УДК 351.862:004.738.5(477)

А. П. Лелеченко,
д. держ. упр., професор,
професор кафедри публічного управління та адміністрування,
Державний університет "Київський авіаційний інститут"
ORCID: https://orcid.org/0000-0002-0850-3724
О. І. Кравченко,
аспірант кафедри публічного управління та адміністрування,
Державний університет "Київський авіаційний інститут"
ORCID ID: https://orcid.org/0009-0006-0759-6830

DOI: 10.32702/2306-6814.2025.15.298

ЗАХИСТ ДЕРЖАВНОГО СУВЕРЕНІТЕТУ ЧЕРЕЗ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ВИКЛИКАМИ

A. Lelechenko,
Doctor of Science in Public Administration, Professor, Professor of the Department of Public Management and Administration, The State University "Kyiv Aviation Institute"
O. Kravchenko,
Postgraduate student of the Department of Public Management and Administration, The State University "Kyiv Aviation Institute"

PROTECTION OF STATE SOVEREIGNTY THROUGH THE MANAGEMENT OF INFORMATION CHALLENGES

У статті досліджено теоретичні та практичні аспекти захисту державного суверенітету через управління інформаційними викликами в умовах сучасних гібридних конфліктів і цифрової трансформації суспільства та визначено напрями удосконалення національної політики в сфері інформаційного захисту. Встановлено, що весь комплекс сучасних інформаційних загроз: дезінформаційні кампанії, штучний інтелект, sleeper-боти і їх алгоритмічний вплив формує багатовимірний інформаційний фронт, який чинить системний тиск на політичні інститути, суспільну єдність і державну безпеку. Відтак, сучасні інформаційні загрози є складними, багатокомпонентними та динамічними. Вони становлять не лише технологічну, а й політичну та цивілізаційну проблему, яка потребує системного наукового осмислення та стратегічної відповіді як з боку держави, так і суспільства.

Обгрунтовано, що ці інформаційні загрози значно впливають на політичну стабільність, суспільну єдність та інституційну довіру. Узагальнено основні характеристики політичного, культурно-психологічного та безпекового векторів інформаційного впливу, їхні інструменти та наслідки для функціонування держави. Доведено, що синергія політичного, культурно-психологічного та безпекового векторів інформаційного впливу призводить до процесу "розмивання суверенітету", унаслідок якого держава втрачає здатність підтримувати контроль над інформаційним простором і формувати цілісну систему комунікації, спрямовану на зміцнення національної ідентичності та легітимності інститутів влади. Встановлено, що для ефективної протидії цим викликам необхідний комплексний міждисциплінарний підхід, що включає правове

врегулювання, розвиток інституційної спроможності державних органів, впровадження технологічних інструментів кіберзахисту, формування стратегічних комунікацій і підвищення рівня медіаграмотності населення. Наголошено на необхідності розробки цілісної державної стратегії, яка дозволить забезпечити баланс між свободою слова та захистом інформаційного суверенітету, а також підкреслено важливість активізації міжнародної співпраці у сфері кібербезпеки. Окреслено перспективи подальших наукових досліджень у напрямі створення адаптивних алгоритмів для виявлення дезінформації, аналізу впливу інформаційних загроз на політичні процеси та розвитку нових моделей інформаційної безпеки в цифрову епоху.

This article explores the theoretical and practical aspects of protecting state sovereignty through the management of information challenges amid modern hybrid conflicts and the digital transformation of society. It outlines directions for improving national policy in the field of information security. The study establishes that the entire spectrum of modern information threats-disinformation campaigns, artificial intelligence, sleeper bots, and their algorithmic influence-creates a multidimensional information front that exerts systemic pressure on political institutions, social cohesion, and national security. These threats are complex, multilayered, and dynamic, posing not only technological but also political and civilizational challenges that require systematic academic analysis and a strategic response from both the state and society.

It is substantiated that such information threats significantly undermine political stability, societal unity, and institutional trust. The article systematizes the key characteristics of political, cultural-psychological, and security-related vectors of information influence, along with their tools and consequences for state functioning. It is proven that the synergy of these vectors leads to a "sovereignty erosion" process, in which the state loses its ability to control the information space and to maintain a coherent system of communication aimed at reinforcing national identity and institutional legitimacy.

