УДК 32:004.9
DOI: https://doi.org/10.17721/1728-2292.2025/2-61/156-161

Сергій ДАНИЛЕНКО, д-р політ. наук, проф.,
ORCID ID: 0000-0003-3435-2146
e-mail: danylenko@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Жанна ПАЦЬОРА, асп.
ORCID ID: 0009-0007-5388-980X
e-mail: jpatsyora@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

"ІНФОРМАЦІЙНА ВАКЦИНА" ЯК ІНСТРУМЕНТ ПРОТИДІЇ ЗАГРОЗАМ КОГНІТИВНІЙ БЕЗПЕЦІ ЛЮДИНИ

Вступ. *У XXI столітті війни дедалі більше переміщуються у сферу свідомості людини, де дезінформація діє як "інформаційний вірус", що підриває довіру, розколює суспільства й послаблює демократію, зокрема дискредитуючи її інституції. Україна з 2014 р. стала однією із найуразливіших країн до систематичних когнітивних атак з боку Росії. Це зумовлює потребу у формуванні превентивних стратегій, за принципом подібних до біологічної імунізації. Назвемо це концепцією "інформаційної вакцини". Відповідно, мета статті – верифікувати теоретичні основи цього поняття, дослідити міжнародний досвід протидії інформаційним загрозам, де ця концепція виступає як теоретичне підґрунтя, та запропонувати підхід до побудови багаторівневої системи когнітивної безпеки людини у сучасному цифровому світі.*

Методи. *Методологічну основу становлять міждисциплінарні підходи, що охоплюють аналіз когнітивних воєн, дослідження трансформації публічної сфери як комунікативного простору, можливості використання положень концепції "м'якої сили", теорії дискурсу і влади, метафори та гіперреальності, а також вивчення діючих конфліктів та їх комунікативного виміру. Для обґрунтування превентивного підходу використано теорію інокуляції, доповнену сучасними емпіричними дослідженнями щодо "prebunking". У роботі застосовано методи контент-аналізу міжнародних звітів, а також проведено порівняльний аналіз досвіду різних країн – США, Європейського Союзу, Китаю та України у питаннях дослідження й використання когнітивних інструментів у захисті державних чи, як у випадку з ЄС, колективних інтересів.*

Результати. *Дослідження показало, що концепт "інформаційної вакцини" має потужне теоретичне обґрунтування й підтверджується емпіричними прикладами. У США ключовим викликом у цій царині стали втручання у вибори та рух QAnon, у ЄС – Brexit та формування механізмів EUvsDisinfo і Digital Services Act, у Китаї – алгоритмічне управління й використання big data. НАТО на російські гібридні впливи проти країн-членів відповіло створенням StratCom COE у Ризі як багатонаціонального центру дослідження та протидії когнітивним загрозам. В Україні після 2014 р. Росія систематично застосовує інформаційні кампанії у контексті тимчасово окупованого Криму і регіонів Донбасу, збиття російськими проксі літака рейсу MH17, вакцинації під час пандемії COVID-19, енергетичної безпеки, а після 2022 р. – для руйнування соціальної стабільності шляхом поширення зневіри у збереження незалежності України. У відповідь Україною, зокрема, створено Центр протидії дезінформації при РНБО, розгорнено програми медіаграмотності, налагоджено співпрацю з міжнародними партнерами. Запропоновано багаторівневу "модель інформаційної вакцини", яка включає індивідуальний, освітній, технологічний, локальний, регіональний, регулятивно-інституційний і міжнародний рівні, що взаємодоповнюють одне одного.*

Висновки. *Концепція "інформаційної вакцини" постає не лише як наукова метафора, а і як комплексна стратегія превентивної інформаційної безпеки. Її ключове завдання – формування стійкості людини, суспільства й держави до когнітивних атак шляхом поєднання освіти, комунікацій, технологічних інновацій і міжнародної співпраці. Вирішальним результатом є досягнення стану "колективного імунітету", коли деструктивні повідомлення не здатні спричинити системних руйнівних наслідків. Україна, з огляду на унікальний досвід протидії масштабним інформаційним атакам, може виступати лідером у розробці та впровадженні глобальної стратегії "інформаційної вакцини".*

Ключові слова: *когнітивна безпека, інформаційна вакцина, стратегічні комунікації, інформаційна стійкість, гібридні загрози, Україна, національна безпека.*

Вступ

У XXI ст. інформація остаточно перетворилася на стратегічний ресурс, що визначає не лише розвиток окремих держав, а й баланс сил у світі. Якщо у попередні епохи основою військової та політичної переваги були чисельність армії, промисловий потенціал чи науково-технічні здобутки, то сьогодні вирішальне значення має здатність впливати на свідомість, емоції та поведінку людей. Це зумовлює появу нового виміру безпеки – когнітивного, у якому боротьба точиться за інтерпретацію реальності, за контроль над наративами та формування довіри у суспільстві.

