DOI: https://doi.org/10.26565/1992-2337-2024-2-22
УДК 351.862.1:007

Хряпинський Антон Петрович,
кандидат юридичних наук,
директор ТОВ «Хряпинський і компанія»,
вулиця Ахсарова, 4/6 А, 61051, м. Харків, Україна,
e-mail: polifil1@ukr.net https://orcid.org/0000-0002-2492-051X

ПЕРСПЕКТИВНІ НАПРЯМИ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ДЛЯ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

Анотація. У статті комплексно досліджено актуальні виклики гібридних загроз для інформаційної безпеки держави та обґрунтовано перспективні напрями вдосконалення інформаційної політики для протидії цим загрозам в умовах динамічних геополітичних трансформацій та стрімкого розвитку цифрових технологій. На основі аналізу сучасних наукових концепцій розкрито сутність та характерні особливості гібридних впливів у інформаційній сфері, які базуються на синергетичному поєднанні традиційних методів пропаганди і дезінформації з інноваційними маніпулятивними технологіями та прихованими формами втручання з метою дестабілізації суспільства, управління масовою свідомістю та підриву довіри до інститутів влади.

Автором ґрунтовно проаналізовано ключові вразливості вітчизняного інформаційного простору до гібридних загроз, зокрема наголошено на проблемах низького рівня медіаграмотності значної частини населення, значного поширення в українському медіа-середовищі російських дезінформаційних наративів та фейків антиукраїнського спрямування, інституційної слабкості та недостатньої скоординованості дій органів державної влади у сфері стратегічних комунікацій та забезпечення інформаційної безпеки. Значну увагу приділено розгляду зовнішнього контексту інформаційної війни проти України, пов'язаного з геополітичним позиціонуванням нашої держави на перехресті інтересів різних центрів сили, які активно застосовують інструменти інформаційно-психологічного впливу для реалізації власних цілей.

На основі систематизації та критичного осмислення передового зарубіжного досвіду у сфері протидії гібридним загрозам засобами інформаційної політики визначено ключові пріоритети розвитку відповідного інструментарію в Україні. Зокрема, особливий акцент зроблено на доцільності розбудови комплексної системи медіаосвіти та підвищення цифрової грамотності громадян на основі кращих європейських практик, посилення інституційної спроможності у сфері стратегічних комунікацій шляхом створення спеціалізованих підрозділів з аналізу дезінформації та розвінчування фейків, налагодження дієвого партнерства держави з провідними соціальними мережами та Інтернет-платформами з метою обмеження поширення деструктивного контенту, а також зміцнення інформаційної взаємодії влади з громадянським суспільством для підвищення довіри до офіційних джерел.

Як цитувати: Хряпинський А. П. Перспективні напрями інформаційної політики для протидії гібридним загрозам. *Державне будівництво.* 2024. № 2 (36). С. 322–334. DOI: https://doi.org/10.26565/1992-2337-2024-2-22

In cites: Khriapynskyi, A.P. (2024). Perspective directions of information policy for countering hybrid threats. *State Formation, no. 2 (36), 322–334.* DOI: https://doi.org/10.26565/1992-2337-2024-2-22 [in Ukrainian].

Аргументовано важливість реалізації проактивної інформаційної політики, спрямованої на формування позитивного порядку денного та утвердження національних наративів, що ґрунтуються на демократичних цінностях та національних інтересах України.

Обґрунтовано, що ефективність протидії гібридним загрозам в інформаційній сфері залежить не лише від застосування адекватного тактичного інструментарію, а й від реалізації системних демократичних реформ, орієнтованих на підвищення інклюзивності, прозорості та підзвітності державного управління. Лише органічне поєднання стратегії розвитку інформаційної політики з практичними кроками, спрямованими на зміцнення національної ідентичності, консолідацію суспільства навколо спільного бачення майбутнього та розвиток громадянської активності здатне забезпечити потрібний рівень стійкості до інформаційних операцій агресора. Водночас підкреслюється потреба у подальших комплексних дослідженнях інноваційних форм та методів протидії гібридним атакам в умовах турбулентності світового розвитку з урахуванням унікальної природи українського контексту.

Ключові слова: публічне управління, інформаційна політика, гібридні загрози, дезінформація, стратегічні комунікації, медіаграмотність, стійкість суспільства.

Постановка проблеми. В умовах динамічного розвитку інформаційно-комунікаційних технологій та загострення геополітичної конкуренції між ключовими центрами сили питання забезпечення інформаційної безпеки перетворилося на одне з найбільш пріоритетних завдань національних урядів. Стрімка цифровізація всіх сфер суспільного життя, з одного боку, відкрила безпрецедентні можливості для розширення доступу громадян до інформації, розвитку електронної демократії та зміцнення механізмів політичної участі, а з іншого – створила сприятливий ґрунт для реалізації гібридних стратегій недружніх держав, спрямованих на дестабілізацію ситуації в країнах-мішенях шляхом деструктивного інформаційно-психологічного впливу.