The study concludes that an effective response to these challenges requires a comprehensive interdisciplinary approach that includes legal regulation, institutional capacity-building, implementation of cyber defense technologies, development of strategic communications, and enhancement of media literacy. The importance of developing an integrated state strategy that ensures a balance between freedom of expression and the protection of information sovereignty is emphasized, along with the need to strengthen international cooperation in the field of cybersecurity. Prospects for further research include the development of adaptive algorithms for disinformation detection, analysis of the impact of information threats on political processes, and the design of new models of information security in the digital age.

Ключові слова: державний суверенітет, інформаційні виклики, інформаційна зброя, гібридна війна, дезінформація, стратегічні комунікації, кіберзагрози, інформаційна безпека, медіаграмотність, інституційна стійкість. транснаціональні комунікації, цифрова трансформація, штучний інтелект.

Key words: state sovereignty, information challenges, information weapons, hybrid warfare, disinformation, strategic communications, cyber threats, information security, media literacy, institutional resilience. transnational communications, digital transformation, artificial intelligence.

У сучасному світі, де інформація стала стратегічним ресурсом, питання захисту державного суверенітету набуває нових форм і значень. Традиційні інструменти безпеки більше не є достатніми для протидії загрозам, що виникають унаслідок поширення дезінформації, інформаційних маніпуляцій, кібератак та втручання у внутрішні справи держав через інформаційний простір. Формування так званої "інформаційної зброї" трансформувало спосіб ведення конфліктів, у яких руйнівна сила не обмежується фізичними діями, а активно проникає у сферу свідомості, політичних процесів, інституційної довіри та національної єдності.

Особливої актуальності це питання набуває для держав, які знаходяться у стані протидії зовнішній аг-

ресії або переживають внутрішні трансформації. У таких умовах ефективне управління інформаційними викликами є запорукою збереження національного суверенітету, територіальної цілісності та демократичних засад.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Інформаційні виклики становлять комплексну загрозу для державного суверенітету, впливаючи не лише на систему безпеки, а й на політичні, економічні, соціокультурні та інституційні аспекти функціонування держави. В умовах гібридних війн, транснаціональних комунікацій та цифрової трансформації, держави опиняються перед необхідністю вироблення дієвих стратегій реагування на ворожі інформаційні впливи. Водночас наукове осмислення цих процесів залишається фрагментарним, що ускладнює формування системної політики інформаційної безпеки.

Проблема управління інформаційними викликами як чинника захисту суверенітету лежить на перетині таких галузей знань, як публічне управління, безпекознавство, інформаційна політика. Її вирішення потребує міждисциплінарного підходу та чіткого визначення механізмів державної відповіді на інформаційні загрози. У цьому контексті особливої ваги набуває вивчення ефективних інструментів інформаційного управління, аналіз міжнародного досвіду, удосконалення національного законодавства та розвиток інституційної спроможності державних органів до протидії інформаційним загрозам. Таким чином, дослідження механізмів управління інформаційними викликами в контексті забезпечення державного суверенітету є не лише науково важливим, але й стратегічно необхідним завданням публічного управління в XXI столітті.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблематика захисту державного суверенітету в умовах інформаційних викликів активно розробляється у сучасному науковому дискурсі. Зокрема, С. Люлько визначає концепт інформаційного суверенітету як здатність держави контролювати інформаційний простір і формувати незалежну політику в інтересах національної безпеки [2]. Н. Млінац [3], В. Мазурчик, Д. Лі та А. Влахос [4] аналізують новітні форми дезінформації, включно з "дезінформацією 2.0", що генерується штучним інтелектом. Д. Доші та І. Новачич [5] розкривають механізм sleeper-ботів, які непомітно впливають на аудиторію; Р. Карр і П. Кьолер [6] характеризують таргетинг на основі поведінкових патернів користувачів. К. Огнянова, Д. Лазер, Р. Робертсон і К. Вілсон [7] доводять зв'язок між впливом фейків і ерозією довіри до медіа. М. Стелла [9] вказує на роль ботів у поширенні деструктивного контенту. М. Гупта і Д. Денегі [10] наголошують на впливі політичних поглядів і культурних цінностей на сприйняття дезінформації. У вітчизняному контексті, окрім зазначених теоретичних розробок, актуальними залишаються законодавчі ініціативи України у сфері нацбезпеки та кіберзахисту [11—13], однак потребують подальшої адаптації до нових викликів.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Метою статті є комплексне дослідження механізмів управління інформаційними викликами як ключового чинника захисту державного суверенітету в умовах сучасних гібридних загроз та визначити напрями удосконалення національної політики в сфері інформаційного захисту.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