Сучасні війни дедалі більше набувають гібридного характеру, поєднуючи традиційні військові дії з інформаційними та психологічними операціями. Дезінформація, маніпуляції, пропаганда, кампанії з дискредитації інституцій і політичних лідерів – усе це стало невід'ємною частиною нових конфліктів. Як наголошує Г. Почепцов (Почепцов, 2020, с. 125), у XXI ст. війна дедалі більше переміщується у свідомість людини, де головною зброєю стають не танки й ракети, а слова, образи та символи.

Україна є одним із найпоказовіших прикладів держави, що перебуває під постійним тиском когнітивних атак. Починаючи з 2014 р., після анексії Криму та початку війни на Донбасі, Росія систематично застосовує інструменти дезінформації для підриву національної єдності, делегітимізації інституцій, поширення страху та недовіри. Після 2022 р., з початком повномасштабної агресії, ці атаки набули безпрецедентного масштабу: створювалися кампанії, спрямовані на руйнування віри у перемогу, поширення паніки через удари по енергетичній інфраструктурі, підрив довіри до союзників і міжнародної підтримки України.

Водночас проблема дезінформації не є виключно українською. Вона має глобальний характер і виявляється у різних формах всіх регіонів світу. У США – це втручання у вибори та поширення конспірологічних рухів, таких як QAnon (Сінгер, & Брукінг, 2018), у

Європейському Союзі – інформаційні кампанії довкола Brexit і спроби зовнішніх акторів вплинути на суспільну думку (EDMO, 2022), у Китаї – використання великих даних та алгоритмічного управління для формування потрібних настроїв серед населення (Кастельс, 2009). У цьому сенсі Україна є лише "передовою лінією" глобальної битви за когнітивну безпеку, але не єдиною її ареною.

Особливістю сучасних інформаційних загроз є їхня здатність підривати довіру – фундамент будь-якого демократичного суспільства. Довіра до інституцій, медіа, експертів і навіть до базових понять правди та брехні стає об'єктом системної атаки. Це створює умови для поляризації, радикалізації та розколу, що послаблює суспільства зсередини й робить їх уразливими до зовнішнього впливу. Як зазначає П. Померанцев, пропаганда діє як інфекція: вона поширюється невидимо, вражає механізми критичного мислення і створює середовище, у якому складно відрізнити реальність від вигадки (Померанцев, 2019, с. 117).

У цих умовах виникає потреба у нових підходах до захисту, які виходять за межі класичних методів протидії пропаганді чи цензури. Захист не може зводитися лише до спростування фейків – адже "потік неправди" (Пол, & Метьюз, 2016) поширюється значно швидше, ніж можливість реагувати на нього. Потрібна стратегія превентивного характеру, яка дозволила б готувати суспільство до зустрічі з інформаційними загрозами ще до їх появи. Саме такою концепцією постає "інформаційна вакцина".

Метафора "інформаційної вакцини" запозичує логіку з медицини: так само як біологічна вакцина формує імунітет проти вірусу, завчасно вводячи ослаблений його варіант, "інформаційна вакцина" передбачає підготовку суспільства до зустрічі з дезінформацією шляхом розвитку критичного мислення, підвищення медіаграмотності та формування навичок розпізнавання маніпуляцій. Це не лише метафоричне порівняння, але й цілком практичний підхід, підтверджений емпіричними дослідженнями (van der Linden et al., 2017).

Таким чином, актуальність цього дослідження визначається трьома чинниками:

1) зростанням ролі інформації як стратегічного ресурсу у XXI ст.;

2) глобальним характером когнітивних атак, які вражають різні країни світу;

3) унікальним досвідом України, яка з 2014 р. перебуває на передньому краї інформаційної війни.

Метою статті є дослідження теоретичних засад концепції інформаційної вакцини, аналіз міжнародного досвіду протидії інформаційним загрозам і розробка багаторівневої моделі когнітивної безпеки, яка може бути використана як Україною, так і міжнародною спільнотою.

