УДК *351.86:327.5:004.056.5*
DOI: *10.31673/2786-7412.2026.011196*

Тетяна ЯРОШОВЕЦЬ
кандидат філософських наук,
докторант кафедри публічного управління та адміністрування
Державного університету інформаційно-комунікаційних технологій, м. Київ
ORCID ID: 0000-0003-3690-416X
e-mail:yti36@ukr.net

Tetiana YAROSHOVETS
PhD in Philosophy,
Doctral Student of the Department of Public Administration and Administration
State University of Information and Communication Technologies, Kyiv
ORCID ID: 0000-0003-3690-416X
e-mail:yti36@ukr.net

ТЕОРЕТИЧНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ «ГІБРИДНИХ ЗАГРОЗ» ТА ЇХ ВПЛИВ НА ІНФОРМАЦІЙНУ СФЕРУ

THEORETICAL APPROACHES TO DEFINING «HYBRID THREATS» AND THEIR IMPACT ON THE INFORMATION SPHERE

Анотація. *Складність сучасного безпекового середовища зумовлює необхідність переосмислення теоретичних підходів до інтерпретації феномену гібридних загроз та їх управлінських наслідків для інформаційної сфери. Розмитість меж між військовими, політичними, економічними й цифровими інструментами впливу створює виклики для державного управління, оскільки традиційні моделі реагування виявляються недостатніми в умовах багатодоменного тиску. Невизначеність дефініцій і фрагментарність нормативних підходів ускладнюють формування узгодженої державної інформаційної політики.*

Метою дослідження є систематизація теоретичних підходів до визначення гібридних загроз та з'ясування механізмів їх впливу на інформаційну сферу в контексті публічного менеджменту. Методологічну основу становлять концептуальний аналіз, порівняльний підхід до інтерпретації дефініцій, елементи системного та інституційного аналізу, а також структурно-функціональне оцінювання впливу на інформаційні процеси.

У результаті дослідження встановлено, що теоретичні підходи до трактування гібридних загроз розвиваються у кількох взаємодоповнювальних вимірах: концептуальному, правовому, безпеково-політичному, інформаційно-комунікаційному та управлінському. Показано, що центральним інструментом впливу на інформаційну сферу виступає дезінформація, яка поєднується з маніпулятивними наративами, алгоритмічним посиленням контенту та поведінковими механізмами впливу на аудиторії. Доведено, що ефективність державної відповіді залежить від здатності поєднати нормативні обмеження із швидкістю комунікаційного реагування, а також від рівня координації між

суб'єктами стратегічних комунікацій і структурами аналізу ризиків. Обґрунтовано доцільність переходу від реактивних моделей до безперервного управлінського циклу моніторингу, оцінювання та коригування інформаційної політики.

Отримані висновки засвідчують, що інтеграція теоретичних підходів у практику публічного менеджменту дозволяє сформувати більш узгоджену модель управління інформаційною стійкістю. Наукова новизна полягає у комплексному поєднанні концептуальних і управлінських інтерпретацій гібридних впливів із фокусом на інституційній спроможності держави. Практична цінність визначається можливістю використання результатів для розроблення стратегій інформаційної безпеки, вдосконалення механізмів стратегічних комунікацій та підвищення адаптивності управлінських рішень у цифровому середовищі.

Ключові слова: *державне управління; інформаційна стійкість; стратегічні комунікації; дезінформаційні впливи; інституційна координація; цифрове середовище.*

Abstract. *The complexity of the modern security environment necessitates a rethinking of theoretical approaches to interpreting the phenomenon of hybrid threats and their managerial consequences for the information sphere. The blurring of boundaries between military, political, economic and digital instruments of influence creates challenges for public administration, as traditional response models prove insufficient in conditions of multi-domain pressure. The uncertainty of definitions and the fragmentation of regulatory approaches complicate the formation of a coordinated state information policy.*

The aim of the study is to systematize theoretical approaches to defining hybrid threats and clarify the mechanisms of their impact on the information sphere in the context of public management. The methodological basis is a conceptual analysis, a comparative approach to interpreting definitions, elements of systemic and institutional analysis, as well as a structural and functional assessment of the impact on information processes.