У сучасних умовах захист державного суверенітету набуває багатовимірного характеру, в якому дедалі більшу роль відіграють нематеріальні чинники, зокрема інформаційні потоки, технології комунікації, цифрова присутність держави та її спроможність реагувати на виклики інформаційного середовища. Ефективне управління такими викликами неможливе без грунтовного розуміння їхньої природи, джерел, форм прояву та механізмів впливу на ключові сфери життєдіяльності держави.

У XXI столітті, на тлі цифрової трансформації, глобалізації комунікацій та загострення гібридних конфліктів, інформаційні загрози стали системною проблемою, що безпосередньо впливає на стан національного суверенітету. Україна, яка вже понад десятиліття є мішенню цілеспрямованих інформаційних атак з боку зовнішнього агресора, стала прикладом перетворення інформаційного простору на арену гібридної війни. Прогноз Центру протидії дезінформації при РНБО України (далі — ЦПД) на першу половину липня 2025 року свідчить, що сучасні інформаційні атаки відзначаються зростаючою системністю, комплексністю та ефективністю. Їхньою головною метою є делегітимізація державної влади, формування в суспільстві настроїв безпорадності, розчарування, недовіри до офіційної інформації, що в результаті підриває політичну суб'єктність держави у власному інформаційному середовищі [1].

Ці процеси зумовили появу в науковому дискурсі концепту інформаційного суверенітету, який трактується як здатність держави захищати та контролювати свій інформаційний простір, формувати незалежну комунікаційну політику, забезпечувати національні інтереси в умовах глобальної цифрової взаємодії. Зокрема, С. Люлько визначає інформаційний суверенітет як "стан політико-правової, технологічної та інституційної спроможності держави управляти процесами створення, поширення та захисту інформації відповідно до національних інтересів" [2]. Це визначення надає важливу методологічну основу для оцінки спроможності держави реагувати на інформаційні виклики в умовах гібридної війни та транснаціональних ризиків.

У межах зазначеної парадигми найбільш загрозливими видами інформаційного впливу залишаються масштабні дезінформаційні кампанії. Як зазначено у згаданому прогнозі ЦПД, ці кампанії реалізуються за до-

помогою скоординованого використання псевдоекспертів, симульованих аналітичних матеріалів та маніпулятивних форматів інформації, що створюють ілюзію об'єктивності. Це сприяє формуванню у суспільстві альтернативної інформаційної реальності та знеціненню офіційного наративу.

Другим виміром загроз є кібернетичні атаки, які поєднують як класичні форми злому систем (атаки на критичну інфраструктуру, витоки персональних даних), так і інноваційні механізми, засновані на застосуванні штучного інтелекту, бот-мереж, діпфейків та алгоритмічного таргетингу.

У науковому дослідженні Н. Млінаца, присвяченому гібридному інтелекту як носію дезінформації у кіберпросторі, показано, що сучасні алгоритми аналізують політичні вподобання користувачів, що дозволяє здійснювати цільові атаки з високим рівнем персоналізації. Це значно ускладнює процес верифікації джерел і відстеження шкідливого контенту, а отже — і державну протидію [3].