Методи

Методологічну основу цього дослідження становлять міждисциплінарні підходи, що дають змогу комплексно пояснити феномен інформаційної вакцини. Інформаційна безпека й когнітивна стійкість – це явища, які неможливо розглядати лише в межах однієї дисципліни, адже вони поєднують політичні, соціальні, психологічні й технологічні виміри. Тому використання методів політології, соціології, медіазнавства, філософії та інформаційних технологій створює цілісну аналітичну рамку.

Одним із ключових підходів є аналіз феномена когнітивних воєн. Г. Почепцов зауважує, що сучасні конфлікти дедалі більше переміщуються у сферу свідомості людини, а отже, саме контроль над інтерпретаціями подій і наративами стає головним інструментом протиборства (Почепцов, 2020, с. 125). Для нашого дослідження цей підхід важливий, оскільки дозволяє визначити інформаційну вакцину як форму превентивної протидії у гібридних війнах.

Не менш важливим є розуміння трансформацій публічної сфери, Габермасом описанних (Габермас, 1991). Він підкреслює, що публічна сфера має потенціал бути простором критичної дискусії, однак у сучасних умовах цифровізації вона стає вразливою до маніпуляцій. Це дозволяє пояснити, чому ключовим завданням інформаційної вакцини є відновлення критичного потенціалу суспільного діалогу.

Концепція "м'якої сили" (Най, 2004) дає змогу розглядати інформаційні кампанії не лише як оборонний механізм, а й як інструмент привабливості, що формує позитивні наративи. У контексті інформаційної вакцини це означає, що потрібно не тільки протидіяти дезінформації, але й створювати контент, який зміцнює національну ідентичність і довіру громадян до власних інституцій.

У своїй концепції ідентичності Фукуяма (Фукуяма, 2018) доводить, що почуття гідності й визнання є ключовими у сучасному суспільстві (Фукуяма, 2018). Інформаційні атаки часто спрямовані на підрив саме цього відчуття. Для інформаційної вакцини це означає врахування психологічного аспекту: створення таких умов, у яких громадяни відчувають безпеку, належність і цінність своєї ідентичності.

Аналіз дискурсу і влади, здійснений Т. ван Дейком (van Dijk, 2008), пояснює, як мова і комунікація структурують відносини домінування. Це дозволяє зрозуміти, що дезінформація не є хаотичною, а навпаки – стратегічно вибудуваною. Відповідно, "інформаційна вакцина" має містити елементи деконструкції маніпулятивних дискурсів, навчати громадян розпізнавати їх і формувати альтернативні інтерпретації.

Теорія метафоричного мислення (Lakoff, & Johnson, 2003) показує, що метафори не лише описують реальність, а й визначають спосіб мислення суспільства. Використання метафори "інформаційної вакцини" саме по собі є елементом методології, адже дозволяє ефективно пояснювати складні явища у зрозумілих образах. Бодрійяр (Бодрійяр, 1994) у своїй теорії симулякрів і гіперреальності наголошує, що сучасні комунікаційні технології створюють середовище, у якому вигадка може видаватися реальнішою за факти. Для інформаційної вакцини це означає, що потрібно не лише боротися з неправдивими повідомленнями, а й навчати суспільство критично сприймати навіть ті повідомлення, які виглядають максимально достовірно.

Д. Бар-Тал у своїх дослідженнях (Бар-Тал, 2013) нерозв'язних конфліктів підкреслює, що інформаційні рамки здатні закріплювати образ ворога і створювати довготривалу суспільну поляризацію. Це пояснює, чому "інформаційна вакцина" має включати елементи примирення, спрямовані на зменшення впливу пропагандистських наративів, що підтримують стан конфлікту.

Теорія інокуляції (Макґвайр, 1964) стала ключовою основою для цього дослідження. Вона доводить, що для формування стійкості до маніпуляцій необхідно заздалегідь знайомити аудиторію зі спрощеними формами аргументів супротивника. Сучасні дослідження Кембриджського університету (van der Linden at al., 2017) підтверджують дієвість цього підходу: так зване "prebunking" дозволяє суспільству відкидати фейки ще до їхнього поширення.

У практичному плані використано метод контент-аналізу міжнародних звітів (Уордл & Дерахшан, 2017;

ЮНЕСКО, 2023; EDMO, 2022; NATO StratCom COE, 2020), що дало змогу систематизувати основні інформаційні загрози та засоби їх подолання. Також проведено порівняльний аналіз досвіду США, Європейського Союзу, Китаю та України. Це дозволило визначити специфічні особливості кожної країни й водночас виділити універсальні закономірності, які стали основою для побудови моделі інформаційної вакцини.

