

ІНФОРМАЦІЙНА ВІЙНА ТА ЇЇ ВПЛИВ НА СУСПІЛЬСТВО

МОНОГРАФІЯ

Інформаційна війна:
поняття, зміст, види та засоби

Вплив інформаційних війн
на економіко-політичні, соціальні
процеси у світі та окремій країні

Інформаційна боротьба:
особливості та структурні елементи

Культура, наука, право, освіта
на захисті людини від деструктивного
впливу інформаційної зброї

Спеціальні
інформаційно-психологічні
операції: сутність,
етапи, методи проведення

Інформаційна безпека
та контрпропаганда
в умовах російсько-
української війни

АНАЛІТИЧНИЙ ЦЕНТР СУЧАСНОЇ ГУМАНІТАРИСТИКИ

ІНФОРМАЦІЙНА ВІЙНА ТА ЇЇ ВПЛИВ НА СУСПІЛЬСТВО

Монографія

Харків
«Право»
2026

Авторський колектив:

Л. М. Алексеєнко, доктор економічних наук, професор; *О. М. Іванченко*, доктор юридичних наук, доцент; *У. В. Ільницька*, кандидат політичних наук, доцент; *О. В. Квасниця*, кандидат економічних наук, доцент; *Н. О. Коннова*, кандидат філософських наук, доцент; *О. С. Копитова*, доктор юридичних наук, старший дослідник; *О. В. Кравченко*, доктор історичних наук, доцент; *К. В. Настояща*, доктор соціологічних наук, доцент; *М. П. Требін*, доктор філософських наук, професор; *Н. В. Федіна*, кандидат юридичних наук, доцент; *Т. О. Чернишова*, кандидат філологічних наук, доцент; *Л. В. Чупрій*, доктор політичних наук, професор

Рецензенти:

Г. М. Куц – доктор політичних наук, професор (Харківський національний педагогічний університет імені Г. С. Сковороди);

В. І. Палагута – доктор філософських наук, професор (Національний технічний університет «Дніпровська політехніка»);

І. В. Процюк – доктор юридичних наук, професор (Національний юридичний університет імені Ярослава Мудрого)

*Рекомендовано до видання вченою радою
ГО «Аналітичний центр сучасної гуманітаристики»
(протокол № 4 від 17 липня 2026 р.)*

Інформаційна війна та її вплив на суспільство : монографія /
I-74 [Л. М. Алексеєнко, О. М. Іванченко, У. В. Ільницька та ін.] ; Аналіт.
центр сучас. гуманітаристики. – Харків : Право, 2026. – 506 с. – DOI:
<https://doi.org/10.31359/9786178852085>.

ISBN 978-617-8852-08-5

Колективну монографію присвячено дослідженню теоретичних, методологічних і практичних основ феномену інформаційної війни, розкрито її поняття, сутність, зміст. Особливу увагу приділено розумінню сутності та специфіки когнітивної війни як концепту сучасного гуманітарного протистояння. Проаналізовано види та засоби ведення інформаційної війни, особливості та структурні елементи інформаційної боротьби, сутність, етапи, методи проведення спеціальних інформаційно-психологічних операцій. Розглянуто вплив інформаційних війн на економіко-правові, соціальні процеси у світі та окремі країни. Особливу увагу приділено інформаційній безпеці, контрпропаганді, захисту людини від деструктивного впливу інформаційної зброї в умовах російсько-української війни.

УДК 14+316+32+33+34+35

© Алексеєнко Л. М., Іванченко О. М.,
Ільницька У. В. та ін., 2026

© ГО «Аналітичний центр сучасної
гуманітаристики», 2026

© ТОВ «Видавничий дім «Право», 2026

ISBN 978-617-8852-08-5

Зміст

Розділ 1

Інформаційна війна: поняття, зміст, види та засоби

1.1. Інформаційна війна в турбулентному світі: теоретико-методологічні засади (Требін М. П., Коннова Н. О.).....	5
Список використаних джерел.	41
1.2. Трансформація змісту інформаційної боротьби: генезис, форми та методи (Требін М. П., Коннова Н. О.)..	47
Список використаних джерел.	79
1.3. Сутність та специфіка когнітивної війни як концепту сучасного гуманітарного протиборства (Требін М. П., Коннова Н. О.)	84
Список використаних джерел.	120
1.4. Феномен когнітивної війни в доктринальному дискурсі НАТО (Чернишова Т. О.).....	124
Список використаних джерел.	154

Розділ 2

Спеціальні інформаційно-психологічні операції: сутність, етапи, методи проведення

2.1. Теоретико-методологічні засади та сутність спеціальних інформаційно-психологічних операцій (ІПсО) у контурі гібридних конфліктів (Требін М. П., Коннова Н. О.).....	158
Список використаних джерел.	191
2.2. Архітектура, етапи проєктування та методи реалізації сучасних ІПсО в цифровому медіасередовищі (Требін М. П., Коннова Н. О.).....	195
Список використаних джерел.	230
2.3. Північнокорейська тематика в спеціальних інформаційно-психологічних операціях російсько-української війни (Чупрій Л. В., Настояща К. В.).....	234
Список використаних джерел.	247

Розділ 3

Вплив інформаційних війн на економіко-правові, соціальні процеси у світі та окремі країни

3.1. Інформаційна війна як фактор трансформації права (Копитова О. С.)..	250
Список використаних джерел.	292

3.2. Інформаційно-безпекові імперативи цифрових і фондових інновацій у сфері публічного управління, фінансів, банків і страхування: міжнародні та національні бізнес-комунікації (Алексєєнко Л. М.) ..	297
Список використаних джерел.	323
3.3. Інформаційно-комунікаційні механізми політики згуртованості економічного розвитку територіально-господарських систем: пріоритети поведінкових фінансів та масштабування фінансової грамотності в умовах євроінтеграції (Квасниця О. В.) ..	334
Список використаних джерел.	366

Розділ 4

Інформаційна безпека та контрпропаганда в умовах російсько-української війни

4.1. Культура, наука, право, освіта на захисті людини від деструктивного впливу інформаційної зброї (Іванченко О. М.) ..	369
Список використаних джерел.	407
4.2. Стратегічні комунікації як механізм формування системи інформаційної безпеки та протидії інформаційним викликам і загрозам (Ільницька У. В.) ..	411
Список використаних джерел.	432
4.3. Особливості забезпечення інформаційної безпеки органами державного адміністрування в умовах правового режиму воєнного стану (Федіна Н. В.) ..	438
Список використаних джерел.	469
4.4. Інформаційна безпека та контрпропаганда в умовах російсько-української війни: стратегії та досвід України і Польщі (Кравченко О. В.) ..	474
Список використаних джерел.	498
Авторський колектив.	503

2.2. Архітектура, етапи проектування та методи реалізації сучасних ІПсО в цифровому медіасередовищі

Требін Михайло Петрович

доктор філософських наук, професор

*професор кафедри міжнародних відносин і політичної філософії
Харківський національний економічний університет імені Семена Кузнеця*

Коннова Ніна Олексіївна

кандидат філософських наук, доцент

*доцент кафедри міжнародних відносин і політичної філософії
Харківський національний економічний університет імені Семена Кузнеця*

Дослідження прикладної архітектури сучасних інформаційно-психологічних операцій вимагає першочергового аналізу специфіки цифрового медіасередовища, яке трансформувалося в провідний простір когнітивного протиборства. Глобальна цифровізація соціуму, стрімкий перехід від традиційних масмедіа до інтерактивних платформ Web 2.0 та децентралізованих рішень Web 3.0 радикально змінили швидкість, масштаби та глибину проникнення деструктивних впливів¹. У сучасних реаліях інформаційно-психологічні операції (ІПсО) еволюціонували з лінійних пропагандистських кампаній минулого у складні, технологічно опосередковані системи поведінкової інженерії². Поява нових комунікаційних платформ, месенджерів та алго-

¹ Див.: Цифрова епоха: міждисциплінарний дискурс: монографія / [А. А. Гедзик, Т. В. Ковальова, О. Ю. Коцюрба та ін.]; Аналіт. центр сучас. гуманітаристики. Харків: Право, 2024. С. 31–50.

² Див.: Певцов Г. В., Залкін С. В., Сідченко С. О., Хударковський К. І. Інформаційно-психологічні операції: планування, протидія, технології: монографія. Харків: ДІСА ПЛЮС, 2020. 252 с.; Проноза І., Сурова М. Інформаційні (психологічні) операції як інструмент інформаційної війни. *Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи* : IV міжнар. наук.-практ. конф., 27 верес. 2023 р.: тези доповідей / Міністерство оборони України, НУОУ. Київ: НУОУ, 2023. С. 121–123; Твердохліб Ю. М., Мороз Ю. М. Інформаційно-психологічні операції в умовах ведення гібридної війни. *Вісник Львівського національного університету імені І. Франка. Серія : Міжнародні відносини*. 2016. №38. С. 97–105; Федонюк С. Інформаційно-психологічні операції на геополітичній арені: навч. посіб. Луцьк: Вежа-Друк, 2024. 104 с.

ритмів генеративного штучного інтелекту (ШІ) дозволила суб'єктам гібридної агресії оптимізувати процеси створення та дистрибуції контенту, мінімізуючи часові витрати на подолання раціональних фільтрів захисту людської психіки.

У цьому контексті цифрове медіасередовище перестало бути просто технічним каналом передачі даних; воно перетворилося на самостійну гібридну екосистему, де межі між комбатантами й некомбатантами, фактами й симулякрами остаточно розмиваються. Сучасні мережеві технології дозволяють агресору здійснювати перманентний, латентний і глибоко таргетований вплив як на індивідуальну свідомість окремого громадянина (зокрема, через концепцію «стратегічного капрала»¹), так і на масову психологію цілих націй. Як наслідок, класичні оборонні інструменти інформаційної безпеки, орієнтовані на реактивне спростування фейків, виявляють свою концептуальну обмеженість перед матричною архітектурою цифрових атак нового покоління.

З огляду на це, виникає об'єктивна інноваційна потреба в експлікації внутрішньої структури цих загроз. Розуміння ІПсО як цілісного технологічного комплексу передбачає декомпозицію його прикладної архітектури, що об'єднує інфраструктурні, аналітичні та інструментальні компоненти у єдину деструктивну систему.

Ефективність сучасних інформаційно-психологічних операцій у цифровому медіасередовищі забезпечується їхньою складною, багаторівневою структурою. Сучасна ІПсО більше не є поодиноким пропагандистським актом чи лінійним вкидом дезінформації; вона функціонує як високотехнологічна екосистема. У межах парадигми гібридних конфліктів ХХІ століття інформаційно-психологічний вплив зазнав кардинальної онтологічної трансформації: від ізольованих тактичних заходів (таких як розкидання листівок чи радіомовлення на територію супротивника) він еволюціонував до стану перманентного, нелінійного середовища когнітивного домінування².

¹ Див.: Krulak C. C. The strategic corporal: Leadership in the three-block war. *Leatherneck*. 1999. Vol. 82, No. 1. P. 14–17. URL: <https://www.mca-marines.org/wp-content/uploads/1999-Jan-The-strategic-corporal-Leadership-in-the-three-block-war.pdf>.

² Див.: Історія інформаційно-психологічного протистояння: підруч. / [Я. М. Жарков, Л. Ф. Компанцева, В. В. Остроухов, В. М. Петрик, М. М. Присяжнюк, Є. Д. Скулиш]; за заг. ред. д. ю. н., проф., засл. юриста України Є. Д. Скулиша. Київ: Наук.-вид.

Теоретичний базис для розуміння цих трансформацій закладено ще у класичних працях Е. Тоффлера, який у своїй концепції «третьої хвилі»¹ та «інформаційної війни»² передбачив зміщення фокусу збройних протистоянь від матеріально-технічного знищення до контролю над знаннями та інформаційними потоками. У сучасних реаліях цей підхід трансформувався в те, що М. Кастельс охарактеризував як «суспільство мережевих структур» (Network Society)³. Дослідник переконливо довів, що влада в сучасному світі належить не просто суб'єктам, які володіють матеріальними ресурсами, а тим структурам, що контролюють коди, алгоритми та так звані «перемикачі мереж» (network switchers). Відтак, сучасне цифрове медіасередовище стало практичним втіленням його концепції «масової самокомунікації» (mass self-communication)⁴, де кожна децентралізована точка мережі (індивідуальний користувач, анонімний канал чи автоматизований бот) перетворюється на потенційного ретранслятора, модератора або безпосереднього генератора деструктивного контенту.

Це зумовлює необхідність перегляду класичних дефініцій та дослідницьких підходів. Розгляд ІПсО крізь призму статичних контент-моделей уже не дозволяє адекватно оцінити загрози, оскільки сучасний деструктивний вплив має розподілений, адаптивний та самоорганізовуваний характер. Як зазначають сучасні західні теоретики когнітивної війни, зокрема експерти Інноваційного хабу НАТО (Ф. дю Клузель, Б. Клавері⁵), людський розум сьогодні офіційно визнано

відділ НА СБ України, 2012. 212 с.

