/ransomware statistics (date of access: 01.10.2025).

[70] Supply Chain Management Review. Analyzing the Supply Chain Risks Behind Top Data Breaches. URL: https://www.scmr.com/article/analyzing-the-supply-chain-risks-behind-the-top-data-breaches-in-2024 (date of access: 01.10.2025).

[71] Industrial Cyber. Manufacturing Sector Ransomware Growth Analysis. URL: https://industrialcyber.co/reports/half of-2025-ransomware-attacks-hit-critical-sectors-as-manufacturing-healthcare-and-energy-top-global-targets/ (date of access: 01.10.2025).

[72] KELA. Geographic Distribution of Ransomware Attacks Report. URL: https://industrialcyber.co/reports/half-of-2025-ransomware-attacks-hit-critical-sectors-as-manufacturing-healthcare-and-energy-top-global-targets/ (date of access: 01.10.2025).

вплинув приблизно на 8,5 млн. дол. США Windows по всьому світу, що стало одним з найбільших збоїв інформаційних технологій в історії. Великі організації стикаються з 25-% ймовірністю кібератаки на ланцюг постачання з середньою вартістю відновлення 4,9 мільйонів доларів.[73] У 2024 році близько 183 тисяч клієнтів постраждали від кібератак на ланцюги постачання по всьому світу. [74] Компанія Gartner прогнозує, що до кінця 2025 року 45% організацій зазнають атак на ланцюги постачання, що становить триразове зростання порівняно з 2021 роком. [75] Cybersecurity Ventures передбачає, що атаки на програмні ланцюги

постачання коштуватимуть підприємствам 138 млн. дол. США глобально до 2031 року, порівняно з 60 мільярдами доларів, прогнозованими на 2025 рік. [76] Витік даних National Public Data, що вплинув на 2,9 мільярди записів, продемонстрував вразливість брокерів даних як критичних вузлів цифрового ланцюга постачання з фінансовим впливом у 501,7 млн. дол. США. Атака на фармацевтичного дистриб'ютора Cencora на початку 2024 року вплинула принаймні на 27 фармацевтичних та біотехнологічних компаній і призвела до крадіжки персональних даних сотень тисяч осіб.[77] Для більшості організацій простій коштує понад 300 тисяч доларів за кожну годину перебування систем у офлайні, при цьому 72% організацій потребують більше тижня для повного відновлення операцій. У промисловому секторі середня вартість витоку даних досягла 5,56 мільйонів доларів у 2024 році, що становить зростання на 18% порівняно з попереднім роком, причому незаплановані простої можуть коштувати до 125 тисяч доларів за годину.[78]

[73] World Economic Forum. Supply Chain Cyber Resilience Report. URL: https://www.weforum.org/stories/2025/04/three-key-directions-for-the-cyber-resiliency-crisis-in-global-supply chains/ (date of access: 01.10.2025).

[74] Statista. Global Supply Chain Cyberattacks Customer Impact. URL: https://www.statista.com/statistics/1375129/supply-chain-attacks-customers-affected-global/ (date of access: 01.10.2025).

[75] Gartner. Supply Chain Attack Forecast 2025. URL: https://cybersecurityventures.com/software-supply-chain-attacks to-cost-the-world-60-billion-by-2025/ (date of access: 01.10.2025).

[76] Cybersecurity Ventures. Software Supply Chain Attack Cost Projection. URL: https://socradar.io/hidden-cost-of supply-chain-breaches-2025-statistics/ (date of access: 01.10.2025).

[77] Supply Chain Management Review. Cencora Pharmaceutical Breach Report. URL: https://www.scmr.com/article/analyzing-the-supply-chain-risks-behind-the-top-data-breaches-in-2024 (date of access: 01.10.2025).

[78] Cybersecurity Ventures. Software Supply Chain Attack Cost Projection. URL: https://socradar.io/hidden-cost-of supply-chain-breaches-2025-statistics/ (date of access: 01.10.2025).

Вплив інформаційного тероризму на малий та середній бізнес набуває особливої гостроти через обмеженість ресурсів та відсутність спеціалізованих захисних механізмів. 43 % кібератак спрямовані саме на малі підприємства, при цьому 46 % атак відбуваються в організаціях з менше ніж 1000 працівниками. [79] 61 % кібератак спрямовані на малі та середні підприємства, причому 51% малих підприємств не мають жодних заходів кібербезпеки.[80] Середня вартість витоку даних для підприємств з менше ніж 500 працівниками становить 2,98 млн. дол.

США, що може бути руйнівним для компаній з обмеженими бюджетами. Середні втрати малих та середніх підприємств від одного кіберінциденту становлять 25 тис. дол. США., хоча діапазон може коливатися від 826 до 653 587 доларів залежно від атаки. 82% атак програм-вимагачів спрямовані на малі підприємства, при цьому середня вартість відновлення після атаки для компаній з річним доходом менше 10 млн. дол. США становить 165 520 дол.. Критичною проблемою є те, що 60 % малих підприємств, які зазнали кібератаки, закриваються протягом шести місяців після інциденту. 51% малих підприємств повідомляють, що їхні вебсайти не працюють протягом 8-24 годин після атаки, що безпосередньо впливає на дохід та операційну ефективність. Лише 14% малих підприємств вважають, що вони підготовлені до захисту від загроз кібербезпеки, тоді як 83% малих та середніх підприємств не готові впоратися з фінансовими наслідками кібератаки.[81] Глобально 48% малих та середніх підприємств зазнали інциденту кібербезпеки протягом минулого року, причому лише 17% респондентів оцінюють поточні можливості кібербезпеки малих підприємств як ефективні.[82] Об'єм кібератак проти малих та середніх підприємств зріс на 150% між 2020 та 2022 роками, досягнувши 31 тисячі атак

[79] Genatec. Small Business Cyber Attack Statistics 2024. URL: https://www.genatec.com/blog/94-of-smbs-attacked cybersecurity-for-small-businesses-in-2024 (date of access: 01.10.2025).
[80] StationX. Cyber Attacks on Small Businesses Statistics. URL: https://www.stationx.net/cyber-attacks-on-small businesses-statistics/ (date of access: 01.10.2025).
[81] Business Dasher. Small Business Website Downtime Statistics. URL: https://www.businessdasher.com/small business-cyber-attack-statistics/ (date of access: 01.10.2025).
[82] Cyber Readiness Institute. State of SMB Cyber Readiness Report. URL: https://cyberreadinessinstitute.org/news-and events/small-and-medium-sized-businesses-face-major-obstacles-in-achieving-cyber-readiness-the-state-of-smb-cyber readiness-2024/ (date of access: 01.10.2025).

на день глобально.[83] Економічні бар'єри для впровадження адекватних заходів кібербезпеки посилюють вразливість малого бізнесу. 52% малих підприємств вважають інвестиції в кібербезпеку надто дорогими, а 44% малих та середніх підприємств глобально стверджують, що економічна невизначеність та вартість життя зменшили бюджети на кібербезпеку. 47% власників малого бізнесу вважають навігацію серед варіантів кібербезпеки складною, називаючи вартість

основним бар'єром, тоді як 68% малих підприємств стверджують, що вони отримали б користь від простих ресурсів кібербезпеки як вступного заходу. [84] Підприємства витрачають від 5 до 20% свого загального бюджету на інформаційні технології на безпеку, що часто виявляється недостатнім для протидії складним загрозам.[85]

Програми-вимагачі як інструмент економічного шантажу еволюціонували від простого шифрування файлів до складних багаторівневих схем екстракції вартості, що включають подвійне та потрійне вимагання. Медіанний розмір викупу у 2024 році становив 2 мільйони доларів порівняно з 400 тис. дол. США у 2023 році, що свідчить про п'ятикратне зростання. Організації, які виплачують викуп, повідомили про середній платіж у 2 млн. дол. США, що становить збільшення на 574% порівняно з 761 тис. дол. США у 2019 році. Загальна кількість атак програм-вимагачів зросла на 11% у 2024 році, досягнувши 5414 інцидентів, при цьому пік активності припав на четвертий квартал з 1827 випадками. Особливо тривожною є тенденція до повторних атак, адже 80 % жертв, які виплатили викуп, зазнали повторної атаки незабаром після цього. Виплата викупу не гарантує відновлення даних, оскільки лише 46 % жертв, які заплатили, отримали доступ до своїх даних, і значна частина відновлених даних виявилася пошкодженою.[86] Глобальна прогнозована вартість програм-вимагачів

[83] StationX. Volume of SMB Cyberattacks 2020-2022. URL: https://www.stationx.net/cyber-attacks-on-small businesses-statistics/ (date of access: 01.10.2025).
[84] StationX. Volume of SMB Cyberattacks 2020-2022. URL: https://www.stationx.net/cyber-attacks-on-small businesses-statistics/ (date of access: 01.10.2025).
[85] Business Dasher. Small Business Website Downtime Statistics. URL: https://www.businessdasher.com/small business-cyber-attack-statistics/ (date of access: 01.10.2025).
[86] Spacelift. Ransomware Payment Trends 2024. URL: https://spacelift.io/blog/ransomware-statistics (date of access: 01.10.2025).