The study found that theoretical approaches to the interpretation of hybrid threats are developing in several complementary dimensions: conceptual, legal, security and political, information and communication and management. It is shown that the central tool of influence on the information sphere is disinformation, which is combined with manipulative narratives, algorithmic content amplification and behavioral mechanisms of influence on the audience. It is proven that the effectiveness of the state response depends on the ability to combine regulatory restrictions with the speed of communication response, as well as on the level of coordination between strategic communications subjects and risk analysis structures. The feasibility of the transition from reactive models to a continuous management cycle of monitoring, evaluating and adjusting information policy is substantiated.

The conclusions obtained indicate that the integration of theoretical approaches into the practice of public management allows for the formation of a more coherent model of information resilience management. The scientific novelty lies in the complex combination of conceptual and managerial interpretations of hybrid impacts with a focus on the institutional capacity of the state. The practical value is determined by the possibility of using the results to develop information security strategies, improve

strategic communication mechanisms, and increase the adaptability of management decisions in the digital environment.

Keywords: *public administration; information resilience; strategic communications; disinformation influences; institutional coordination; digital environment.*

Постановка проблеми. Стрімка трансформація безпекового середовища зумовила перегляд традиційних підходів до розуміння загроз у системі державного управління. Поняття «гібридні загрози» використовується для позначення поєднання військових і невійськових інструментів впливу, що діють синхронно та адаптивно [1]. Водночас у науковому дискурсі відсутня єдина дефініція цього феномену, що ускладнює вироблення цілісної державної політики у сфері інформаційної безпеки. Зазначена концептуальна невизначеність безпосередньо впливає на управлінські рішення, особливо в умовах цифровізації комунікацій та зростання ролі соціальних мереж.

Європейські дослідження підкреслюють, що гібридні загрози мають багатовимірний характер і охоплюють інформаційні операції, кіберінциденти, економічний тиск та маніпуляції громадською думкою [2]. North Atlantic Treaty Organization (NATO) визначає їх як сукупність координованих дій, спрямованих на підрив стабільності держави без формального оголошення війни [3]. Такий підхід акцентує увагу на інформаційній складовій як ключовому інструменті впливу. Однак у сфері державного управління залишається відкритим питання інтеграції цих положень у національні механізми стратегічних комунікацій.

Інформаційна сфера стає центральним простором реалізації гібридних стратегій, оскільки саме через неї формуються наративи, які впливають на політичні рішення та суспільну поведінку. Дезінформація, поширювана через цифрові платформи, розглядається як окрема форма гібридної активності, що здатна трансформувати суспільні настрої та підривати довіру до державних інституцій. За таких умов постає потреба у науково обґрунтованому визначенні гібридних загроз з урахуванням їхнього впливу на державну інформаційну політику.

Таким чином, проблема полягає у необхідності теоретичного уточнення категорії «гібридні загрози» та систематизації підходів до оцінювання їхнього впливу на інформаційну сферу як об’єкт державного управління. Актуальність дослідження зумовлена потребою розроблення дієвих управлінських інструментів протидії дезінформаційним кампаніям і підвищення стійкості інформаційного простору держави.

Аналіз останніх досліджень і публікацій. У сучасному науковому дискурсі поняття гібридних загроз формується на перетині безпекових, правових та управлінських підходів. Однією з концептуально ґрунтовних праць є дослідження Г. Джаннопулоса (G. Giannopoulos), Г. Сміта (H. Smith) та М. Теохаріду (M. Theocharidou), які запропонували багаторівневу модель гібридних загроз, що поєднує державні та недержавні інструменти впливу [1]. Автори акцентують на розмитості меж між війною та миром і вказують на системність таких дій. Варто зауважити, що модель залишається переважно описовою та не пропонує управлінських критеріїв вимірювання впливу на інформаційну сферу.

Правовий вимір проблеми детально досліджено С. Санц-Кабальєро (S. Sanz-Caballero), яка аналізує застосовність міжнародного права до гібридних загроз у

європейському контексті [2]. Авторка обґрунтовує, що гібридні дії часто перебувають у «сірій зоні» правового регулювання. У свою чергу, Н. Голуб'як та І. Голуб'як розглядають гібридні загрози як системний виклик безпековій політиці ЄС [4], підкреслюючи необхідність координації міждержавних зусиль.