¹ Див.: Тоффлер Е. Третя хвиля / пер. з англ. А. Євса; ред. пер. В. Шовкун. Київ: Видавничий дім «Всесвіт», 2000. 475 с.

² Див.: Toffler A., Toffler H. War and anti-war: survival at the dawn of the 21st century. Boston: Little, Brown, 1993. xiii, 302 p.

³ Див.: Castells M. The rise of the network society. 2nd ed., with a new pref. Malden, MA: Wiley-Blackwell, 2010. lvii, 597 p.

⁴ Див.: Castells M. Communication power. 2nd ed. Oxford: Oxford University Press, 2013. xlvii, 574 p.

⁵ Див.: Claverie B., du Cluzel F. «Cognitive Warfare»: The Advent of the Concept of «Cognitics» in the Field of Warfare. *Cognitive Warfare: The Future of Cognitive Dominance*: Proceedings of the First NATO Scientific Meeting on Cognitive Warfare, Bordeaux, France, 21 June 2021. Neuilly-sur-Seine: NATO Collaboration Support Office, 2022. P. 2–1–2–7. URL: https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare-Symposium-ENSC-March-2022-Publication.pdf?utm_

шостим операційним доменом ведення бойових дій (поряд із землею, морем, повітрям, космосом та кіберпростором). У цьому контексті цифрова ПСО розглядається не просто як інформаційна атака, а як системне «когнітивне хакерство» (Cognitive Hacking), спрямоване на експлуатацію вразливостей людської архітектури обробки даних (когнітивних упереджень та евристик). Динамічна стійкість таких операцій базується на принципах синергії, коли деградація або ліквідація одного з елементів системи (наприклад, блокування конкретного медіаресурсу чи викриття фейку) не призводить до зупинки всієї кампанії, а лише стимулює її автоматичну перебудову за рахунок альтернативних каналів та інструментів.

Для глибокого теоретико-прикладного аналізу цієї системи доцільно застосувати метод трирівневої декомпозиції, виокремивши інфраструктурний, технологічний та наративний рівні її системної архітектури. Такий методологічний підхід дозволяє досліджувати ПСО не як розрізнені тексти чи технічні інциденти, а як цілісну матричну структуру, де кожен рівень виконує свою специфічну функцію, перебуваючи у стані жорсткої функціональної взаємозалежності з іншими.

Інфраструктурний рівень, як «фізичне тіло», формує просторово-комунікаційний базис операції та забезпечує латентні шляхи доступу до цільових аудиторій у межах кастельсівського «простору потоків».

Технологічний рівень виконує роль операційно-динамічного двигуна, що відповідає за автоматизацію, обробку великих масивів даних (Big Data), алгоритмізацію дистрибуції та масштабування впливу, реалізуючи тоффлерівську ідею про технологічне випередження в управлінні знаннями.

Наративний рівень є безпосереднім семантичним ядром («зброєю кінцевого ураження»), яке здійснює інтервенцію у смислове поле

source=chatgpt.com; Claverie B., du Cluzel F., Desclaux G. Cognitive Warfare and C2. *Operationalizing the Concept of Cognitive Warfare* : 2nd Scientific and Strategic Workshop on «Cognitive Warfare», US Military Academy West Point, March 4, 2022. URL: <https://hal.science/hal-04189572v1/file/WP%20-%20CW%26C2%20Claverie-DuCluzel-Desclaux%20-%202022.pdf>; du Cluzel F. Cognitive Warfare. Norfolk, VA: NATO Allied Command Transformation, Innovation Hub, 2021. 45 p. URL: https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf.

індивіда чи соціуму з метою трансформації їхньої поведінкової моделі та досягнення когнітивного паралічу супротивника.

Тільки за умови комплементарної взаємодії цих трьох рівнів досягається синергетичний ефект ІПсО – формування штучної когнітивної реальності, яка сприймається об'єктом впливу як власна суб'єктивна очевидність. Розглянемо специфіку та внутрішню архітектуру кожного із зазначених рівнів детальніше.

Інфраструктурний рівень є базовим фундаментом архітектури сучасних інформаційно-психологічних операцій, визначаючи просторово-комунікаційну архітектуру каналів, а також конфігурацію фізичних і віртуальних майданчиків, через які здійснюється безпосередній доступ до цільових аудиторій. У межах кастельсівської парадигми «простору потоків» (space of flows) цей рівень матеріалізує мережеву географію деструктивного впливу, перетворюючи її на «по-запросторовий простір», де географічні кордони держав нівелюються швидкістю передачі пакетів даних. У сучасних медіареаліях інфраструктурний рівень зазнав радикальної децентралізації, диверсифікації та структурної розподіленості, що дозволяє суб'єктам гібридної агресії мінімізувати ризики технічного блокування чи законодавчого регулювання з боку суверенних акторів¹.

Ключовим елементом цієї оновленої інфраструктури стала екосистема кросплатформових месенджерів (зокрема Telegram та WhatsApp). Telegram еволюціонував у провідний інструмент проектування та реалізації сучасних ІПсО за рахунок гібридизації функцій індивідуального месенджера та повноцінної макромедійної платформи. Системними перевагами цієї платформи для суб'єктів впливу є архітектурно закладений високий рівень анонімності, відсутність дієвих механізмів зовнішньої чи внутрішньої модерації, а також спрощений інструментарій створення масштабних, розгалужених мереж «сірих» і «чорних» (анонімних) каналів². Такі канали мімікрують під джерела легітимних, об'єктивних новин, регіональних

¹ Див.: Lewis T. G. Network science: theory and practice. Hoboken, N. J.: John Wiley & Sons, 2009. xi, 512 p.

² Див.: NATO STRATCOMCOE podcast explores Telegram app. LSM. September 27, 2024. URL: <https://eng.lsm.lv/article/features/video/27.09.2024-nato-stratcomcoe-podcast-explores-telegram-app.a570335/>

інсайдерів чи військово-аналітичних пулів. Це дозволяє утворювати герметичні, вертикально інтегровані інформаційні колодязі, у межах яких цільова аудиторія піддається систематичній і безальтернативній психоемоційній обробці.

Паралельно з месенджерами, глобальні соціальні мережі епохи Web 2.0 – такі як платформи корпорації Meta (Facebook, Instagram), мікроблогінгова мережа X (колишній Twitter) та відеохостинг TikTok – продовжують виконувати функцію магістральних арен для досягнення максимального охоплення (вірусизації). Попри перманентне декларування цими технологічними гігантами політики безпеки та впровадження автоматизованих систем модерації, суб'єкти когнітивного впливу успішно адаптують свою технічну інфраструктуру для нівелювання цих фільтрів. Обхід алгоритмів безпеки реалізується через розгортання складних мереж проксі-серверів, резидентних VPN-сервісів, а також оренду або викуп автентичних, верифікованих акаунтів реальних користувачів із довгою цифровою історією. Це дозволяє маскувати деструктивну активність під природну поведінку користувачів та уникати превентивного бану¹.

Новим та найбільш технологічно складним викликом є інтеграція в архітектуру ІПСО децентралізованих медіа та технологічних рішень епохи Web 3.0. Використання блокчейн-платформ, децентралізованих автономних організацій (DAO) та протоколів розподіленого зберігання даних (на кшталт IPFS) створює стійку до цензури комунікаційну інфраструктуру. Оскільки в архітектурі Web 3.0 відсутній єдиний центральний сервер або юридичний власник платформи, видалення деструктивного маніпулятивного контенту, його верифікація чи блокування з боку національних урядів та регуляторних органів стає технічно неможливим, що забезпечує тривалу життєздатність ворожих наративів в інформаційному полі².

¹ Див.: Howard P. N. *Lie machines: how to save democracy from troll armies, deceitful robots, junk news operations, and political operatives*. New Haven; London: Yale University Press, 2020. xviii, 221 p.; *Computational Propaganda: Political Parties, Politicians, and Automated Networks on Social Media* / ed. by S. C. Woolley, P. N. Howard. Oxford: Oxford University Press, 2019. 288 p.

² Див.: Benkler Y., Faris R., Roberts H. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. New York: Oxford University Press, 2018. ix, 462 p.

Тіньовим забезпечувальним компонентом описаної структури є анонімна мережа Даркнет (Dark Web)¹. У системній архітектурі ІПсО вона функціонує як замкнута логістична та інфраструктурна база. Саме на майданчиках Даркнету здійснюється координація дій проурядових хакерських угруповань (АРТ-груп) та так званих «хактивістів», купуються бази викрадених персональних даних, які згодом використовуються для точкового психографічного профілювання суспільства та мікротаргетингу². Крім того, Даркнет через ринки криптовалют забезпечує безперерйне, анонімне та транскордонне фінансування всієї інфраструктури ІПсО (від оплати праці медіатехнологів до закупівлі серверних потужностей для ботоферм), залишаючи фінансовий моніторинг держав-мішеней поза процесом контролю.

Технологічний рівень системної архітектури ІПсО є операційно-динамічним ядром, яке координує процеси автоматизації, оптимізації, математичного моделювання та масштабування деструктивного впливу. Якщо інфраструктурний рівень забезпечує канали комунікації, то технологічний визначає швидкість, точність та економічну ефективність доставки деструктивного сигналу до об'єкта ураження. Протягом 2022–2026 років саме цей сегмент зазнав найбільш радикальних, революційних змін, що було зумовлено стрімкою конвергенцією технологій генеративного штучного інтелекту, великих мовних моделей (LLM) та інструментів інтелектуального аналізу великих масивів даних (Big Data / Data Mining). Це змістило стратегічний баланс сил у бік суб'єктів агресії, оскільки дозволило подолати проблему обмеженості людського ресурсу в процесі ведення когнітивної війни.

Основою оновленого технологічного рівня стало масове інтегрування генераторів контенту на базі штучного інтелекту (Generative AI) та просунутих LLM-моделей. Використання інструментів класу GPT-4, Claude 3.5 чи спеціалізованих локальних моделей (fine-tuned

¹ Див.: Moore D., Rid T. Cryptopolitik and the Darknet. *Survival*. 2016. Vol. 58, Issue 1. P. 7–38. DOI: <https://doi.org/10.1080/00396338.2016.1142085>.

² Див.: Moore D. Targeting technology: Mapping military offensive network operations. *10th International Conference on Cyber Conflict. CyCon X: Maximising Effects* (29 May – 01 June 2018, Tallinn, Estonia) / T. Minárik, R. Jakschis, L. Lindström (Eds.). Tallinn: NATO CCD COE Publications, 2018. P. 89–108. URL: https://ccdcoe.org/uploads/2018/10/CyCon_2018_Full_Book.pdf.

LLMs), навчених на специфічних текстових масивах, повністю трансформувало економіку інформаційного протистояння. Дослідники когнітивної та обчислювальної пропаганди констатують, що вартість виробництва унікальних, граматично бездоганих, стилістично різно-рідних маніпулятивних текстів, аналітичних псевдодосліджень, вірусних коментарів та візуальних креативів упала майже до нуля¹. ШІ усунув так званий «мовний та культурний бар'єр»: якщо раніше іноземні спецслужби видавали себе через русизми чи помилки у синтаксисі української мови, то сучасні моделі генерують автентичний контент, адаптований під специфічний сленг, соціолекти чи регіональні діалекти націй-мішеней. Це дозволяє здійснювати одночасну генерацію тисяч унікальних варіацій одного наративу протягом лічених хвилин, повністю перевантажуючи фільтри фактчекінгу.

Паралельно відбулася якісна еволюція засобів реплікації – розумних бот-мереж нового покоління (AI-driven bots). Традиційні, технічно примітивні ботоферми, що функціонували на основі жорстких скриптів і займалися масовим копіюванням однакових гасел, остаточно виявили свою неефективність та були замінені автономними агентами штучного інтелекту (AI agents). Сучасні когнітивні боти здатні не просто репостити контент, а самостійно інтегруватися у складні людські дискусії в коментарях, гнучко адаптуватися під контекст бесіди, застосовувати складні психологічні техніки переконання чи дискредитації та імітувати поведінкові патерни реальних користувачів (публікація особистих фото, взаємодія з побутовими темами тощо). Завдяки цьому вони успішно долають сучасні евристичні системи захисту та технічні фільтри (капчі, антифрод-системи), створюючи для реальних громадян стійку, математично прораховану ілюзію «суспільної більшості» (social proof) навколо штучно сконструйованих деструктивних тем².

¹ Див.: Goldstein J. A., Sastry G., Musser M., DiResta R., Gentzel M., Sedova K. Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations. *arXiv preprint arXiv:2301.04246*. 2023. 82 p. DOI: 10.48550/arXiv.2301.04246.