Таким чином, застосування міждисциплінарного підходу дало змогу поєднати теоретичні концепції, практичні методи й емпіричний матеріал, створивши цілісну методологічну основу для дослідження інформаційної вакцини як багаторівневої стратегії когнітивної безпеки.

Результати

Результати проведеного дослідження засвідчили, що концепція інформаційної вакцини має не лише потужне теоретичне підґрунтя, а й підтверджується конкретними емпіричними прикладами з міжнародного та українського досвіду. Її цінність полягає у здатності поєднати попередження когнітивних атак із формуванням стійкості суспільства до маніпуляцій, що дозволяє перейти від реактивної до превентивної моделі захисту.

Міжнародний досвід

У США ключовими викликами стали втручання у вибори 2016 і 2020 рр., поширення руху QAnon та масові кампанії дезінформації під час пандемії COVID-19. QAnon перетворився на глобальну конспірологічну мережу, яка через соціальні медіа поширювала радикальні наративи, що підірвали довіру до державних інституцій і традиційних медіа. Цей приклад доводить, що навіть у розвиненій демократії дезінформація може швидко поширюватися і мати серйозні наслідки для політичної стабільності. Саме тут виявилася особлива актуальність концепції "інформаційної вакцини" – замість спроб повністю блокувати чи цензурувати повідомлення, варто заздалегідь готувати громадян до розпізнавання маніпуляцій і критичного аналізу інформації.

В Європейському Союзі важливим кейсом стала кампанія навколо Brexit, у якій дезінформаційні наративи безпосередньо вплинули на стратегічний вибір мільйонів громадян. Це стало поштовхом до створення цілого ряду інституцій та ініціатив, серед яких EUvsDisinfo, Європейська обсерваторія цифрових медіа (EDMO) та ухвалення Digital Services Act. Усі ці заходи можна розглядати як елементи колективної інформаційної вакцини на рівні регіону. Особливістю європейського підходу стало поєднання нормативного регулювання з розвитком медіаграмотності, що дозволяє виробляти системну стійкість не лише на індивідуальному, а й на суспільному рівні.

Китай демонструє протилежну модель – алгоритмічне управління інформаційними потоками та використання великих даних для моніторингу настроїв населення. Така модель ґрунтується на авторитарних практиках контролю й суттєво відрізняється від демократичних підходів. Вона підтверджує, що "інформаційна вакцина" не може бути універсальною у формі, але може мати різні модифікації залежно від політичних систем. Для глобальної безпеки важливо, щоб демократичні країни виробили спільні стандарти, які б протидіяли експорту авторитарних методів управління свідомістю.

НАТО відповіло на зростання когнітивних загроз створенням у 2014 р. Центру передового досвіду зі стратегічних комунікацій у Ризі. StratCom COE став багатонаціональним майданчиком для обміну досвідом, дослідження тактик і методів дезінформації та вироблення практичних рішень. Це приклад того, як "інформаційна вакцина" може реалізовуватися на рівні міжнародної організації, забезпечуючи координацію дій між державами.

Український контекст

Для України проблема когнітивної безпеки має екзистенційний характер. Починаючи з 2014 р., Росія систематично застосовує дезінформаційні кампанії:

1) проти Криму (легітимація окупації через міфи про "історичну справедливість");

2) Донбасу (створення образу "громадянської війни");

3) катастрофи МН17 (спроби перекласти відповідальність);

4) вакцинації (поширення фейків про "біолабораторії" та "чипізацію");

5) енергетичної безпеки (маніпуляції довкола залежності від російського газу).

Після 2022 р. ці кампанії лише посилилися. Пропаганда намагається підірвати віру українців у перемогу, поширює паніку через обстріли енергетичної інфраструктури, дискредитує західну допомогу, розпалює внутрішні суперечності тощо. У відповідь було створено Центр протидії дезінформації при РНБО, розгорнено програми медіаграмотності для школярів і студентів, започатковано співпрацю з міжнародними партнерами, що можна розглядати як поступове формування елементів національної інформаційної вакцини.

Багаторівнева модель інформаційної вакцини

Результати дослідження дозволили сформулювати багаторівневу модель, яка складається з кількох взаємодоповнювальних рівнів (табл.1).

