Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.
Державне управління: удосконалення та розвиток. 2026. № 2.
ISSN 2307-2156

DOI: http://doi.org/10.32702/2307-2156.2026.2.23

УДК 354:328.185

О. О. Любиченко,

аспірантка кафедри глобальної та національної безпеки Навчально-наукового інституту публічного управління та державної служби, Київський національний університет імені Тараса Шевченка

ORCID ID: https://orcid.org/0000-0002-3638-3280

ІНФОРМАЦІЙНА СТІЙКІСТЬ У ДОСЛІДЖЕННЯХ ГІБРИДНИХ ЗАГРОЗ: ТЕОРЕТИЧНІ ІНТЕРПРЕТАЦІЇ ТА УКРАЇНСЬКИЙ ДОСВІД

O. Liubychenko,

Postgraduate student of the Department of Global and National Security, Educational and Scientific Institute of Public Administration and Civil Service, Taras Shevchenko University of Kyiv

INFORMATION RESILIENCE IN HYBRID THREAT RESEARCH: THEORETICAL INTERPRETATIONS AND THE UKRAINIAN EXPERIENCE

Сучасне безпекове середовище характеризується глибокою трансформацією форм і методів протистояння, у межах яких ключового

значення набувають немілітарні інструменти впливу, зокрема інформаційні. Гібридні загрози постають як комплексне багатовимірне явище, що поєднує військові, політичні, економічні, інформаційні та соціокультурні компоненти, спрямовані на підрив внутрішньої цілісності та стійкості держави і суспільства. Особливу роль у структурі гібридних впливів відіграє інформаційний компонент, який охоплює як інституційний рівень функціонування держави, так і когнітивно-поведінкові аспекти життєдіяльності громадян, впливаючи на їхні цінності, ідентичності та моделі сприйняття реальності.

У сучасному науковому дискурсі зростає увага до категорії «інформаційна стійкість», яка дедалі частіше використовується як аналітичний інструмент для осмислення здатності суспільства протидіяти системним інформаційним впливам, дезінформації, маніпуляціям та когнітивним атакам. На відміну від традиційного підходу до інформаційної безпеки, орієнтованого переважно на технічний та нормативний захист інформаційного простору й інфраструктури, концепт інформаційної стійкості фокусується на адаптивних можливостях суспільства, рівні суб'єктності соціальних а́кторів, ступені соціальної довіри, зрілості національної ідентичності та інституційній спроможності. Такий підхід дозволяє трактувати інформаційну стійкість як динамічну характеристику соціальної системи, що визначає її здатність зберігати функціональність і ціннісну інтеграцію в умовах зовнішнього інформаційного тиску.

Український досвід протидії гібридним загрозам, сформований у контексті тривалої агресії з боку Російської Федерації, створив унікальне емпіричне підґрунтя для теоретичного переосмислення інформаційної стійкості. Україна стала прикладом суспільства, яке в умовах постійного інформаційного впливу було змушене розвивати механізми резильєнтності на основі взаємодії державних та недержавних суб'єктів — органів влади, медіа, громадянського суспільства, волонтерських ініціатив, експертних та цифрових спільнот. Це зумовлює потребу комплексного, міждисциплінарного

та концептуального осмислення інформаційної стійкості як інтегральної складової безпекових досліджень, що поєднує у собі політичні, соціальні, комунікативні та когнітивні підходи.

Дослідження інформаційної стійкості в українському контексті дозволяє не лише проаналізувати особливості національної відповіді на гібридні загрози, а й розширити теоретичні моделі сучасних безпекових студій, інтегруючи фактори соціальної взаємодії, ідентичнісних процесів, медіакомунікацій та інституційної адаптивності. Таким чином, інформаційна стійкість постає як ключовий концепт, що визначає спроможність держави й суспільства функціонувати, відновлюватися та протидіяти загрозам у багатовимірному інформаційному середовищі.

The contemporary security environment is characterized by a profound transformation of the forms and methods of confrontation, within which non-military instruments of influence — particularly informational ones — are gaining decisive importance. Hybrid threats emerge as a complex multidimensional phenomenon that integrates military, political, economic, informational, and sociocultural components aimed at undermining the internal cohesion and resilience of the state and society. The informational dimension of hybrid influence plays a special role, as it encompasses both the institutional level of state functioning and the cognitive-behavioral aspects of citizens' everyday life, shaping their values, identities, and models of perception.

In the modern scholarly discourse, growing attention is paid to the category of information resilience, which is increasingly used as an analytical tool for understanding a society's ability to withstand systemic informational influences, disinformation, manipulation, and cognitive attacks. In contrast to the traditional approach to information security—focused primarily on the technical and regulatory protection of the information space and infrastructure—the concept of information resilience emphasizes the adaptive capacities of society, the agency of social actors, the degree of social trust, the maturity of national identity, and

institutional capability. This approach enables the interpretation of information resilience as a dynamic characteristic of a social system that determines its ability to maintain functionality and value integrity under conditions of external informational pressure.