демонструє катастрофічну траєкторію зростання. За оцінками аналітиків, вартість програм-вимагачів досягне 265 млн. дол. США щорічно до 2031 року, що становить зростання більш ніж на 20 млн. дол. США на місяць порівняно з приблизно 20 мільярдами доларів на рік у 2021 році. Німеччина повідомила про економічні збитки від кібератак на суму 178,6 млрд. євро у 2024 році порівняно з

30,4 млрд. євро у попередньому році. Консолідація ринку програм-вимагачів серед кримінальних груп посилює загрозу, оскільки лише п'ять груп відповідали за майже 25% усіх інцидентів.[87] Група Qilin стала найактивнішою групою програм-вимагачів до червня 2025 року, здійснивши 81 атаку за один місяць, що становить зростання на 47,3%.[88]

Дезінформація та маніпулятивні наративні атаки представляють додатковий вимір економічних загроз. Всесвітній економічний форум у Звіті про глобальні ризики 2025 року вдруге поспіль визначив дезінформацію як найбільшу короткострокову загрозу.[89] Компанії втрачають приблизно 39 млн. дол. США щорічно через волатильність фондового ринку, спричинену дезінформацією.[90] У 2024 році половина всіх підприємств стала жертвами атак з використанням глибоких підробок, що призвело до середніх втрат на один інцидент майже в 450 тисяч доларів.[91] 42% компаній визначили крадіжку особистих даних як найбільший ризик, пов'язаний з глибокими підробками. Консалтингова компанія Gartner прогнозує, що до 2028 року корпоративні витрати на боротьбу з дезінформацією перевищать 30 млн. дол. США.[92] Інвестиції в кібербезпеку зростають відповідно до масштабів загроз. Компанія PwC констатувала, що 85 % організацій планують збільшити свої бюджети на

[87] KELA. Ransomware Group Market Consolidation. URL: https://industrialcyber.co/reports/half-of-2025-ransomware attacks-hit-critical-sectors-as-manufacturing-healthcare-and-energy-top-global-targets/.
[88] Fortinet. Ransomware Statistics Report 2024. URL: https://www.fortinet.com/resources/cyberglossary/ransomware statistics (date of access: 01.10.2025).
[89] World Economic Forum. Global Risks Report 2025. {World Economic Forum}, 2025. URL: https://www.weforum.org/publications/global-risks-report-2025/ (date of access: 01.10.2025).
[90] Melillo Consulting. Disinformation Economic Impact on Corporations. URL: https://www.melillo.com/2025/03/24/disinformation-is-the-next-big-cybersecurity-threat-and-heres-why/ (date of access: 01.10.2025).
[91] World Economic Forum. Deepfake Risk Assessment. URL: https://www.weforum.org/stories/2025/07/financial impact-of-disinformation-on-corporations/ (date of access: 01.10.2025).
[92] IBM, {Ponemon Institute}. Cost of a Data Breach Report 2024. URL: https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics (date of access: 01.10.2025).

кібербезпеку у 2024 році, при цьому 19 % очікують зростання на 15% або більше. Компанія IDC прогнозує, що глобальні витрати на кібербезпеку зростуть на 12,2 % у 2025 році та перевищать 377 млн. дол. США до 2028 року.

Незважаючи на значні інвестиції, глобальний дефіцит спеціалістів з кібербезпеки становить понад 3 мільйони осіб, при цьому попит зростає вдвічі швидше за пропозицію. [93]

Організації з високим рівнем дефіциту навичок безпеки мали середню вартість витоку даних на рівні 5,36 мільйонів доларів, що приблизно на 20% вище за фактичну середню вартість.[94]

Системні ризики для глобальної фінансової стабільності посилюються зростаючою взаємозалежністю фінансових установ та їхньою залежністю від постачальників послуг інформаційних технологій третіх сторін. Атака програми вимагача у 2023 році на постачальника хмарних IT-послуг спричинила одночасні збої в роботі 60 кредитних спілок США. Кіберінциденти, які порушують критичні послуги, можуть серйозно вплинути на економічну діяльність, про що свідчить атака на Центральний банк Лесото, яка порушила національну платіжну систему. Опитування центральних банків та наглядових органів МВФ показало, що лише близько половини опитаних країн мали національну стратегію кібербезпеки.[95] На сьогодні, вимір інформаційного тероризму характеризується зростанням державно-спонсорованих атак. Китайські операції кібершпигунства зросли на 150% загалом у 2024 році, при цьому атаки проти фінансових, медійних, виробничих та промислових секторів зросли до 300%. [96] Російські кібератаки на Україну зросли майже на 70% у 2024 році, з 4315 інцидентами. [97] Кібератаки на Тайвань подвоїлися до 2,4 мільйонів щоденних спроб у 2024 році.

[93] World Economic Forum. Global Cybersecurity Workforce Gap. URL: https://www.weforum.org/stories/2024/02/3-trends-ransomware-2024/ (date of access: 01.10.2025).

[94] International Monetary Fund. Third-Party IT Provider Risk Case Study. URL: https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial stability (date of access: 01.10.2025).

[95] International Monetary Fund. Global Cybersecurity Policy Survey Results. URL: https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial stability (date of access: 01.10.2025).

[96] CSIS. Chinese Cyber Espionage Operations Report. URL: https://www.csis.org/programs/strategic-technologies program/significant-cyber-incidents (date of access: 01.10.2025).

[97] Ukraine Cybersecurity Agency. Russian Cyberattacks on Ukraine 2024. URL: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (date of access: 01.10.2025).

Північнокорейські хакери вкрали 1,5 млрд. дол. США в Ethereum з дубайської

біржі ByBit.[98] Економічні наслідки інформаційного тероризму виявляють системний характер та охоплюють усі рівні глобальної економіки, стабільності до мікрорівня функціонування окремих підприємств. Зростання кількості та складності кіберзагроз перетворює цифровий простір на основну арену економічного протистояння між державами, корпораціями та злочинними угрупованнями. Масштаби прямих фінансових втрат, які досягають десятків трильйонів доларів, свідчать про перетворення інформаційного тероризму на один із головних факторів дестабілізації світової економіки.

Висока частка атак на критичні інфраструктури, фінансовий сектор, охорону здоров'я та виробництво підкреслює стратегічний вимір цих загроз і їхню здатність викликати каскадні ефекти через глобальні ланцюги постачання. Додатковим чинником стає маніпулятивний вплив дезінформації, який призводить до значних втрат капіталізації, репутаційних збитків і посилення економічної турбулентності. У таких умовах кібербезпека постає як критичний елемент глобальної фінансової стабільності та конкурентоспроможності, а інвестиції у захисні технології, штучний інтелект і кадровий потенціал стають ключовими передумовами економічної витривалості у добу цифрових ризиків.

Таблиця 2.2. Економічні наслідки інформаційного тероризму для глобальної безпеки

Сфера впливу	Основні прояви загрози	Кількісні показники та динаміка	Економічні наслідки
Глобальна економіка	Кіберзлочинність як макроекономічний феномен	Сукупні втрати -10,5 трлн дол. США щороку до 2025 р.; зростання на 10 % щороку	Формування «тіньової цифрової економіки», яка за масштабом посідає третє місце після США і Китаю
Фінансовий сектор	Атаки програм вимагачів, компрометація облікових даних, експлуатація вразливостей	65 % фінансових організацій зазнали атак у 2024 р.; розмір екстремальних збитків зріс у 4 рази (до 2,5 млрд дол.)	Порушення ліквідності, репутаційні втрати, підвищення регуляторних витрат; зниження довіри до фінансових установ
Охорона здоров'я	Витоки медичних даних, атаки на госпітальні мережі	630+ інцидентів у 2024 р.; середня вартість витоку -10,93 млн дол.; витрати на захист -125 млрд дол. (2020–2025)	Порушення надання медичних послуг, ризики для життя пацієнтів, гуманітарна складова економічної шкоди

[98] CSIS. North Korean Cryptocurrency Theft Report. URL: https://www.csis.org/programs/strategic-technologies program/significant-cyber-incidents (date of access: 01.10.2025).