Таблиця 1

Структура інформаційної вакцини

№ з/п	Рівень моделі інформаційної вакцини	Опис
1	Рівень індивідуального імунітету	На особистісному рівні інформаційна вакцина забезпечує розвиток критичного мислення, уміння перевіряти джерела, розпізнавати маніпулятивні повідомлення та розуміти приховані комунікаційні тактики. Це формує основу індивідуальної інформаційної стійкості
2	Рівень освітнього впливу	Освіта та медіаграмотність виступають ключовим елементом. Інформаційна вакцина містить навчальні програми, тренінги та просвітницькі ініціативи, які дозволяють засвоювати "ослаблені дози" маніпулятивних прикладів, тренуючи здатність суспільства їх розпізнавати без шкоди для стабільності
3	Технологічний рівень	Сучасні цифрові технології стають інструментами для формування інформаційного імунітету. Використання алгоритмів штучного інтелекту, систем раннього попередження та аналізу великих даних дозволяє виявляти інформаційні загрози ще до їхнього масового поширення
4	Локальний рівень	Діяльність органів місцевого самоврядування, спрямована на формування довіри між владою та населенням; розвиток муніципальних ініціатив із протидії дезінформації; створення локальних центрів стратегічних комунікацій; поширення позитивних інформаційних наративів на рівні громади

Закінчення табл. 1

№ з/п	Рівень моделі інформаційної вакцини	Опис
5	Регіональний рівень	Координація діяльності органів місцевого самоврядування на рівні області; розробка регіональних стратегій протидії дезінформації; створення "хабів стійкості"; підтримка регіональних медіа та платформ; інтеграція локальних ініціатив у національні програми
6	Регулятивно-інституційний рівень	Формування гнучкої нормативної та політичної бази, що дозволяє застосовувати інформаційну вакцину в добровільному форматі через стратегії, програми та стандарти, але передбачає можливість її обов'язкового використання у критичних умовах (масовані інформаційні атаки, кризи, воєнні дії)
7	Міжнародний рівень і колективний імунітет	Ефективність інформаційної вакцини зростає, коли вона впроваджується не лише на рівні держави, але й у глобальному масштабі. Міжнародна співпраця, уніфікація стандартів і спільні протоколи реагування створюють умови для досягнення "колективного імунітету", який зменшує вплив когнітивних атак на суспільства

Порівняльний аналіз

Порівнюючи досвід України зі США та ЄС, можна дійти висновку, що українська модель має унікальну особливість: вона формується в умовах реальної війни, де ціна інформаційної поразки надзвичайно висока. Це робить український досвід більш практичним і насиченим, на відміну від західних держав, які працюють здебільшого у превентивному режимі. Саме тому Україна може стати центром вироблення нових стандартів когнітивної безпеки, що матимуть глобальне значення.

Дискусія і висновки

Концепція інформаційної вакцини, запропонована у цьому дослідженні, демонструє перехід від образного порівняння до комплексної стратегії превентивної інформаційної безпеки. У сучасному світі, де інформація стала ресурсом влади, впливу та контролю, саме здатність суспільства завчасно формувати імунітет до маніпуляцій визначає його стійкість до когнітивних атак. Досвід останніх десятиліть доводить, що інформаційні загрози вже не є локальним явищем: вони набули глобального характеру та здатні підривати демократичні інститути, формувати атмосферу недовіри та змінювати політичні процеси у різних державах.

Результати дослідження підтверджують, що "інформаційна вакцина" має міцне теоретичне підґрунтя, яке поєднує класичні й сучасні підходи. Теорія когнітивних воєн (Почепцов, 2020, с. 125) дозволяє пояснити, чому сучасні конфлікти переміщуються у сферу свідомості, а концепція трансформації публічної сфери (Габермас, 1991) демонструє вразливість демократичного дискурсу до маніпуляцій. Ідеї "м'якої сили" (Най, 2004), ідентичності (Фукуяма, 2018), дискурсивного домінування (ван Дейк, 2008), метафоричного мислення (Lakoff, & Johnson, 2003), симулякрів і гіперреальності (Бодрійяр, 1994), а також нерозв'язних конфліктів (Bar-Tal, 2013) формують багатовимірну рамку для розуміння когнітивних загроз. Теорія інокуляції (Макґвайр, 1964), підтверджена емпіричними дослідженнями Cambridge University (van der Linden at al., 2017), створює методологічну основу для практичної реалізації концепції інформаційної вакцини.