The Ukrainian experience of countering hybrid threats, shaped by prolonged aggression from the Russian Federation, has created a unique empirical foundation for the theoretical reconsideration of information resilience. Ukraine has become an example of a society that, under conditions of continuous information pressure, was compelled to develop mechanisms of resilience through the interaction of state and non-state actors — government institutions, the media, civil society, expert communities, volunteer initiatives, and digital networks. This necessitates a comprehensive, interdisciplinary, and conceptual understanding of information resilience as an integral component of contemporary security studies, combining political, social, communicative, and cognitive perspectives.

Research on information resilience in the Ukrainian context not only allows for an analysis of the specific features of the national response to hybrid threats but also broadens the theoretical models of modern security scholarship by integrating factors of social interaction, identity processes, media communications, and institutional adaptability. Thus, information resilience appears as a key concept that determines the capacity of the state and society to function, recover, and counter threats within a multidimensional information environment.

Ключові слова: *інформаційна стійкість, гібридні загрози, резильєнтність, інформаційна безпека, стратегічні комунікації, дезінформація, когнітивні впливи, соціальна довіра, національна ідентичність, інституційна спроможність.*

Keywords: *information resilience, hybrid threats, resilience, information security, strategic communications, disinformation, cognitive influence, social trust, national identity, institutional capacity.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями.

Трансформація сучасного безпекового середовища, зумовлена ескалацією гібридних форм протистояння, актуалізує необхідність поглибленого теоретичного та прикладного аналізу механізмів протидії інформаційним загрозам. Гібридна війна створює ситуацію, у якій традиційних підходів до забезпечення інформаційної безпеки вже недостатньо для гарантування стабільності держави та суспільства. Інформаційний компонент гібридних загроз, спрямований на вплив на свідомість, поведінкові моделі та ціннісні орієнтації населення, стає одним із ключових викликів для національної безпеки.

Таким чином, проблема дослідження полягає у необхідності концептуального уточнення змісту інформаційної стійкості, визначення її місця у системі аналізу гібридних загроз, а також окреслення специфіки українського досвіду формування резильєнтності в умовах сучасного інформаційного протистояння. Розв'язання цієї проблеми є важливою передумовою для вдосконалення національних безпекових стратегій та розроблення ефективних інституційних механізмів протидії гібридним впливам.

Аналіз останніх досліджень і публікацій.

У сучасному українському та міжнародному науковому дискурсі концепт інформаційної стійкості дедалі частіше набуває статусу ключової аналітичної категорії, необхідної для осмислення процесів, що відбуваються в умовах гібридної війни, дезінформаційної агресії та інфомедійних трансформацій. Якщо раніше домінував підхід, зосереджений переважно на інформаційній безпеці у її техніко-нормативному вимірі, то нині спостерігається перехід до інтегральної моделі, що охоплює когнітивні, соціокультурні, інституційні та комунікаційні параметри функціонування суспільства.

Важливу роль у теоретизації цього поняття відіграли українські дослідники. Зокрема, Ірина Мельник акцентує на багатовимірності інформаційної стійкості, визначаючи її як здатність суспільства зберігати критичне мислення, соціальну довіру та комунікативну цілісність у контексті гібридних загроз. Науковиця підкреслює, що формування інформаційної стійкості пов'язане не лише з індивідуальними компетентностями громадян, а й із якістю інституцій, станом медіасередовища та рівнем політичної культури [3]. Таким чином, інформаційна стійкість у її трактуванні виступає не просто оборонною характеристикою, а індикатором соціальної життєздатності та консолідованості**.**

У порівняльній перспективі категорія інформаційної стійкості ґрунтовно розглядається у праці М. Гладиш, С. Пахоменка та О. Кучика, які аналізують взаємозв'язок між стійкістю інформаційного простору, інституційною спроможністю та якістю демократичних процедур. Дослідники наголошують, що інформаційна резильєнтність забезпечує здатність суспільства та держави зберігати раціональність ухвалення рішень, запобігати деструкції соціальних зв'язків та підтримувати ефективність інституцій навіть у ситуаціях інтенсивної дезінформаційної дії [7]. У такий спосіб інформаційна стійкість постає як категорія, що поєднує когнітивні та політичні механізми опору.

Суттєвий внесок у практичне осмислення інформаційної стійкості робить також українське експертне середовище. Аналітичний документ RES-POL «Медіаграмотність та інформаційна стійкість: істотні питання політики» розглядає інформаційну стійкість як стратегічний ресурс публічної політики у сфері медіа. У документі зазначається, що стійкість інформаційного середовища залежить від рівня медіаграмотності, критичної автономії громадян, прозорості регулювання та якості роботи журналістської спільноти. Підкреслюється також, що державна політика у сфері інформаційної безпеки повинна бути зосереджена не лише на протидії загрозам, а й на розвитку адаптивної спроможності суспільства [4].