² Див.: Ferrara E. The Generative AI Paradox: GenAI and the Erosion of Trust, the Corrosion of Information Verification, and the Demise of Truth. *Future Internet*. 2026. Vol. 18, Issue 2. Art. 73. DOI: <https://doi.org/10.3390/fi18020073>; Woolley S. Manufacturing

Заключним компонентом технологічного рівня є маніпулювання алгоритмами рекомендацій глобальних цифрових платформ. Суб'єкти ІПсО здійснюють реверс-інжиніринг математичних моделей формування стрічок новин і трендів у таких медіапросторах, як TikTok, YouTube чи X (колишній Twitter). Будь-який алгоритм рекомендацій оптимізований під утримання уваги користувача та миттєве реагування на спалахи активності¹. Координуючи початкову синергетичну дію ІІІ-ботів на інфраструктурному рівні (миттєве проставлення тисяч лайків, поширень, штучне утримання перегляду відео на перших секундах), агресор змушує нейромережі самих платформ сприймати дезінформаційний або панічний контент як «високовірусний». Як наслідок, алгоритми платформ починають самостійно просувати деструктивні наративи у персоналізовані стрічки реальних користувачів, максимізуючи органічне охоплення та створюючи штучні «інформаційні бульбашки», які радикалізують суспільство зсередини².

Наративний (семантичний) рівень є завершальним та критично важливим елементом системної архітектури ІПсО, як безпосередня «зброя кінцевого ураження» когнітивної сфери об'єкта. Якщо інфраструктурний рівень визначає логістику доставки контенту, а технологічний – масштабованість та автоматизацію процесу, то наративний рівень відповідає за смислове, семантичне й психоемоційне наповнення операції. Головною метою цього рівня є не просто інформування чи дезінформування аудиторії, а фундаментальна трансформація її світоглядної матриці, руйнування критичного мислення та формування штучної системи координат, у якій об'єкт впливу починає діяти в інтересах суб'єкта агресії, вважаючи власні рішення абсолютно суверенними й раціональними.

У сучасній практиці проектування ІПсО лінійні фейки поступилися місцем складним матричним наративам (метаконтекстам).

Consensus: Understanding Propaganda in the Era of Automation and Anonymity. New Haven, CT: Yale University Press, 2023. 232 p.

¹ Див.: Spohr D. Fake news and ideological polarization: Filter bubbles and echo chambers on social media. *Business Information Review*. 2017. Vol. 34, No. 3. P. 150–160. DOI: <https://doi.org/10.1177/0266382117722446>.

² Див.: Bak-Coleman J. B., Alfano M., West C. T. et al. Stewardship of global collective behavior. *Proceedings of the National Academy of Sciences (PNAS)*. 2021. Vol. 118, No. 27. e2025764118. DOI: 10.1073/pnas.2025764118.

Суб'єкти впливу усвідомлюють, що точкова неправдива інформація швидко деконструюється сучасними інструментами фактчекінгу. Тому замість поодиноких інформаційних вкидів створюється стійка смислова рамка (фрейм), яка базується на реальних, але тенденційно підібраних і гіперболізованих соціально-політичних тригерах (наприклад, наративи «тотальної корумпованості військово-політичного керівництва», «зради з боку геополітичних партнерів», «безперспективності оборонного спротиву»). Такі матричні конструкти апелюють до базових архетипів, історичних травм, колективних страхів або існуючих у соціумі поляризаційних ліній¹. Тексти та повідомлення кодуються таким чином, щоб будь-який новий реальний факт (навіть позитивний) автоматично інтерпретувався об'єктом крізь призму вже імплантованого деструктивного метанаративу.

Центральним методологічним інструментом наративного рівня є конструювання симулякрів. У межах філософської концепції Ж. Бодрієра, сучасне цифрове медіасередовище продукує знаки та копії, які не мають реального референта (оригіналу) в об'єктивній дійсності². У контексті ІПСО симулякрами стають штучно змодельовані події (сфабриковані акції протесту, зрежисовані відеоінтерв'ю), вигадані соціологічні дані чи повністю вигадані цифрові особистості (лідери думок, яких не існує, але чії профілі наповнюються згенерованим ІІІ контентом). Завдяки високій щільності та швидкості дистрибуції на технологічному рівні, ці симулякри починають витісняти реальні факти з інформаційного поля держави-мішені. Пересічний споживач контенту опиняється в ситуації «гіперреальності», де межа між істинним та сконструйованим остаточно деконструюється, що викликає когнітивну дезорієнтацію та апатію.

Важливим компонентом цього процесу є експлуатація когнітивних пасток (упереджень та евристик) людського мислення, що визначається теоретиками когнітивної війни як ядро «когнітивного хакерства»

¹ Див.: Benkler Y., Faris R., Roberts H. Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics.

² Див.: Бодріяр Ж. Симулякри і симуляція / пер. з фр. В. Ховхун. Київ : Видавництво Соломії Павличко «Основи», 2004. 230 с.

(Cognitive Hacking)¹. Наративи оптимізуються під запуск несвідомих ментальних автоматизмів, зокрема «ефекту ілюзорної правди» (illusory truth effect) – коли багаторазове повторення тези (забезпечене ІП-ботами) змушує мозок сприймати її як істинну лише через чинник знайомості. Крім того, активно експлуатується «схильність до підтвердження» (confirmation bias), за якої індивід охоче вірить у деструктивний контент, якщо той відповідає його початковим фрустраціям чи політичним уподобанням. Для ускладнення критичного аналізу повідомлень застосовується метод «семантичного отруєння» або «напівправди», де реальний, часто дрібний факт майстерно вплітається у заздалегідь підготовлену конспірологічну концепцію.

Для закріплення та автоматичного поширення наративу на емоційному рівні використовується технологія емоційного зараження (Emotional Contagion)². Контент наративного рівня кодується з використанням високоінтенсивних лексичних та візуальних маркерів, що викликають первісні, важкоконтрольовані емоції: гнів, панічний страх, відразу, гостру екзистенційну тривогу або моральне обурення. Сучасні нейробіологічні та психологічні дослідження доводять, що високе емоційне збудження блокує роботу префронтальної кори головного мозку, яка відповідає за логіку та аналіз ризиків. Індивід, перебуваючи в стані штучно спровокованого афекту, втрачає здатність до раціональної фільтрації та верифікації інформації, трансформуючись із пасивного споживача контенту на активного, лояльного та абсолютно безкоштовного ретранслятора ворожого наративу в межах своєї власної соціальної мережі.

Таким чином, системна архітектура цифрових ІПсО є синергетичним комплексом: інфраструктура забезпечує приховані шляхи доставки, технології гарантують масштабованість та автоматизацію впливу, а наративи здійснюють безпосереднє ураження психоемоційної та когнітивної стійкості мішені. Жоден із цих трьох рівнів не здатний

¹ Див.: Claverie B., Du Cluzel F. «Cognitive Warfare»: The Advent of the Concept of «Cognitics» in the Field of Warfare; Thompson P. Cognitive hacking and intelligence and security informatics. *Proc. SPIE 5423, Enabling Technologies for Simulation Science VIII, null (13 Aug 2004)*. DOI: <https://doi.org/10.1117/12.554454>.

² Див.: Bak-Coleman J. B., Alfano M., West C. T. et al. Stewardship of global collective behavior.

досягти стратегічного деструктивного ефекту ізолювано. Інфраструктурні канали залишалися б порожніми технологічними судинами без динамічних алгоритмів дистрибуції та змістовного семантичного наповнення. У свою чергу, навіть найбільш лінгвістично досконалі наративи виявляються безсилими в сучасному перенасиченому медіапросторі, якщо вони не масштабуються штучним інтелектом і позбавлені прихованих логістичних шляхів укорінення в аудиторію.

Складний матричний характер цієї тривірневої архітектури обумовлює концептуальну зміну підходів до забезпечення національної безпеки. Ефективна протидія таким операціям вимагає системних кроків на кожному з трьох окреслених рівнів, що унеможливує використання застарілих лінійних чи реактивних інструментів захисту. Боротьба виключно на наративному рівні за допомогою класичного фактчекінгу та спростування фейків є тактично обмеженою, оскільки вона лікує симптоми, а не причину, залишаючи недоторканими ворожі технологічні двигуни та інфраструктурні бази дистрибуції.

Відтак, комплексна архітектура оборони держави-мішені повинна передбачати:

- на інфраструктурному рівні – правове, регуляторне та технічне обмеження діяльності анонімних і децентралізованих майданчиків ворожого впливу;
- на технологічному рівні – розгортання власних III-систем сенсидент-аналізу для раннього виявлення аномальної активності ботмереж та маніпуляцій алгоритмами платформ;
- на наративному рівні – перехід від пасивного спростування до проактивного стратегічного комунікування (StratCom) та формування системної когнітивної стійкості суспільства.

Утім, розуміння статичної архітектури ІІІсО є лише першим кроком до розкриття їхньої сутності. Для повноцінного теоретичного осмислення та побудови прикладних моделей протидії необхідно дослідити ці операції в їхньому динамічному розгортанні – як структурований, покроковий процес, керований за законами проєктного менеджменту. Це актуалізує потребу в декомпозиції часових та операційних фаз розгортання деструктивного впливу в межах аналізу їхнього повного життєвого циклу.

Сучасне проектування інформаційно-психологічних операцій у цифровому медіасередовищі остаточно відійшло від інтуїтивних, хаотичних медіакампаній, трансформувавшись у суворо алгоритмізований процес, підпорядкований методології проєктного менеджменту та загальновійськовим стандартам планування і ведення спільних операцій¹. У межах цього підходу, закріпленого у фундаментальних доктринах НАТО оперативні заходи розглядаються як чітко структуровані проєкти з обмеженими ресурсами та вимірюваними критеріями успішності². Динамічне існування такого проєкту описується концепцією життєвого циклу, що охоплює послідовну зміну фаз: від виявлення вразливостей держави-мішені до остаточного згортання активності чи переходу кампанії у перманентний стан утримання результату. Декомпозиція цього життєвого циклу дозволяє розкрити внутрішню логіку дій агресора, де кожен попередній етап є жорсткою інформаційною та аналітичною базою для наступного.

Етап 1. Стратегічне планування та OSINT-розвідка.

Початкова фаза життєвого циклу цифрової ІПсО є виключно аналітичною і закладає стратегічний вектор для всієї майбутньої кампанії. Будь-яке прикладне проектування деструктивного впливу розпочинається з формулювання фінального деструктивного чи маніпулятивного ефекту. На цьому рівні суб'єкт агресії визначає, яка саме трансформація колективної чи індивідуальної поведінки в державі-мішені є метою проєкту (наприклад, зрив мобілізаційних заходів, штучне провокування внутрішньополітичної кризи, зниження рівня довіри до державних інституцій або дестабілізація фінансової системи).

¹ Див.: Твердохліб Ю. М. Інформаційно-психологічні операції: процес планування та реалізації. *Вісник Маріупольського державного університету. Серія: Історія, політологія*. 2017. №18. С. 360–364.

² Див.: Allied Joint Publication (AJP) – 3.10.1. Allied Joint Doctrine for Psychological Operations (Edition B Version 1). Brussels: NATO Standardization Office (NSO), 2014. 89 p. URL: https://assets.publishing.service.gov.uk/media/6a0452f88cc72d2f863ea875/ARCHIVED-AJP_3_10_1_B_PSYOPS_with_UK_Green_pages.pdf; Allied Joint Publication (AJP) – 3. Allied Joint Doctrine for the Conduct of Operations (Edition D Version 1). Brussels: NATO Standardization Office (NSO), 2025. 214 p. URL: https://assets.publishing.service.gov.uk/media/6964e72799fbdc498faecce2/AJP_3_Ed_D_V1-O.pdf.

Після дефініції стратегічних цілей операція переходить до стадії глибокої розвідки на основі відкритих джерел (OSINT – Open Source Intelligence) та інтелектуального аналізу даних (Data Mining). Завдяки глобальній цифровізації та концепції «цифрових слідів» (digital footprints) сучасний агресор отримує можливість здійснювати безпрецедентно точне психографічне та соціокультурне картографування суспільства без проведення класичних соціологічних опитувань¹.

Процес OSINT-розвідки на цьому етапі містить:

- аналіз інформаційного ландшафту: парсинг та моніторинг національного сегменту соціальних мереж, месенджерів та онлайн-ЗМІ за допомогою автоматизованих ІІІ-систем для визначення домінуючих тем, ключових опініон-лідерів (інфлюенсерів) та швидкості поширення інформаційних хвиль;

- виявлення психологічних та соціальних тригерів: фіксація точок найбільшої суспільної напруги, незадоволення чи колективного страху. У фокус аналітиків потрапляють лінії соціокультурного розлому (економічна нерівність, етнічні чи мовні питання, корупційні скандали, втома від війни), які згодом будуть використані як «вхідні ворота» для ворожих наративів;

- психографічне профілювання аудиторії: сегментація суспільства на мікрогрупи на основі їхніх цифрових інтересів, поведінки в мережі, маркерів вразливості та специфічних психотипів (згідно з модифікованими моделями типу OCEAN / Big Five), що дозволяє підготувати ґрунт для майбутнього високоточного мікротаргетингу².