Вивчення міжнародного досвіду показало, що жодна країна світу не застрахована від дезінформаційних кампаній. США стикнулися із втручанням у вибори, поширенням конспірологічних рухів на зразок QAnon і масштабною хвилею дезінформації під час пандемії COVID-19. В Європейському Союзі одним із найяскравіших прикладів стала кампанія навколо Brexit, що підтвердила вразливість навіть розвинених демократій до маніпуляцій громадською думкою. Відповіддю стало створення інституцій EUvsDisinfo, EDMO, а також ухвалення Digital Services Act, який накладає відповідальність на цифрові платформи. Китай, у свою чергу, розвиває власну модель алгоритмічного управління, де big data та штучний інтелект використовуються для контролю настроїв населення, що ставить нові виклики для глобальної когнітивної безпеки. НАТО відреагувало створенням StratCom COE у Ризі – багатонаціонального центру, який систематизує досвід держав-членів і розробляє підходи до протидії когнітивним загрозам.

Особливе місце у цій картині посідає Україна. Із 2014 р., після анексії Криму та початку війни на Донбасі, а особливо із 2022 р. – після повномасштабного вторгнення, вона стала унікальною лабораторією для дослідження інформаційних війн. Пропагандистські кампанії проти Криму, Донбасу, катастрофи МН17, вакцинації, енергетичної безпеки та віри у перемогу показують, як багатовекторно може діяти агресор. Відповіддю стали створення Центру протидії дезінформації, масштабні програми медіаграмотності, співпраця з міжнародними організаціями тощо. Український досвід свідчить: ефективність протидії залежить не лише від державних інституцій, а й від залучення громадянського суспільства, освіти й технологічних інновацій.

Запропонована модель інформаційної вакцини має багаторівневу структуру. На індивідуальному рівні – це розвиток критичного мислення та навичок перевірки фактів. На освітньому – впровадження системної медіаграмотності у школах і університетах. Технологічний рівень передбачає використання штучного інтелекту, алгоритмів раннього попередження й автоматизованих систем моніторингу. Локальний рівень включає участь органів місцевого самоврядування у розробці стратегій комунікаційної безпеки. Регіональний рівень передбачає узгодженість між різними регіонами України та транскордонну взаємодію із сусідніми державами. Регулятивно-інституційний рівень полягає у створенні законодавчих і нормативних аспектів, що унеможливлюють поширення деструктивних наративів. Міжнародний рівень спрямований на інтеграцію зусиль у рамках НАТО, ЄС, ООН та інших організацій. У сукупності ці рівні створюють ефект "колективного імунітету", коли навіть сильні деструктивні атаки не здатні спричинити системних руйнівних наслідків.

У стратегічній перспективі когнітивна безпека стане одним із ключових елементів національної безпеки, нарівні з військовою та енергетичною складовою. Світ уже сьогодні стикається з викликами, які визначатимуть майбутнє: поширення штучного інтелекту, здатного генерувати реалістичні deepfake-відео; розвиток алгоритмів, що формують інформаційні "бульбашки" і поляризують суспільство; зростання впливу транснаціональних цифрових корпорацій на політичні процеси. Це означає, що майбутні стратегії мають бути адаптивними, гнучкими та заснованими на міжнародній співпраці.

Для України стратегічний прогноз є подвійним. З одного боку, вона залишається найвразливішою державою до інформаційних атак, що зумовлено тривалою війною. З іншого боку, саме цей унікальний досвід робить її природним лідером у розробці нових стандартів когнітивної безпеки. Україна може виступати генератором інноваційних рішень – від створення освітніх програм до впровадження технологічних інструментів виявлення дезінформації. Її досвід може стати основою для формування глобальних практик, які поширюватимуться на інші держави.

У майбутньому "інформаційна вакцина" має розвиватися у трьох головних напрямах. Перший – це поглиблення освіти й медіаграмотності, що забезпечить формування покоління, стійкого до маніпуляцій. Другий – розвиток технологій штучного інтелекту й аналітичних систем, здатних виявляти дезінформацію в режимі реального часу. Третій – посилення міжнародної координації, що дозволить об'єднувати ресурси та створювати єдині стандарти.