У науково-освітньому середовищі концепт інформаційної стійкості поглиблюється через міждисциплінарні підходи. Зокрема, у межах проєкту EUresissecur (Erasmus+ Jean Monnet) подано визначення інформаційної стійкості як здатності органів державної влади забезпечувати неперервність управлінських і комунікаційних процесів, оперативно реагувати на інформаційні кризи та ефективно використовувати цифрові інструменти в умовах гібридних загроз [2]. Такий підхід демонструє, що інформаційна стійкість — це не лише характеристика суспільства, а й інституційна властивість держави, пов'язана зі стійкістю публічного управління.

Окремого значення концепт набуває у рамках дослідження національної стійкості. Модель, запропонована Н. Хомою, І. Кресіною та їхніми колегами, виокремлює інформаційну стійкість як складову, що безпосередньо впливає на здатність суспільства протистояти зовнішньому впливу, підтримувати внутрішню згуртованість і забезпечувати функціонування демократичних інститутів. Інформаційний вимір у цій моделі постає фундаментальним чинником, що визначає якість політичного процесу, рівень довіри та загальну стабільність суспільства [8].

У науковому дискурсі стійкість визначається як здатність суспільства та держави адаптуватися до змін безпекового середовища й зберігати стабільність функціонування, зокрема через інструменти управління ризиками. Водночас сучасні українські дослідження конкретизують цей концепт на прикладному рівні. Важливим внеском у вимірювання інформаційної стійкості є дослідження організації «Стійка Україна», у яких вона операціоналізується через систему емпіричних індикаторів: рівень доступу до українського медіаконтенту, масштаби поширення дезінформації, структуру медіаспоживання та динаміку довіри до джерел інформації. Такий підхід забезпечує можливість регулярного моніторингу стану інформаційного середовища та формує доказову основу для розроблення й коригування державної політики у сфері безпеки [1].

Важливе місце у сучасних дослідженнях гібридних загроз посідають напрацювання Європейського центру передового досвіду з протидії гібридним загрозам (European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE), які формують міжінституційний підхід до аналізу інформаційної та суспільної стійкості. У межах Спільноти інтересів зі стратегії та оборони (COI S&D) розвивається напрям когнітивних стратегій і культурної стійкості, що зосереджується на інструменталізації ідентичності та соціальних розломів у гібридних і дезінформаційних операціях, а також на підвищенні спроможності державних інституцій протидіяти ціннісно орієнтованій дезінформації.

У співпраці з Об'єднаним дослідницьким центром Європейської комісії (European Commission's Joint Research Centre) в межах COI V&R Центр продовжує концептуалізацію гібридних загроз і механізмів стійкості, орієнтуючись на формування комплексної політики реагування на рівні держав-учасниць, ЄС та НАТО. Окремий блок досліджень присвячено аналізу інституційної готовності — урядових структур, законодавства та механізмів координації, зокрема у сфері скринінгу прямих іноземних інвестицій як інструменту запобігання стратегічним ризикам [6].

Узагальнюючи, слід зазначити, що концепт інформаційної стійкості поступово перетворюється на комплексну аналітичну рамку, яка охоплює: когнітивний вимір — критичне мислення, опір маніпуляціям; соціальний вимір — довіра, згуртованість, ідентичність; інституційний вимір — спроможність держави та управлінських структур; технологічний вимір — цифрова стабільність, стратегічні комунікації; освітній вимір — формування компетентностей інформаційної резильєнтності.

Формулювання цілей статті.

Метою цієї статті є аналіз теоретичних інтерпретацій інформаційної стійкості у дослідженнях гібридних загроз та визначення особливостей українського досвіду її формування в умовах гібридної війни. Для досягнення поставленої мети передбачається розгляд еволюції підходів до

трактування інформаційної стійкості, окреслення її суб'єктного та інституційного вимірів, а також зіставлення теоретичних моделей із практикою їх реалізації в українському безпековому контексті.

Виклад основного матеріалу дослідження.

Гібридні загрози у сучасних безпекових дослідженнях розглядаються як багатовимірна форма протиборства, що поєднує різні інструменти впливу в єдиній стратегії тиску на державу та суспільство. Їхньою визначальною особливістю є інтегрованість та адаптивність, у межах яких інформаційний вимір набуває системоутворювального характеру, забезпечуючи когерентність військових, політичних, економічних і соціокультурних дій. У цій логіці інформаційна стійкість постає не як допоміжний елемент, а як один із ключових параметрів загальної спроможності протидії гібридним загрозам.

На відміну від класичних форм конфлікту, у гібридній війні інформаційні впливи не обмежуються пропагандою або окремими кампаніями дезінформації. Вони є постійним фоном, що супроводжує всі етапи протиборства — від мирного періоду до фаз відкритої ескалації. Саме тому інформаційний домен у структурі гібридних загроз виконує функцію «м'якого середовища», яке підготовлює умови для використання інших інструментів впливу, знижуючи поріг опору суспільства та легітимність державних рішень.

У теоретичному вимірі інформаційна стійкість у структурі гібридних загроз може бути визначена як здатність соціально-політичної системи зберігати цілісність інтерпретацій реальності в умовах цілеспрямованого наративного та когнітивного тиску. Гібридні впливи спрямовані не стільки на переконання, скільки на фрагментацію спільного символічного простору, розмивання меж між правдою і маніпуляцією, формування стану хронічної недовіри та інформаційної втоми. У такому середовищі рівень інформаційної стійкості визначає, чи здатне суспільство підтримувати функціональну єдність попри наявність конкуруючих і часто взаємовиключних наративів.