Подальшу еволюцію цієї загрози досліджують В.Мазурчик, Д.Лі, А.Влахос у праці "Disinformation 2.0 in the Age of AI", у якій розкривається феномен так званої "дезінформації 2.0" [4]. На думку авторів, нова генерація фейкових повідомлень, згенерованих штучним інтелектом, є найбільш витонченою, масовою і здатною обходити класичні механізми фільтрації вмісту в соціальних мережах. У цьому контексті держава стикається з викликом, коли швидкість і складність атак перевищує здатність інституцій вчасно на них реагувати.

Також дослідники ідентифікували появу новітніх загроз: "sleeper social bots", тобто AI-агентів, які здатні діяти непомітно тривалий час, створюючи довіру серед аудиторії, а згодом активізуватися для інформаційної атаки. Експеримент, проведений дослідниками з Університету Південної Каліфорнії, продемонстрував, що навіть підготовлені користувачі (зокрема студенти) не можуть розпізнати таких ботів, коли ті ведуть тривалі дискусії або виступають "лідерами думок" [5].

Водночас, як показує аналітична доповідь Мюнхенської безпекової конференції (2024), розробка та використання алгоритмічного таргетування на основі поведінкових патернів користувачів призводить до так званої "праймеризації аудиторії". Відтак, атаки адаптуються не лише до демографічних чи політичних ознак, а й до когнітивних та емоційних станів конкретного користувача [6]. У результаті, інформаційна агресія набуває форми тонкого, прихованого тиску, що значно ускладнює її розпізнавання і протидію.

Очевидно, що весь комплекс сучасних інформаційних загроз: дезінформаційні кампанії, штучний інтелект, sleeper-боти і їх алгоритмічний вплив формує багатовимірний інформаційний фронт, який чинить системний тиск на політичні інститути, суспільну єдність і державну безпеку. Вони не лише трансформують природу інформаційної війни, а й висувають безпрецедентні виклики до моделі національного управління інформаційною сферою. Відтак, сучасні інформаційні загрози є складними, багатокомпонентними та динамічними. Вони становлять не лише технологічну, а й політичну та цивілізаційну проблему, яка потребує системного науково-го осмислення та стратегічної відповіді з боку держави й суспільства. Від здатності ефективно реагувати на ці виклики залежить не лише збереження інформаційного суверенітету, а й реальна стійкість держави у протистоянні гібридній агресії.

У сучасному інформаційному середовищі виклики, пов'язані з інформаційною безпекою, набули критичного значення, оскільки здатні впливати не лише на зовнішньополітичну ситуацію, але й на внутрішню стабільність, легітимність публічної влади та єдність суспільства. Інформаційні загрози мають багатовекторний характер, проникаючи в політичну, соціальну та безпекову сфери держави. Вони трансформують суспільну свідомість, знижують рівень довіри до інституцій, дестабілізують політичну ситуацію та підривають національну єдність. Такий вплив відбувається не через відкрите силове втручання, а через систематичний і нав'язливий інформаційний тиск, який поступово розмиває основи державності зсередини.

Одним із головних векторів впливу інформаційних загроз є підрив політичної стабільності, що проявляється в ерозії легітимності влади, делегітимізації публічних інституцій та маніпуляції демократичними процесами. Особливо небезпечними є інформаційні атаки, спрямовані на створення атмосфери недовіри до урядових структур, підрив авторитету політичного керівництва та вплив на результати виборів шляхом поширення фейкових повідомлень, спотворених наративів або підтасованих фактів.

Значну увагу цьому аспекту приділяє дослідження американських вчених: К. Огнянової, Д. Лазера, Рональд Е. Робертсона, Ч. Вілсона. У роботі "Дезінформація в дії: поширення фейкових новин пов'язане з нижчою довірою до ЗМІ та вищою довірою до уряду, коли ваша сторона при владі" (Misinformation in action: Fake news exposure is linked to lower trust in media, higher trust in government when your side is in power) автори на основі масштабного емпіричного аналізу доводять, що контакт із фейковими новинами призводить до зниження довіри до незалежних ЗМІ, водночас підвищуючи довіру до уряду — якщо цей уряд відповідає політичним симпатіям реципієнта [7]. Такий ефект, з одного боку, посилює підтримку певних політичних сил, а з іншого, підриває загальну довіру до інформаційної системи в суспільстві, створюючи небезпечне середовище для маніпуляцій, у якому факти втрачають цінність, а інформація сприймається крізь призму політичної лояльності.