Гібридні загрози в інформаційній сфері, які поєднують використання традиційних методів пропаганди, дезінформації та маніпулювання з інноваційними технологіями соціальної інженерії, фактчекінгу і BigData, стали потужним інструментом геополітичного протиборства в епоху постправди. Їх деструктивний вплив на індивідуальну та масову свідомість призводить до ерозії раціональних основ суспільного дискурсу, загострення ціннісних конфліктів та зростання соціальної напруженості. За таких умов цілеспрямовані інформаційні операції зовнішніх гравців здатні послабити державні інститути, підірвати довіру громадян до влади та дестабілізувати ситуацію в країні без застосування засобів збройного втручання.

Особливо вразливими до гібридних інформаційних атак є транзитивні демократії пострадянського простору, які одночасно переживають болісні процеси політичної та соціокультурної трансформації. В умовах слабкості демократичних інститутів, відсутності усталених традицій політичної культури та наявності чисельних соціальних розколів ці країни стають легкою здобиччю для реалізації підривних стратегій зовнішніх центрів впливу. Ця теза повною мірою стосується України, яка з 2014 р. є об’єктом масштабної інформаційної агресії з боку РФ, що розгортається як на тактичному рівні (поширення антиукраїнських фейків, тиражування проросійських наративів і меседжів в

медіапросторі), так і на стратегічному (формування негативного іміджу України у світі, розмивання ідентичності та цінностей українського суспільства).

Окрім зовнішніх викликів, вітчизняний інформаційний простір характеризується низкою внутрішніх факторів вразливості до гібридних загроз. Серед них варто відзначити недостатній рівень медіаграмотності значної частини населення, обмежені можливості держави щодо регулювання контенту в цифровому середовищі, непрозорість медіавласності та редакційної політики багатьох ЗМІ, відсутність усталеної системи фактчекінгу та верифікації інформації. В результаті дезінформація та маніпулятивний контент безперешкодно поширюються не лише в сегменті соціальних медіа, але й у професійних засобах масової інформації, які мали б слугувати надійним джерелом об'єктивних даних для громадян.

Аналіз останніх досліджень і публікацій. Проблематика гібридних загроз та шляхів протидії їм перебуває у фокусі уваги багатьох зарубіжних дослідників. Зокрема, концептуальні засади гібридної війни та її вплив на безпекове середовище розкрито у працях Hoffman F., Lanoszka A., Renz B. Особливості гібридних впливів у інформаційній сфері та інструменти протидії дезінформації проаналізовано у публікаціях Hellman M., Wagnsson C., Paul C., Matthews M., Pomerantsev P. Досвід Європейського Союзу щодо розбудови стійкості до гібридних загроз висвітлено у роботах Annala M., Fiott D., Parkes R.

В українському науковому дискурсі проблеми гібридної війни та інформаційної безпеки розглянуто у працях Горбуліна В., Власюка О., Кононенка С., Дубова Д., Саєнка О. та ін. Разом з тим, комплексні дослідження перспективних напрямів інформаційної політики для протидії гібридним загрозам в Україні з урахуванням передового світового досвіду поки що представлені недостатньо.

Мета статті полягає у визначенні пріоритетних напрямів трансформації інформаційної політики України для підвищення стійкості держави та суспільства до гібридних загроз крізь призму провідного зарубіжного досвіду.

Застосована методологія і методи. Для вирішення поставлених завдань використано комплекс загальнонаукових і спеціальних методів, зокрема: аналіз, синтез, порівняння, систематизацію, узагальнення. Метод концептуального аналізу застосовано для розкриття сутності гібридних загроз. Методи системного та контекстуального аналізу дозволили комплексно дослідити слабкі місця національного інформаційного простору України. Компаративний метод використано для порівняння зарубіжних практик протидії гібридним загрозам. Методи логічного узагальнення та стратегічного планування було покладено в основу розробки рекомендацій щодо удосконалення інформаційної політики.

Виклад основного матеріалу. Гібридний характер сучасних конфліктів та протистоянь суттєво підвищує роль інформаційно-психологічних впливів у досягненні політичних та військових цілей. Інформаційна зброя стає потужним інструментом дестабілізації держав, підриву їхньої обороноздатності та управлінських спроможностей без застосування звичайних засобів збройної боротьби [10, с. 10]. При цьому гібридні загрози в інформаційній сфері мають

низку характерних особливостей, які дозволяють розглядати їх як інноваційну форму геополітичного протиборства в цифрову епоху.

Перш за все, гібридні впливи спираються на комплексне та синхронізоване використання широкого спектру інформаційних інструментів – від традиційної пропаганди та дезінформації до складних маніпулятивних технологій соціальної інженерії та кібератак [6, с. 2]. Водночас, ключову роль у їх реалізації часто відіграють не державні, а недержавні актори (proxy-групи), що забезпечує агресору необхідне алібі та можливість заперечення своєї причетності.