Важливим аспектом є те, що інформаційна стійкість у гібридних загрозах має виразно міжрівневий характер. На макрорівні вона пов’язана зі здатністю держави формувати узгоджену стратегічну комунікацію та забезпечувати інституційну послідовність. На мезорівні ключову роль відіграють медіа, експертні спільноти та громадянське суспільство, які виконують функцію посередника між владою і населенням. На мікрорівні інформаційна стійкість інтерпретується через призму індивідуальних когнітивних навичок, рівня медіаграмотності та здатності до критичного мислення. Гібридні загрози водночас впливають на всі ці рівні, що ускладнює вироблення одновимірних відповідей.

Особливе значення в структурі гібридних загроз має наративний вимір. Контроль над інтерпретаціями подій, історичної пам’яті, понять легітимності та ідентичності стає не менш важливим, ніж контроль над територіями чи ресурсами. Інформаційна стійкість у цьому контексті передбачає спроможність суспільства відтворювати власні наративи та адаптувати їх до змінного середовища без втрати базових ціннісних орієнтирів. Це особливо актуально для держав, що перебувають у стані трансформації або зазнають зовнішнього ідентичнісного тиску.

У документах та аналітичних підходах НАТО і Європейський Союз гібридні загрози визначаються як такі, що навмисно експлуатують відкритість демократичних суспільств. Відповідно, інформаційна стійкість не може обмежуватися контрольними чи репресивними механізмами, оскільки вони самі по собі здатні підірвати довіру та легітимність. Натомість ідеться про баланс між безпекою та свободою, де ключовим ресурсом виступає соціальний капітал і включеність громадян у процеси колективного смислотворення.

Таким чином, у структурі гібридних загроз інформаційна стійкість виконує подвійну функцію. З одного боку, вона є об’єктом атак, оскільки підрив довіри, ідентичності та когнітивної спроможності суспільства є стратегічною метою гібридного впливу. З іншого — вона виступає чинником

стримування, здатним зменшити ефективність інших компонентів гібридної агресії. Саме в цій точці перетину теорії та практики доцільно розглядати український досвід як емпіричний приклад формування інформаційної стійкості в умовах системного гібридного тиску.

Аналітична типологія інформаційних впливів у структурі гібридних загроз

Для глибшого осмислення ролі інформаційної стійкості в умовах гібридних загроз доцільним є застосування аналітичної типології інформаційних впливів, яка дає змогу систематизувати різнорідні інструменти гібридного протиборства та визначити напрями їхнього впливу на суспільну стабільність і процеси ухвалення рішень. Такий підхід дозволяє вийти за межі фрагментарного аналізу окремих дезінформаційних кампаній і розглядати інформаційні впливи як структурований елемент комплексної гібридної стратегії.

У цьому контексті показовими є напрацювання американської дослідниці Террі Боррас, яка аналізує механізми когнітивного втручання та підкреслює, що об’єктом первинного впливу в сучасних конфліктах стає «людський вимір» — сприйняття, довіра, інтерпретаційні рамки та психологічні реакції [5]. Такий підхід зміщує фокус із суто інформаційного контенту на процеси формування суджень і рішень, що безпосередньо пов’язано з вразливістю управлінського середовища до викривлених наративів. Водночас дослідниця наголошує на необхідності проактивного формування когнітивної стійкості управлінських команд ще до моменту, коли інформаційні викривлення починають впливати на процес прийняття рішень.

З огляду на це у межах даної статті пропонується типологія інформаційних впливів за функціональною спрямованістю, що корелює з ключовими параметрами інформаційної стійкості — когнітивним, інституційним і соціальним. Така класифікація дозволяє не лише описувати

форми інформаційної агресії, а й визначати відповідні механізми запобігання та підвищення стійкості в умовах гібридної війни.

1. Когнітивні інформаційні впливи

Когнітивний тип інформаційних впливів спрямований на зміну способів сприйняття, інтерпретації та оцінювання реальності. Йдеться про маніпуляцію фактами, підміну причинно-наслідкових зв'язків, створення псевдонаукових пояснень і нав'язування альтернативних картин світу. У структурі гібридних загроз такі впливи виконують функцію дезорієнтації та зниження здатності до раціонального колективного судження.

З точки зору інформаційної стійкості, основним контрресурсом виступають рівень освіти, критичного мислення та медіаграмотності, а також наявність авторитетних експертних спільнот, здатних оперативно інтерпретувати складні події.

2. Наративно-ідентичнісні інформаційні впливи

Цей тип впливів скерований на трансформацію або підрив колективної ідентичності, історичної пам'яті та символічних маркерів спільноти. Його характерними ознаками є реінтерпретація історії, делегітимація державності, дискредитація культурних і мовних практик, а також нав'язування зовнішніх ідентичнісних моделей.

