

ІНФОРМАЦІЙНА ПОЛІТИКА УКРАЇНИ: РОЛЬ ДЕРЖАВИ
В УМОВАХ ГІБРИДНИХ ЗАГРОЗ ТА ІНФОРМАЦІЙНОЇ ВІЙНИINFORMATION POLICY OF UKRAINE: THE ROLE OF THE STATE
IN THE CONDITIONS OF HYBRID THREATS AND INFORMATION WARFARE

У сучасному світі інформація стала ключовим ресурсом, який визначає політичну, економічну та соціальну динаміку суспільства. Україна, з огляду на геополітичне положення та поточні виклики, стикається з інтенсивними гібридними загрозами та активною інформаційною війною, спрямованою на підірив національної безпеки та суверенітету. Стаття присвячена дослідженню ролі держави у формуванні та реалізації ефективної інформаційної політики в умовах таких викликів. Метою роботи є аналіз сучасного стану інформаційної політики України та визначення стратегічних напрямів її вдосконалення для протидії гібридним загрозам і забезпечення інформаційної безпеки. У дослідженні використовуються методи системного аналізу, порівняльний підхід та експертна оцінка, що дозволяє комплексно оцінити проблему та запропонувати практичні рекомендації. У статті розглядаються основні аспекти гібридних загроз, включаючи дезінформацію, кібератаки та інформаційні маніпуляції, які спрямовані на дестабілізацію внутрішньої ситуації в країні. Аналізується роль державних інституцій у реагуванні на ці виклики, включаючи законодавчі ініціативи, створення спеціалізованих органів та впровадження національних програм з кібербезпеки та медіаграмотності. Автор підкреслює необхідність вдосконалення законодавчої бази з метою забезпечення ефективних механізмів протидії інформаційним загрозам та притягнення до відповідальності за інформаційні правопорушення. Особлива увага приділяється розвитку медіаграмотності населення як стратегічному напрямку, що підвищує стійкість суспільства до деструктивних інформаційних впливів. Розглядаються можливості міжнародної співпраці та обміну досвідом з метою зміцнення національної інформаційної безпеки. У результаті дослідження встановлено, що ефективною інформаційна політика України повинна базуватися на комплексному підході, який поєднує законодавчі реформи, технологічні інновації, освітні програми та міжнародну взаємодію. Держава має виступати активним суб'єктом у формуванні безпечного та стійкого інформаційного простору, забезпечуючи прозору комунікацію з громадянами та зміцнюючи довіру в суспільстві. У висновках статті наголошується, що лише за умови активної та скоординованої ролі держави можливе ефективне протистояння гібридним загрозам та забезпечення національної безпеки в інформаційній сфері. Запропоновані рекомендації можуть служити основою для подальшого розвитку інформаційної політики України в умовах сучасних викликів.

Ключові слова: інформаційна політика України, роль держави, гібридні загрози, інформаційна війна, інформаційна безпека, дезінформація, кібербезпека, медіаграмотність, національна безпека, законодавча база, міжнародна співпраця, інформаційний

простір, протидія дезінформації, державні інституції, технологічні інновації.

In the modern world, information has become a key resource that determines the political, economic and social dynamics of society. Ukraine, given its geopolitical situation and current challenges, faces intense hybrid threats and active information warfare aimed at undermining national security and sovereignty. The article is devoted to the study of the role of the state in the formation and implementation of effective information policy in the conditions of such challenges. The purpose of the work is to analyze the current state of Ukraine's information policy and to identify strategic directions for its improvement to counter hybrid threats and ensure information security. The research uses the methods of system analysis, a comparative approach and expert assessment, which allows for a comprehensive assessment of the problem and offers practical recommendations. The article examines the main aspects of hybrid threats, including disinformation, cyber attacks and information manipulation, which are aimed at destabilizing the internal situation in the country. The role of state institutions in responding to these challenges is analyzed, including legislative initiatives, the creation of specialized bodies, and the implementation of national programs on cyber security and media literacy. The author emphasizes the need to improve the legislative framework in order to ensure effective mechanisms for countering information threats and bringing to justice for information crimes. Special attention is paid to the development of media literacy of the population as a strategic direction that increases society's resistance to destructive informational influences. Possibilities of international cooperation and exchange of experience with the aim of strengthening national information security are being considered. As a result of the study, it was established that an effective information policy of Ukraine should be based on a comprehensive approach that combines legislative reforms, technological innovations, educational programs and international cooperation. The state should act as an active subject in the formation of a safe and stable information space, ensuring transparent communication with citizens and strengthening trust in society. The conclusions of the article emphasize that effective resistance to hybrid threats and ensuring national security in the information sphere is possible only with an active and coordinated role of the state. The proposed recommendations can serve as a basis for the further development of the information policy of Ukraine in the conditions of modern challenges.