По-друге, через стрімкий розвиток інформаційно-комунікаційних технологій та платформ (Інтернет, соціальні мережі, месенджери) гібридні загрози набули безпрецедентних масштабів охоплення і глибини проникнення в інформаційний простір держав-мішеней. Це створює практично необмежені можливості для пропагандистського навіювання, психологічного тиску, керованого емоційного «зараження» масової цільової аудиторії [5, с. 37].

По-третє, значна частина гібридних операцій здійснюється приховано і поступово, протягом тривалого часу, що дозволяє уникнути рішучого силового реагування на них з боку державних органів. Водночас навіть очевидні факти дезінформації та пропаганди важко кваліфікувати як акти агресії в юридичній площині, тобто відповісти на них в рамках чинної нормативно-правової бази [12, с. 87].

По-четверте, гібридні впливи мають системний і цілеспрямований характер, орієнтуючись на найбільш значущі больові точки і соціокультурні розколи суспільств-мішеней. Вони живлять існуючі соціальні протиріччя і суперечності, протиставляють одні групи населення іншим, сприяють десуверенізації держав через підрив довіри до влади та інституційного стрижня [4, с. 76]. Водночас форми гібридних загроз постійно еволюціонують та адаптуються до контрзаходів, що вживаються для протидії їм.

Аналіз вітчизняної практики свідчить, що інформаційний простір України має суттєві вразливості до системних гібридних впливів з боку РФ. По-перше, значна частина українських громадян досі сприйнятлива до російської пропаганди через спільне історичне минуле, родинні зв’язки та вплив російських медіа. За даними соцопитувань, кожен п’ятий українець вважає, що основним джерелом інформації про події в країні та світі для нього є російське телебачення [11, с. 25].

По-друге, значне поширення отримали російські дезінформаційні наративи та фейки, спрямовані на формування негативного іміджу України у світі і всередині країни. Дослідження показують, що з початку російської агресії на Донбасі у 2014 р. в українському сегменті інтернету було зафіксовано понад 18 тис. дезінформаційних повідомлень, які охопили понад 200 млн користувачів [7, с. 14]. При цьому до 70% дезінформаційного контенту містить антиукраїнську, антизахідну та проросійську пропаганду.

По-третє, Україна перебуває на перехресті геополітичних інтересів різних зовнішніх гравців, які використовують інформаційно-психологічні операції для

просування своїх цілей. Так, відомі випадки втручання РФ у виборчі процеси в Україні через соціальні мережі, а також намагання дискредитації євроінтеграційного та євроатлантичного курсу країни [2, с. 104]. Крім того, Україна неодноразово зазнавала масованих кібератак на державні інформаційні ресурси та об'єкти критичної інфраструктури, ймовірним організатором яких є РФ.

По-четверте, існують суттєві проблеми інституційного характеру, пов'язані з недостатньою координацією дій різних державних органів у сфері протидії гібридним загрозам. Бракує стратегічного планування, єдиного центру прийняття рішень, оперативного реагування та ефективної взаємодії в системі інформаційної безпеки [3, с. 185]. У результаті заходи з протидії носять фрагментарний і реактивний характер, не завжди базуються на глибокій аналітиці та достовірних даних.

Узагальнення зарубіжного досвіду свідчить, що провідні країни Заходу напрацювали потужний інструментарій протидії гібридним загрозам, який може бути адаптований до українських реалій. Зокрема, в Європейському Союзі розроблено цілісну Спільну рамку протидії гібридним загрозам, яка передбачає низку стратегічних напрямів – від підвищення ситуаційної обізнаності та зміцнення стійкості критичної інфраструктури до розвитку партнерства з НАТО та третіми країнами [8, с. 9]. Ключова роль у цій системі відводиться розбудові медіаграмотності населення, формуванню культури безпеки та стійкості до дезінформації, а також ефективній стратегічній комунікації.

Доцільно виділити такі елементи найкращих європейських практик, які можуть слугувати орієнтирами для удосконалення інформаційної політики України:

1. Розвиток комплексної системи медіаосвіти та цифрової грамотності громадян. У Фінляндії, наприклад, медіаграмотність інтегрована в усі рівні освіти – від дошкільної до вищої, а також реалізуються спеціальні програми підвищення критичного мислення і стійкості до дезінформації для дорослого населення [9, с. 23]. Такий підхід сприяє формуванню свідомих та освічених споживачів інформації, здатних ідентифікувати фейки та маніпуляції.

2. Посилення інституційної спроможності у сфері стратегічних комунікацій. У багатьох країнах ЄС (Великобританія, Німеччина, Литва та ін.) створено спеціальні підрозділи, які займаються аналізом дезінформаційних кампаній, розвінчуванням фейків та просуванням альтернативних наративів [5, с. 41]. Важливим напрямом їх роботи є також налагодження діалогу з суспільством та громадянськими ініціативами задля підвищення довіри до офіційних повідомлень.