Виробництво та промисловість	Програми вимагачі, порушення ланцюгів постачання	4701 інцидент у 2025 р.; 50 % атак -на критичні сектори; втрати від простою -до 125 тис. дол./год	Зрив виробничих процесів, каскадний ефект на глобальні постачальні ланцюги, збитки від простоїв
Малий і середній бізнес	Недостатність захисту, економічна вразливість	61 % атак спрямовано на МСП; середня вартість витоку -2,98 млн дол.; 60 % підприємств закриваються після інциденту	Масове банкрутство МСП, втрата робочих місць, зниження інноваційного потенціалу
Програми вимагачі (ransomware)	Економічний шантаж, подвійне вимагання	Медіанний викуп -2 млн дол. у 2024 р. (+574 % від 2019 р.); прогноз до 265 млрд дол. щорічно до 2031 р.	Ерозія цифрової довіри, прямі втрати бізнесу, повторні атаки на 80 % жертв
Дезінформація та deepfake технології	Маніпуляції ринками, інформаційні кампанії	Втрати капіталізації -39 млрд дол./рік; середні втрати від deepfake-інциденту -450 тис. дол.	Волатильність фондових ринків, репутаційні втрати, підрив інституційної стабільності
Інвестиції в кіберзахист	Реакція ринку на зростання ризиків	85 % організацій підвищили бюджети у 2024 р.; глобальні витрати зростуть до 377 млрд дол. до 2028 р.	Підвищення вартості операцій, дефіцит кадрів (3+ млн фахівців), зростання попиту на ШІ-рішення
Геополітичний вимір	Державні та спонсоровані атаки	Китай -+150 % атак у 2024 р.; РФ -+70 % атак на Україну; Північна Корея -1,5 млрд дол. крадіжок криптовалют	Економічна дестабілізація, зниження стійкості фінансових систем, політична ескалація у цифровій сфері

Джерело: сформовано самостійно автором на основі власного дослідження

Економічні наслідки інформаційного тероризму мають системний характер, охоплюючи як глобальний макрорівень, так і функціонування окремих галузей. Зростання обсягів збитків, кількості атак та геополітичної залученості держав свідчить про перетворення цифрових загроз на один із ключових факторів дестабілізації світової економіки. Особливу небезпеку становлять комбіновані атаки на фінансову, медичну та виробничу інфраструктуру, які створюють ефект

доміно у глобальних ланцюгах постачання. Одночасно посилюється економічний тиск через дезінформацію та дефіцит кваліфікованих кадрів, що формує потребу у стратегічному зміцненні кіберстійкості, розвитку технологій штучного інтелекту та міжнародній координації у сфері кібербезпеки.

2.3. Соціальні наслідки інформаційного тероризму: дезінформація та маніпуляція суспільною думкою

Інформаційний тероризм впливає на ідентичність особистості. Через цілеспрямоване поширення дезінформації, теорій змов та маніпулятивного контенту в соціальних мережах відбувається розмивання ціннісних орієнтирів, національної ідентичності та історичної пам'яті. Це особливо небезпечно для

держав, які переживають складні періоди національного самовизначення або протистоять зовнішній агресії. Набір алгоритмів, таргетованої реклами, поширюваної в інтернеті дезінформації та теорій змов у соціальних мережах впливають не тільки на політичні процеси, але і на кожного окремого громадянина та його сприйняття світу. Захищеність психіки та здоров'я людини від деструктивного інформаційного впливу забезпечує існування сприятливих можливостей для задоволення та реалізації життєвих, духовних і матеріальних потреб громадян, створює для них необхідний мінімум сталості, стабільності, соціального імунітету, готовності та здатності протистояти деструктивним впливам, небезпекам та загрозам життю, здоров'ю, майну, всій сукупності прав, свобод, законних інтересів. Соціальні мережі трансформують міжособистісну комунікацію, стосунки в родинах, і навіть змінюють ідентичності людей.[99] Цей вплив має глибокий і довготривалий характер, формуючи нові патерни поведінки та мислення, які можуть як зміцнювати, так і послаблювати стійкість особистості до маніпулятивних впливів. Особливої уваги заслуговує феномен «інформаційних бульбашок», коли алгоритми соціальних мереж створюють замкнене інформаційне середовище, в якому користувачі отримують лише ту інформацію, яка підтверджує їхні існуючі переконання, що призводить до

радикалізації поглядів та зниження критичного мислення.

У сучасному цифровому просторі цілеспрямоване поширення неправдивої інформації трансформувалося у феномен, що отримав назву інформаційного тероризму. Це явище являє собою систематичний психологічний вплив через дезінформацію та пропагандистські меседжі з метою формування викривленої картини реальності у масовій свідомості. Починаючи з 2019 року, дезінформаційні кампанії та маніпуляція громадською думкою набули характеру глобального виклику, проявившись у контексті виборчих процесів, пандемії COVID-19 та збройних конфліктів, зокрема повномасштабної російської агресії проти України. Інформаційні атаки стали невід'ємним компонентом гібридних

[99] Гончар М. В. Вплив соціальних мереж на політичні системи у контексті суперництва демократичних та авторитарних режимів. Науковий журнал «Політикус». 2024. Випуск 5. С. 11-18. DOI: https://doi.org/10.24195/2414-9616.2024-5.2 (дата звернення: 01.10.2025).

воєн, оскільки держави-агресори використовують фальсифіковані наративи для досягнення стратегічних військових та геополітичних цілей. [100] Наслідки цього феномену виявляються на рівні соціальних структур через підрив інституційної довіри, поглиблення суспільної поляризації, дестабілізацію демократичних механізмів та ескалацію міжгрупових конфліктів. Інформаційний тероризм не обмежується дезорієнтацією реципієнтів інформації, а здатен провокувати панічні реакції, насильницькі дії та фізичні загрози безпеці громадян.

Систематичні дезінформаційні операції цілеспрямовано деформують колективну свідомість, замінюючи емпіричну реальність сконструйованими хибними уявленнями. Завдяки технологічним можливостям соціальних мереж та месенджерів фальсифіковані повідомлення досягають широкої аудиторії з високою швидкістю, часто мімікруючи під легітимні новинні матеріали чи експертні оцінки. Унаслідок тривалого перебування в такому спотвореному інформаційному середовищі населення втрачає здатність до критичної верифікації даних та диференціації достовірної інформації від маніпулятивних конструктів. Дослідники фіксують, що пролонгована експозиція дезінформації призводить до ерозії самого концепту поінформованості, коли суспільство

поступово втрачає розуміння того, що означає бути належно обізнаним.[101]

Замість накопичення знань відбувається формування впевненості у хибних твердженнях, що особливо небезпечно за умови їх цілеспрямованого та зловмисного поширення. Масштаби таких викривлених переконань демонструвалися під час пандемії COVID-19, коли мільйони людей асимілювали фальсифіковані дані про етіологію захворювання та вакцинацію, а також у політичних контекстах, де електорат орієнтується на емоційно насичені, проте фактологічно неспроможні повідомлення. Механізми впливу на свідомість включають нав'язування деструктивних наративів через координовані бот-

[100] European Council Library. The fight against pro-Kremlin disinformation. *Consilium*. 2023. URL: https://www.consilium.europa.eu/en/documents-publications/library/library-blog/posts/the-fight-against-pro kremlin-disinformation/ (date of access: 01.10.2025).

[101] The Weaponization of Fiction and Truth: Disinformation as Hybrid Warfare and its Strategic Use in the United States 2024 Election. *NSF Journal*. 2024. URL: https://www.nsf-journal.hr/nsf-volumes/focus/id/1513/p/1 (date of access: 01.10.2025).

мережі та псевдомедійні платформи. У Сполучених Штатах упродовж останніх виборчих циклів спостерігалося експоненційне зростання конспірологічних теорій, зокрема QAnon та концепції фальсифікованих виборів, що поширювалися через цифрові канали комунікації. Попри відсутність емпіричних підстав, ці конструкти набували популярності та формували політичні переконання значної частини американського електорату. Аналогічно в європейському просторі російська пропагандистська машина просувала міфологеми про деградацію західних демократій та тотальний контроль еліт, намагаючись індукувати недовіру громадян до національних урядів. Критичним наслідком є те, що під впливом дезінформації громадяни ухвалюють важливі політичні рішення, зокрема на референдумах та виборах, базуючись не на перевірених фактах, а на маніпулятивних конструктах. Freedom House у звіті констатує, що в численних країнах виборці вимушені приймати рішення щодо майбутнього, орієнтуючись на спотворене та обмежене інформаційне середовище.[102] Дезінформація підриває фундаментальну основу громадянської компетентності, масово насаджуючи викривлену свідомість, що ставить під

сумнів спроможність суспільства ухвалювати раціональні рішення.[103]

Одним із найбільш деструктивних наслідків інформаційних атак є системна ерозія суспільної довіри на вертикальному рівні до інституцій та на горизонтальному рівні між громадянами. Механізм цього процесу полягає у тому, перманентний потік фальсифікованих повідомлень та конспірологічних конструктів індукує сумніви щодо легітимності офіційної інформації, медійних повідомлень та наукових фактів. Населення розвиває схильність до відторгнення будь-яких повідомлень, що суперечать попередньо сформованим упередженням, які самі є продуктом дезінформації. Європейський Союз офіційно визнає, що дезінформація деструктурує основи демократичного устрою, підриваючи довіру

-[102] House F. The Struggle for Trust Online. URL: https://freedomhouse.org/report/freedom-net/2024/struggle-trust online (date of access: 01.10.2025).