Отже, "інформаційна вакцина" є не лише метафорою, а й практичним інструментом формування когнітивної стійкості. Її стратегічне значення полягає в тому, що вона дозволяє перейти від реактивної до превентивної моделі захисту. У майбутньому саме ті суспільства, які першими інтегрують таку стратегію, здобудуть перевагу у глобальній конкуренції. Україна, яка вже сьогодні перебуває на передньому краї боротьби з дезінформацією, має всі підстави стати не лише об'єктом атак, а й суб'єктом формування нової архітектури когнітивної безпеки у XXI ст. Її досвід може служити дороговказом для інших держав, які прагнуть досягти стану інформаційного "колективного імунітету" і забезпечити стабільність демократичного розвитку.

Внесок авторів: Сергій Даниленко – участь у підготовці матеріалів, технічна підтримка, консультаційний внесок. Жанна Пацьора – концептуалізація, ідея та розробка дослідження, методологія, написання й редагування.

Джерела фінансування. Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

Список використаних джерел

Бар-Тал, Д. (2013). *Нерозв'язні конфлікти: соціально-психологічні основи та динаміка*. Кембриджський університет.

Бодрійяр, Ж. (1994). *Симулякри і симуляція*. Університет Мічиган Прес.

ван Дейк Т. А. (2008). *Дискурс і влада*. Палгрейв Макміллан.

ван дер Лінден, *С.,* Левандовскі, С., Екер, У., ван Бавел, Дж., Чепмен, Дж., Кук, Дж., Фінкель, Е., & Ренд, Д. (2017). *Prebunking: превентивне пояснення маніпулятивних тактик.* Кембридж.

Габермас, Ю. (1991). *Структурні перетворення публічної сфери*. MIT Press.

Європейська обсерваторія цифрових медіа. (2022). *Щорічний звіт 2022*. EDMO.

Кастельс, М. (2009). *Влада комунікації*. Видавництво Оксфордського університету.

Лакофф, Дж., & Джонсон, М. (2023). *Метафори, якими ми живемо*. Університет Чикаго Прес.

Макґвайр, В. (1964). Індукування опору переконанню: сучасні підходи. *Advances in Experimental Social Psychology*, 1, 191–229.

Най, Дж. *М'яка сила: засоби досягнення успіху у світовій політиці*. Паблік Афферс, 2004.

Почепцов, Г. Г. (2020). *Когнітивні війни та нові виміри інформаційної безпеки*. Вид. дім "Києво–Могилянська академія".

Померанцев, П. (2019). *Це не пропаганда: пригоди у війні проти реальності*. Фабер і Фабер.

Пол, К., & Метьюз, М. (2016). *Російська "пожежна брандспойт" модель пропаганди*. RAND.

Сінгер, П., & Брукінг, Е. (2018). *Like War: мілітаризація соціальних медіа*. Готон Міффлін Харкорд.

Уордл, К., & Дерахшан, Х. (2017). *Інформаційний безлад: до міждисциплінарної рамки для досліджень і формування політики*. Звіт Ради Європи.

Фукуяма, Ф. (2018). *Ідентичність: прагнення до гідності та політика образи*. Фаррар, Страус і Жиру.

Центр передового досвіду НАТО зі стратегічних комунікацій. (2020). *Когнітивна війна.*

UNESCO. (2023). *Guidelines for Regulating Digital Platforms.*

Reference

Bar-Tal, D. (2013). *Intractable Conflicts: Socio-Psychological Foundations and Dynamics*. Cambridge University Press.

Baudrillard, J. (1994). *Simulacra and Simulation*. University of Michigan Press.

Castells, M. (2009). *Communication Power*. Oxford University Press.

European Digital Media Observatory (EDMO). (2022). *Annual Report 2022*. EDMO.

Fukuyama, F. (2018). *Identity: The Demand for Dignity and the Politics of Resentment*. Farrar, Straus and Giroux.

Habermas, J. (1991(. *The Structural Transformation of the Public Sphere*. MIT Press.

Lakoff, G., & Johnson, M. (2003). *Metaphors We Live By*. University of Chicago Press.

McGuire, W. J. (1964). Inducing resistance to persuasion: Some contemporary approaches. *Advances in Experimental Social Psychology*, 1, pp. 191–229.

NATO StratCom COE. (2020). *Cognitive Warfare*. Riga: NATO Strategic Communications Centre of Excellence.

Nye, J.S. (2004). *Soft Power: The Means to Success in World Politics*. Public Affairs.

Paul, C., & Matthews, M. (2016). *The Russian "Firehose of Falsehood" Propaganda Model*. RAND Corporation.