У контексті цифрового поширення дезінформації важливу роль відіграють боти як автоматизовані цифрові агенти, які масово ретранслюють контент у соціальних мережах. У дослідженні М.Стелла з групою вчених "Боти збільшують кількість негативного та провокаційного контенту в онлайн-соціальних системах" (Bots increase exposure to negative and inflammatory content in online social systems) на прикладі мережевого аналізу Twitter, автори показують, що боти активно сприяють поширенню негативно забарвленого, емоційно деструктивного та конфліктного контенту. Їхня діяльність змінює топологію інформаційних потоків, збільшуючи "видимість" радикальних повідомлень і, відповідно,

Таблиця 1. Основні характеристики векторів інформаційного впливу, їхні інструменти та наслідки для функціонування держави

Вектор впливу	Основні характеристики	Інструменти впливу	Основні наслідки для державного суверенітету
Політичний	Делегітимізація влади, маніпуляції виборами	Фейки, дезінформація, таргетовані кампанії	Підрив політичної стабільності, ерозія легітимності влади
Культурно-психологічний	Формування альтернативних цінностей, поляризація суспільства	Пропаганда, соціальні мережі, бот-мережі	Розкол суспільства, зниження довіри, поширення радикалізму
Безпековий	Кібератаки, інформаційна диверсія	Кіберзлочини, AI-боти, алгоритмічний таргетинг	Порушення роботи інституцій, загроза критичній інфраструктур

Джерело: складено автором.

формуючи когнітивно поляризоване інформаційне середовище [8]. Це особливо загрозливо для демократичних процесів, де настрої громадськості можуть бути штучно радикалізовані, створюючи передумови для дестабілізації виборів, протестних рухів або делегітимізації політичної опозиції.

Не менш важливою є культурно-психологічна складова сприйняття інформації. У міждисциплінарному дослідженні М. Гупта та Д. Деннехі "Достовірність фейкових новин: вплив політичних переконань та пропагованих культурних цінностей" (Fake news believability: The effects of political beliefs and espoused cultural values) вивчається вплив індивідуальних цінностей і політичних переконань на сприйняття фейкових новин. Автори використовують теорію культурних вимірів та дані опитувань, аби показати: особи з високим рівнем колективізму, схильністю до уникнення невизначеності та консервативною ідентичністю, демонструють підвищену довіру до неправдивої інформації, якщо вона відповідає їхній ідеологічній картині світу [9]. Вказане засвідчує, що дезінформація не лише вводить в оману, а й глибоко вкорінюється у свідомість, стаючи частиною культурно-політичної ідентичності громадян.

З безпекової точки зору інформаційні атаки, що поєднуються з кібератаками, створюють нову форму гібридних загроз. Інструменталізація штучного інтелекту дозволяє формувати персоналізовані дезінформаційні кампанії, активувати так званих sleeper-ботів як цифрових агентів, які слугують для психологічної диверсії або деморалізації цивільного населення. Додаткова складність виникає через алгоритмічне таргетування, що адаптує контент під індивідуальні поведінкові патерни, роблячи атаки більш точними та непомітними, як показано у звіті Мюнхенської безпекової конференції [6].

Таким чином, багатовимірна природа інформаційних викликів безпосередньо формує інформаційний простір та визначає ступінь захищеності державного суверенітету. Коли вектори політичного, культурно-психологічного та безпекового впливів взаємодіють, виникає потужна синергія загроз: кожна кампанія підсилює іншу. Це і є ядром процесу "розмивання суверенітету", держава втрачає здатність підтримувати єдиний інформаційний простір, контролювати достовірність, формувати національний наратив та забезпечувати легітимність інститутів. Інформаційна війна в цьому контексті стає не лише технологічною проблемою, а й кризою цивілізаційної моделі, що ставить під загрозу саму здатність держави виступати суб'єктом міжнародних відносин.