[103] European Council Library. The fight against pro-Kremlin disinformation. *Consilium*. 2023. URL: https://www.consilium.europa.eu/en/documents-publications/library/library-blog/posts/the-fight-against-pro kremlin-disinformation/ (date of access: 01.10.2025).

громадян до демократичних інституцій.[104] Дефіцит довіри проявляється у зростанні скептицизму щодо урядових заяв та журналістських розслідувань, коли значна частина аудиторії схильна апріорі відкидати їх як фальсифікації без будь-яких доказових підстав. Окрім вертикальної довіри до державних структур та медіа, інформаційний тероризм руйнує горизонтальну довіру між членами суспільства. Коли різні сегменти населення споживають діаметрально протилежні інформаційні потоки завдяки алгоритмічній персоналізації соціальних мереж та цільової пропаганди, формується постправдовий простір, у якому кожна група функціонує у власній інформаційній реальності. За таких умов у суспільстві прогресує поляризація поглядів та ідеологічна фрагментація. Дезінформація навмисно розколює соціальний організм, акцентуючи конфліктні теми та радикалізуючи публічний дискурс. Європейська рада констатує, що дезінформація каталізує поляризацію суспільних настроїв, штучно сегментуючи населення на протиборчі групи. Це проявляється у формуванні ворожого сприйняття політичних опонентів чи представників інших соціальних груп, коли

замість конструктивного діалогу домінує атмосфера взаємної недовіри та непримиренності. Емпіричні дослідження підтверджують прямий кореляційний зв'язок між експозицією дезінформації та деградацією суспільної довіри.[105]

Аналітики констатують, що масове споживання фальсифікованої інформації не лише завдає прямої шкоди дезорієнтованим індивідам, але й системно розхитує довіру в суспільстві як до інших громадян, так і до авторитетних інформаційних джерел. Результатом є зниження колективної здатності до обміну достовірною інформацією та мобілізації перед викликами. Така фрагментація інформаційного поля послаблює соціальний взаємозв'язок, оскільки замість єдиного наративу реальності співіснують множинні взаємозаперечні версії. Втрата спільної фактологічної основи руйнує

[104] European Council Library. The fight against pro-Kremlin disinformation. *Consilium*. 2023. URL: https://www.consilium.europa.eu/en/documents-publications/library/library-blog/posts/the-fight-against-pro kremlin-disinformation/ (date of access: 01.10.2025).

[105] The Weaponization of Fiction and Truth: Disinformation as Hybrid Warfare and its Strategic Use in the United States 2024 Election. *NSF Journal*. 2024. URL: https://www.nsf-journal.hr/nsf-volumes/focus/id/1513/p/1 (date of access: 01.10.2025).

фундаментальні соціальні зв'язки та ускладнює досягнення консенсусу щодо критично важливих питань. Іншими словами, коли громадяни не здатні досягти згоди навіть щодо базових фактів, довіра як соціальний капітал зникає, а з нею й готовність до кооперації заради спільного блага.[106]

Інформаційний тероризм генерує прямі наслідки для політичної стабільності та функціонування демократичних механізмів. Дезінформація використовується для втручання у виборчі процеси, руйнуючи вплив владних інституцій та провокування політичних криз. Учасники дезінформаційних кампаній, як зовнішні держави-агресори, так і внутрішні радикальні політичні групи, поширюють фальсифікації з метою маніпулювання електоральними результатами або індукування сумнівів щодо їх легітимності. Наслідком є девальвація виборчого процесу у сприйнятті громадян та потенційне масове невизнання результатів волевиявлення. Показовим прикладом є ситуація у Сполучених Штатах після президентських виборів 2020 року. Незважаючи на

відсутність емпіричних доказів масштабних порушень, теорія про фальсифіковані вибори поширилася через консервативні медіа та соціальні мережі, спричинивши глибоку недовіру значної частини електорату до офіційних результатів. Спостерігачі констатували масовану дезінформаційну кампанію, що висувала безпідставні заяви про вибори 2020 року, розділяючи американське суспільство та примушуючи значну частину громадян втратити довіру до демократичного процесу. Кульмінацією цього процесу став інцидент 6 січня 2021 року, коли радикалізовані конспірологічними теоріями прихильники теорії змови штурмували Капітолій США. Цей епізод продемонстрував, як фальсифікована інформація може трансформуватися у фізичну загрозу конституційному ладу.[107] Учасники цих подій діяли на основі щирої віри у дезінформаційні наративи, що поставили під сумнів легітимність демократичного волевиявлення. Така втрата віри у виборчу систему є критично

[106] The Weaponization of Fiction and Truth: Disinformation as Hybrid Warfare and its Strategic Use in the United States 2024 Election. *NSF Journal*. 2024. URL: https://www.nsf-journal.hr/nsf-volumes/focus/id/1513/p/1 (date of access: 01.10.2025).

[107] Issue One. Truthtellers. URL: https://issueone.org/projects/truthtellers/ (date of access: 01.10.2025).

небезпечним соціальним наслідком, оскільки вона підточує принцип мирної передачі влади та може каталізувати насильницькі дії з боку громадян, переконаних у необхідності захисту демократії від уявної змови.

Міжнародний досвід підтверджує, що аналогічні процеси відбуваються не лише у Сполучених Штатах. Freedom House зафіксував, що у 21 з 41 досліджуваної країни, де відбувалися загальнонаціональні вибори, онлайн маніпуляції інформацією індукували сумніви у чесності голосування та генерували довготривалу недовіру до демократичних інституцій.[108] Дезінформація набуває різноманітних форм від фальсифікованих викриттів порушень до координованих атак на незалежних спостерігачів та фактчекерів. Стратегічна мета полягає у примушенні громадян засумніватися у справедливості виборів та відмовитися визнати їх результати. У демократичних державах Європи неодноразово фіксувалися інформаційні операції, спрямовані

на дискредитацію окремих кандидатів або політичних партій перед виборами. Такі кампанії часто координуються іноземними акторами, зокрема розвідувальні служби США та ЄС встановили факти російського втручання у референдум щодо Brexit 2016 року та вибори у Франції 2017 року. У новітній період кремлівські тролінгові структури та підставні медіа продовжували спроби впливати на європейські виборчі процеси, поширюючи фальсифіковані історії про корумпованість проєвропейських сил чи зовнішнє управління цими країнами. Окрім виборів, дезінформація атакує інші елементи політичної стабільності, підриваючи авторитет державних інституцій та міжнародних структур. У країнах Східної Європи ворожі інформаційні кампанії систематично спрямовані на дискредитацію НАТО та ЄС, нав'язуючи громадянам думку про загрози з боку цих інституцій або їх втручання у внутрішні справи. Мета полягає у послабленні підтримки євроатлантичного курсу та внесенні розколу між союзниками. Російська пропаганда регулярно тиражує міфологеми про агресивність НАТО, намагаючись індукувати страх серед населення країн-членів

[108] House F. The Struggle for Trust Online. URL: https://freedomhouse.org/report/freedom-net/2024/struggle-trust online (date of access: 01.10.2025).

Альянсу та вплинути на їхню зовнішню політику. Це складова ширшої стратегії, у якій комбінуються військові та інформаційні засоби тиску в рамках гібридних методів ведення війни. У підсумку суспільство стає більш вразливим до маніпуляції, а політична система втрачає стійкість до зовнішніх впливів, що становить загрозу національній безпеці та державному суверенітету.[109]

Україна перетворилася на один із головних полігонів інформаційної війни у глобальному масштабі. Російська дезінформаційна кампанія проти України розгорнулася з 2014 року, а з початком повномасштабного вторгнення у лютому 2022 року досягла безпрецедентного розмаху. За даними платформи EUvsDisinfo, понад 40% усіх зафіксованих випадків дезінформації у їхній базі даних стосуються саме України. [110] Кремлівська пропагандистська машина систематично конструювала міфологеми та фальсифіковані приводи для агресії,

звинувачуючи Україну у нацизмі, геноциді російськомовного населення та створенні загрози НАТО з української території. [111] Ці наративи мали на меті не лише виправдати воєнні дії Російської Федерації перед власним населенням, але й деморалізувати українців та знизити міжнародну підтримку України.

Соціальні наслідки цієї інформаційної агресії для українського суспільства є масштабними та багатовимірними. По-перше, ворожа пропаганда систематично намагалася індукувати паніку та недовіру всередині країни. У перші дні вторгнення лютого 2022 року російські джерела масово поширювали фальсифікацію про те, що президент Володимир Зеленський покинув Київ та евакуювався за кордон.[112] Російські медіа тиражували брехню про втечу Зеленського, що, за оцінками експертів, мало на меті деморалізувати українське населення та посіяти міжнародну зневіру щодо спроможності України чинити опір агресору. Оперативна комунікаційна стратегія української влади, зокрема безпосередні звернення Зеленського з центру Києва, нейтралізувала цю

- [109] House F. The Struggle for Trust Online. URL: https://freedomhouse.org/report/freedom-net/2024/struggle-trust online (date of access: 01.10.2025).
[110] EUvsDisinfo. Ukraine. URL: https://euvsdisinfo.eu/ukraine/ (date of access: 01.10.2025). [111] EUvsDisinfo. Ukraine. URL: https://euvsdisinfo.eu/ukraine/ (date of access: 01.10.2025). [112] AP News. Russian propaganda 'outgunned' by social media rebuttals. 2022. URL: https://apnews.com/article/russia ukraine-volodymyr-zelenskyy-kyiv-technology-misinformation-5e884b85f8dbb54d16f5f10d105fe850 (date of access: 01.10.2025).