3. Налагодження ефективного державно-приватного партнерства з соціальними мережами та Інтернет-платформами. Зокрема, в ЄС створено Кодекс практики протидії дезінформації, до якого долучилися такі компанії як Facebook, Google, Twitter, Microsoft тощо [6, с. 6]. Вони зобов'язалися видаляти фейкові облікові записи, маркувати політичну рекламу, блокувати монетизацію дезінформаційних ресурсів та ін.

4. Реалізація проактивної інформаційної політики, спрямованої на формування позитивного порядку денного та зміцнення національної ідентичності. Замість реактивного реагування на дезінформаційні атаки, провідні країни використовують наступальні інформаційні стратегії, які дозволяють домінувати в інформаційному просторі та ефективно доносити власні наративи й цінності до цільової аудиторії [7, с. 19].

5. Інвестування в розвиток технологічних рішень для протидії гібридним загрозам в інформаційній сфері. Наприклад, в ЄС запущено платформу EUvsDisinfo, яка в автоматичному режимі відстежує та спростовує дезінформацію, пов'язану з євроінтеграційною тематикою [8, с. 14]. Також розробляються інноваційні алгоритми на основі штучного інтелекту для верифікації контенту в соцмережах.

Суттєву роль у підвищенні стійкості українського суспільства до гібридних загроз відіграє розвиток інформаційної культури та підвищення рівня обізнаності громадян щодо механізмів, форм та інструментів деструктивного інформаційного впливу. Недостатня медіаграмотність значної частини населення, нездатність критично сприймати та аналізувати інформацію з різних джерел створюють сприятливий ґрунт для реалізації масштабних дезінформаційних кампаній та поширення фейкових наративів. Відтак, надзвичайно важливо розбудовувати системну роботу з медіаосвіти та формування навичок критичного мислення на всіх рівнях – від молодшої школи до освіти дорослих. Державна інформаційна політика у цій сфері має спрямовуватися на стимулювання запровадження окремих освітніх курсів з медіаграмотності у закладах середньої та вищої освіти, підтримку громадських ініціатив і проєктів з підвищення інформаційної культури різних соціальних груп, розгортання широкої роз'яснювальної роботи щодо викликів гібридної війни та особливостей маніпулятивних технологій.

Поряд з розвитком медіаграмотності громадян, важливим завданням є також посилення стійкості національної медіасфери до проникнення дезінформації та шкідливого контенту. Йдеться, зокрема, про необхідність запровадження ефективних механізмів саморегулювання медіаіндустрії на основі принципів професійної етики, редакційної незалежності та дотримання стандартів якісної журналістики. Провідну роль у цих процесах мають відігравати медійні громадські організації та професійні об'єднання, здатні напрацювати консенсусні правила та процедури для захисту інформаційного простору. Водночас держава повинна створювати сприятливе регуляторне середовище для діяльності відповідальних медіа, забезпечувати рівні умови доступу до інформації та підтримувати ініціативи, спрямовані на підвищення якості контенту і дотримання етичних стандартів.

Ключовою умовою ефективної протидії інформаційним атакам в цифрову епоху є налагодження тісної взаємодії держави з глобальними технологічними компаніями та соціальними платформами, які фактично монополізували віртуальний медіапростір. Хоча провайдери цифрових послуг зазвичай

позиціонують себе як нейтральні майданчики, що не несуть відповідальності за генерований користувачами контент, в умовах загострення гібридних загроз вони повинні демонструвати більшу проактивність і залученість до захисту інтересів держав. У цьому контексті важливо віднаходити розумний баланс між свободою слова в Інтернеті та практичними кроками з модерації шкідливого контенту, блокування фейкових акаунтів, обмеження таргетованої дезінформації тощо. Держава має стимулювати глобальні технологічні компанії до більшої прозорості їх алгоритмів, посилення контролю за політичною рекламою та забезпечення транспарентності користувацьких даних.

Вагомий потенціал для підвищення стійкості суспільства до гібридних загроз має розвиток незалежних аналітичних центрів та експертних мереж, які здатні оперативно виявляти та спростовувати дезінформацію, здійснювати стратегічний аналіз актуальних викликів та надавати рекомендації щодо адекватних заходів реагування. В Україні вже напрацьовано позитивний досвід функціонування таких організацій, як «StopFake», «Інститут масової інформації», «Детектор медіа», «Інтерньюз-Україна» та ін., які займаються системним моніторингом інформаційного середовища, верифікацією фактів, викриттям фейків і маніпуляцій. Водночас держава має більшою мірою використовувати експертний потенціал аналітичних інституцій для формування та реалізації інформаційної політики, зокрема шляхом залучення фахівців до розробки стратегічних документів, реалізації цільових проектів та програм, проведення нав чальних заходів для публічних службовців.