У контексті гібридних загроз наративно-ідентичнісні впливи мають довгостроковий характер і націлені на ерозію ціннісних підвалин суспільства. Інформаційна стійкість у цьому вимірі залежить від наявності узгоджених національних наративів, інституцій пам'яті та здатності суспільства до рефлексивного переосмислення власної історії без зовнішнього нав'язування.

3. Емоційно-психологічні інформаційні впливи

Емоційно-психологічні впливи апелюють до страху, тривоги, гніву або апатії як засобів дестабілізації суспільства. Їхньою метою є не переконання, а виснаження, формування відчуття безсилля та відсутності контролю над подіями. Такі впливи часто використовують шокову інформацію,

перебільшення втрат, акцент на внутрішніх конфліктах і соціальній несправедливості.

Інформаційна стійкість у цьому випадку пов’язана зі спроможністю колективного емоційного регулювання, рівнем довіри до офіційних і неофіційних джерел, а також ефективністю кризових комунікацій з боку держави та медіа.

4. Інституційно-деструктивні інформаційні впливи

Цей тип спрямований на підрив легітимності державних інституцій та їхньої здатності діяти ефективно. Основними інструментами є дискредитація органів влади, делегітимація рішень, стимулювання недовіри до виборчих процесів, правосуддя та системи безпеки.

У структурі гібридних загроз інституційно-деструктивні інформаційні впливи знижують ефективність державного управління без прямого застосування сили. Відповідно, інформаційна стійкість на цьому рівні визначається прозорістю інституцій, якістю публічних комунікацій і здатністю до збереження довіри навіть у кризових умовах.

5. Мережево-маніпулятивні інформаційні впливи

Мережево-маніпулятивні впливи реалізуються через цифрові платформи, соціальні мережі та алгоритмічні механізми поширення контенту. Вони ґрунтуються на фрагментації аудиторії, створенні інформаційних «бульбашок», використанні бот-мереж та координованої неавтентичної поведінки.

У гібридних загрозах цей тип впливів підсилює всі попередні, забезпечуючи масштабованість і швидкість поширення деструктивних повідомлень. Інформаційна стійкість у мережевому середовищі залежить від цифрової грамотності, регулювання платформ, а також розвитку горизонтальних мереж фактчекінгу та аналітики.

Запропонована типологія дозволяє розглядати інформаційні впливи не як хаотичний набір дій, а як системно організований елемент гібридної стратегії. Вона також створює аналітичний міст між теорією інформаційної

стійкості та практикою її формування, дозволяючи ідентифікувати вразливості на різних рівнях та співвіднести їх із відповідними ресурсами резильєнтності.

Застосування цієї схеми до українського досвіду відкриває можливість оцінювати не лише інтенсивність інформаційних атак, а й еволюцію відповідей на них — від реактивних заходів до комплексних моделей інформаційної стійкості, інтегрованих у систему національної безпеки.

Український досвід формування інформаційної стійкості в умовах гібридної війни.

Український досвід протидії гібридним загрозам є показовим прикладом практичної реалізації теоретичних підходів до інформаційної стійкості в умовах тривалого та системного зовнішнього тиску. Починаючи з 2014 року, Україна опинилася в ситуації асиметричного конфлікту, у межах якого інформаційний вимір став одним із ключових інструментів агресії. Масштабність і тривалість інформаційних впливів зумовили необхідність не лише кризового реагування, а й поступового формування стійких механізмів адаптації на рівні держави та суспільства.

На першому етапі протидії гібридним загрозам домінували реактивні підходи, зосереджені переважно на нейтралізації окремих інформаційних кампаній та обмеженні доступу до відверто пропагандистських ресурсів. У цей період інформаційна стійкість формувалася фрагментарно, значною мірою завдяки ініціативам громадянського суспільства, волонтерських і експертних спільнот, які компенсували обмежену інституційну спроможність держави. Саме в цей час зароджуються мережеві форми взаємодії між журналістами, аналітиками, активістами та цифровими спільнотами, що згодом стали важливим елементом української резильєнтності.

Подальший етап характеризується поступовою інституціоналізацією підходів до інформаційної стійкості. Держава починає усвідомлювати інформаційний домен як складову національної безпеки, що потребує стратегічного планування та координації. Формуються елементи

стратегічних комунікацій, розвиваються спроможності з протидії дезінформації, а також зростає увага до питань інформаційної гігієни та медіаграмотності. Водночас важливою ознакою українського підходу залишається збереження активної ролі недержавних суб'єктів, що запобігає надмірній централізації та підсилює довіру до антикризових повідомлень.

Повномасштабне вторгнення Російської Федерації у 2022 році стало критичним випробуванням для наявних механізмів інформаційної стійкості. У цей період відбулася якісна трансформація інформаційного середовища, що засвідчила перехід від переважно оборонних практик до проактивного управління інформаційними процесами. Вирішальним чинником стала здатність українського суспільства швидко мобілізуватися навколо спільних наративів спротиву, солідарності та суб'єктності, що значною мірою нейтралізувало деструктивний вплив ворожих інформаційних операцій.