дезінформацію, проте сам факт такої атаки демонструє, як інформаційний тероризм може створювати загрозу національній стійкості у критичний момент. По-друге, ворожі наративи були спрямовані на провокування внутрішнього розколу українського суспільства. У 2022 році, на тлі масових внутрішніх переміщень населення та безпрецедентного соціального стресу, російські інформаційні операції намагалися створити конфлікт між різними групами українців. Зокрема, фіксувалися повідомлення, що розпалювали антагонізм між внутрішньо переміщеними особами з регіонів активних бойових дій та місцевими громадами західних областей, а також між україномовними та російськомовними громадянами. Мета таких інформаційних вкидів полягала у посіянні недовіри та ворожнечі там, де українці демонстрували солідарність.

Хоча спроби не досягли стратегічного успіху завдяки високій соціальній когезії, вони створювали локальні напруження. По-третє, російська дезінформація безпосередньо загрожувала життю та безпеці цивільного населення. Центр з питань захисту цивільних у конфлікті задокументував численні фальсифікації, що наражали мирних мешканців на фізичну небезпеку. Зокрема, у березні 2022 року проросійські джерела публікували неправдиві повідомлення про маршрути евакуації з оточених міст, стверджуючи, що ці дороги обстрілюють українські війська, щоб перешкодити виїзду населення.[113] Поширювалися фальсифікації про неіснуючі гуманітарні коридори, внаслідок чого дезорієнтовані люди могли потрапити під обстріли або в руки окупаційних сил. Центр констатує, що такі тактичні фальсифікації безпосередньо призводили до загибелі та страждань цивільних і підривали довіру населення до будь-яких повідомлень про безпеку. Тривалий потік пропаганди має на меті виснажити суспільство у довгостроковій перспективі, підриваючи соціальну стійкість, когезію та довіру громадян один до одного та до державних інституцій. Російські наративи намагаються переконати українців у марності опору, системній корумпованості керівництва та зраді західних союзників. Водночас ці меседжі адресовані

[113] EUvsDisinfo. Navigating the harmful consequences of Disinformation in War. URL: https://euvsdisinfo.eu/navigating-the-harmful-consequences-of-disinformation-in-war/ (date of access: 01.10.2025).

зовнішній аудиторії з метою підірвати міжнародну підтримку України, конструюючи образ неспроможної держави або звинувачуючи саму жертву агресії у воєнних злочинах, як це відбулося з цинічним запереченням різанини в Бучі російськими офіційними особами.[114] Протидіючи такій масованій дезінформації, Україна демонструє глобальну модель інформаційної резилієнтності. У країні активно функціонують державні та громадські ініціативи з викриття фальсифікацій, зокрема Центр протидії дезінформації при РНБО, проєкти StopFake та VoxCheck. Проте масштаб російської кампанії є безпрецедентним: у перші місяці вторгнення соціальні мережі видалили десятки тисяч одиниць дезінформаційного контенту, при цьому лише TikTok у березні 2022 року заблокував понад 41 тисячу відео, 81% з яких порушували політику

щодо неправдивої інформації.[115] Ці дані підкреслюють колосальний масштаб спроби нав'язати фальсифіковані наративи про війну глобальній аудиторії.

Країни Європейського Союзу, особливо в східноєвропейському регіоні, стали об'єктом інформаційного тероризму у період 2019–2025 років. Головним актором у цій сфері залишається Російська Федерація, що прагне індукувати нестабільність і розбрат всередині європейських суспільств. Методи варіюються від поширення панічних чуток до ретельно координованих багатомовних кампаній на численних платформах. У країнах Балтії російська пропаганда присутня десятиліттями, проте за останні роки її тактика трансформувалася від відкритої радянської пропаганди до прихованих мереж дезінформації у соціальних мережах та медіа. Стратегічна мета полягає у дестабілізації цих держав, індукуванні страху та підриві довіри до державних інституцій.[116]

Пропагандистські повідомлення систематично фокусуються на таких темах, як історична пам'ять з перекрученням фактів про радянську окупацію та

[114] EUvsDisinfo. Navigating the harmful consequences of Disinformation in War. URL: https://euvsdisinfo.eu/navigating-the-harmful-consequences-of-disinformation-in-war/ (date of access: 01.10.2025).
[115] Freedom House. Ukraine: Freedom on the Net 2022 Country Report. 2022. URL: https://freedomhouse.org/country/ukraine/freedom-net/2022 (date of access: 01.10.2025). [116] AP News. Russian propaganda 'outgunned' by social media rebuttals. 2022. URL: https://apnews.com/article/russia ukraine-volodymyr-zelenskyy-kyiv-technology-misinformation-5e884b85f8dbb54d16f5f10d105fe850 (date of access: 01.10.2025).

звинуваченнями балтійців у фашизмі, права російськомовної меншини з конструюванням образу їх утисків, членство в НАТО з залякуванням військовою загрозою з боку Альянсу. В умовах російської війни проти України інтенсивність дезінформації в Балтії зросла, оскільки Кремль прагнув послабити підтримку балтійцями України та сконструювати образ небезпечної війни поруч. Уряди балтійських країн фіксували хвилі фальсифікацій про українських біженців, марність санкцій проти Російської Федерації та те, що Захід втягує Литву та Латвію у воєнний конфлікт. Ці меседжі розраховані на індукування страхів з метою вплинути на політику, наприклад, викликати опір розміщенню військ НАТО або зменшити суспільну підтримку санкцій та допомоги Україні.[117]

Попри постійний інформаційний тиск, балтійські країни демонструють високу резилієнтність до дезінформації завдяки історичному досвіду та проактивним заходам. У Литві, Латвії та Естонії функціонують програми медіаграмотності, уряди оперативно спростовують фальсифікації, а громадяни організовують ініціативи на кшталт кібер-ельфів, що протидіють інтернет тролям. Водночас загроза не зникає, оскільки Москва дедалі активніше застосовує новітні технології, зокрема штучний інтелект для створення дипфейків, що робить пропаганду більш переконливою. Це ставить перед демократичними суспільствами нові виклики щодо постійного вдосконалення методів виявлення та нейтралізації інформаційних атак.[118] У країнах Західної Європи дезінформація також генерує соціальні наслідки, хоча специфіка відрізняється. Під час пандемії 2020–2021 років у Франції, Німеччині, Італії та інших державах ЄС широка антивакцинаторська пропаганда, значною мірою підтримувана зовнішніми акторами, призвела до зниження рівня довіри до медичних інституцій та науки, що ускладнило боротьбу з пандемією та поляризувало суспільство. Інший приклад міграційна криза, коли російські та ультраправі джерела систематично перебільшували та перекручували факти про

[117] Foundation J. Russia's Hybrid Warfare Tactics Target the Baltics. 2024. URL: https://jamestown.org/program/russias hybrid-warfare-tactics-target-the-baltics/ (date of access: 01.10.2025).
[118] Foundation J. Russia's Hybrid Warfare Tactics Target the Baltics. 2024. URL: https://jamestown.org/program/russias hybrid-warfare-tactics-target-the-baltics/ (date of access: 01.10.2025).

біженців з Близького Сходу, поширюючи алармістські наративи про їхню поведінку. Це стимулювало зростання ксенофобських настроїв та зміцнювало позиції радикальних політиків, що експлуатують міграційну тематику. Такі наслідки розпалювання ненависті до меншин та радикалізація частини населення також є соціально небезпечним результатом інформаційного тероризму.

Європейський Союз усвідомив критичну серйозність загрози і з другої половини 2010-х років розбудовує систему протидії дезінформації. Був створений підрозділ East StratCom Task Force та платформа EUvsDisinfo, що відстежує і викриває фальсифікації. У 2018 році ЄС ухвалив план дій боротьби з

дезінформацією, а з 2022 року на тлі війни ще більше активізував зусилля, запровадивши санкції проти російських пропагандистських ресурсів та підтримуючи незалежні медіа. Європейська рада прямо заявила, що протидія дезінформації є довгостроковим викликом для європейських демократій, оскільки від цього залежить збереження довіри громадян і стійкість демократичного процесу.[119] Аналіз емпіричного матеріалу за період 2019–2025 років дозволяє систематизувати ключові соціальні наслідки інформаційного тероризму за основними параметрами впливу. Наведена нижче таблиця синтезує дані щодо форм дезінформації, механізмів впливу, соціальних ефектів та географічних проявів цього феномену. Таблиця демонструє системний характер інформаційного тероризму, що впливає одночасно на множинні рівні соціальної організації від індивідуальної свідомості до міжнародних відносин. Критично важливим є те, що ці наслідки не є ізольованими, а формують каскадний ефект, коли деформація масової свідомості призводить до ерозії довіри, що у свою чергу підриває політичну стабільність та загострює міжгрупові конфлікти.