Особливу увагу слід приділяти розвитку наукових досліджень у сфері інформаційної безпеки та протидії гібридним загрозам. Попри існування окремих наукових шкіл та напрацювань вітчизняних учених, проблематика інформаційного протиборства в умовах «сірої зони» поки не отримала належного концептуального осмислення. Бракує комплексних міждисциплінарних досліджень, які б поєднували теоретичні та емпіричні підходи, враховували специфіку українського контексту та пропонували інноваційні рішення на основі передового світового досвіду. Відтак, існує потреба у формуванні цілісних дослідницьких програм на базі провідних університетів та наукових установ, стимулюванні прикладних розробок, активізації грантової підтримки відповідних проектів та ініціатив.

Велике значення має посилення інституційної спроможності держави у сфері стратегічних комунікацій, що передбачає розбудову цілісної та скоординованої системи взаємодії органів влади з цільовими аудиторіями. Йдеться про необхідність формування у структурі ключових міністерств і відомств спеціалізованих підрозділів, відповідальних за аналіз інформаційного середовища, планування та реалізацію узгоджених комунікативних кампаній, спрямованих на роз’яснення та просування офіційної позиції. При цьому стратегічні комунікації мають будуватися не лише на вертикальних зв’язках «влада-суспільство», а й стимулювати горизонтальну взаємодію між різними державними інституціями, місцевим самоврядуванням, бізнесом,

громадськістю навколо вирішення спільних безпекових завдань. Особливу роль відіграє синхронізація меседжів та координація зусиль усіх комунікаторів у протидії ворожим інформаційним кампаніям.

Ще одним важливим аспектом є зміцнення кібербезпеки як невід'ємного компоненту інформаційної стійкості держави. В умовах гібридної війни деструктивні інформаційні впливи часто супроводжуються кібератаками на об'єкти критичної інфраструктури, державні реєстри, бази даних тощо. Відтак, здатність своєчасно виявляти та нейтралізувати кіберзагрози набуває критичного значення для захисту суверенітету та обороноздатності країни. Це вимагає розробки проактивних стратегій кібероборони, інвестування у сучасні технології захисту інформації, посилення координації між профільними відомствами, налагодження тісного партнерства з приватним сектором у форматі обміну даними про загрози та кращими практиками реагування на інциденти.

Надзвичайно важливим напрямом діяльності є розвінчування фейків та дезінформації, які становлять основу гібридних інформаційних атак. Окрім зусиль державних органів та громадських ініціатив, спрямованих на викриття маніпулятивних меседжів, необхідно розбудовувати культуру критичного споживання інформації серед широких верств населення. Користувачі медіа повинні мати базові навички перевірки даних, вміти розпізнавати ознаки фейкових повідомлень, розуміти природу маніпулятивних технологій. Лише поєднання інституційної роботи з фактчекінгом та розвитком медіаграмотності громадян здатне мінімізувати руйнівний вплив дезінформації на суспільну свідомість та процеси вироблення політичних рішень.

Значну увагу слід приділяти розробці позитивного стратегічного наративу України, який би чітко артикулював національні цінності, пріоритети розвитку та принципи взаємодії з зовнішнім світом. В умовах інформаційної війни вкрай важливо формувати власний порядок денний, що ґрунтується на ствердженні української ідентичності, просуванні європейського та євроатлантичного вибору, захисті національних інтересів на міжнародній арені. Такий підхід дозволяє мінімізувати ефект ворожих інформаційних кампаній, які прагнуть нав'язати Україні чужі наративи та змусити грати за правилами агресора. Натомість послідовне обстоювання власних смислів та інтерпретацій є запорукою збереження стратегічної суб'єктності держави в гібридному протистоянні.

Протидія деструктивним інформаційним впливам вимагає зміцнення механізмів демократичної участі та розширення можливостей громадянського суспільства. Що більш інклюзивними та підзвітними є процеси вироблення державної політики, то важче маніпулювати громадською думкою та дестабілізувати ситуацію ззовні. Відтак, розвиток електронної демократії, забезпечення доступу до публічної інформації, налагодження системних комунікацій влади з населенням не лише сприяють ефективному урядуванню, але й виступають дієвими запобіжниками проти гібридних атак. У цьому контексті особливо важливо підтримувати громадські медіапроекти, спрямовані на підвищення прозорості влади, боротьбу з корупцією та дезінформацією.

Потужним інструментом протидії ворожим інформаційним кампаніям є розвиток якісної журналістики, орієнтованої на відстоювання суспільних інтересів та цінностей демократії. В умовах інформаційної війни професійні та етичні ЗМІ здатні чинити опір поширенню фейків та маніпуляцій, забезпечувати громадян збалансованою та достовірною інформацією, викривати приховані впливи та зловживання з боку можновладців. Для цього необхідно зміцнювати редакційну незалежність медіа, стимулювати дотримання професійних стандартів, розвивати економічні моделі, що дозволяють мінімізувати залежність ЗМІ від політичних та бізнесових груп впливу. Держава має створювати сприятливе регуляторне середовище для розвитку якісних медіа, забезпечуючи прозорі та рівні правила гри на медіаринку.