Key words: information policy of Ukraine, role of the state, hybrid threats, information war, information security, disinformation, cyber security, media literacy, national security, legislative framework, international cooperation, information space, countering disinformation, state institutions, technological innovations.

УДК 351.74: 075.2
DOI <https://doi.org/10.32782/rma2663-5240-2022.32.20>

Димитрієв В.В.
здобувач наукового ступеня
кандидата наук

Постановка проблеми. Інформаційна політика є важливим компонентом національної безпеки кожної держави, а в умовах гібридних загроз та інформаційної війни вона набуває критичного значення. Сучасний світ зіткнувся з новими викликами, де традиційні військові дії доповнюються інформаційними та кібернетичними атаками. В умовах гібридної війни, яку Росія розгорнула проти України з 2014 року, ключову роль відіграє здатність держави ефективно управляти інформаційним простором, захищати його від зовнішніх впливів та дезінформації, а також формувати власні наративи, які здатні консолідувати суспільство та підтримувати національну єдність. Проблематика інформаційної політики в умовах гібридних загроз полягає в необхідності одночасно протидіяти деструктивному впливу з боку противника та забезпечувати об'єктивне інформування громадян, яке б не підривало довіру до державних інститутів. Важливим завданням для України є створення цілісної та скоординованої системи стратегічних комунікацій, яка б об'єднала зусилля державних органів, медіа, громадських організацій та приватного сектору для досягнення спільних цілей в умовах сучасних інформаційних викликів. Аналіз сучасного стану інформаційної політики України дозволить оцінити ефективність державних заходів протидії дезінформації, визначити слабкі місця в існуючій системі та окреслити шляхи підвищення стійкості національного інформаційного простору. Таким чином, дослідження в цій сфері є актуальним та своєчасним, оскільки інформаційна війна залишається одним із основних елементів гібридної агресії проти України. Для ефективного реагування на ці виклики необхідно комплексно підійти до питання інформаційної політики, поєднуючи державні ініціативи з активною участю громадянського суспільства та міжнародних організацій.

Аналіз останніх досліджень і публікацій. Аналіз наукових досліджень у сфері трансформації державної політики в інформаційній сфері України показує, що ця тема активно вивчається як вітчизняними, так і міжнародними дослідниками, враховуючи її значимість у контексті глобальних викликів. Такі автори, як В. Грицай та О. Карпенко, досліджують вплив проектів, на кшталт «Дія», на підвищення прозорості управління та доступу громадян до державних послуг. О. Шульга та Л. Мельник, аналізують роль державних інституцій у побудові системи кібербезпеки. У контексті дезінформації дослідники, зокрема С. Шабунін та О. Ємельянова, зосереджують увагу на впливі російських дезінформаційних кампаній на

громадську думку та політичну стабільність в Україні. У працях О. Дубровської та І. Лисенка розглядається участь України в міжнародних програмах, таких як НАТО та ЄС, з акцентом на їхній вплив на посилення кібербезпеки та розвиток цифрових технологій.

Мета статті полягає в тому, щоб дослідити роль держави у формуванні та реалізації інформаційної політики України в умовах гібридних загроз та інформаційної війни, а також виявити основні напрями для вдосконалення інформаційної безпеки.

Виклад основного матеріалу. Гібридні загрози та інформаційна війна стали невід'ємною частиною сучасної геополітичної реальності, в якій опинилася Україна. З 2014 року, після початку агресії Російської Федерації, ці загрози перетворилися на систематичну складову військових і політичних дій, що спрямовані на дестабілізацію внутрішньої ситуації в країні та піддрив довіри до державних інститутів. Гібридні загрози включають широкий спектр заходів, таких як дезінформаційні кампанії, кібератаки, економічний тиск, використання політичних і соціальних впливів, які об'єднані в єдиний комплексний механізм впливу. Основною метою цих заходів є не тільки отримання військової переваги, але й руйнація національної єдності, піддрив довіри до влади та маніпулювання суспільною свідомістю.