Завершальним і найбільш технологічним елементом першого етапу є визначення KPI (Key Performance Indicators) операції. Проектний підхід вимагає від архітекторів ІІсО чіткого математичного визначення метрик, за якими оцінюватиметься успішність проходження кожної фази. Сучасні цифрові ІІсО оперують суворими дата-метриками, які в межах сучасного аналізу можливостей ІІІ у сфері StratCom поділяють на два ключові кластери³.

¹ Див.: Estrada E., Knight P. A. A first course in network theory. Oxford: Oxford University Press, 2015. xiv, 254 p.

² Див.: Woolley S. Manufacturing Consensus: Understanding Propaganda in the Era of Automation and Anonymity.

³ Див.: Barbu E., Banerjee S., Lim T., Zivere L. AI in Support of StratCom: The Use and Evaluation of Large Language Models in Less Widely Used Official EU Languages.

1. Метрики технічного охоплення (Technical Reach / Output Metrics): суто кількісні показники дистрибуції – сумарна кількість унікальних переглядів контенту, геометрична прогресія репостів, темпи приросту підписників на «сірих» інфраструктурних каналах.

2. Метрики когнітивно-поведінкового впливу (Cognitive & Behavioral Outcome Metrics): показники індексу сентименту (sentiment analysis) в інфополі, а також вихід деструктивного ефекту за межі віртуального простору в об'єктивну реальність (наприклад, реальні відмови від виконання обов'язків)¹.

Таким чином, ретельна реалізація першого етапу в межах проєктного підходу дозволяє суб'єкту ІПсО мінімізувати операційні ризики, оптимізувати фінансові витрати та створити математично прораховану, глибоко таргетовану дорожню карту деструктивного впливу на когнітивну систему суспільства.

Етап 2. Створення контенту та тестування наративів.

Після завершення аналітичної фази OSINT-розвідки життєвий цикл проєкту ІПсО переходить до стадії практичного виробництва та верифікації деструктивних матеріалів. Цей етап поєднує креативно-семантичну генерацію контенту та математично прораховані алгоритми його попереднього тестування на обмежених вибірках цільової аудиторії.

Процес реалізації другого етапу містить такі взаємопов'язані кроки.

1. Генерація матриці наративів та ШІ-виробництво. На основі виявлених тригерів і психографічних профілів створюється розгалужена текстова та мультимедійна база операції. Замість залучення великих штатів копірайтерів сучасний агресор використовує технології великих мовних моделей (LLMs) для автоматизованого розгортання наративів, моделювання топиків та виявлення прихованих

Riga: NATO Strategic Communications Centre of Excellence, 2025. 40 p. URL: <https://stratcomcoe.org/publications/ai-in-support-of-stratcom-the-use-and-evaluation-of-large-language-models-in-less-widely-used-official-eu-languages/326>.

¹ Див.: Bergmanis-Korāts G., Bertolin G., Pužule A., Zeng Y. AI in Support of StratCom Capabilities. Riga: NATO Strategic Communications Centre of Excellence, 2024. 48 p. URL: <https://stratcomcoe.org/publications/ai-in-support-of-stratcom-capabilities/296>.

смислових ліній¹. Як доводять дослідження НАТО, сучасні LLM здатні бездоганно адаптувати деструктивний текст під лінгвістичні та стилістичні особливості конкретної нації, повністю усуваючи культурний та мовний бар'єр, що раніше видавав іноземне походження пропаганди².

2. Виготовлення синтетичних мультимедійних матеріалів. Паралельно з текстовими масивами здійснюється генерація візуальних когнітивних пасток – від високоякісної інфографіки та емоційно забарвлених мемів (як носіїв деструктивних ідеологем) до синтетичних аудіо- та відеоматеріалів (дипфейків), призначених для миттєвої дискредитації чиновників чи військового командування суспільства-мішені.

3. Мікротаргетинг та А/В тестування (Cambridge Analytica style). Створений контент не запускається в загальне інфополе масово без попередньої перевірки. Суб'єкт ІІсО застосовує методику мікротаргетингу, адаптовану під сучасні ІІІ-платформи. Первинні «пробні» вкиди здійснюються на вузькі, ізольовані сегменти аудиторії (наприклад, через таргетовану рекламу або закриті групи месенджерів). Аналізуючи реакцію аудиторії, алгоритми ІІсО коригують стилістику, емоційне забарвлення або семантичні акценти повідомлень. Цей ітераційний процес повторюється доти, доки контент не продемонструє найвищий рівень емоційного залучення (engagement rate), мінімізуючи час на подолання раціональних фільтрів психіки³.

Таким чином, успішне завершення другого етапу (виробництва та верифікації контенту) дозволяє архітекторам ІІсО сформувати адаптивну, лінгвістично бездоганну та емоційно насичену контентну матрицю операції. Використання генеративного штучного інтелекту в поєднанні з прецизійним мікротаргетингом мінімізує операційні часові витрати та усуває ризик передчасного викриття кампанії через мовні чи культурні аномалії. Шляхом ітераційного А/В тестування

¹ Див.: Barbu E., Banerjee S., Lim T., Zivere L. AI in Support of StratCom: The Use and Evaluation of Large Language Models in Less Widely Used Official EU Languages.

² Там само.

³ Див.: Woolley S. Manufacturing Consensus: Understanding Propaganda in the Era of Automation and Anonymity.

на ізольованих вибірках суб'єкт впливу отримує математично перевірені семантичні та візуальні конструкти, що мають гарантовано найвищий коефіцієнт ураження когнітивних фільтрів психіки та готові до безпечного масового виведення у відкрите інформаційне поле.

Етап 3. Поширення та дистрибуція.

Після завершення фази виробництва та верифікації деструктивного контенту на обмежених вибірках, життєвий цикл проєкту ІПсО переходить до фази первинного виведення матеріалів у відкритий інформаційний простір держави-мішені. Ця стадія у проєктному менеджменті когнітивних операцій визначається як поширення (seeding) і є критичним містком між латентним плануванням та масовою вірусизацією наративів. Головне завдання етапу полягає в легітимізації штучно створеного контенту, подоланні первинних систем модерації цифрових платформ та формуванні ілюзії природного, органічного походження інформаційного приводу¹. У сучасній практиці це досягається через синергетичне поєднання двох інструментів: залучення легітимних лідерів суспільної думки та розгортання технологій астротурфіngu.

Процес реалізації етапу поширення передбачає використання таких механізмів.

1. Координація дій та використання опініон-лідерів (інфлюенсерів). Суб'єкти ІПсО усвідомлюють, що пересічний користувач виявляє вищий рівень довіри до повідомлень конкретних індивідів, ніж до офіційних медіа чи анонімних джерел. Легітимізація наративу здійснюється через залучення трьох кластерів інфлюенсерів: «всліпу» (шляхом майстерного маніпулювання патріотичними чи опозиційними почуттями реальних блогерів, які ретранслюють вклад, вважаючи його сенсаційною правдою); через фінансову мотивацію («сіра» закупівля публікацій у комерційних блогерів); або через пряме використання агентів впливу. Поява деструктивного тезового ряду на верифікованих акаунтах із великою аудиторією автоматично знімає з нього тавро «ворожої пропаганди» та переводить у розряд легітимної суспільної дискусії.

¹ Див.: Woolley S. Manufacturing Consensus: Understanding Propaganda in the Era of Automation and Anonymity.

2. Штучна імітація масової підтримки (Astroturfing). Синхронно із залученням інфлюенсерів запускається технологія астротурфінгу – конструювання штучної «ініціативи знизу» або ілюзії масового народного гніву / підтримки за допомогою координованої діяльності мереж ботів та тролів¹. Сучасні автономні AI-агенти, керовані технологіями великих мовних моделей, миттєво заповнюють секції коментарів під постами інфлюенсерів, створюючи ефект масового консенсусу навколо потрібного наративу. Мета астротурфінгу полягає в психологічному тиску на реальних користувачів: людина, яка бачить сотні однотипних схвальних чи панічних коментарів, зазнає впливу «ефекту конформізму» та починає сумніватися у власній раціональній оцінці подій, приймаючи штучно нав'язану позицію за думку реальної більшості суспільства;

3. Синхронізація інфраструктурних вертикалей. Поширення здійснюється не ізольовано, а каскадним методом за чітким часовим графіком (таймінгом). Повідомлення одночасно з'являється в мережі анонімних Telegram-каналів, підхоплюється бот-мережами в X (Twitter), візуалізується через короткі відео в TikTok та легітимізується обговоренням на сторінках опініон-лідерів у Facebook. Така всеохопна присутність створює для об'єкта впливу ефект «інформаційної облоги», коли з якого б цифрового джерела людина не отримувала дані, вона натрапляє на один і той самий заздалегідь сконструйований наратив.

З огляду на це, ретельна реалізація третього етапу забезпечує подолання критичного бар'єру між латентним виробництвом деструктивного сигналу та його легітимізацією у публічному дискурсі держави-мішені. Завдяки синергетичному поєднанню авторитету реальних опініон-лідерів із технологіями координованого III-астротурфінгу агресор нівелює перманентні загрози алгоритмічного блокування з боку цифрових платформ. Фаза поширення трансформує штучно сконструйований ворожий наратив на легітимний предмет гострої внутрішньосупільної дискусії. Це дозволяє створити стійку ілюзію органічного походження інформаційного приводу, формує навколо

¹ Див.: Howard P. N. Lie machines: how to save democracy from troll armies, deceitful robots, junk news operations, and political operatives.

нього штучний консенсус більшості та закладає інфраструктурну основу для подальшого неконтрольованого, лавиноподібного самопоширення деструктивного контенту самим суспільством.

Етап 4. Масштабування та вірусизація (ефект лавини).

У точці, де первинне поширення деструктивного контенту успішно пододало раціональні фільтри початкових цільових груп, життєвий цикл проекту ІПсО переходить у свою найбільш руйнівну фазу – масштабування та вірусизація. Метою цього етапу в проєктному менеджменті когнітивних операцій є переведення локального, штучно інкубованого інформаційного приводу в статус загальнонаціонального (або глобального) мейнстріму. На цій стадії суб'єкт гібридної агресії прагне запустити ефект лавини (інформаційного каскаду), за якого подальше поширення деструктивного контенту відбувається автономно, без додаткових фінансових чи технічних витрат з боку агресора, а за рахунок внутрішніх ресурсів самої держави-мішені¹.

Процес реалізації етапу масштабної вірусизації базується на трьох взаємопов'язаних механізмах.

1. Нейропсихологічне емоційне зараження (Emotional Contagion). Перехід від штучного поширення до органічного тиражування спирається на експлуатацію інтенсивних психоемоційних тригерів. Контент модифікується таким чином, щоб викликати в користувачів ефекти екзистенційного страху, моральної паніки, гніву або когнітивного дисонансу. Нейробіологічні дослідження інформаційних каскадів доводять, що в умовах високого емоційного збудження в людини пригнічується активність префронтальної кори, відповідальної за критичний аналіз, та активізується амігдала². Як наслідок, пересічний користувач відчуває непереборне підсвідоме прагнення негайно поділитися цим контентом зі своїм оточенням, щоб попередити їх або висловити обурення. Таким чином, суспільство-мішень саме стає головним безкоштовним дистриб'ютором ворожої операції.

2. Технологія мімікрії під авторитетні бренди (Media Impersonation). Для легітимізації контенту на макрорівні сучасні операції (зокрема

¹ Див.: Howard P. N. Lie machines: how to save democracy from troll armies, deceitful robots, junk news operations, and political operatives.

² Див.: Bak-Coleman J. B., Alfano M., West C. T. et al. Stewardship of global collective behavior.

російські системні кампанії «Doppelgänger» та «Matryoshka», що активно діють у період 2022–2026 рр.) використовують глибинне клоування легітимного медіапростору¹. Маніпулятивні матеріали, дипфейки та сфабриковані відео розповсюджуються через дзеркала та точні копії вебсайтів провідних світових та національних медіа (таких як BBC, Deutsche Welle, France 24, AFP тощо)². Коли споживач бачить звичний логотип, дизайн та стилістику авторитетного видання, він автоматично переносить рівень довіри до бренду на ворожий симулякр, що різко прискорює темпи геометричного поширення інформаційної інфекції.