Важливо підкреслити, що українська інформаційна стійкість формується не лише через офіційну комунікацію державних органів, а й через широку мережу горизонтальних зв'язків. Громадянське суспільство, незалежні медіа, волонтерські платформи та аналітичні центри виступають не пасивними реципієнтами інформації, а активними виробниками смислів. Саме ця багаторівнева мережевість забезпечує високий ступінь адаптивності інформаційного середовища та ускладнює його централізовану дестабілізацію.

Окремої уваги заслуговує роль національної ідентичності як підґрунтя інформаційної стійкості. В умовах гібридної війни ідентичність стає одночасно мішенню та ресурсом протидії. Український досвід демонструє, що чітке усвідомлення власної історичної суб'єктності, політичного вибору та ціннісної орієнтації сприяє зниженню ефективності маніпулятивних наративів і підвищує стійкість до когнітивних атак. У цьому сенсі інформаційна стійкість постає як похідна не лише від комунікаційних стратегій, а й від глибших соціокультурних процесів.

Таким чином, український досвід підтверджує тезу про те, що інформаційна стійкість у структурі гібридних загроз формується як результат динамічної взаємодії державних і недержавних а́кторів, інституційних рішень і мережевих практик, а також ідентичнісних і ціннісних чинників. Це дозволяє розглядати Україну не лише як об'єкт гібридних впливів, а й як джерело емпірично обґрунтованих висновків для подальшого розвитку теорії гібридних загроз та інформаційної стійкості.

Інформаційна стійкість до когнітивних впливів: український досвід.

Досвід України в умовах тривалої гібридної агресії з боку Російської Федерації надає унікальний емпіричний матеріал для аналізу когнітивного виміру інформаційної стійкості. Починаючи з 2014 року, український інформаційний простір перебуває в умовах перманентного цілеспрямованого впливу, що поєднує дезінформаційні кампанії, наративні атаки, емоційний тиск і маніпуляцію контекстом. За таких умов саме когнітивний рівень — сприйняття, інтерпретації та колективного смислотворення — став одним із ключових полів протиборства.

Увага як початкова точка когнітивного впливу в українському контексті.

Український кейс демонструє, що первинною мішенню інформаційних операцій є не зміст повідомлення, а організація уваги аудиторії. У періоди високої суспільної напруги — під час військових загострень, масових ракетних атак, енергетичних криз або політично чутливих подій — спостерігається підвищена вразливість до інформаційних сигналів із високим емоційним зарядом. Саме в такі моменти деструктивні повідомлення найчастіше інтегруються в інформаційний потік під виглядом «термінових», «інсайдерських» або «приховуваних» новин.

Практика показує, що фактори когнітивної вразливості — втома, перевантаження, відчуття ізольованості — системно експлуатуються зовнішнім а́ктором, зокрема через синхронізацію інформаційних впливів із

військовими або соціально-економічними подіями. Це дозволяє знижувати поріг критичного сприйняття без необхідності створювати достовірно переконливий контент.

Емоційна інтенсифікація як інструмент дестабілізації.

Український інформаційний простір характеризується високою емоційною мобілізованістю, що є водночас ресурсом спротиву і потенційною зоною вразливості. Емоційні впливи, спрямовані на формування страху, паніки, відчуття зради або внутрішнього розколу, системно використовуються для прискорення когнітивних реакцій і зниження здатності до раціональної оцінки інформації.

Український досвід свідчить, що навіть за високого рівня патріотичної консолідації короткочасні емоційні сплески можуть створювати локальні когнітивні збої — наприклад, у формі поширення неперевіреної інформації або емоційно забарвлених інтерпретацій. Водночас стабілізуючу роль відіграє набута спроможність суспільства розпізнавати емоційні тригери як компонент ворожого впливу, а не як достовірні індикатори реальності.

Маніпуляція контекстом у наративах щодо України.

Колапс контексту є одним із найактивніше застосовуваних механізмів впливу в інформаційній війні проти України. Йдеться про системне вилучення історичних, політичних або правових рамок із повідомлень, що дозволяє нав’язувати альтернативні інтерпретації подій без прямого спотворення фактів. Типовими прикладами є переінтерпретація окремих висловлювань українських посадовців, фрагментарне використання статистичних даних або ізольоване цитування міжнародних документів.

Українська практика протидії таким впливам поступово сформувала розвинену культуру контекстуальної верифікації, зокрема завдяки діяльності незалежних медіа, аналітичних центрів і фактчекінгових ініціатив. Ці практики суттєво підвищили загальний рівень інформаційної стійкості, зменшивши ефективність маніпуляцій, що ґрунтуються на неповноті інформації.

Організаційний вимір когнітивної стійкості в Україні.

На рівні державних і недержавних організацій когнітивні впливи в українському контексті нерідко проявляються у формі внутрішніх комунікаційних збоїв, загострення недовіри або некоректного визначення пріоритетів загроз. У ранні періоди гібридної агресії такі явища часто сприймалися як виключно внутрішні проблеми управління або міжособистісної взаємодії.