таблиця 2.3. Соціальні наслідки інформаційного тероризму: дезінформація та маніпуляція суспільною думкою

Категорія соціального впливу	Механізм реалізації інформаційного тероризму	Соціальні наслідки	Приклади та емпіричні прояви (2019–2025 рр.)
Деформація колективної свідомості та ідентичності	Масоване поширення дезінформації, теорій змов, маніпулятивних меседжів у соціальних мережах; алгоритмічне таргетування контенту	Розмивання національної ідентичності, девальвація історичної пам’яті, підрив культурної самоідентифікації; формування «інформаційних бульбашок» та радикалізація поглядів	Маніпуляції під час пандемії COVID-19 (2020–2021 рр.); кампанії QAnon у США; фальсифіковані наративи щодо війни в Україні у 2022–2025 рр.

[119] AP News. Russian propaganda 'outgunned' by social media rebuttals. 2022. URL: https://apnews.com/article/russia ukraine-volodymyr-zelenskyy-kyiv-technology-misinformation-5e884b85f8dbb54d16f5f10d105fe850 (date of access: 01.10.2025).

Ерозія суспільної довіри	Потік фейкових повідомлень, псевдоновин і конспірологічних конструкцій; делегітимізація офіційних джерел інформації	Зниження довіри до інституцій влади, ЗМІ та експертного середовища; послаблення горизонтальної довіри між громадянами; формування постправдової реальності	Звіт Freedom House (2023): у 21 з 41 країни дезінформаційні кампанії підірвали віру у чесність виборів; деструкція суспільної згоди в Україні під час воєнного стану
Поляризація суспільства та радикалізація дискурсу	Алгоритмічна персоналізація контенту, що підсилює протиставлення груп; поширення пропаганди через бот-мережі	Поглиблення ідеологічних розколів, зростання ненависті між соціальними групами, радикалізація політичного поля	Кампанії у США після виборів 2020 р.; інформаційні атаки в ЄС щодо міграційної кризи; російські операції з розпалювання внутрішнього конфлікту в Україні (2022 р.)
Підрив демократичних процесів	Втручання у виборчі кампанії, поширення фейкових заяв про фальсифікації, підрив легітимності результатів	Делегітимізація виборів, зниження політичної участі громадян, девальвація демократичного процесу	США — кампанія про «фальсифіковані вибори 2020» і штурм Капітолію (6 січня 2021 р.); втручання РФ у Brexit 2016 та вибори у Франції-2017
Дестабілізація політичної системи та національної безпеки	Використання пропаганди як складової гібридної війни; створення образу зовнішньої чи внутрішньої загрози	Ослаблення довіри до держави, деморалізація населення, політична фрагментація; загроза конституційному ладу	Російські інформаційні атаки проти України (2014–2025 рр.); спроби дискредитації НАТО та ЄС у Східній Європі; кампанії залякування у Балтії
Психологічні наслідки та соціальна резилієнтність	Тривала експозиція деструктивного контенту, маніпуляція емоціями, страхом, гнівом	Підвищення рівня тривожності, соціальна апатія, дезорієнтація; зниження критичного мислення, розвиток віктимності	Антивакцинаторські рухи в ЄС (2020–2021 рр.); панічні чутки в Україні під час вторгнення 2022 р.; фейки про евакуаційні маршрути
Соціальна когезія та опірність маніпуляціям	Реактивна діяльність державних і громадських інституцій із протидії фейкам; розвиток медіаграмотності	Формування колективного імунітету до дезінформації; підвищення спроможності суспільства	Українські ініціативи StopFake, VoxCheck, Центр протидії дезінформації при РНБО; «кібер-ельфи»

		розпізнавати маніпуляції	у Балтії; програми медіаосвіти у Литві, Латвії, Естонії

Джерело: сформовано самостійно автором на основі власного дослідження

Комплексний аналіз соціальних наслідків інформаційного тероризму у період 2019–2025 років дозволяє сформулювати наступні висновки щодо природи, механізмів та ефектів цього явища. Інформаційний тероризм

трансформувався з локальних епізодичних кампаній у системну глобальну загрозу, що застосовується як інструмент гібридної війни державами-агресорами та використовується внутрішніми політичними акторами для досягнення стратегічних цілей. Масштаб цього феномену підтверджується емпіричними даними: понад 40% всіх випадків дезінформації, зафіксованих EUvsDisinfo, стосуються лише однієї країни України, що свідчить про концентрацію інформаційної агресії проти держав, що чинять опір авторитарним режимам. Водночас поширення дезінформації у 21 з 41 країни під час виборів, за даними Freedom House, демонструє універсальний характер цієї загрози для демократичних процесів у глобальному масштабі. Соціальні наслідки дезінформації носять багаторівневий та каскадний характер. Первинний вплив на індивідуальну свідомість через конспірологічні теорії та фейкові наративи трансформується у колективні ефекти на рівні соціальних груп, що проявляється через ерозію міжособистісної довіри та поляризацію суспільства. Цей процес далі масштабується на інституційний рівень, підриваючи легітимність демократичних інститутів, виборчих процесів та міжнародних союзів. Кульмінацією є дестабілізація на рівні національної безпеки, коли інформаційні атаки безпосередньо загрожують життю громадян, як це документовано у випадку України, де фальсифікації про евакуаційні маршрути призводили до фізичних жертв серед цивільного населення. Механізми поширення дезінформації характеризуються зростаючою технологічною складністю та індустріалізацією. Використання бот-мереж, алгоритмічного посилення через

соціальні мережі, штучного інтелекту для генерації дипфейків та координованих багатоплатформних атак демонструє перехід від спонтанних дезінформаційних епізодів до професійно організованих операцій з чіткими стратегічними цілями. Масштаб цих операцій ілюструється тим фактом, що лише одна платформа TikTok заблокувала понад 41 тисячу відео за один місяць березень 2022 року, 81% з яких містили дезінформацію про війну в Україні. Це свідчить про безпрецедентні обсяги виробництва та поширення фальсифікованого контенту.

72

Ефективність дезінформаційних кампаній корелює з існуючими соціальними розколами та рівнем медіаграмотності населення. Найбільший вплив дезінформація має у суспільствах з високим рівнем політичної поляризації, як продемонстровано на прикладі США, де теорії про фальсифіковані вибори 2020 року призвели до штурму Капітолію. Водночас балтійські країни, незважаючи на інтенсивний інформаційний тиск з боку Росії, демонструють вищу резилієнтність завдяки історичному досвіду, програмам медіаграмотності та проактивним заходам протидії. Це підтверджує тезу, що соціальна вразливість до інформаційного тероризму не є сталою характеристикою, а може бути знижена через цілеспрямовані превентивні заходи. Довгострокові соціальні наслідки інформаційного тероризму проявляються у формуванні постправдового простору, де різні сегменти суспільства функціонують у паралельних інформаційних реальностях з взаємозаперечними системами фактів. Це створює фундаментальний виклик для демократичного процесу, оскільки раціональний політичний діалог та досягнення консенсусу стають неможливими за відсутності спільної фактологічної основи. Американський досвід демонструє, що відновлення втраченої довіри є значно складнішим та довготривалішим процесом, ніж її деструкція, що означає, що наслідки дезінформаційних кампаній 2020–2022 років відчуватимуться упродовж наступного десятиліття. Географічний аналіз виявляє, що Україна стала епіцентром інформаційної війни, будучи об'єктом понад 40% всіх зафіксованих випадків дезінформації. Це робить український досвід критично важливим для розуміння еволюції тактик інформаційного

тероризму та розробки ефективних механізмів протидії.

Водночас українська резилієнтність, що проявилася через швидке спростування фейків, високу соціальну когезію та активність громадянських ініціатив з фактчекінгу, демонструє можливість ефективного опору масованій дезінформаційній агресії навіть в умовах повномасштабної війни. Інституційна відповідь на загрозу інформаційного тероризму залишається фрагментованою та недостатньою відносно масштабу виклику. Хоча Європейський Союз створив

спеціалізовані структури типу East StratCom Task Force та платформи EUvsDisinfo, а окремі країни розробили національні стратегії протидії дезінформації, глобальна координація залишається обмеженою. Технологічні платформи, незважаючи на видалення мільйонів одиниць дезінформаційного контенту, не спроможні повністю нейтралізувати потік фальсифікацій через їх індустріальні масштаби виробництва. Це вказує на необхідність розробки більш комплексних міжнародних механізмів протидії, що поєднували б технологічні, законодавчі, освітні та комунікаційні компоненти. Соціальні наслідки інформаційного тероризму мають виражену асиметричну природу: відносно невеликі інвестиції в дезінформаційні кампанії здатні генерувати непропорційно великі соціальні та політичні ефекти. Це робить інформаційний тероризм привабливим інструментом для держав-агресорів та недержавних акторів, що прагнуть дестабілізувати противника без застосування прямої військової сили. Водночас ця асиметрія означає, що навіть демократичні суспільства з розвиненими інституціями залишаються вразливими до інформаційних атак, особливо в періоди соціальних криз, виборів або інших критичних подій.