3. Втягування традиційних масмедіа в реплікацію цифрових трендів. Кінцевою точкою масштабування є подолання бар'єру між соціальними мережами та класичними ЗМІ (телебачення, преса, радіо). Коли штучно створена за допомогою ШІ-ботів тема досягає пікових охоплень у Telegram чи X, традиційні редакції, перебуваючи в умовах жорсткого дедлайну та погоні за клікбейтом, починають реплікувати цей цифровий тренд як «гарячу новину дня» без належної перевірки першоджерела. Як демонструють звіти Європейської служби зовнішніх зв'язків (EEAS), такий каскадний перехід остаточно легітимізує деструктивний наратив, роблячи його частиною офіційного порядку денного держави³.

Таким чином, успішна реалізація четвертого етапу призводить до формування самопідтримуваного інформаційного цунамі, за якого початковий суб'єкт ІПсО може повністю згорнути пряму технічну підтримку операції. Завдяки інструментам емоційного зараження

¹ Див.: Doppelgänger / RRN Disinformation Infrastructure Ecosystem Report. *DomainTools Research*. March 1, 2026. URL: <https://dti.domaintools.com/research/doppelganger-rrn-disinformation-infrastructure-ecosystem>.

² Див.: Бот-мережа «Matryoshka» здійснює масштабну кампанію проти України та західних лідерів. *Центр протидії дезінформації*. 05.02.2026. URL: <https://cpd.gov.ua/en/international-threats-en/europe/matryoshka-botnet-campaign-against-ukraine-and-western-leaders/>; Russian fake news network targets Ukraine at Winter Olympics. *BBC News*. February 18, 2026. URL: <https://www.bbc.com/news/live/cr512p3j261t>.

³ Див.: 4th EEAS Threat Report on Foreign Information Manipulation and Interference Threats. Brussels: European Union External Action, 2026. 40 p. URL: https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf.

та масштабної мімікрії контенту під авторитетні ЗМІ (через архітектурні матриці типу «Doppelgänger» та «Matryoshka») ворожий наратив набуває пандемічного характеру. На цій стадії досягається головний проміжний ефект когнітивної війни – перевантаження національного інформаційного простору шумом, розмивання критеріїв істини у масовій свідомості та примус державних інституцій діяти у реактивному, виправдовувальному режимі, що значно знижує загальну когнітивну стійкість нації перед подальшими етапами гібридної агресії.

Етап 5. Оцінка ефективності та моніторинг (Battle Damage Assessment).

Фінальною, але циклічно замкненою фазою проектування сучасних деструктивних впливів є оцінка ефективності та моніторинг результатів¹. У межах проєктного підходу та сучасних стандартів когнітивного протистояння цей етап виконує роль аналітичного зворотного зв'язку і класифікується військовими аналітиками за аналогією до кінетичних операцій як оцінка бойових збитків в інфопросторі (Battle Damage Assessment – BDA)². Сучасна ІПсО ніколи не зупиняється після етапу вірусизації; вона вимагає перманентного зчитування реакції суспільства-мішені з метою динамічного коригування наративної матриці в реальному часі за допомогою алгоритмів штучного інтелекту.

Процес реалізації етапу в сучасних реаліях 2022–2026 років містить такі ключові компоненти.

1. Автоматизований ІІІ-аналіз метрик залученості та настроїв. Замість ручного підрахунку лайків та переглядів суб'єкт гібридної агресії використовує просунуті ІІІ-системи інтелектуального дата-майнінгу та настроїв-аналізу (automated sentiment analysis)³. Ці алгоритми у реальному часі парсять сотні тисяч публікацій, коментарів та репостів, відстежуючи динаміку зміщення емоційного фону сус-

¹ Див.: Allied Joint Publication (AJP) – 3. Allied Joint Doctrine for the Conduct of Operations (Edition D Version 1).

² Див.: Bolt N., Haiden L. Improving NATO Strategic Communications Terminology. Riga: NATO Strategic Communications Centre of Excellence, 2019. 75 p. URL: https://stratcomcoe.org/cuploads/pfiles/nato_stratcom_terminology_review_10062019.pdf.

³ Див.: Bergmanis-Korāts G., Bertolin G., Pužule A., Zeng Y. AI in Support of StratCom Capabilities.

пільства від початкових маркерів (наприклад, тривоги) до цільових (гострий суспільний гнів чи паніка). Спеціалізовані платформи аналізу поведінки здатні моментально виявляти «точки згасання» інформаційного приводу або, навпаки, вектори його найбільшої вірулентності¹.

2. Синхронне коригування та ітераційне моделювання. Отримані дані моніторингу є основою для миттєвої оптимізації кампанії. Якщо ІІІ-моделі фіксують, що певний наратив (наприклад, фейк про дефіцит енергоресурсів) не досягає цільових когнітивних КРІ через швидке спростування національними органами безпеки, операційна система ІІсО автоматично переформатує семантичне ядро. Через підключені великі мовні моделі (LLM) генерується нова, модифікована версія повідомлення з урахуванням виявлених ліній спростування². Це створює ефект «рухомої мішені» для фактчекерів, коли дезінформація мутує швидше, ніж її встигають деконструювати оборонні інституції.

3. Верифікація поведінкових зрушень (Behavioral Outcomes). Найвищим пріоритетом ВДА є фіксація конверсії віртуального шуму у реальні деструктивні дії соціуму. Як свідчать офіційні спільні аналітичні звіти Європейської служби зовнішніх зв'язків та Центру протидії дезінформації при РНБО України, російські скоординовані мережі (на кшталт ботнетів типу «Matryoshka») ретельно моніторять ефективність своїх операцій саме за поведінковими маркерами нації-мішені: від динаміки погіршення показників внутрішньополітичного консенсусу до масштабів реальних протестних акцій чи зриву державних програм³.

Таким чином, ретельна реалізація п'ятого етапу замикає життєвий цикл ІІсО в нескінченну спіраль деструктивного впливу. Фаза ВДА трансформує статичну інформаційну атаку на гнучку, самонавчувану

¹ Див.: Ferrara E. The Generative AI Paradox: GenAI and the Erosion of Trust, the Corrosion of Information Verification, and the Demise of Truth.

² Див.: Barbu E., Banerjee S., Lim T., Zivere L. AI in Support of StratCom: The Use and Evaluation of Large Language Models in Less Widely Used Official EU Languages.

³ Див.: New EEAS-CCD report exposes Russian FIMI targeting Ukraine's EU future. EUvsDisinfo / European External Action Service. June 23, 2026. URL: <https://euvsdisinfo.eu/new-eeas-ccd-report-exposes-russian-fimi-targeting-ukraines-eu-future/>

систему поведінкової інженерії. Оцінивши когнітивні збитки, завдані суспільству, та зафіксувавши нові вразливості та тригери за допомогою штучного інтелекту, агресор автоматично повертає проєкт ІПсО на Етап 1 – для запуску наступної, ще більш точної та скоординованої хвилі гібридної агресії, що вимагає від систем національної безпеки переходу до перманентного технологічного моніторингу та проактивного StratCom.

Узагальнення результатів дослідження динамічних характеристик інформаційно-психологічних операцій дозволяє констатувати, що впровадження проєктного підходу до планування та реалізації деструктивних впливів остаточно закріпило перехід когнітивного протиборства в категорію високотехнологічних інженерних процесів. Сучасний життєвий цикл цифрової ІПсО є строго алгоритмізованою, замкненою та ітераційною системою, де кожна фаза – від початкової аналітики до фінального моніторингу – жорстко взаємопов'язана з іншими та оптимізована за допомогою алгоритмів штучного інтелекту й інтелектуального аналізу великих масивів даних (Big Data).

Аналіз архітектоніки життєвого циклу операцій нового покоління дозволяє сформулювати такі ключові висновки.

По-перше, революція аналітичного базису (Етап 1). Завдяки тотальному збору цифрових слідів (Data Mining) та автоматизованій OSINT-розвідці, суб'єкт гібридної агресії отримав можливість проводити перманентне, непомітне психографічне картографування суспільства-мішені. Це дозволяє виявляти внутрішні лінії соціокультурних розломів та фіксувати точні математичні метрики КРІ задовго до початку активної фази операції, мінімізуючи фінансові та операційні ризики проєкту.

По-друге, трансформація контентного виробництва (Етап 2 та 3). Інтеграція великих мовних моделей (LLM) змістила баланс сил на користь агресора. ШІ повністю нівелював лінгвістичні бар'єри та знизив вартість генерації контенту до нуля. Послання ітераційного А/В тестування контенту на ізольованих групах із методами автоматизованого ШІ-астротурфіngu забезпечує швидку легітимізацію ворожих наративів у медіапросторі, трансформуючи штучний деструктивний вкид на предмет легітимної суспільної дискусії.

По-третє, ефект пандемічного масштабування (Етап 4 та 5). На стадії вірусизації сучасні ІПсО набувають характеру самопідтримуваного інформаційного цунамі. Через механізми нейропсихологічного емоційного зараження та масштабного клонування легітимного медіапростору (як у системних операціях «Doppelgänger» та «Matryoshka») суспільство держави-мішені зазнає когнітивної дезорієнтації та самостійно реплікує ворожі смисли. Цикл завершується фазою Battle Damage Assessment (BDA), де ІІІ оцінює когнітивні збитки нації та автоматично повертає проєкт на першу фазу для проєктування наступної, ще більш точної хвилі атаки.

З огляду на це, реактивні системи національної безпеки, орієнтовані на запізніле спростування фейків, виявляють свою повну концептуальну обмеженість. Проєктний характер сучасних ІПсО вимагає від держав-мішеней дзеркального переходу до проактивного проєктного менеджменту у сфері StratCom, створення національних автоматизованих систем превентивного моніторингу інформаційних аномалій та перманентного зміцнення когнітивної стійкості суспільства.

Утім, глибина розуміння етапів проєктування ІПсО є неповною без детального аналізу конкретного інструментарію, який уможливило настільки швидко та латентну реалізацію деструктивних впливів. Це актуалізує потребу в експлікації новітніх методів та інструментів когнітивного ураження, які виникли внаслідок синергетичного злиття децентралізованих архітектур Web 3.0 та обчислювальних потужностей генеративного штучного інтелекту.

Стрімка конвергенція децентралізованих рішень епохи Web 3.0 та інструментів генеративного штучного інтелекту зумовила появу принципово нових методів ураження ментальної сфери супротивника. Сучасний інструментарій інформаційно-психологічного протидіювання змістив фокус із кількісного перенасичення інформаційного простору (так званого «білого шуму») на якісне, технологічно опосередковане переформатування сприйняття об'єктивної реальності. Центральне місце в цій оновленій парадигмі деструктивного впливу посіли дві взаємопов'язані категорії: когнітивне хакерство як загальна методологія маніпулювання людськими ментальними автоматиз-

мами та дипфейки разом із синтетичними медіа як головна технологічна зброя верифікації штучної гіперреальності.

У межах сучасної доктрини ведення когнітивної війни, розробленої аналітиками Інноваційного хабу НАТО, категорія «когнітивного хакерства» визначається не як атака на комп'ютерні мережі чи системне програмне забезпечення, а як цілеспрямована інженерна атака на «вразливості» архітектури людського мислення¹. Комп'ютер або смартфон у цій системі координат є лише технічним вікном доступу, тоді як безпосередній об'єкт зламу – біологічна система обробки інформації, а саме людський мозок. Методологія когнітивного хакерства базується на експлуатації сталих еволюційних архітектурних особливостей психіки, тобто когнітивних упереджень (cognitive biases) та ментальних евристик².

Суб'єкти сучасних ІПсО трансформували психологічні теорії Даніеля Канемана в прикладну зброю. Розрахунок робиться на запуск так званої «Системи 1» – швидкого, автоматичного, емоційного та підсвідомого мислення, за одночасного блокування «Системи 2» – повільного, логічного та аналітичного контролю. Шляхом синергетичного злиття алгоритмів ШІ та психографічного профілювання (Data Mining), когнітивне хакерство реалізує такі методи кібер-психологічного ураження:

- експлуатація ефекту ілюзорної правди (Illusory Truth Effect) – нейромережі бот-систем забезпечують таку щільність і частоту повторення деструктивного наративу в різних вузлах цифрового середовища, за якої людський мозок починає сприймати інформацію як істинну лише на основі чинника когнітивної легкості та знайомості тексту³;

- селективна ампліфікація фрустрацій (Confirmation Bias Exploration) – алгоритми рекомендацій Web 2.0/3.0 ізолюють користувача в індивідуальній «інформаційній бульбашці», куди ШІ-

¹ Див.: Claverie B., du Cluzel F. «Cognitive Warfare»: The Advent of the Concept of «Cognitics» in the Field of Warfare; du Cluzel F. Cognitive Warfare.

² Див.: Kahneman D. Thinking, Fast and Slow. New York: Farrar, Straus and Giroux, 2011. 499 p.