Серед українських досліджень важливе місце посідає робота А. Хмеля, який визначає інформаційну війну як ключовий компонент гібридної війни [5]. Автор аргументує, що інформаційні операції формують стратегічний ефект, впливаючи на суспільну свідомість. О. Корістін та Н. Свиридюк пропонують методичні підходи до оцінювання гібридних загроз у системі стратегічних комунікацій [6], що має прикладне значення для державного управління. Разом з тим критерії оцінювання залишаються недостатньо стандартизованими.

Проблематику дезінформації як складника гібридних загроз досліджують О. Чуб та К. Ніколаєв, які розглядають інтелектуальну безпеку держави крізь призму протидії інформаційним впливам [7]. З іншої сторони І. Хмиров, А. Хмиров та М. Бирняк розробляють методологічні засади формування державної інформаційної політики в умовах гібридних загроз [8], підкреслюючи роль стратегічного планування, проте дослідження потребує розширення емпіричної бази.

Міжнародні дослідження деталізують цифровий вимір проблеми. Р. Аркос (R. Arcos) та співавтори здійснили систематичний огляд ефективності фактчекінгу та дебанкінгу як відповіді на цифрову дезінформацію [9]. Вони доводять, що спростування може зменшувати вплив неправдивих повідомлень, однак його ефективність залежить від контексту. У свою чергу, Р. Іванчік (R. Ivančík) та П. Нечас (P. Nečas) аналізують соціальні мережі як середовище поширення дезінформації [10], вказуючи на їхню роль у транснаціональних інформаційних операціях. Т. Азад (T. Azad), М. Хайдер (M. Haider) та М. Садік (M. Sadiq) розглядають гібридні дії в межах концепції «сірої зони» [11], що розширює теоретичну рамку аналізу. Разом з тим їх підхід орієнтований на воєнно-стратегічний аспект, а не на інформаційно-управлінський. І. Хмиров (I. Khmyrov) та співавтори досліджують вплив дезінформації на державну інформаційну політику [12], наголошуючи на необхідності інституційної координації.

Отже, аналіз наукових джерел засвідчує значний поступ у дослідженні гібридних загроз, однак виявляє низку невирішених аспектів. По-перше, відсутня узгоджена дефініція, що поєднує правовий, безпековий та управлінський виміри. По-друге, бракує комплексної моделі впливу гібридних загроз саме на інформаційну сферу як об'єкт державного менеджменту. По-третє, спостерігається розрив між теоретичними концепціями та інструментами практичної реалізації державної інформаційної політики.

Метою статті є теоретичне уточнення змісту поняття «гібридні загрози» та обґрунтування їх впливу на інформаційну сферу в системі державного управління. Для досягнення мети визначено такі завдання:

1) Дослідити основні наукові підходи до трактування гібридних загроз у міжнародному та національному дискурсі.

2) Проаналізувати механізми впливу гібридних загроз на інформаційну сферу держави.

3) Виявити напрями вдосконалення державної інформаційної політики та надати рекомендації щодо протидії гібридним загрозам.

Виклад основного матеріалу. Поняття «гібридні загрози» розвивається у п'яти взаємопов'язаних площинах: концептуальній, правовій, безпеково-політичній, воєнно-інформаційній та стратегічно-конкурентній. У концептуальній площині гібридні загрози описуються як багатодоменне явище, що поєднує акторів, інструменти, вразливості та фази впливу [1; 2; 3; 4, с. 54–56; 9]. У правовій площині акцентується проблема дефініційної невизначеності та функціонування гібридних дій у «сірій зоні» міжнародного права.

У безпеково-політичному вимірі гібридні загрози розглядаються як комплексний виклик політиці Європейського Союзу, що потребує координації інституційних відповідей і спільних механізмів реагування. Воєнно-інформаційний підхід зосереджується на ролі інформаційної війни як ключового елементу гібридного протиборства, який забезпечує стратегічний ефект через вплив на свідомість і поведінку аудиторій. Стратегічно-конкурентний підхід, пов'язаний із концепцією «сірої зони», інтерпретує гібридні дії як форму тривалої конкуренції між державами нижче порогу відкритого збройного конфлікту.

Для систематизації виявлених підходів до визначення гібридних загроз здійснено їх порівняльний аналіз за ключовими аналітичними критеріями. Узагальнення концептуальних, правових і безпеково-управлінських позицій дозволило виокремити їх змістовні особливості та практичну цінність для державного управління. Результати такого зіставлення подано в табл. 1.