У таблиці 1 узагальнено основні характеристики політичного, культурно-психологічного та безпекового векторів інформаційного впливу, їхні інструменти та наслідки для функціонування держави.

Таким чином, сучасні інформаційні атаки мають багатошаровий характер: технологічна складова (бот-мережі, таргетинг), комунікативна (фейки, маніпулятивні наративи) та соціокультурна (цінності, переконання) формують цілісну екосистему впливу, здатну розхитати основи легітимності політичної влади. Це ставить перед державами принципово нові виклики, зокрема, потребу розробки стратегій захисту від когнітивного та емоційного впливу інформаційних операцій, які стають ключовим інструментом сучасної гібридної агресії.

Для протидії таким викликам потрібен синтез інструментів: технологічних (моніторинг, підвищення медіаграмотності), правових (регулювання платформ), непередбачуваних комунікацій (фактчекінг, прозорість), а також міжнародної співпраці. Необхідним є формування чіткої стратегії реагування, яке має базуватися на системному підході, що включає правове регулювання, інституційну спроможність державних структур, застосування сучасних технологій кіберзахисту, розвиток стратегічних комунікацій і підвищення рівня медіаграмотності населення.

Правова база є основою для побудови системи національної інформаційної безпеки. В умовах гібридних загроз держави повинні забезпечити чітке визначення понять, зон відповідальності та процедур реагування на інформаційні атаки. Національне законодавство має охоплювати не лише питання захисту інформаційної інфраструктури, а й забезпечення балансу між свободою слова та інформаційною безпекою.

В Україні діють такі базові документи, як закони України "Про національну безпеку" [10], "Про основні засади забезпечення кібербезпеки України" [11]; Стратегія інформаційної безпеки [12], а також низка підзаконних актів. Однак, у багатьох випадках актуальним

залишається питання адаптації законодавства до нових форм загроз, які стрімко еволюціонують у цифровому середовищі. Наприклад, необхідним є правове врегулювання діяльності платформ соціальних мереж, механізмів протидії дезінформації, а також процедур взаємодії державних органів із приватним сектором у сфері кіберзахисту. Крім того, важливим є гармонізація національного законодавства з європейськими та міжнародними стандартами, зокрема у межах виконання Україною зобов'язань щодо інтеграції до ЄС.

Ефективне реагування на інформаційні загрози потребує не лише нормативного забезпечення, а й наявності дієвих організаційних механізмів. У цьому контексті вирішальну роль відіграють профільні державні органи (Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації, Центр стратегічних комунікацій та ін.), які здійснюють безперервний моніторинг інформаційного середовища, виявляють загрози та координують дії у разі інформаційних атак.

Серед ключових технологічних рішень ? побудова національних систем раннього виявлення дезінформації, створення системи кіберзахисту критичної інфраструктури, використання систем штучного інтелекту для виявлення бот-мереж і маніпулятивного контенту. Також зростає значення співпраці держави з провайдерами інтернет-послуг, медіа-платформами та великими технологічними компаніями у питанні швидкого реагування на поширення шкідливого контенту. Організаційні заходи також передбачають регулярні тренінги, розробку протоколів взаємодії між органами влади, а також міждержавну координацію в межах міжнародних ініціатив з кібербезпеки.

Стратегічні комунікації є не лише інструментом реагування на зовнішні інформаційні атаки, а й засобом формування стійкості суспільства до маніпуляцій. Ефективна державна інформаційна політика має передбачати проактивне формування наративів, інституційну присутність у публічному просторі, цілеспрямоване інформування населення у кризові періоди, а також розбудову довіри до офіційних джерел.