³ Див.: Ferrara E. The Generative AI Paradox: GenAI and the Erosion of Trust, the Corrosion of Information Verification, and the Demise of Truth.

генератори контенту точково постачають саме ті дезінформаційні матеріали, які відповідають початковим страхам, політичним уподобанням чи образам індивіда. Це повністю паралізує здатність до об'єктивного сумніву;

– алгоритмічне маніпулювання увагою – використання механіки децентралізованих автономних мереж (Web 3.0) дозволяє створювати стійкі до блокування «інформаційні бульбашки», де деструктивні ідеологеми штучно підтримуються та радикалізуються без можливості проникнення альтернативної, об'єктивної інформації¹.

Якщо когнітивне хакерство формує методологічну рамку зламу психіки, то дипфейки (Deepfakes) та синтетичні медіа є головним прикладним інструментом верифікації та унаочнення штучної реальності. Дипфейк є продуктом передових технологій штучного інтелекту, заснованих на архітектурі генеративно-змагальних мереж (GANs) або дифузійних моделей нового покоління, які дозволяють здійснювати бездоганний синтез людського обличчя, голосу чи відеорядів².

У системній архітектурі сучасних ІПСО епохи III дипфейки пройшли еволюцію від низькоякісних підробок (low-fakes) до бездоганних синтетичних клонів, які використовуються як інструменти стратегічної дискредитації, дестабілізації та делегітимізації³. Специфіка застосування цього інструменту в сучасних операціях полягає в реалізації концепції «інформаційного нігілізму» або «дивіденду від брехні» (liar's dividend).

Практичними векторами реалізації синтетичних медіа в ІПСО є такі.

1. Миттєвий шоківий вплив (Tactical Deception) – генерація та каскадне вкидання (через анонімні мережі Telegram та ботнети типу «Matryoshka») сфабрикованих аудіо- та відеозаяв вищого військово-

¹ Див.: Benkler Y., Faris R., Roberts H. Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics.

² Див.: Goldstein J. A., Sastry G., Musser M., DiResta R., Gentzel M., Sedova K. Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations.

³ Див.: Nimmo B. AI and Covert Influence Operations: Latest Trends. San Francisco: OpenAI Academic Press, 2024. 39 p. URL: <https://cdn.openai.com/threat-intelligence-reports/threat-intel-report-may-2024.pdf>.

політичного керівництва держави в критичні моменти конфлікту (наприклад, фейкові накази про капітуляцію, відступ чи оголошення евакуації)¹. Навіть якщо таке відео спростовується протягом тридцяти хвилин, у перші хвилини воно встигає викликати паніку та дезорієнтувати систему управління;

2. Ерозія інституційної довіри. Систематичне виробництво високоякісних дипфейків призводить до того, що суспільство взагалі втрачає здатність вірити будь-якому відео- чи аудіодоказу в цифровому середовищі. Агресор досягає своєї мети тоді, коли пересічний громадянин починає відкидати навіть реальні, автентичні звернення легітимної влади, вважаючи їх «черговим ІШ-продуктом».

3. Мімікрія під міжнародну верифікацію. Сучасні нейромережі дозволяють здійснювати автоматичне дублювання (voice-cloning) деструктивного контенту будь-якою мовою світу з повним збереженням інтонаційних особливостей та артикуляції (ліпсінк) реальних світових лідерів чи міжнародних журналістів². Це дозволяє створювати симулякри «міжнародної підтримки» ворожих наративів або імітувати засудження України з боку західних інституцій³.

Таким чином, синергія когнітивного хакерства та синтетичних медіа створює умови для формування автономного, стійкого до зовнішнього впливу середовища маніпуляції. Епоха Web 3.0 та ІШ трансформувала ІПсО із зовнішнього тиску на внутрішній процес самодеструкції суспільства-мішені, де технології штучного інтелекту бездоганно грають на біологічних слабкостях людської природи.

Паралельно з розвитком синтетичних медіа та когнітивного хакерства архітектура сучасних ІПсО інтегрувала новітні механізми децентралізованого медіапростору, спрямовані на довгострокове утримання уваги та латентну зміну ціннісних орієнтирів. У цьому контексті алгоритмічна маніпуляція увагою (створення фільтраційних бульбашок) є системним інструментом фрагментації суспільства, тоді як гейміфікація та експлуатація ігрових платформ (Discord, Twitch,

¹ Див.: Бот-мережа «Matryoshka» здійснює масштабну кампанію проти України та західних лідерів; Russian fake news network targets Ukraine at Winter Olympics.

² Див.: Barbu E., Banerjee S., Lim T., Zîvere L. AI in Support of StratCom: The Use and Evaluation of Large Language Models in Less Widely Used Official EU Languages.

³ Див.: New EEAS-CCD report exposes Russian FIMI targeting Ukraine's EU future.

Steam) перетворилися на інноваційні канали латентної радикалізації, вербування та формування закритих екстремістських спільнот, які тривалий час залишаються поза полем зору класичних інституцій національної безпеки.

Умови функціонування економіки уваги (attention economy) змушують алгоритми сучасних цифрових платформ максимізувати час перебування користувача в мережі. Нейромережеві моделі рекомендаційних стрічок оптимізовані під просування контенту, який викликає найвищий рівень емоційного відгуку. Суб'єкти деструктивного впливу експлуатують цю особливість, здійснюючи алгоритмічну маніпуляцію увагою¹.

Шляхом штучного наповнення інфополя скоординованими коментарями та реакціями ШІ-ботів, алгоритми платформ спонукаються до ізоляції користувачів у межах «інформаційних бульбашок» (filter bubbles). Усередині цих герметичних цифрових просторів користувач споживає виключно однобічний, штучно підібраний і радикалізований контент, що призводить до руйнування загальнонаціонального консенсусу, поляризації суспільної думки та формування стійкого когнітивного розколу між різними соціальними групами².

Проте найбільш латентним та небезпечним інструментом сучасних ІІсО є гейміфікація деструктивного впливу та експлуатація інфраструктури спеціалізованих ігрових майданчиків:

– комунікаційні хаби Discord – платформа, що первісно створювалася для геймерів, трансформувалася в закриту, децентралізовану екосистему серверів, які надають суб'єктам ІІсО унікальні інструменти латентного впливу. Високий рівень анонімності, відсутність глобальної публічної стрічки новин (що унеможливило моніторинг класичними OSINT-системами) та можливість створення приватних закритих каналів дозволяють ворожим медіатехнологам формувати контрольовані мікроспільноти. У цих закритих хабах через поширення специфічної мем-культури, ідеологем та теорій змови відбувається

¹ Див.: Spohr D. Fake news and ideological polarization: Filter bubbles and echo chambers on social media.

² Див.: Bak-Coleman J. B., Alfano M., West C. T. et al. Stewardship of global collective behavior.

ся латентне психологічне оброблення підлітків та молоді, що веде до їх поступової радикалізації¹;

- стрімінгові платформи (Twitch, Kick) – функціонують як майданчики для перманентного психоемоційного зараження в реальному часі. Використовуючи авторитет популярних ігрових стрімерів (які можуть залучатися «всліпу» або на комерційній основі), суб'єкти гібридної агресії інтегрують деструктивні політичні та соціальні наративи безпосередньо в багатогодинні трансляції чи інтерактивні чати, де рівень раціонального захисту та критичного мислення молодіжної аудиторії є мінімальним;

- ігрова екосистема Steam – найбільша у світі цифрова вітрина та соціальна мережа для геймерів перетворилася на «сіру зону» когнітивного протистояння. Дослідження безпекових інституцій фіксують створення у Steam тисяч закритих груп та профілів, які використовують ігрову стилістику (аватари, нікнейми, кастомні ігри) для пропаганди екстремізму, мілітаризму та дискредитації державних інституцій держав-мішеней. Гейміфікація передбачає перетворення реальних деструктивних дій на віртуальні квести або місії, за виконання яких користувач отримує ігровий статус чи внутрішньоігрові преференції, що стимулює його до перенесення радикальної активності у реальне життя².

Таким чином, синергетичне злиття алгоритмічних маніпуляцій увагою, синтетичних медіа та гейміфікованих комунікаційних платформ сформувало безпрецедентний за своєю руйнівною силою інструментарій сучасних ІПсО. Епоха Web 3.0 та штучного інтелекту змінила саму природу загрози: якщо класична пропаганда минулого діяла як зовнішній ідеологічний тиск, то новітні методи діють як латентний внутрішній вірус. Експлуатуючи базові еволюційні слабкості людської психіки, алгоритми рекомендацій та ігрові механізми змушують суспільство-мішень самостійно інкубувати, розвивати

¹ Див.: 4th EEAS Threat Report on Foreign Information Manipulation and Interference Threats.

² Див.: Росія використовує ігрові платформи для вербування іноземців у війну проти України. *Центр протидії дезінформації*. 07.01.2026. URL: <https://cpd.gov.ua/international-direction/evropa/rosiya-vykorystovuye-igrovi-platfony-dlya-verbuвання-inozemciv-u-vijnu-proty-ukrayiny/>

та поширювати деструктивні смисли, що веде до саморуйнування когнітивної стійкості нації та вимагає від архітекторів національної безпеки розробки принципово нових, проактивних концепцій когнітивної оборони.

Практичний досвід України в протидії зовнішнім деструктивним впливам є найбільш репрезентативним кейсом у сучасній історії безпекових студій, оскільки саме на вітчизняному інформаційному ландшафті суб'єкти російської гібридної агресії тестували та шліфували новітні технології когнітивного ураження. Ретроспективний аналіз цього протиборства у період з 2014 по 2026 роки дозволяє виокремити чітку еволюційну траєкторію ворожих ІПСО: від лінійних, відносно примітивних пропагандистських кампаній «першої хвилі» до створення повністю автономних, технологічно опосередкованих систем поведінкової інженерії нового покоління.

На початковому етапі агресії (2014–2021 рр.) ворожий вплив мав здебільшого фрагментарний і реактивний характер. Операції спиралися на традиційні медіаплатформи (телебачення, пресу) та перші покоління вітчизняних і російських соціальних мереж. Технологічний інструментарій обмежувався розгортанням класичних «тупих» ботоферм, що функціонували на основі жорстких текстових скриптів і займалися масовим дублюванням однакових дезінформаційних тез (астротурфінгом), які легко ідентифікувалися національними органами безпеки та громадянським суспільством. Основні зусилля ворога були зосереджені на легітимізації анексії Криму та окупації окремих районів Донецької та Луганської областей через лінійні історичні міфи.

Із початком повномасштабного вторгнення у 2022 році та його розгортанням у перманентну фазу конфлікту протягом 2024–2026 років архітектура російських ІПСО зазнала докорінної цифровізації та інтелектуалізації. Суб'єкти гібридної агресії інтегрували у свої операційні цикли технології великих мовних моделей (LLM) та генеративного ШІ, повністю усунувши мовні й культурні бар'єри¹. До-

¹ Див.: Nimmo B. AI and Covert Influence Operations: Latest Trends; Barbu E., Banerjee S., Lim T., Zivere L. AI in Support of StratCom: The Use and Evaluation of Large Language Models in Less Widely Used Official EU Languages.

слідження OpenAI та Ради національної безпеки і оборони України фіксують перехід ворога до створення транскордонних цифрових екосистем деструктивного впливу¹.

Найбільш масштабними проявами цієї еволюції стали скоординовані кампанії нового покоління:

- екосистема «Doppelgänger» (2022–2026 рр.) – масштабна інфраструктурна мережа, що спеціалізується на прецизійному клонуванні (віддзеркалюванні) вебсайтів авторитетних національних та міжнародних медіа (BBC, Deutsche Welle, France 24, провідні українські інформаційні ресурси)². Через ці симулякри споживачам постачався згенерований ШІ маніпулятивний контент, спрямований на руйнування міжнародної підтримки України та штучне провокування розколу між військовим та політичним керівництвом держави;

- ботнет-система «Matryoshka» (2024–2026 рр.) – високотехнологічна мережа автономних ШІ-агентів, яка здійснює каскадні посіви деструктивних наративів у месенджерах (Telegram, WhatsApp) та соціальних мережах (X, TikTok)³. Особливістю мережі є використання просунутого voice-cloning та ліпсінк-дипфейків для дискредитації процесів мобілізації, створення панічних настроїв навколо енергетичної безпеки та підриву інституційної довіри громадян до власної держави.

Концептуальний аналіз еволюції ІПсО доводить, що класичні інструменти інформаційної безпеки, орієнтовані на пасивне, реактивне спростування фейків (debunking) та постфактум-фактчекінг, виявляють свою повну обмеженість і неспроможність протидіяти матричним ШІ-атакам нового покоління. Боротьба з дезінформацією виключно на наративному рівні лікує симптоми, але залишає недоторканими технологічні двигуни агресора. Крім того, в умовах пандемічної швидкості поширення синтетичних медіа, час, витрачений

¹ Див.: Metz C. OpenAI Says Russia and China Used Its A. I. in Covert Campaigns. *The New York Times*. May 30, 2024. URL: <https://www.nytimes.com/2024/05/30/technology/openai-influence-campaigns-report.html>; Nimmo B. AI and Covert Influence Operations: Latest Trends.