Таблиця 1

Порівняння теоретичних підходів до визначення гібридних загроз

Підхід	**Ключовий зміст**	**Аналітична цінність для державного управління**	**Обмеження**
Концептуально-модельний	Багаторівнева модель: актори, цілі, інструменти, вразливості, фази	Дає рамку для структуризації загроз у міжвідомчому аналізі	Обмежена операціоналізація індикаторів впливу
Правовий	Дефініційна невизначеність та складність правової кваліфікації дій у «сірій зоні»	Допомагає визначити межі легітимної відповіді держави	Недостатня деталізація управлінських процедур
Безпеково-політичний (ЄС)	Гібридні загрози як системний виклик безпековій політиці та координації	Акцентує інституційну взаємодію та колективну стійкість	Інформаційний вимір подано узагальнено
Воєнно-інформаційний	Інформаційна війна як ключовий елемент гібридного протиборства	Пояснює роль наративів і психологічного впливу	Звужує явище до інформаційного компонента
«Сіра зона»	Конкуренція нижче порогу війни, комбінованість інструментів впливу	Дозволяє аналізувати латентні форми тиску на інститути	Менше уваги до державної інформаційної політики

Джерело: сформовано автором на основі даних [1; 2; 3; 4, с. 54–56; 9; 11, p. 83–85]

Центральним каналом впливу на інформаційну сферу є дезінформація, яка поєднується з маніпулятивними наративами, цифровим тиражуванням і поведінковим впливом на аудиторії. Зазначені процеси розглядаються крізь призму інтелектуальної безпеки держави з акцентом на необхідності превентивних заходів та системного моніторингу інформаційного простору [7, с. 174–176]. Окремо конкретизується роль соціальних мереж як середовища швидкого поширення дезінформації, де алгоритмічне посилення контенту збільшує охоплення та ускладнює перевірку змісту повідомлень [10, p. 347–349]. Водночас повторюваний інформаційний тиск і масоване тиражування повідомлень сприяють нормалізації викривлених наративів у публічному дискурсі, що підвищує ризик інституційної дискредитації.

У міжнародних дослідженнях механізми впливу деталізовано через оцінку наслідків і відповідей на цифрову дезінформацію. Встановлено, що вона впливає на сприйняття ризиків, рівень довіри до інституцій та готовність підтримувати публічні рішення, тоді як ефективність фактчекінгу залежить від часу реагування, формату подачі та характеристик аудиторії [9]. Зафіксовано також, що дезінформаційні кампанії можуть формувати довготривалі когнітивні установки, які складно коригувати навіть після спростування. Дезінформація деформує державну інформаційну політику через розрив між нормативними цілями та реальною комунікаційною поведінкою користувачів цифрового середовища.

Управлінський вимір впливу пов'язується із системою стратегічних комунікацій та оцінюванням ризиків у сфері безпеки [6, с. 69–71; 8, с. 298–299]. Підкреслюється, що фрагментарне або запізніле реагування держави посилює первинний ефект дезінформації та знижує довіру до офіційних джерел. Наголошується на потребі методологічно узгодженої державної інформаційної політики, в межах якої реагування на гібридні загрози розглядається як безперервний процес, що охоплює раннє виявлення, координацію суб'єктів та оцінювання результативності управлінських рішень.

Для узагальнення встановлених механізмів впливу гібридних загроз на інформаційну сферу здійснено їх структуризацію за функціональними ознаками з урахуванням каналів реалізації, наслідків та управлінських реакцій. Це дозволило пов'язати зміст інформаційних впливів із конкретними інституційними викликами у сфері публічного менеджменту. Систематизовані результати наведено в табл. 2.