Не менш важливим є розвиток медіаграмотності громадян як елементу "соціального імунітету" до дезінформації. Інформаційна стійкість суспільства базується на здатності громадян критично оцінювати джерела, розрізняти факти й маніпуляції, а також усвідомлювати ризики, пов'язані з участю в інформаційних кампаніях. У цьому напрямі держава має інвестувати в освітні програми, інтеграцію медіаграмотності в шкільну та університетську освіту, а також підтримку ініціатив громадянського суспільства.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У сучасному безпековому середовищі, де інформація стала інструментом впливу та засобом ведення гібридної війни, управління інформаційними викликами є критично важливим елементом забезпечення державного суверенітету. Інформаційні атаки, дезінформаційні кампанії, використання бот-мереж, таргетованих наративів і штучного інтелекту створюють багатовекторний тиск на ключові інститути держави, підриваючи легітимність влади, політичну стабільність, суспільну згуртованість і довіру до демократичних процедур. Особливу загрозу становить ефект "розмивання суверенітету", коли без застосування фізичної сили відбувається трансформація інформаційного середовища в інструмент внутрішньої дестабілізації.

Ефективне реагування на ці загрози потребує міждисциплінарного підходу, що охоплює правове врегулювання, розвиток інституційної спроможності, впровадження технологічних рішень з кіберзахисту та стратегічних комунікацій, а також формування інформаційної культури в суспільстві. Особливо важливим є забезпечення балансу між свободою слова і необхідністю захисту від інформаційної агресії, а також адаптація законодавства до новітніх форм загроз. У цьому контексті стратегія захисту інформаційного суверенітету має включати проактивне формування національного наративу, підтримку довіри до офіційних джерел, посилення міжнародної співпраці у сфері кібербезпеки та просування медіаграмотності як елемента соціального імунітету.

Перспективи подальших наукових розвідок у цьому напрямі передбачають вивчення механізмів формування інформаційної стійкості держави, аналіз моделей стратегічних комунікацій у кризових умовах, розробку адаптивних алгоритмів виявлення фейків на базі штучного інтелекту, а також оцінку впливу інформаційних загроз на електоральну поведінку, інституційну довіру та соціальну згуртованість. Не менш актуальним є дослідження можливостей інтеграції механізмів цифрової дипломатії, кібербезпеки та інформаційної політики в єдину систему реагування на гібридні виклики. Крім того, потребує подальшого концептуального опрацювання проблема інформаційного суверенітету, що може стати основою нової парадигми публічного управління у цифрову епоху.

Література:

1. Прогноз Центру щодо інформаційних загроз на першу половину липня 2025 року. URL: https://cpd.gov.ua/international-direction/yevropa/prognoz-czentru-shhodo-informaczijnyh-zagroz-na-pershu-polovynu-lypnya-2025-roku/

2. С.Люлько. Інформаційний суверенітет держави: сутнісні характеристики. URL: https://www.researchgate.net/publication/393146287_INFORMACIJNIJ_-SUVERENITET_DERZAVI_SUTNISNI_HARAKTERISTIKI

3. Nikola Mlinac. Hybrid Intelligence as a Carrier of Disinformation and Hybrid Threats in Cyberspace. URL: https://www.nsf-journal.hr/nsf-volumes/focus/id/1521

4. Wojciech Mazurczyk, Dongwon Lee, Andreas Vlachos. Disinformation 2.0 in the Age of AI: A Cybersecurity Perspective. Communications of the ACM. Volume 67, Number 3 (2024), Pages 36—39. URL: https://dl.acm.org/doi/fullHtml/10.1145/3624721

5. Jaiiv Doshi, Ines Novacic and others. Sleeper Social Bots: a new generation of AI disinformation bots are already a political threat. URL: https://arxiv.org/abs/2408.12603

6. Randolf Carr, Paula K?hler. AI-pocalypse Now? Disinformation, AI, and the Super Election Year. https://

securityconference.org/en/publications/analyses/ai-pocalypse-disinformation-super-election-year

7. K.Ognyanova, D.Lazer, Ronald E. Robertson, C.Wilson. Misinformation in action: Fake news exposure is linked to lower trust in media, higher trust in government when your side is in power. URL: https://misinforeview.hks.harvard.edu/article/misinformation-in-action-fake-news-exposure-is-linked-to-lower-trust-in-media-higher-trust-in-government-when-your-side-is-in-power/

8. Massimo Stella ets. Bots increase exposure to negative and inflammatory content in online social systems. Proceedings of the National Academy of Sciences. URL: https://www.researchgate.net/publication/329079116_Bots_increase_exposure_to_negative_and_inflammatory_content_in_online_social_systems