² Див.: Doppelgänger / RRN Disinformation Infrastructure Ecosystem Report.

³ Див.: Бот-мережа «Matryoshka» здійснює масштабну кампанію проти України та західних лідерів.

органами безпеки на верифікацію та офіційне спростування дипфейку, грає на користь ворога, оскільки емоційне зараження аудиторії та когнітивне ураження психіки встигають відбутися у перші хвилини вкиду¹.

Це зумовлює об'єктивну потребу переходу національних безпекових систем до проактивної парадигми, закладеної в сучасних доктринальних документах оперативних фреймворків НАТО, – концепції когнітивної стійкості (cognitive resilience)². У межах методології когнітивної війни когнітивна стійкість визначається не як технічний захист інфраструктури чи видалення контенту, а як формування системного імунітету та психоемоційної опірності індивідуальної та масової свідомості громадян перед будь-якими деструктивними маніпулятивними впливами³.

Теоретико-методологічний каркас когнітивної стійкості базується на таких засадах:

- концепція «пребункінгу» (Prebunking / Inoculation Theory) – психологічна теорія інокуляції (щеплення) передбачає, що замість спростування вже поширеної брехні, суспільство необхідно заздалегідь «інфікувати» мікродозами послаблених ворожих наративів з одночасним поясненням маніпулятивних технологій, які агресор використовуватиме⁴. Розуміння механіки маніпуляції (наприклад, як працює астротурфінг чи алгоритми «інформаційних бульбашок») формує в громадян стійкі раціональні фільтри («Систему 2» за Д. Канеманом), які автоматично блокують спроби емоційного зараження під час реальної атаки⁵;

- формування інформаційного імунітету через медіаграмотність – переведення кібергігієни на рівень базової соціальної навички. Громадянин має усвідомлювати себе не пасивним споживачем інформа-

¹ Див.: Bak-Coleman J. B., Alfano M., West C. T. et al. Stewardship of global collective behavior.

² Див.: Allied Joint Publication (AJP) – 3; du Cluzel F. Cognitive Warfare.

³ Див.: Claverie B., du Cluzel F. «Cognitive Warfare»: The Advent of the Concept of «Cognitics» in the Field of Warfare.

⁴ Див.: 4th EEAS Threat Report on Foreign Information Manipulation and Interference Threats.

⁵ Див.: Kahneman D. Thinking, Fast and Slow.

ції, а активним вузлом мережевого суспільства, чий репост чи коментар має безпекові наслідки. Когнітивна стійкість передбачає розвиток навичок розпізнавання ІІІ-синтезованого контенту, верифікації першоджерел та контролю за власними психоемоційними реакціями в моменти споживання клікбейтного контенту;

– перехід до проактивного StratCom – замість виправдовувальної позиції та реакцій на ворожі інфоприводи, держава-мішень формує власний сильний, прозорий та інклюзивний наративний порядок денний. Високий рівень довіри між суспільством та державними інституціями, забезпечений чесною та оперативною комунікацією, звужує «вхідні ворота» для ворожих ІПсО, унеможливаючи експлуатацію внутрішніх соціальних фрустрацій та ліній соціокультурного розлому.

Таким чином, убезпечення цифрового медіасередовища в епоху Web 3.0 та штучного інтелекту вимагає синергетичного поєднання технологічного моніторингу аномалій на ранніх етапах життєвого циклу ІПсО та глибокої соціокультурної роботи над когнітивним імунітетом нації. Тільки трансформація суспільства з вразливої мішені на стійку, самовідновлювану екосистему дозволяє нівелювати стратегічні загрози сучасного когнітивного хакерства.

Узагальнення результатів теоретико-прикладного аналізу архітектури, життєвого циклу та методів реалізації інформаційно-психологічних операцій у сучасному цифровому медіасередовищі дозволяє сформулювати такі наукові та практичні висновки.

По-перше, сучасні ІПсО еволюціонували з лінійних пропагандистських актів минулого у складні, технологічно опосередковані системи поведінкової інженерії¹. Їхня стабільність та ефективність забезпечуються жорсткою взаємозалежністю трьох рівнів системної архітектури: інфраструктурного (децентралізована мережева екосистема месенджерів Web 2.0/3.0 та сірих зон комунікації), технологічного (автоматизований двигун на базі LLM-моделей та розумних ІІІ-ботів, що керують алгоритмами рекомендацій) та наративного (семантичне ядро ураження, засноване на конструюванні симулякрів та експлуа-

¹ Див.: Clow R. Psychological Operations: The Need to Understand the Psychological Plane of War. *Canadian Military Journal*. 2008. Vol. 9. No. 1. P. 21–29.

тації когнітивних пасток). Деградація одного з елементів не зупиняє роботу всієї системи, а лише стимулює її автоматичну перебудову.

По-друге, проектування ІПСО нового покоління здійснюється за суворими законами проєктного менеджменту та концепції оперативних циклів розвідки. Повний життєвий цикл операції охоплює п'ять ітераційних фаз: від глибокої аналітики і картографування суспільства методами OSINT та Data Mining на першому етапі – через ІІІ-генерацію контенту, мікротаргетинг, каскадне поширення (seeding) та масштабну вірусизацію (на прикладі клонованих медіаструктур типу «Doppelgänger» та «Matryoshka») – до фінального оцінювання когнітивних збитків (Battle Damage Assessment). Фаза BDA замикає цикл, перетворюючи статичну атаку на гнучку, самонавчувану систему впливу.

По-третє, стрімкий розвиток генеративного штучного інтелекту та децентралізованих майданчиків (Discord, Twitch, Steam) призвів до формування феномену когнітивного хакерства – зламу біологічної системи обробки інформації людини через уразливості її мислення. Використання високоточних дипфейків, інструментів voice-cloning та алгоритмічних маніпуляцій увагою призводить до ерозії інституційної довіри, формування екстремістських «інформаційних бульбашок» та запуску неконтрольованого емоційного зараження, за якого суспільство-мішень самостійно реплікує деструктивні ворожі смисли.

Можна також запропонувати практичні рекомендації для оптимізації національних систем інформбезпеки.

1. Визнати людський розум окремим доменом протиборства. Класичний реактивний фактчекінг та спростування фейків (debunking) виявляють концептуальну обмеженість, оскільки борються з наслідками, а не з причинами атак. Оборонна стратегія держави має зміститися в бік пребункінгу (превентивного психологічного щеплення соціуму) – масового навчання громадян механізмам розпізнавання ІІІ-маніпуляцій та алгоритмів «інформаційних бульбашок» до моменту початку атаки.

2. Для ефективної протидії технологічному рівню ІПСО необхідно інтегрувати в архітектуру ситуаційних центрів національної безпеки проактивні системи нейромережевого моніторингу. Вони мають

у реальному часі здійснювати автоматизований сентимент-аналіз цифрового простору, маркувати синтетичний (генеративний) контент на ранніх етапах посіву та виявляти аномальні патерни координації бот-мереж до моменту початку масової вірусизації.

3. Найкращим захистом від семантичного отруєння є формування власного сильного, прозорого та інклюзивного наративного порядку денного. Високий рівень довіри між суспільством та державними інституціями, забезпечений оперативним інформуванням, звужує «вхідні ворота» для ворожих ІПсО, унеможливаючи експлуатацію внутрішніх соціальних фрустрацій супротивником.

Резюмуючи вищевикладене, слід наголосити, що в епоху тотальної цифровізації та інтелектуалізації гібридних конфліктів питання про здатність або нездатність соціуму до опору вирішується, головним чином, у боротьбі на інформаційному полі¹. Якими б потужними не були кінетичні чи технологічні ресурси сторін, кінцевий результат протиборства визначається стійкістю ментальної сфери людини. У цьому контексті безперечно мав рацію британський військовий капелан Норман Коупленд, який у своїй класичній праці з психології військового духу стверджував, що «армія не розбита, поки вона не перейнялася свідомістю поразки. Поразка – це висновок розуму, а не фізичний стан»². Сучасні цифрові ІПсО є не чим іншим, як високотехнологічною інженерією, спрямованою на примус держави-мішені до цього деструктивного «висновку розуму». Відтак, головним вектором захисту національного суверенітету в епоху штучного інтелекту та Web 3.0 стає не просто кібербезпека технічних мереж, а проактивне проектування когнітивного імунітету нації, здатного зберегти волю до спротиву та концептуальну автономію мислення в умовах будь-яких матричних маніпуляцій противника³.

¹ Див.: Специфіка розвитку сучасного соціально-гуманітарного середовища: кол. моногр. / Березовська-Чміль О. Б., Кучин С. П., Чернишова Т. О. та ін. Харків: СГ НТМ «Новий курс», 2021. С. 20–27.

² Коупленд Н. Психология и солдат / Пер. с англ. А. Т. Сапронова и В. М. Катеринича. 2-е изд. Москва: Воениздат, 1991. С. 69.

³ Див.: Требін М. П., Чернишова Т. О. Боротьба за свідомість людей в епоху постправди. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія*. 2021. № 3 (50). С. 153–171.

==== Список використаних джерел

1. Бодріяр Ж. Симулякри і симуляція / пер. з фр. В. Ховхун. Київ : Видавництво Соломії Павличко «Основи», 2004. 230 с.
2. Бот-мережа «Matryoshka» здійснює масштабну кампанію проти України та західних лідерів. *Центр протидії дезінформації*. 05.02.2026. URL: <https://cpd.gov.ua/en/international-threats-en/europe/matryoshka-botnet-campaign-against-ukraine-and-western-leaders/>
3. Історія інформаційно-психологічного протиборства: підруч. / [Я. М. Жарков, Л. Ф. Компанцева, В. В. Остроухов, В. М. Петрик, М. М. Присяжнюк, Є. Д. Скулиш]; за заг. ред. д. ю. н., проф., засл. юриста України Є. Д. Скулиша. Київ: Наук.-вид. відділ НА СБ України, 2012. 212 с.
4. Коупленд Н. Психология и солдат / Пер. с англ. А. Т. Сапронова и В. М. Катеринича. 2-е изд. Москва: Воениздат, 1991. 96 с.
5. Певцов Г. В., Залкін С. В., Сідченко С. О., Хударковський К. І. Інформаційно-психологічні операції: планування, протидія, технології: монографія. Харків: ДІСА ПЛЮС, 2020. 252 с.
6. Проноза І., Суrowa М. Інформаційні (психологічні) операції як інструмент інформаційної війни. *Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи* : IV міжнар. наук.-практ. конф., 27 верес. 2023 р.: тези доповідей / Міністерство оборони України, НУОУ. Київ: НУОУ, 2023. С. 121–123.
7. Росія використовує ігрові платформи для вербування іноземців у війну проти України. *Центр протидії дезінформації*. 07.01.2026. URL: <https://cpd.gov.ua/international-direction/evropa/rosiya-vykorystovuye-igrovi-platformy-dlya-verbuvannya-inozemcziv-u-vijnu-proty-ukrayiny/>
8. Специфіка розвитку сучасного соціально-гуманітарного середовища: кол. моногр. / Березовська-Чміль О. Б., Кучин С. П., Чернишова Т. О. та ін. Харків: СГ НТМ «Новий курс», 2021. 124 с.
9. Твердохліб Ю. М. Інформаційно-психологічні операції: процес планування та реалізації. *Вісник Маріупольського державного університету. Серія: Історія, політологія*. 2017. № 18. С. 360–364.
10. Твердохліб Ю. М., Мороз Ю. М. Інформаційно-психологічні операції в умовах ведення гібридної війни. *Вісник Львівського національного університету імені І. Франка. Серія : Міжнародні відносини*. 2016. № 38. С. 97–105.
11. Тоффлер Е. Третя хвиля / пер. з англ. А. Євса; ред. пер. В. Шовкун. Київ: Видавничий дім «Всесвіт», 2000. 475 с.