Таблиця 2

Механізми впливу гібридних загроз на інформаційну сферу та їх управлінські наслідки

Механізм впливу	**Канал реалізації**	**Зафіксований наслідок для інформаційної сфери**	**Управлінський наслідок**
Дезінформаційне поширення	Соціальні мережі, цифрові платформи	Викривлення фактів, поляризація, падіння довіри	Потреба у системному моніторингу та швидкому спростуванні

Механізм впливу	**Канал реалізації**	**Зафіксований наслідок для інформаційної сфери**	**Управлінський наслідок**
Маніпулятивні наративи	Медіа, мережеві спільноти, лідери думок	Формування хибних інтерпретацій подій	Необхідність проактивних стратегічних комунікацій
Повторюваний інформаційний тиск	Масоване тиражування контенту	Нормалізація дезінформації в публічному дискурсі	Посилення аналітики контенту та міжвідомчої координації
Інституційна дискредитація	Цільові інформаційні кампанії	Зниження легітимності державних органів	Потреба у кризових протоколах комунікації
Запізніла відповідь держави	Фрагментарне реагування	Посилення ефекту первинного фейку	Вимога до стандартів реагування та розподілу повноважень

Джерело: сформовано автором на основі даних [1; 3; 6, с. 69–71; 7, с. 174–176; 8, с. 298–299; 9; 10, p. 347–349].

Ефективна протидія гібридним загрозам в інформаційній сфері передбачає інтегровану модель управління, що охоплює концептуальний, нормативно-правовий, організаційний, операційний та оціночний рівні. На концептуальному рівні необхідним є закріплення узгодженого робочого визначення гібридних загроз у державній інформаційній політиці, що дозволяє чітко відмежувати їх від суміжних явищ, зокрема дезінформації та інформаційної війни. Нормативно-правовий рівень передбачає визначення процедур реагування з урахуванням вимог законності та особливостей дій у «сірій зоні» міжнародного права.

На організаційному рівні ключовим є забезпечення координації між суб'єктами стратегічних комунікацій, аналітичними підрозділами та структурами оцінювання ризиків. Операційний рівень охоплює впровадження протоколів раннього виявлення, системного моніторингу, фактчекінгу та адресного спростування інформаційних впливів. Оціночний рівень пов'язаний із формуванням індикаторів результативності державних комунікацій та вимірюванням рівня довіри й стійкості аудиторій.

Зіставлення українських і міжнародних досліджень показало, що найбільш стійкі управлінські рішення формуються за умови розгляду протидії дезінформації як безперервного процесу, а не як реакції на окремі інформаційні інциденти [7, с. 175–177; 12]. Водночас у наукових працях недостатньо деталізовано механізм узгодження правових обмежень із необхідністю швидкого комунікаційного реагування, що створює практичну колізію між принципом законності та вимогами оперативності [2; 11, p. 100–102]. Систематизацію запропонованих напрямів удосконалення державної інформаційної політики подано в табл. 3.

Таблиця 3

Рекомендовані напрями вдосконалення державної інформаційної політики щодо протидії гібридним загрозам

Рівень управління	**Рекомендований напрям**	**Практичний зміст**
Концептуальний	Уніфікація робочої дефініції	Встановити єдині ознаки гібридної загрози для аналітики та планування
Нормативно-правовий	Узгодження процедур реагування	Визначити межі правомірного реагування на дезінформаційні кампанії
Організаційний	Міжвідомча координація	Синхронізувати стратегічні комунікації, аналіз ризиків, інформаційну політику
Операційний	Раннє виявлення та спростування	Запровадити регулярний моніторинг, фактчекінг, дебанкінг
Оціночний	Система індикаторів ефективності	Вимірювати вплив комунікаційних рішень на довіру та стійкість аудиторій

Джерело: власна розробка автора

Вдосконалення державної інформаційної політики має спиратися на інтегровану модель управління, у якій понятійна визначеність, координація інституцій та операційна швидкість розглядаються як взаємозалежні умови протидії гібридним загрозам.

Висновки. Питання управління безпекою праці в територіальних громадах набуває особливої ваги в умовах децентралізації, кадрового дефіциту та асиметрії фінансових можливостей. Посилення відповідальності місцевого рівня за результати управління ризиками потребує узгодження кадрових рішень із ресурсним забезпеченням, інакше формальні політики не трансформуються у відтворювані практики. Саме поєднання інституційної визначеності ролей із фінансово-організаційною спроможністю визначає сталість профілактичних заходів у публічному секторі.