З часом відбулося переосмислення цих ознак як потенційних індикаторів зовнішнього інформаційного втручання. Це, своєю чергою, сприяло розвитку превентивних підходів до інформаційної стійкості, зокрема впровадженню стандартів кризових комунікацій, підвищенню прозорості ухвалення рішень і формуванню горизонтальних каналів довіри між інституціями та громадянським суспільством.

Людський рівень інформаційної стійкості в українській моделі.

Український досвід демонструє, що ключовим чинником стійкості є не лише інституційна регламентація інформаційної сфери, а й наявність розвиненого людського рівня інформаційної безпеки. Йдеться про здатність громадян, експертних спільнот і професійних груп до усвідомленої паузи, критичного аналізу, емоційної саморегуляції та колективної перевірки інформації.

Особливо показовою є роль громадянського суспільства та волонтерських мереж, які не лише компенсували обмежені спроможності держави на початкових етапах, а й стали каталізатором формування мережевої моделі інформаційної стійкості. У цій моделі об’єкти впливу трансформуються на активних суб’єктів протидії, здатних швидко адаптуватися до змін характеру загроз.

Ідентичність і суб’єктність як основа когнітивної резильєнтності.

В умовах гібридної війни український кейс переконливо демонструє, що національна ідентичність виконує функцію когнітивного стабілізатора. Усвідомлення політичної суб’єктності, чіткого цивілізаційного вибору та

історичної тяглості обмежує ефективність маніпулятивних наративів, спрямованих на делегітимацію державності або фрагментацію суспільства.

Таким чином, інформаційна стійкість в українському вимірі формується як інтегральний результат поєднання інституційних механізмів, мережевої взаємодії та ідентичнісних чинників. Це дозволяє розглядати Україну не лише як кейс протидії гібридним загрозам, а як джерело узагальнювальних висновків для подальшого розвитку теорії інформаційної стійкості.

Висновки та перспективи подальших розвідок у даному напрямі.

Український досвід протидії гібридним загрозам дозволяє сформулювати низку емпірично обґрунтованих положень, які конкретизують теоретичні підходи до інформаційної стійкості та розкривають її когнітивний вимір.

По-перше, встановлено, що первинною мішенню гібридних інформаційних впливів є увага як обмежений когнітивний ресурс, а не зміст інформації. В українському контексті ефективність деструктивних повідомлень значною мірою залежить від їхнього таймінгу та емоційної насиченості, зокрема в періоди суспільної напруги, військових загострень або кризових подій. Це підтверджує доцільність розгляду управління увагою як одного з ключових індикаторів інформаційної стійкості.

По-друге, емпіричні спостереження свідчать, що емоційна інтенсифікація є центральним механізмом когнітивного впливу. В українському інформаційному просторі емоції страху, тривоги, обурення або фрустрації системно використовуються для прискорення інтерпретаційних процесів і зниження рівня критичного осмислення. Водночас суспільна здатність розпізнавати емоційні тригери як елемент маніпуляції суттєво знижує ефективність таких впливів, що підтверджує важливість емоційної саморегуляції як складової інформаційної стійкості.

По-третє, одним із найбільш результативних інструментів гібридного впливу є маніпуляція контекстом, зокрема штучне вилучення історичних,

правових або соціальних рамок повідомлень. Український кейс демонструє, що підвищення спроможності до контекстуальної верифікації — через незалежні медіа, експертні спільноти та фактчекінгові ініціативи — істотно обмежує потенціал таких маніпуляцій. Це дозволяє розглядати відновлення контексту як базовий операційний елемент інформаційної стійкості.

По-четверте, виявлено, що когнітивні інформаційні впливи на організаційному рівні часто маскуються під внутрішні управлінські або комунікаційні проблеми. Український досвід засвідчує важливість інтерпретації таких відхилень (раптова впевненість щодо неперевіреної інформації, непропорційні емоційні реакції, зниження міжінституційної довіри) не лише як організаційних збоїв, а як потенційних індикаторів зовнішнього деструктивного впливу.

По-п’яте, емпірично підтверджено ключову роль людського рівня інформаційної стійкості, сформованого через повторювані когнітивні й поведінкові практики: усвідомлену паузу перед реакцією, критичний аналіз, емоційну рефлексію та колективну верифікацію інформації. В українських умовах ці практики закріплювалися переважно завдяки активності громадянського суспільства та горизонтальних мереж, що доповнювали обмежені інституційні ресурси держави.

По-шосте, український кейс демонструє, що національна ідентичність і усвідомлення політичної суб’єктності виконують стабілізувальну когнітивну функцію. Чітке розуміння ціннісних орієнтирів і цивілізаційного вибору зменшує вразливість до наративних ідентичнісних атак і підвищує загальний рівень інформаційної стійкості.

По-сьоме, узагальнення українського досвіду дозволяє зробити висновок, що ефективна інформаційна стійкість у когнітивному вимірі формується як результат поєднання інституційних механізмів, мережевої взаємодії та ідентичнісних чинників. Така модель виходить за межі традиційних підходів до інформаційної безпеки й підтверджує доцільність

концептуалізації інформаційної стійкості як динамічної, багаторівневої та соціально детермінованої спроможності.