Pocheptsov, G.G. (2020). *Cognitive Wars and New Dimensions of Information Security*. Kyiv-Mohyla Academy Publishing House.

Pomerantsev, P. (2019). *This is Not Propaganda: Adventures in the War Against Reality*. Faber & Faber.

Singer, P.W., & Brooking, E.T. (2018). *LikeWar: The Weaponization of Social Media*. Houghton Mifflin Harcourt.

UNESCO. (2023). *Guidelines for Regulating Digital Platforms*. UNESCO.

van Dijk, T.A. (2008). *Discourse and Power*. Palgrave Macmillan.

van der Linden, S., Levandovsky, S., Eker, U., van Bavel, J. J., Chapman, J., Cook, J., Finkel, E., & Rand, D. (2017). *Prebunking: A Preventive Explanation of Manipulative Tactics*. Cambridge.

Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Council of Europe.

Отримано редакцією журналу / Received: 09.10.25
Прорецензовано / Revised: 22.10.25
Схвалено до друку / Accepted: 23.12.25

Serhiy DANYLENKO, DSc (Polit.), Prof.
ORCID ID: 0000-0003-3435-2146
e-mail: danylenko@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Zhanna PATSORA, PhD Student
ORCID ID: 0009-0007-5388-980X
e-mail: jpatsyora@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

"INFORMATION VACCINE" AS A TOOL FOR COUNTERING THREATS TO HUMAN COGNITIVE TO SECURITY

Background. ***In the 21st century, wars are increasingly shifting into the realm of human consciousness, where disinformation acts as an "information virus" that undermines trust, divides societies, and weakens democracy, in particular by discrediting its institutions. Since 2014, Ukraine has become one of the most vulnerable countries to systematic cognitive attacks from Russia. This necessitates the development of preventive strategies, based on principles similar to biological immunization. We call this the concept of an "information vaccine." Accordingly, the purpose of the***

article is to verify the theoretical foundations of this concept, to examine international experience in countering information threats where this concept serves as a theoretical basis, and to propose an approach to building a multilevel system of human cognitive security in the modern digital world.

Methods. ***The methodological basis consists of interdisciplinary approaches encompassing the analysis of cognitive wars, the study of the transformation of the public sphere as a communicative space, the application of the concept of "soft power," theories of discourse and power, metaphor and hyperreality, as well as the study of ongoing conflicts and their communicative dimensions. To substantiate the preventive approach, the inoculation theory is applied, complemented by modern empirical research on "prebunking." The study employs content analysis of international reports, as well as a comparative analysis of the experiences of various countries – the United States, the European Union, China, and Ukraine – in the study and application of cognitive instruments for the protection of state or, as in the case of the EU, collective interests.***

Results. ***The study has shown that the concept of the "information vaccine" has a strong theoretical foundation and is supported by empirical examples. In the United States, the key challenges in this domain have been election interference and the QAnon movement; in the EU – Brexit and the development of mechanisms such as EUvsDisinfo and the Digital Services Act; in China – algorithmic governance and the use of big data. NATO has responded to Russian hybrid influence against member states by creating the StratCom COE in Riga as a multinational center for research and countering cognitive threats. In Ukraine, since 2014 Russia has systematically carried out information campaigns regarding the temporarily occupied Crimea and the Donbas regions, the downing of flight MH17 by Russian proxies, vaccination during the COVID-19 pandemic, and energy security; after 2022, these campaigns have aimed to undermine social stability by spreading doubts about Ukraine's ability to preserve its independence. In response, Ukraine has established the Center for Countering Disinformation under the National Security and Defense Council, launched media literacy programs, and developed cooperation with international partners. The study proposes a multilevel "information vaccine model" that includes individual, educational, technological, local, regional, regulatory–institutional, and international levels, which complement one another.***

Conclusions. ***The concept of the "information vaccine" emerges not only as a scientific metaphor but also as a comprehensive strategy of preventive information security. Its key objective is to build the resilience of individuals, society, and the state against cognitive attacks through the combination of education, communications, technological innovation, and international cooperation. The decisive outcome is the achievement of a state of "collective immunity," where destructive messages are unable to cause systemic and devastating consequences. Given its unique experience in countering large-scale information attacks, Ukraine can act as a leader in the development and implementation of a global "information vaccine" strategy.***

Keywords: ***cognitive security, information vaccine, strategic communications, information resilience, hybrid threats, Ukraine, national security.***

Автор заявляє про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The author declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.