Досліджено кадрову структуру управління безпекою праці на рівні територіальних громад та встановлено, що результативність управлінського циклу зростає за умов чіткого інституційного закріплення відповідальності, уніфікації функціональних ролей і синхронізації локальних процедур із багаторівневою системою управління охороною праці. Проаналізовано ресурсне забезпечення як інтегровану сукупність нормативно-організаційних, фінансово-економічних, інформаційно-комунікативних та аналітично-ризикових компонентів; доведено, що саме їх узгодженість визначає здатність громади підтримувати безперервний процес ідентифікації та мінімізації ризиків. Сформовані рекомендації щодо інтеграції кадрової політики з ризик-орієнтованим ресурсним плануванням засвідчують, що пріоритезація фінансування за рівнем небезпеки та впровадження цифрових інструментів моніторингу підвищують керованість і прозорість управлінських рішень.

Отримані результати можуть бути використані органами місцевого самоврядування, керівниками комунальних підприємств та установ під час формування програм безпеки праці, бюджетного планування, розроблення положень про відповідальних осіб і впровадження інформаційно-аналітичних систем обліку інцидентів. Наукова новизна полягає в обґрунтуванні інтегрованої моделі, яка поєднує кадрову політику з ресурсним плануванням у межах управлінського циклу охорони праці на місцевому рівні. Практична цінність визначається можливістю підвищення відтворюваності профілактичних заходів і зменшення фрагментарності управлінських дій.

Подальші дослідження доцільно спрямувати на емпіричне тестування запропонованої моделі в громадах різного типу, розроблення індикаторів оцінювання управлінської спроможності у сфері безпеки праці та аналіз впливу цифрових платформ на скорочення управлінського циклу реагування на ризики. Перспективним є також порівняльний аналіз міжсекторних відмінностей у впровадженні систем управління охороною праці та їх впливу на показники виробничої безпеки.

ДЖЕРЕЛА ТА ЛІТЕРАТУРА

1. Giannopoulos G., Smith H., Theocharidou M. The landscape of Hybrid Threats: A conceptual model. *Publications Office of the European Union.* 2021. DOI: https://doi.org/10.2760/44985.
2. Sanz-Caballero, S. The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanit Soc Sci Commun.* 2023. Vol. 10. Art. 360. DOI: https://doi.org/10.1057/s41599-023-01864-y.
3. North Atlantic Treaty Organization (NATO). Countering hybrid threats. *North Atlantic Treaty Organization.* 2024. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats (дата звернення: 23.02.2026).
4. Голуб'як Н., Голуб'як І. Гібридні загрози як виклики безпековій політиці ЄС. *Вісник Прикарпатського університету.* 2023. Вип. 15. С. 53–59. DOI: https://doi.org/10.32782/2312-1815/2024-1-7.
5. Хмель А. Інформаційна війна як ключовий елемент гібридної війни. *Acta de Historia & Politica: Saeculum XXI.* 2021–2022. № 3. С. 91–101. DOI: https://doi.org/10.26693/ahpsxxi2021-2022.03.091.
6. Корістін О., Свиридюк Н. Оцінювання гібридних загроз та спроможностей протидії їм при формуванні стратегічних комунікацій. *Науковий вісник Ужгородського Національного Університету. Серія: Право.* 2023. Вип. 77. Ч. 2. С. 66–74. DOI: https://doi.org/10.24144/2307-3322.2023.77.2.9.
7. Чуб О., Ніколаєв К. Попередження дезінформаційних впливів та основні напрями забезпечення інтелектуальної безпеки держави. *Актуальні проблеми у сфері публічного управління.* 2022. Вип. 2. С. 173–177. DOI: https://doi.org/10.32782/TNU-2663-6468/2022.6/27.
8. Хмиров І., Хмиров А., Бирняк М. Методологічні засади формування та реалізації державної інформаційної політики в умовах гібридних загроз. *Пропілеї права та безпеки.* 2025. Вип. 8. С. 298–300. DOI: https://doi.org/10.32620/pls.2025.8.79.

9. Arcos R., Gertrudix M., Arribas C., Cardarilli M. Responses to digital disinformation as part of hybrid threats: a systematic review on the effects of disinformation and the effectiveness of fact-checking/debunking. *Open Research Europe.* 2022. Vol. 2. Art. 8. DOI: https://doi.org/10.12688/openreseurope.14088.1.
10. Ivančík R., Nečas P. On disinformation as a hybrid threat spread through social networks. *Entrepreneurship and Sustainability Issues.* 2022. Vol. 10. № 1. P. 344–357. DOI: https://doi.org/10.9770/jesi.2022.10.1(18).
11. Azad T., Haider M., Sadiq M. Understanding gray zone warfare from multiple perspectives. *World Affairs.* 2023. Vol. 186. Iss. 1. P. 81–104. DOI: https://doi.org/10.1177/00438200221141101.
12. Khmyrov I., Khriapynskyi A., Svoboda I., Shevchuk M., Dotsenko K. The impact of disinformation on the state information policy. *Amazonia Investiga*. 2023. Vol. 12. Iss. 71. P. 93–102. DOI: https://doi.org/10.34069/AI/2023.71.11.8.