Література

1. Вартовник І., Теперик Д. Грамотність майбутнього для покращення управління кризами : аналіт. огляд. Київ : Стійка Україна, 2025. 21 с. URL: https://resilient-ukraine.org/activities/126

2. Кивлюк О. Б., Іва М. М., Дідора К. О., Пахомова Т. І., Домашевська К. О. Стійкість до небезпекових викликів: Україна та європейський контекст : навч. посібник. Одеса : НУ «Одеська політехніка», 2025. 175 с. URL: https://op.edu.ua/sites/default/files/publicFiles/node_int_progs/navchalnyy_posibnyk_2025_proyekt_no_101175025_-_euresissecur.pdf

3. Мельник І. В. До проблеми формування інформаційної стійкості України: вибір трендів масової культури та їх вплив на суспільну свідомість і стратегію державного управління // Публічне управління та адміністрування. 2021. № 2. С. 69–74. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2021/2_2021/14.pdf

4. RES-POL. Медіаграмотність та інформаційна стійкість: істотні питання політики : аналіт. зап. 2025. https://doi.org/10.7079/respol2025.59

5. Borras T. The human firewall™ [Electronic resource] // LinkedIn. 2025. 30 Nov. URL: https://www.linkedin.com/pulse/human-firewall-terri-borras-wvnpe/

6. European Centre of Excellence for Countering Hybrid Threats. Hybrid CoE Key Themes for 2025. Helsinki : European Centre of Excellence for Countering Hybrid Threats, 2025. URL: https://www.hybridcoe.fi/wp-content/uploads/2025/01/Hybrid-CoE-key-themes-for-2025.pdf

7. Gladysch M., Pakhomenko S., Kuchyk O. The Information Resilience of Ukraine and the EU in Terms of Russian Aggression // Language – Culture –

Politics. 2023. Vol. 1. P. 227–245. URL: https://bibliotekanauki.pl/articles/22180752

8. Khoma N., Kresina I., Nikolaiev O., Patalakha V. National Resilience of Ukraine: Content and Security Strategy in the Context of a War and Post-war Recovery // European Political and Law Discourse. 2025. Vol. 12. No. 3. P. 41–52. https://doi.org/10.46340/eppd.2025.12.3.4

References

1. Vartovnyk, I. and Teperyk, D. (2025), Hramotnist maibutnoho dlia pokrashchennia upravlinnia kryzamy [Futures literacy for improving crisis management], Stiika Ukraina, Kyiv, Ukraine, available at: https://resilient-ukraine.org/activities/126 (Accessed 25 Jan 2026).

2. Kyvliuk, O. B., Iva, M. M., Didora, K. O., Pakhomova, T. I. and Domashevska, K. O. (2025), Stiikist do nebezpekovykh vyklykiv: Ukraina ta yevropeiskyi kontekst [Resilience to security challenges: Ukraine and the European context], NU “Odeska politekhnika”, Odesa, Ukraine, available at: https://op.edu.ua/sites/default/files/publicFiles/node_int_progs/navchalnyy_posibnyk_2025_proyekt_no_101175025_-_euresissecur.pdf (Accessed 25 Jan 2026).

3. Melnyk, I. V. (2021), “On the problem of forming information resilience of Ukraine: Selection of mass culture trends and their influence on public consciousness and public administration strategy”, Publichne upravlinnia ta administruvannia, vol. 2, pp. 69–74, available at: https://www.pubadm.vernadskyjournals.in.ua/journals/2021/2_2021/14.pdf (Accessed 25 Jan 2026).

4. RES-POL (2025), “Media literacy and information resilience: Key policy issues”, https://doi.org/10.7079/respol2025.59

5. Borras, T. (2025), “The human firewall™”, LinkedIn, available at: https://www.linkedin.com/pulse/human-firewall-terri-borras-wvnpe/ (Accessed 25 Jan 2026).

6. European Centre of Excellence for Countering (2025), “Hybrid Threats. Hybrid CoE Key Themes for 2025”, available at: https://www.hybridcoe.fi/wp-content/uploads/2025/01/Hybrid-CoE-key-themes-for-2025.pdf (Accessed 25 Jan 2026).

7. Gladysch, M., Pakhomenko, S. and Kuchyk, O. (2023), “The Information Resilience of Ukraine and the EU in Terms of Russian”, Aggression Language – Culture – Politics, Vol. 1, pp. 227–245, https://bibliotekanauki.pl/articles/22180752 (Accessed 25 Jan 2026).

8. Khoma, N., Kresina, I., Nikolaiev, O. and Patalakha, V. (2025), “National Resilience of Ukraine: Content and Security Strategy in the Context of a War and Post-war Recovery”, European Political and Law Discourse, Vol. 12, No. 3, pp. 41–52, https://doi.org/10.46340/eppd.2025.12.3.4

Отримано редакцією журналу / Received: 09.02.26

Прорецензовано / Revised: 16.02.26

Схвалено до друку / Accepted: 19.02.26