Висновки до розділу II

Узагальнюючи результати розділу, слід констатувати, що інформаційний тероризм сформувався як системна багаторівнева загроза, яка одночасно діє на індивідуальному, суспільному та державному рівнях і інтегрує інструменти дезінформації, пропаганди, кібератак і психологічних операцій. На політичному рівні він підточує легітимність демократичних інститутів і виборчих процедур

через делегітимаційні наративи, що відтворюються алгоритмічно персоналізованими каналами, фабриками тролів і мережами ботів. На економічному рівні він матеріалізується у вигляді прямих і непрямих збитків від кібератак, порушень ланцюгів постачання та волатильності ринків, індукованої маніпулятивними інформаційними кампаніями, що робить цифровий простір ключовою ареною геоекономічного протистояння.

Ключовий механізм дії інформаційного тероризму полягає у зсуві від емпірично верифікованої інформації до афективно насичених маніпулятивних конструктів, які алгоритмічно підсилюються, нормалізуються і зрештою формують паралельні інформаційні реальності. Саме ця інституціоналізація постправдового середовища трансформує локальні інформаційні інциденти у системні ризики, оскільки підрив довіри до джерел знань зменшує ймовірність колективної дії, що у свою чергу сприяє політичній фрагментації, ускладнює ухвалення рішень і відкриває вікно можливостей для зовнішнього втручання. В умовах гібридних війн інформаційний вплив синергує з кібероперaціями та військовими діями, створюючи ефект взаємного підсилення, коли психологічний тиск і панічні наративи збільшують уражуваність критичної інфраструктури, а технічні збої екстраполюються пропагандою до масштабного суспільного дестабілізаційного ефекту. Емпіричні дані, розглянуті у підрозділах, демонструють, що вразливість політичних систем корелює з інтенсивністю поляризації та дефіцитом медіаграмотності, а економічна шкода зумовлюється щільністю цифрових зв’язків, залежністю від постачальників інформаційних технологій третіх сторін і складністю виробничо логістичних ланцюгів.

Структурний висновок полягає в тому, що інформаційний тероризм не є побічним продуктом цифрової доби, а становить автономну стратегію примусу і дестабілізації з високою віддачею для агресора за мінімальних витрат. Відповідно, суто реактивні або суто технократичні підходи є недостатніми, отже поєднання правових, технологічних, комунікаційних і освітніх інструментів має бути інтегроване в національні та наднаціональні рамки безпеки. Ефективні контрзаходи повинні охоплювати не лише кіберзахист і регулювання цифрових

платформ, а й інституційну комунікацію ризиків, розвиток критичного мислення, підвищення прозорості даних і зміцнення довіри як суспільного капіталу. Інформаційний тероризм виступає каталізатором політичної нестабільності, економічної турбулентності та соціальної дезінтеграції, а також фактором, що знижує ефективність демократичного врядування.

РОЗДІЛ ІІІ. МІЖНАРОДНА ПРОТИДІЯ ІНФОРМАЦІЙНОМУ ТЕРОРИЗМУ

3.1. Міжнародні стратегії боротьби з інформаційним тероризмом

Трансформація інформаційного тероризму у комплексну міжнародну загрозу вимагає координованої відповіді світової спільноти через багаторівневу архітектуру стратегій, що охоплює глобальні, регіональні та національні рівні. Аналіз еволюції цих стратегій демонструє поступовий перехід від реактивних механізмів безпеки до проактивних систем стримування та превентивної протидії гібридним загрозам у кіберпросторі. Глобальні стратегії Організації Об'єднаних Націй формують фундамент міжнародного правового регулювання протидії кіберзагрозам та інформаційному тероризму. Конвенція ООН проти кіберзлочинності, прийнята Генеральною Асамблеєю 24.12.2024 року та відкрита для підписання 25 жовтня 2025 року у Ханої, стала першим комплексним глобальним договором, що забезпечує держави механізмами запобігання та боротьби з кіберзлочинністю. Зазначений документ охоплює незаконний доступ до інформаційних систем, кібершахрайство, програми вимагачі та фінансові злочини, критично інтегруючи захист прав людини у протокли протидії. [120] Конвенція набуде чинності після ратифікації сорокома державами, що засвідчує міжнародний консенсус щодо необхідності юридично зобов'язуючих норм у кіберпросторі. Ініціатива CT TECH (Counter-Terrorism Technology Initiative) Управління ООН з боротьби з тероризмом, запущена у 2021 році з розширенням CT TECH+ у листопаді 2024 року, демонструє еволюцію розуміння технологічних аспектів терористичних загроз.[121]

Програма зосереджується на зміцненні спроможностей правоохоронних органів протидіяти використанню нових технологій терористами, охоплюючи темний веб, криптовалюти та цифрову криміналістику. Звіт UNCCT 2024 року

-[120] United Nations Office on Drugs and Crime. United Nations Convention against Cybercrime. URL: https://www.unodc.org/unodc/cybercrime/convention/home.html (date of access: 01.10.2025). [121] United Nations Office of Counter-Terrorism. CT TECH Initiative. URL: https://www.un.org/counterterrorism/ct-tech initiative (date of access: 01.10.2025).

засвідчує, що терористичні групи демонструють підвищену здатність адаптуватися та розширювати операції, експлуатуючи нестабільність у конфліктних регіонах та використовуючи пропаганду і нові технології для рекрутування, підбурювання до насильства та поширення терору. [122] Дебати Ради Безпеки ООН з питань кібербезпеки у червні 2024 року підкреслили критичну ситуацію глобального кіберпростору. Генеральний секретар ООН зазначив, що цифрові технології розвиваються з «надшвидкістю», але якість безшовної миттєвої зв'язності, що забезпечує величезні переваги кіберпростору, може також залишати людей, інституції та цілі країни глибоко вразливими.[123]

Європейська архітектура протидії інформаційним загрозам представляє найбільш інтегровану регіональну модель. Стратегія кібербезпеки ЄС для цифрового десятиліття, презентована у грудні 2020 року Європейською Комісією та Високим представником Союзу з питань зовнішньої політики та політики безпеки, встановлює три ключові стовпи: стійкість та технологічний суверенітет, оперативні можливості для запобігання та реагування на кіберзагрози, та просування глобального відкритого кіберпростору.[124] Стратегія пропонує переглянуту Директиву NIS2, мережу центрів операцій безпеки та спільний кіберпідрозділ, створюючи комплексну екосистему координації.

Директива NIS2, прийнята у листопаді 2022 року з терміном транспозиції 18 жовтня 2024 року, розширила сферу охоплення на більше критичних секторів, гармонізувала вимоги звітності та впровадила суворіші заходи забезпечення виконання.[125] Документ охоплює основні та важливі суб'єкти в охороні здоров'я, енергетиці, транспорті, цифровій інфраструктурі, фінансових послугах та

державному управлінні. Держави-члени отримали термін до 17 квітня 2025 року для складання переліку суб'єктів, що підпадають під сферу дії NIS2, який

[122] United Nations Counter-Terrorism Centre. UNCCT Annual Report 2024. URL: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/250815_uncct_ar_2024_en.pdf (dat e of access: 01.10.2025).
[123] United Nations Security Council. Digital Breakthroughs Must Serve Betterment of People, Planet. URL: https://press.un.org/en/2024/sc15738.doc.htm (date of access: 01.10.2025).
[124] European Commission. EU Cybersecurity Strategy for the Digital Decade. URL: https://digital strategy.ec.europa.eu/en/policies/cybersecurity-strategy (date of access: 01.10.2025).
[125] Council of the European Union. EU cybersecurity: strategy and key policies. URL: https://www.consilium.europa.eu/en/policies/cybersecurity/ (date of access: 01.10.2025).

повинен оновлюватися щонайменше кожні два роки. Акт про кіберстійкість ЄС, що набув чинності 10 грудня 2024 року, встановлює вимоги кібербезпеки для продуктів з цифровими елементами, підключених до інтернету або інших пристроїв, забезпечуючи безпеку таких продуктів до їх розміщення на ринку та протягом всього життєвого циклу.[126] Акт про кіберсолідарність, прийнятий Радою 2 грудня 2024 року, створює загальноєвропейські можливості для підвищення стійкості та реактивності Європи перед кіберзагрозами, зміцнюючи механізми співпраці. Документ передбачає створення системи попередження про кібербезпеку, пан'європейської інфраструктури, що складається з національних та транскордонних кіберцентрів, відповідальних за підтримку виявлення кіберзагроз та інцидентів. Кібербезпековий план дій ЄС (EU Cyber Blueprint), прийнятий 6 червня 2025 року, представляє крок вперед у управлінні масштабними кіберінцидентами.[127] План забезпечує чітке пояснення, коли повинна бути активована криза рамкова система та які ролі належать відповідним мережам, акторам та механізмам на рівні Союзу. Документ підкреслює важливість цивільно-військової співпраці у контексті управління кіберкризами, включаючи з НАТО, через посилені механізми обміну інформацією де це можливо та необхідно.