Успішність протидії гібридній агресії багато в чому залежить від здатності мобілізувати суспільство навколо спільних цінностей та змістів. Особливо важливу роль у цих процесах відіграє національна еліта – інтелектуальні та моральні авторитети країни, які через власну активну громадянську позицію задають тренди суспільного дискурсу. Їхні голоси мають бути добре чутними в медіапросторі, а меседжі – спрямованими на консолідацію соціуму, зміцнення державницьких засад, просування реформ та цивілізаційного вибору України. Натомість багато представників вітчизняного істеблішменту досі відтворюють шкідливі наративи «русского міра», що лише посилює вразливість до інформаційних атак агресора. Відтак, назріла потреба в оновленні національної еліти, яка має стати локомотивом кардинальних змін у державі та запорукою інформаційної стійкості українства.

У цілому, для реалізації зазначених вище напрямів інформаційної політики для протидії гібридним загрозам в українську практику доцільно здійснити таку низку першочергових кроків у напрямі розвитку інформаційної політики:

1. Розробити та затвердити на законодавчому рівні Стратегію інформаційної безпеки України, яка закріпить ключові пріоритети та механізми протидії гібридним загрозам з урахуванням актуальних викликів і передового світового досвіду.

2. Створити міжвідомчий координаційний орган (Центр протидії дезінформації) із залученням представників силових структур, медіаспільноти та експертного середовища для забезпечення оперативного реагування на інформаційні атаки та реалізації стратегічних комунікацій.

3. Запровадити комплексну систему медіаосвіти у закладах формальної та неформальної освіти, яка охоплюватиме різні цільові аудиторії та ґрунтуватиметься на кращих європейських практиках розвитку медіаграмотності і критичного мислення громадян.

4. Налагодити регулярний діалог та співпрацю з провідними соціальними мережами та Інтернет-платформами щодо протидії поширенню дезінформації та шкідливого контенту, втіленню в життя положень Кодексу практики ЄС.

5. Започаткувати цільові програми підтримки незалежних ЗМІ, розслідувальної журналістики та фактчекінгових ініціатив, які відіграють важливу роль у викритті гібридних впливів та просуванні достовірної інформації.

Висновки з даного дослідження і перспективи подальших досліджень. Підсумовуючи, слід наголосити, що розвиток та імплементація ефективної інформаційної політики є ключовою умовою зміцнення стійкості Української держави та суспільства до гібридних загроз, які становлять екзистенційний виклик національній безпеці в умовах цифрової епохи. Агресивне застосування інформаційної зброї з боку РФ кидає серйозний виклик збереженню суверенітету та територіальної цілісності України, сталому функціонуванню її демократичних інститутів. Щоб мінімізувати деструктивні впливи, державна інформаційна політика має вибудовуватися на принципах системності, адаптивності та багаторівневості, охоплюючи широкий спектр напрямків – від розвитку медіаграмотності населення та посилення інституційної спроможності у сфері стратегічних комунікацій до налагодження партнерства з громадянським суспільством та соціальними платформами.

Важливо усвідомлювати, що в умовах гібридної війни саме інформація та когнітивна сфера стають головним полем битви за уми і серця людей. Перемогу в цьому протистоянні здобуде той, хто зможе ефективніше мобілізувати власне суспільство навколо певного світоглядного проекту, змусити його повірити у спільне майбутнє та об'єднатися заради його реалізації. Відтак Україні вкрай необхідно сформувати привабливий та консолідуючий національний наратив, який би чітко артикулював її цивілізаційну суб'єктність, прагнення до свободи і демократії, готовність обстоювати власну ідентичність у протиборстві з неоімперськими зазіханнями Кремля. Саме змістовне наповнення інформаційної політики, її ідейне ядро, а не суто технологічні аспекти мають вирішальне значення для забезпечення стійкості держави в умовах гібридних загроз.

При цьому варто чітко усвідомлювати, що ефективність інформаційної політики не може розглядатися у відриві від загального контексту системних внутрішніх реформ, покликаних модернізувати країну на засадах належного врядування, верховенства права та інклюзивного розвитку. Лише послідовна розбудова сильних державних інститутів, здатних забезпечувати якісні публічні послуги, гарантувати безпеку громадян та стимулювати сталий суспільний поступ, здатна створити запас міцності, необхідний для протистояння гібридній агресії ззовні. В цьому сенсі удосконалення інформаційної політики та розвиток демократії є двома взаємопов'язаними та взаємодоповнюваними процесами, які потребують комплексного підходу з боку держави та активного залучення структур громадянського суспільства.