12. Требін М. П., Чернишова Т. О. Боротьба за свідомість людей в епоху постправди. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія*. 2021. № 3 (50). С. 153–171.
13. Федонюк С. Інформаційно-психологічні операції на геополітичній арені: навч. посіб. Луцьк: Вежа-Друк, 2024. 104 с.
14. Цифрова епоха: міждисциплінарний дискурс: монографія / [А. А. Гедзик, Т. В. Ковальова, О. Ю. Коцюрба та ін.]; Аналіт. центр сучас. гуманітаристики. Харків: Право, 2024. 214 с.
15. 4th EEAS Threat Report on Foreign Information Manipulation and Interference Threats. Brussels: European Union External Action, 2026. 40 p. URL: https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf.
16. Allied Joint Publication (AJP) – 3. Allied Joint Doctrine for the Conduct of Operations (Edition D Version 1). Brussels: NATO Standardization Office (NSO), 2025. 214 p. URL: https://assets.publishing.service.gov.uk/media/6964e72799fbdc498faecce2/AJP_3_Ed_D_V1-O.pdf.
17. Allied Joint Publication (AJP) – 3.10.1. Allied Joint Doctrine for Psychological Operations (Edition B Version 1). Brussels: NATO Standardization Office (NSO), 2014. 89 p. URL: https://assets.publishing.service.gov.uk/media/6a0452f88cc72d2f863ea875/ARCHIVED-AJP_3_10_1_B_PSYOPS_with_UK_Green_pages.pdf.
18. Bak-Coleman J. B., Alfano M., West C. T. et al. Stewardship of global collective behavior. *Proceedings of the National Academy of Sciences (PNAS)*. 2021. Vol. 118, No. 27. e2025764118. DOI: 10.1073/pnas.2025764118.
19. Barbu E., Banerjee S., Lim T., Zivere L. AI in Support of StratCom: The Use and Evaluation of Large Language Models in Less Widely Used Official EU Languages. Riga: NATO Strategic Communications Centre of Excellence, 2025. 40 p. URL: <https://stratcomcoe.org/publications/ai-in-support-of-stratcom-the-use-and-evaluation-of-large-language-models-in-less-widely-used-official-eu-languages/326>.
20. Benkler Y., Faris R., Roberts H. Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics. New York: Oxford University Press, 2018. ix, 462 p.
21. Bergmanis-Korāts G., Bertolin G., Pužule A., Zeng Y. AI in Support of StratCom Capabilities. Riga: NATO Strategic Communications Centre of Excellence, 2024. 48 p. URL: <https://stratcomcoe.org/publications/ai-in-support-of-stratcom-capabilities/296>.

22. Bolt N., Haiden L. Improving NATO Strategic Communications Terminology. Riga: NATO Strategic Communications Centre of Excellence, 2019. 75 p. URL: https://stratcomcoe.org/cuploads/pfiles/nato_stratcom_terminology_review_10062019.pdf.
23. Castells M. Communication power. 2nd ed. Oxford: Oxford University Press, 2013. xlvii, 574 p.
24. Castells M. The rise of the network society. 2nd ed., with a new pref. Malden, MA: Wiley-Blackwell, 2010. lvii, 597 p.
25. Claverie B., du Cluzel F. «Cognitive Warfare»: The Advent of the Concept of «Cognitics» in the Field of Warfare. *Cognitive Warfare: The Future of Cognitive Dominance* : Proceedings of the First NATO Scientific Meeting on Cognitive Warfare, Bordeaux, France, 21 June 2021. Neuilly-sur-Seine: NATO Collaboration Support Office, 2022. P. 2–1–2–7. URL: https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare-Symposium-ENSC-March-2022-Publication.pdf?utm_source=chatgpt.com.
26. Claverie B., du Cluzel F., Desclaux G. Cognitive Warfare and C2. *Operationalizing the Concept of Cognitive Warfare* : 2nd Scientific and Strategic Workshop on «Cognitive Warfare», US Military Academy West Point, March 4, 2022. URL: <https://hal.science/hal-04189572v1/file/WP%20-%20CW%26C2%20Claverie-DuCluzel-Desclaux%20-%202022.pdf>.
27. Computational Propaganda: Political Parties, Politicians, and Automated Networks on Social Media / ed. by S. C. Woolley, P. N. Howard. Oxford: Oxford University Press, 2019. 288 p.
28. Doppelgänger / RRN Disinformation Infrastructure Ecosystem Report. *DomainTools Research*. March 1, 2026. URL: <https://dti.domaintools.com/research/doppelganger-rrn-disinformation-infrastructure-ecosystem>.
29. du Cluzel F. Cognitive Warfare. Norfolk, VA: NATO Allied Command Transformation, Innovation Hub, 2021. 45 p. URL: https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf.
30. Estrada E., Knight P. A. A first course in network theory. Oxford: Oxford University Press, 2015. xiv, 254 p.
31. Ferrara E. The Generative AI Paradox: GenAI and the Erosion of Trust, the Corrosion of Information Verification, and the Demise of Truth. *Future Internet*. 2026. Vol. 18, Issue 2. Art. 73. DOI: <https://doi.org/10.3390/fi18020073>.
32. Goldstein J. A., Sastry G., Musser M., DiResta R., Gentzel M., Sedova K. Generative Language Models and Automated Influence Operations:

- Emerging Threats and Potential Mitigations. *arXiv preprint arXiv:2301.04246*. 2023. 82 p. DOI: 10.48550/arXiv.2301.04246.
33. Howard P. N. Lie machines: how to save democracy from troll armies, deceitful robots, junk news operations, and political operatives. New Haven; London: Yale University Press, 2020. xviii, 221 p.
34. Kahneman D. Thinking, Fast and Slow. New York: Farrar, Straus and Giroux, 2011. 499 p.
35. Krulak C. C. The strategic corporal: Leadership in the three-block war. *Leatherneck*. 1999. Vol. 82, No. 1. P. 14–17. URL: <https://www.mca-marines.org/wp-content/uploads/1999-Jan-The-strategic-corporal-Leadership-in-the-three-block-war.pdf>.
36. Lewis T. G. Network science: theory and practice. Hoboken, N. J.: John Wiley & Sons, 2009. xi, 512 p.
37. Metz C. OpenAI Says Russia and China Used Its A. I. in Covert Campaigns. *The New York Times*. May 30, 2024. URL: <https://www.nytimes.com/2024/05/30/technology/openai-influence-campaigns-report.html>.
38. Moore D. Targeting technology: Mapping military offensive network operations. *10th International Conference on Cyber Conflict. CyCon X: Maximising Effects* (29 May – 01 June 2018, Tallinn, Estonia) / T. Minárik, R. Jakschis, L. Lindström (Eds.). Tallinn: NATO CCD COE Publications, 2018. P. 89–108. URL: https://ccdcoc.org/uploads/2018/10/CyCon_2018_Full_Book.pdf.
39. Moore D., Rid T. Cryptopolitik and the Darknet. *Survival*. 2016. Vol. 58, Issue 1. P. 7–38. DOI: <https://doi.org/10.1080/00396338.2016.1142085>.
40. NATO STRATCOMCOE podcast explores Telegram app. *LSM*. September 27, 2024. URL: <https://eng.lsm.lv/article/features/video/27.09.2024-nato-stratcomcoe-podcast-explores-telegram-app.a570335/>
41. New EEAS-CCD report exposes Russian FIMI targeting Ukraine's EU future. EUvsDisinfo / European External Action Service. June 23, 2026. URL: <https://euvsdisinfo.eu/new-eeas-ccd-report-exposes-russian-fimi-targeting-ukraines-eu-future/>
42. Nimmo B. AI and Covert Influence Operations: Latest Trends. San Francisco : OpenAI Academic Press, 2024. 39 p. URL: <https://cdn.openai.com/threat-intelligence-reports/threat-intel-report-may-2024.pdf>.
43. Russian fake news network targets Ukraine at Winter Olympics. *BBC News*. February 18, 2026. URL: <https://www.bbc.com/news/live/cr5l2p3j261t>.
44. Spohr D. Fake news and ideological polarization: Filter bubbles and echo chambers on social media. *Business Information Review*. 2017. Vol. 34, No. 3. P. 150–160. DOI: <https://doi.org/10.1177/0266382117722446>.

45. Thompson P. Cognitive hacking and intelligence and security informatics. *Proc. SPIE 5423, Enabling Technologies for Simulation Science VIII, null (13 Aug 2004)*. DOI: <https://doi.org/10.1117/12.554454>.
46. Toffler A., Toffler H. War and anti-war: survival at the dawn of the 21st century. Boston: Little, Brown, 1993. xiii, 302 p.
47. Woolley S. Manufacturing Consensus: Understanding Propaganda in the Era of Automation and Anonymity. New Haven, CT: Yale University Press, 2023. 232 p.

2.3. Північнокорейська тематика в спеціальних інформаційно- психологічних операціях російсько- української війни

Чупрій Леонід Васильович

*доктор політичних наук, професор
завідувач кафедри політології та соціології
Київський столичний університет імені Бориса Грінченка.*

Настояща Катерина Василенко

*доктор соціологічних наук, доцент
завідувач Центру соціологічних досліджень
Інститут національної стійкості та безпеки;
Науково-дослідний інститут українознавства
Київський національний університет імені Тараса Шевченка*

Повномасштабна російсько-українська війна триває вже понад чотири роки і завдала Україні колосальних людських, економічних та культурних втрат. За різними оцінками, сукупний обсяг збитків перевищує 700 млрд доларів США. Значних руйнувань зазнали не лише житлові будинки та об'єкти критичної інфраструктури, а й пам'ятки історико-культурної спадщини. За даними Міністерства культури та інформаційної політики України, пошкоджено або повністю знищено сотні об'єктів культурної спадщини, кількість яких перевищує шістсот.

== Авторський колектив

Алексєєнко Людмила Михайлівна, доктор економічних наук, професор, професор кафедри управління та адміністрування, Івано-Франківський навчально-науковий інститут менеджменту Західноукраїнського національного університету.

Іванченко Ольга Миколаївна, доктор юридичних наук, доцент, доцент кафедри загальної теорії права та держави, Національний університет «Одеська юридична академія».

Ільницька Уляна Вікторівна, кандидат політичних наук, доцент, доцент кафедри політології та міжнародних відносин, Національний університет «Львівська політехніка».

Квасниця Оксана Василівна, кандидат економічних наук, доцент, доцент кафедри фінансів ім. С. І. Юрія, Західноукраїнський національний університет (м. Тернопіль).

Коннова Ніна Олексіївна, кандидат філософських наук, доцент, доцент кафедри міжнародних відносин і політичної філософії, Харківський національний економічний університет імені Семена Кузнеця.

Копитова Олена Сергіївна, доктор юридичних наук, старший дослідник, доцент кафедри економіко-правових дисциплін Навчально-наукового інституту права і психології, Національна академія внутрішніх справ (м. Київ).

Кравченко Олена Валентинівна, доктор історичних наук, доцент, професор кафедри міжнародних відносин і політичної філософії, Харківський національний економічний університет імені Семена Кузнеця.

Настояща Катерина Василівна, доктор соціологічних наук, доцент, завідувач Центру соціологічних досліджень, Інститут національної стійкості та безпеки; Науково-дослідний інститут українознавства Київського національного університету імені Тараса Шевченка.

Требін Михайло Петрович, доктор філософських наук, професор, професор кафедри міжнародних відносин і політичної філософії, Харківський національний економічний університет імені Семена Кузнеця.

Федіна Наталія Василівна, кандидат юридичних наук, доцент, доцент кафедри адміністративно-правових дисциплін Навчально-наукового інституту права та правоохоронної діяльності, Львівський державний університет внутрішніх справ.

Чернишова Таїсія Олексіївна, кандидат філологічних наук, доцент, доцент кафедри гуманітарних та соціальних дисциплін, Харківський національний університет Повітряних Сил імені Івана Кожедуба.

Чупрій Леонід Васильович, доктор політичних наук, професор, завідувач кафедри політології та соціології, Київський столичний університет імені Бориса Грінченка.

Наукове видання

Алексесенко Людмила Михайлівна,
Іванченко Ольга Миколаївна,
Ільницька Уляна Вікторівна та ін.

ІНФОРМАЦІЙНА ВІЙНА ТА ЇЇ ВПЛИВ НА СУСПІЛЬСТВО

Монографія

Редактор *Т. О. Чернишова*

Підписано до друку 28.07.2026. Формат 60×84/16.
Ум. друк. арк. 29,4. Обл.-вид. арк. 24. Тираж 100 пр. Зам. № 729

ТОВ «Видавничий дім «Право»,
вул. Харківських Дивізій, 11/2, м. Харків, Україна
Для кореспонденції: а/с 822, м. Харків, 61023, Україна
Тел.: (050) 409-08-69, (067) 574-81-20

Вебсайт: <https://pravo-izdat.com.ua>

E-mail для замовників послуг: verstka@pravo-izdat.com.ua

E-mail для покупців: sales@pravo-izdat.com.ua

Свідоцтво суб'єкта видавничої справи ДК № 8024 від 05.12.2023

Виготовлено ТОВ «Промарт Плюс»,
вул. Весніна, 12, м. Харків, 61023, Україна
Тел. (097) 445-07-79

Вебсайт: <https://promart.in.ua>

Свідоцтво суб'єкта видавничої справи ДК № 8388 від 16.07.2025