Організація з безпеки і співробітництва (ОБСЄ) розробила специфічний підхід до протидії інформаційним загрозам через призму захисту свободи медіа. Представник ОБСЄ зі свободи медіа, інституція створена у 1997 році, моніторить порушення свободи вираження поглядів у 57 державах-учасницях. Звіт 2022

року «Чи може бути безпека без свободи медіа?» демонструє надійні дослідження взаємозв'язку між свободою медіа, демократією та безпекою, доводячи, що вільні медіа є необхідними для мирного вирішення конфліктів.[128]

[126] European Commission. Cyber Resilience Act. URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity policies (date of access: 01.10.2025).
[127] European Union. European Cyber Defence Policy. URL: https://www.european-cyber-defence-policy.com/ (date of access: 01.10.2025).
[128] Organization for Security and Co-operation in Europe. OSCE Representative on Freedom of the Media. URL: https://www.osce.org/representative-on-freedom-of-media (date of access: 01.10.2025).

Альянс НАТО розробив всеохоплюючу політику протидії інформаційному тероризму та кіберзагрозам, що еволюціонувала від розгляду кіберпростору як периферійної проблеми до визнання його основним елементом колективної оборони. Стратегічна концепція НАТО 2022 року, прийнята на саміті в Мадриді 29 червня 2022 року, експліцитно заявляє, що «кіберпростір постійно оспорюється» зловмисними акторами, які прагнуть деградувати критичну інфраструктуру та втручатися в урядові послуги. [129] Концепція ідентифікує Російську Федерацію як найбільш значущу загрозу та примусову політику Китаю як системний виклик для євро-атлантичної безпеки. Всеохоплююча політика кіберзахисту НАТО, схвалена на Брюссельському саміті 2021 року, підтримує три основні завдання Альянсу та визнає кібер як операційний домен з 2016 року.[130] На саміті НАТО 2024 року у Вашингтоні союзники погодилися створити Інтегрований центр кіберзахисту НАТО (NATO Integrated Cyber Defence Centre) для покращення захисту мереж, ситуаційної обізнаності та імплементації кіберпростору як операційного домену. Центр об'єднує цивільних та військових кіберзахисників, включаючи промисловість, на цілодобовій основі для покращення ситуаційної обізнаності та посилення колективної стійкості проти кіберзагроз.[131] Оновлені керівні принципи політики протидії тероризму НАТО 2024 року визнають, що тероризм залишається найбільш прямою асиметричною загрозою безпеці громадян та міжнародному миру.[132]

Документ підкреслює, що терористи продовжують демонструвати здатність

перетинати міжнародні кордони, розширювати свої мережі, посилювати спроможності та інвестувати в нові технології для збільшення досяжності та летальності. Стратегія цифрової трансформації НАТО, імплементаційна стратегія якої була затверджена 17 жовтня 2024 року, стала першим

[129] North Atlantic Treaty Organization. NATO Strategic Concept 2022. URL: https://www.nato.int/cps/en/natohq/topics_56626.htm (date of access: 01.10.2025).
[130] North Atlantic Treaty Organization. NATO Cyber Defence. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm (date of access: 01.10.2025).
[131] North Atlantic Treaty Organization. NATO Secretary General at Cyber Defence Conference 2025. URL: https://www.nato.int/cps/en/natohq/news_238333.htm (date of access: 01.10.2025).
[132] North Atlantic Treaty Organization. Updated Counter-Terrorism Policy Guidelines 2024. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2025/8/pdf/Counter-Terrorism-Policy-Guidelines 2024.pdf (date of access: 01.10.2025).

комплексним планом модернізації цифрової інфраструктури Альянсу.[133] Стратегія спрямована на трансформацію способу роботи НАТО шляхом експлуатації потенціалу, що пропонується сучасними технологіями, для проведення мультидоменних операцій, забезпечення інтероперабельності через всі домени, посилення ситуаційної обізнаності та полегшення політичних консультацій і прийняття рішень на основі даних. Саміт НАТО 2025 року у Гаазі став критичною віхою для кібербезпеки альянсу. Держави-члени погодились підвищити загальні витрати на оборону та безпеку до 5% ВВП до 2035 року, з яких 1.5% буде спеціально виділено на некінетичні можливості, головним чином кібербезпеку, захист критичної інфраструктури та національні ініціативи стійкості.[134] Це позначає стратегічний зсув у визнанні кібербезпеки не вторинною функцією підтримки, а формалізованим і фінансованим аспектом національних та загальносоюзницьких стратегій оборони.

Національні стратегії провідних держав демонструють різноманітні підходи до протидії інформаційному тероризму, що відображають специфічні геополітичні та технологічні контексти. Національна стратегія кібербезпеки США 2023 року представляє дві фундаментальні зміни парадигми: перебалансування відповідальності за захист кіберпростору на найбільш спроможних акторів та переорієнтацію стимулів для довгострокових інвестицій. П'ять стовпів стратегії охоплюють захист критичної інфраструктури, руйнування

акторів загроз, формування ринкових сил для безпеки та стійкості, інвестиції в стійке майбутнє та формування міжнародних партнерств для досягнення спільних цілей. План імплементації, опублікований у липні 2023 року, містить понад 65 ініціатив високого впливу з чіткими часовими рамками та відповідальними агенціями.[135] Національна кіберстратегія Великобританії 2022 року виділяє 2.6 мільярда фунтів стерлінгів інвестицій та встановлює

-[133] North Atlantic Treaty Organization. NATO's Digital Transformation Implementation Strategy. URL: https://www.nato.int/cps/en/natohq/official_texts_229801.htm (date of access: 01.10.2025). [134] Cyber Security District. Key Cybersecurity Takeaways from the 2025 NATO Summit. URL: https://www.cybersecuritydistrict.com/key-cybersecurity-takeaways-from-the-2025-nato-summit/ (date of access: 01.10.2025).
[135] The White House. National Cybersecurity Strategy 2023. URL: https://bidenwhitehouse.archives.gov/oncd/national cybersecurity-strategy/ (date of access: 01.10.2025).

Національні кіберсили (National Cyber Force) для наступальних можливостей. Стратегія зосереджується на захисті критичної інфраструктури, вирішенні вразливостей ланцюга постачання та обмеженні залежності від технологій авторитарних режимів, які не поділяють цінностей Великобританії. Документ підкреслює важливість державно-приватних партнерств та розвитку національних кіберкомпетенцій.[136] Стратегія кібербезпеки Німеччини 2021 року, прийнята 8 вересня 2021 року, містить 44 стратегічні цілі з вимірюваними критеріями імплементації.[137] Чотири сфери дії охоплюють суспільство (підвищення кіберграмотності громадян), приватну індустрію (захист критичної інфраструктури та бізнесу), уряд (зміцнення державних можливостей) та ЄС/міжнародне співробітництво (просування європейської цифрової автономії та захист демократичних цінностей у кіберпросторі).

Стратегія кібербезпеки України 2021-2025, затверджена 26 серпня 2021 року Указом Президента №447/2021, базується на трьох фундаментальних принципах: стримування (зміцнення можливостей запобігання збройній агресії в кіберпросторі), кіберстійкість (здатність адаптуватися до загроз та швидко відновлюватися після атак) та розвиток партнерства на національному і міжнародному рівнях. Стратегія враховує унікальний досвід України у протидії російським кібероперація м та дезінформації з 2014 року, інтегруючи уроки

гібридної війни у національну архітектуру кібербезпеки.[138] Стратегія кібербезпеки Естонії 2024-2030 «Кібер-свідома Естонія» збільшила бюджет з 3.9 мільйона євро у 2020 році до 16.1 мільйона євро у 2024 році у відповідь на зростаючі політично мотивовані атаки. [139] Як мала держава з високим рівнем цифровізації, Естонія розглядає кібербезпеку як захист усього цифрового

-[136] UK Government. UK National Cyber Strategy 2022. URL: https://www.thestack.technology/uks-2022-national cyber-security-strategy/ (date of access: 01.10.2025).

[137] Federal Ministry of the Interior. Cyber Security Strategy for Germany 2021. URL: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for germany2021.pdf (date of access: 01.10.2025).

[138] Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy" : Ukaz Prezydenta Ukrainy vid 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (data zvernennia: 01.10.2025).

[139] Republic of Estonia. Cybersecurity Strategy 2024-2030: Cyber-Conscious Estonia. URL: https://dig.watch/resource/cybersecurity-strategy-2024-2030-cyber-conscious-estonia (date of access: 01.10.2025).