9. Manjul Gupta, Denis Dennehy. Fake news believability: The effects of political beliefs and espoused cultural values. Information & Management. 2023. URL: https://www.sciencedirect.com/science/article/pii/S0378720622001537

10. Про національну безпеку України: закон України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

11. Про основні засади забезпечення кібербезпеки України: закон України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

12. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України №685/2021. URL: https://www.president.gov.ua/documents/6852021-41069

References:

1. Center for Countering Disinformation (2025), "Forecast of the Center on information threats for the first half of July 2025", Available at: https://cpd.gov.ua/international-direction/yevropa/prognoz-czentru-shhodo-informaczijnyh-zagroz-na-pershu-polovynu-lypnya-2025-roku/ (Accessed: 15 March 2025).

2. Liulko, S. (2025), "Informational sovereignty of the state: essential characteristics", Available at: https://www.researchgate.net/publication/393146287_INFORMACIJNIJ_SUVERENITET_DERZAVI_-SUTNISNI_HARAKTERISTIKI (February: 18 March 2025).

3. Mlinac, N. (2024), "Hybrid Intelligence as a Carrier of Disinformation and Hybrid Threats in Cyberspace", National Security and the Future, Available at: https://www.nsf-journal.hr/nsf-volumes/focus/id/1521 (Accessed: 25 April 2025).

4. Mazurczyk, W., Lee, D. and Vlachos, A. (2024), "Disinformation 2.0 in the Age of AI: A Cybersecurity Perspective", Communications of the ACM, Vol. 67, No. 3, pp. 36—39, Available at: https://dl.acm.org/doi/fullHtml/10.1145/3624721 (Accessed: 22 May 2025).

5. Doshi, J. and Novacic, I. (2024), "Sleeper Social Bots: A New Generation of AI Disinformation Bots Are Already a Political Threat", Available at: https://arxiv.org/abs/2408.12603 (Accessed: 15 February 2025).

6. Carr, R. and K?hler, P. (2024), "AI-pocalypse Now? Disinformation, AI, and the Super Election Year", Available at: https://securityconference.org/en/publications/analyses/ai-pocalypse-disinformation-super-election-year (Accessed: 3 April 2025).

7. Ognyanova, K., Lazer, D., Robertson, R.E. and Wilson, C. (2020), "Misinformation in Action: Fake News Exposure Is Linked to Lower Trust in Media, Higher Trust in Government When Your Side Is in Power", Harvard Kennedy School Misinformation Review, Available at: https://misinforeview.hks.harvard.edu/article/misinformation-in-action-fake-news-exposure-is-linked-to-lower-trust-in-media-higher-trust-in-government-when-your-side-is-in-power/ (Accessed: 11 March 2025).

8. Stella, M. (2018), "Bots Increase Exposure to Negative and Inflammatory Content in Online Social Systems", Proceedings of the National Academy of Sciences, Available at: https://www.researchgate.net/publication/329079116_Bots_increase_exposure_to_negative_and_inflammatory_content_in_online_social_systems (Accessed: 14 April 2025).

9. Gupta, M. and Dennehy, D. (2023), "Fake News Believability: The Effects of Political Beliefs and Espoused Cultural Values", Information & Management, Available at: https://www.sciencedirect.com/science/article/pii/S0378720622001537 (Accessed: 17 May 2025).

10. Verkhovna Rada of Ukraine (2018), Law of Ukraine "On National Security of Ukraine ", Available at: https://zakon.rada.gov.ua/laws/show/2469-19#Text (Accessed: 5 March 2025).

11. Verkhovna Rada of Ukraine (2017), Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity in Ukraine", Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text (Accessed: 4 March 2025).

12. President of Ukraine (2021), Decree "On the Decision of the National Security and Defense Council of Ukraine of October 15, 2021 "On the Information Security", Available at: https://www.president.gov.ua/documents/6852021-41069 (Accessed: 10 May 2025).

Стаття надійшла до редакції 09.07.2025 р.