Подальші дослідницькі зусилля доцільно спрямувати на вироблення галузевих інформаційних стратегій у таких сферах як оборона, зовнішня політика, економічна безпека, які враховуватимуть специфічні особливості та потреби кожної царини державної політики. Не менш важливим завданням є опрацювання та апробація релевантної системи індикаторів та критеріїв

оцінювання ефективності заходів інформаційної політики з протидії гібридним загрозам, яка б дозволила відслідковувати прогрес та оперативно коригувати обрані механізми у разі потреби. Актуальною також видається проблематика синхронізації національних підходів у сфері захисту інформаційного простору з практиками країн ЄС та НАТО, що сприятиме зміцненню колективної стійкості демократичних держав у протиборстві з гібридними викликами сучасності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Patrikarakos D. War in 140 characters: How social media is reshaping conflict in the twenty-first century. New York: Basic Books, 2017. 320 p.
2. Hoffman F. Examining complex forms of conflict: Gray zone and hybrid challenges. *PRISM*. 2018. Vol. 7. No. 4. P. 30–47. URL: https://cco.ndu.edu/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/ (last accessed: 26.10.2024).
3. Lanoszka A. Russian hybrid warfare and extended deterrence in eastern Europe. *International Affairs*. 2016. Vol. 92. No. 1. P. 175–195. DOI: https://doi.org/10.1111/1468-2346.12509
4. Renz B. Russia and 'hybrid warfare'. *Contemporary Politics*. 2016. Vol. 22. No. 3. P. 283–300. DOI: https://doi.org/10.1080/13569775.2016.1201316
5. Hellman M., Wagnsson C. How can European states respond to Russian information warfare? An analytical framework. *European Security*. 2017. Vol. 26. No. 2. P. 153–170. DOI: https://doi.org/10.1080/09662839.2017.1294162
6. Paul C., Matthews M. The Russian "firehose of falsehood" propaganda model. Santa Monica, CA: RAND Corporation, 2016. 16 p. URL: https://www.rand.org/pubs/perspectives/PE198.html (last accessed: 26.10.2024).
7. Pomerantsev P. How to beat the Kremlin's propaganda machine. *World Affairs*. 2015. Vol. 177. No. 6. P. 36–42. URL: https://www.jstor.org/stable/43555279 (last accessed: 26.10.2024).
8. Annala M. Responding to hybrid threats: The EU's resilience agenda. *CSS Analyses in Security Policy*. 2018. No. 233. P. 1–4. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse233-EN.pdf (last accessed: 26.10.2024).
9. Fiott D., Parkes R. Protecting Europe: The EU's response to hybrid threats. Paris: EUISS, 2019. 66 p. URL: https://www.iss.europa.eu/content/protecting-europe-eus-response-hybrid-threats (last accessed: 26.10.2024).
10. Горбулін В. П., Власюк О. С., Кононенко С. В. Світова гібридна війна: український фронт: монографія / за заг. ред. В. П. Горбуліна. К.: НІСД, 2017. 496 с.
11. Дубов Д. В. Стратегічні комунікації: проблеми концептуалізації та практичної реалізації. *Стратегічні пріоритети*. 2016. № 4. С. 9–23.
12. Саєнко О. Г. Механізм інформаційно-психологічного впливу в умовах гібридної війни. *Вісник Національної академії державного управління при Президентові України. Серія «Державне управління»*. 2017. № 1. С. 125–132.
13. Bjola, C., & Pamment, J. Countering Online Propaganda and Extremism: The Dark Side of Digital Diplomacy. Abingdon: Routledge, 2019. DOI: https://doi.org/10.4324/9781351264082
14. Bârgăoanu, A., & Radu, L. Fake News or Disinformation 2.0? Some Insights into Romanians' Digital Behaviour. *Romanian Journal of European Affairs*. 2018. 18(1). P. 24–38. URL: https://rjea.ier.gov.ro/wp-content/uploads/articole/RJEA_vol.18_no.1_June2018_art.2.pdf
15. Kapantai, E., Christopoulou, A., Berberidis, C., & Peristeras, V. A systematic literature review on disinformation: Toward a unified taxonomical framework. *New Media & Society*. 2021. 23(5). P. 1301–1326. DOI: https://doi.org/10.1177/1461444820959296

Стаття надійшла до редакції 28.10.2024 р.
Стаття рекомендована до друку 02.12.2024 р.

Khriapynskyi A. P.,
PhD. in Law,
Director of LLC "Khryapynskyi and Company", Kharkiv, Ukraine
4/6 A, Akhsarova St., Kharkiv, 61051, Ukraine
e-mail: polifil1@ukr.net https://orcid.org/0000-0002-2492-051X

PERSPECTIVE DIRECTIONS OF INFORMATION POLICY FOR COUNTERING HYBRID THREATS

Annotation. The article comprehensively investigates the current challenges of hybrid threats to the information security of the state and substantiates promising areas for improving information policy to counter these threats in the context of dynamic geopolitical transformations and the rapid development of digital technologies. Based on the analysis of modern scientific concepts, the essence and characteristic features of hybrid influences in the information sphere are revealed, which are based on a synergistic combination of traditional methods of propaganda and disinformation with innovative manipulative technologies and covert forms of intervention with the aim of destabilizing society, controlling mass consciousness and undermining trust in government institutions. The author thoroughly analyzes the key vulnerabilities of the domestic information space to hybrid threats, in particular, he emphasizes the problems of the low level of media literacy of a significant part of the population, the significant spread of Russian disinformation narratives and fakes of an anti-Ukrainian direction in the Ukrainian media environment, institutional weakness and insufficient coordination of actions of state authorities in the field of strategic communications and ensuring information security. Considerable attention is paid to the consideration of the external context of the information war against Ukraine, associated with the geopolitical positioning of our state at the intersection of the interests of various centers of power, which actively use the tools of information and psychological influence to achieve their own goals.