REFERENCES

1. Giannopoulos, G., Smith, H., & Theocharidou, M. (2021). *The landscape of Hybrid Threats: A conceptual model*. Publications Office of the European Union. https://doi.org/10.2760/44985
2. Sanz-Caballero, S. (2023). The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanities and Social Sciences Communications, 10*, Article 360. https://doi.org/10.1057/s41599-023-01864-y
3. North Atlantic Treaty Organization (NATO). (2024). *Countering hybrid threats*. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats (Accessed: February 23, 2026)
4. Holubiak, N., & Holubiak, I. (2023). Hibrydni zahrozy yak vyklyky bezpekovii polityts YeS [Hybrid threats as challenges to the EU security policy]. *Visnyk Prykarpatskoho universytetu [Bulletin of Precarpathian University], 15*, 53–59. https://doi.org/10.32782/2312-1815/2024-1-7
5. Khmel, A. (2021–2022). Informatsiina viina yak kliuchovyi element hibrydnoi viiny [Information warfare as a key element of hybrid warfare]. *Acta de Historia & Politica: Saeculum XXI, 3*, 91–101. https://doi.org/10.26693/ahpsxxi2021-2022.03.091
6. Koristin, O., & Svyrydiuk, N. (2023). Otsiniuvannia hibrydnykh zahroz ta spromozhnostei protydii im pry formuvanni stratehichnykh komunikatsii [Assessment of hybrid threats and capabilities to counter them in the formation of strategic communications]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia: Pravo [Uzhhorod National University Herald. Series: Law], 77*(2), 66–74. https://doi.org/10.24144/2307-3322.2023.77.2.9
7. Chub, O., & Nikolaiev, K. (2022). Poperedzhennia dezinformatsiinykh vplyviv ta osnovni napriamy zabezpechennia intelektualnoi bezpeky derzhavy [Prevention of disinformation influences and main directions of ensuring intellectual security of the state]. *Aktualni problemy u sferi publichnoho upravlinnia [Actual problems in the sphere of public administration], 2*, 173–177. https://doi.org/10.32782/TNU-2663-6468/2022.6/27
8. Khmyrov, I., Khmyrov, A., & Byrniak, M. (2025). Metodolohichni zasady formuvannia ta realizatsii derzhavnoi informatsiinoi polityky v umovakh

hibrydnykh zahroz [Methodological principles of formation and implementation of state information policy in the context of hybrid threats]. *Propilei prava ta bezpeky [Propylaea of Law and Security], 8*, 298–300. https://doi.org/10.32620/pls.2025.8.79

9. Arcos, R., Gertrudix, M., Arribas, C., & Cardarilli, M. (2022). Responses to digital disinformation as part of hybrid threats: a systematic review on the effects of disinformation and the effectiveness of fact-checking/debunking. *Open Research Europe, 2*, Article 8. https://doi.org/10.12688/openreseurope.14088.1
10. Ivančík, R., & Nečas, P. (2022). On disinformation as a hybrid threat spread through social networks. *Entrepreneurship and Sustainability Issues, 10*(1), 344–357. https://doi.org/10.9770/jesi.2022.10.1(18
11. Azad, T., Haider, M., & Sadiq, M. (2023). Understanding gray zone warfare from multiple perspectives. *World Affairs, 186*(1), 81–104. https://doi.org/10.1177/00438200221141101
12. Khmyrov, I., Khriapynskyi, A., Svoboda, I., Shevchuk, M., & Dotsenko, K. (2023). The impact of disinformation on the state information policy. *Amazonia Investiga, 12*(71), 93–102. https://doi.org/10.34069/AI/2023.71.11.8

Received (надійшла до редакції): 27.02.2026
Accepted (прийнята до друку): 17.03.2026
Published (опублікована): 25.03.2026