Based on the systematization and critical reflection of advanced foreign experience in the field of countering hybrid threats by means of information policy, key priorities for the development of the relevant tools in Ukraine have been identified. In particular, special emphasis is placed on the feasibility of building a comprehensive system of media education and increasing the digital literacy of citizens based on best European practices, strengthening institutional capacity in the field of strategic communications by creating specialized units for the analysis of disinformation and debunking fakes, establishing an effective partnership of the state with leading social networks and Internet platforms in order to limit the spread of destructive content, as well as strengthening information interaction between the authorities and civil society to increase trust in official sources. The importance of implementing a proactive information policy aimed at forming a positive agenda and establishing national narratives based on democratic values and national interests of Ukraine is argued.

It is substantiated that the effectiveness of countering hybrid threats in the information sphere depends not only on the use of adequate tactical tools, but also on the implementation of systemic democratic reforms aimed at increasing the inclusiveness, transparency and accountability of public administration. Only an organic combination of the information policy development strategy with practical steps aimed at strengthening national identity, consolidating society around a common vision of the future and developing civic activism can ensure the necessary level of resilience to the aggressor's information operations. At the same time, the need for further comprehensive research into innovative forms and methods of countering hybrid attacks in the conditions of turbulence in global development, taking into account the unique nature of the Ukrainian context, is emphasized.

Keywords: public administration, information policy, hybrid threats, disinformation, strategic communications, media literacy, societal resilience.

REFERENCES

1. Patrikarakos, D. (2017). *War in 140 characters: How social media is reshaping conflict in the twenty-first century*. New York: Basic Books.

2. Hoffman, F. (2018). Examining complex forms of conflict: Gray zone and hybrid challenges. *PRISM, 7(4), 30–47*. URL: https://cco.ndu.edu/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/

3. Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe. *International Affairs, 92(1), 175–195*. DOI: https://doi.org/10.1111/1468-2346.12509

4. Renz, B. (2016). Russia and 'hybrid warfare'. *Contemporary Politics, 22(3), 283–300*. DOI: https://doi.org/10.1080/13569775.2016.1201316

5. Hellman, M., & Wagnsson, C. (2017). How can European states respond to Russian information warfare? An analytical framework. *European Security, 26(2), 153–170*. DOI: https://doi.org/10.1080/09662839.2017.1294162

6. Paul, C., & Matthews, M. (2016). *The Russian "firehose of falsehood" propaganda model*. Santa Monica, CA: RAND Corporation. URL: https://www.rand.org/pubs/perspectives/PE198.html

7. Pomerantsev, P. (2015). How to beat the Kremlin's propaganda machine. *World Affairs, 177(6), 36–42*. URL: https://www.jstor.org/stable/43555279

8. Annala, M. (2018). Responding to hybrid threats: The EU's resilience agenda. *CSS Analyses in Security Policy, 233, 1–4*. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse233-EN.pdf

9. Fiott, D., & Parkes, R. (2019). *Protecting Europe: The EU's response to hybrid threats*. Paris: EUISS. URL: https://www.iss.europa.eu/content/protecting-europe-eus-response-hybrid-threats

10. Horbulin, V.P., Vlasiuk, O.S., & Kononenko, S.V. (2017). *The world hybrid war: Ukrainian forefront*. Kyiv: NISD. [in Ukrainian].

11. Dubov, D.V. (2016). Strategic communications: problems of conceptualization and practical implementation. *Strategic Priorities, 4, 9-23*. [in Ukrainian].

12. Saienko, O.H. (2017). The mechanism of information and psychological influence in a hybrid war. *Bulletin of the National Academy for Public Administration under the President of Ukraine. Public Administration Series, 1, 125–132*. [in Ukrainian].

13. Bjola, C., & Pamment, J. (2019). *Countering Online Propaganda and Extremism: The Dark Side of Digital Diplomacy*. Abingdon: Routledge. DOI: https://doi.org/10.4324/9781351264082

14. Bârgăoanu, A., & Radu, L. (2018). Fake News or Disinformation 2.0? Some Insights into Romanians' Digital Behaviour. *Romanian Journal of European Affairs, 18(1), 24–38*. URL: https://rjea.ier.gov.ro/wp-content/uploads/articole/RJEA_vol.18_no.1_June2018_art.2.pdf

15. Kapantai, E., Christopoulou, A., Berberidis, C., & Peristeras, V. (2021). A systematic literature review on disinformation: Toward a unified taxonomical framework. *New Media & Society, 23(5), 1301–1326*. DOI: https://doi.org/10.1177/1461444820959296

The article was received by the editors 28.10.2024.
The article is recommended for printing 02.12.2024.