Одним із найбільших викликів для України в цьому контексті є дезінформаційні кампанії, які активно використовуються Росією для формування негативного іміджу країни як на внутрішньому, так і на міжнародному рівнях. Дезінформація спрямована на створення альтернативної реальності, де агресор виступає у ролі жертви, а власні дії виправдовуються маніпулятивними аргументами. Завдяки використанню фейкових новин, пропагандистських медіаресурсів та соціальних мереж, ця інформаційна зброя проникає у свідомість громадян, розмиває реальне уявлення про ситуацію та викликає сумніви в об'єктивності офіційних джерел інформації.

Кіберзагрози є ще одним важливим елементом гібридної війни, з яким стикається Україна. Кібератаки спрямовані не лише на знищення або виведення з ладу інформаційних систем державних органів та критичної інфраструктури, але й на отримання конфіденційної інформації та її використання у власних цілях. Успішні атаки на українські енергетичні об'єкти, фінансові установи та інші важливі сфери демонструють високий рівень організованості та підготовленості цих загроз. Здатність вчасно виявляти та реагувати на кібератаки стає ключовим фактором у забезпеченні національної безпеки [1].

Пропаганда є ще однією потужною зброєю, що активно використовується у рамках гібридної війни проти України. Пропагандистські медіа та контрольовані інформаційні ресурси поширюють спотворені наративи, спрямовані на формування негативного образу українського уряду, дискредитацію української армії та поширення страху та невпевненості серед населення. Важливою метою такої пропаганди є створення внутрішнього розколу серед громадян, посилення міжетнічних та регіональних конфліктів, а також піддрив довіри до демократичних процесів.

Україні доводиться одночасно протидіяти цим багатогранним загрозам, що вимагає від держави стратегічного підходу до розробки комплексної інформаційної політики. Важливо забезпечити координацію дій між усіма державними інституціями, приватним сектором та громадянським суспільством для створення стійкої системи протидії гібридним загрозам. Необхідним є також активне міжнародне співробітництво та інтеграція у глобальні ініціативи, спрямовані на захист інформаційного простору, обмін досвідом та технологіями з країнами, які також стикаються з подібними викликами.

Таким чином, гібридні загрози та інформаційна війна є одним із найбільших викликів, що стоять перед Україною. Для ефективної протидії необхідно не лише розвивати технологічні можливості та вдосконалювати інформаційні стратегії, але й формувати культуру критичного мислення серед громадян, яка допоможе їм відрізнити правдиву інформацію від маніпуляцій. Лише за таких умов Україна зможе забезпечити свою інформаційну безпеку та зберегти національну стійкість у часи постійних викликів.

Роль держави у формуванні інформаційної політики є критично важливою, особливо в умовах сучасних гібридних загроз та інформаційної війни, що їх ведуть проти України. В умовах активного використання інформаційних технологій для маніпуляцій, дезінформації та пропаганди, держава повинна виступати в якості ключового гравця, здатного захистити національний інформаційний простір та забезпечити ефективну комунікацію з громадськістю.

Одним із основних завдань держави є розробка та впровадження чіткої нормативно-правової бази, яка регулює питання інформаційної безпеки та діяльність медіа. Це включає прийняття законів, які спрямовані на боротьбу з фейковими новинами, поширенням дезінформації та пропагандою. Наприклад, в Україні було прийнято низку законів, спрямованих на

обмеження діяльності проросійських медіа та блокування доступу до інформаційних ресурсів, які ведуть антиукраїнську пропаганду. Такі законодавчі ініціативи є важливою складовою захисту інформаційного простору від зовнішніх впливів.

Крім того, стратегічні комунікації є ще одним важливим елементом державної інформаційної політики. Держава повинна забезпечити єдину, скоординовану систему комунікацій між різними органами влади для того, щоб надати громадянам достовірну та об'єктивну інформацію. Це включає проведення інформаційних кампаній, що спрямовані на підвищення рівня обізнаності населення щодо національних і безпекових питань, а також швидке реагування на дезінформаційні атаки та спроби маніпулювання суспільною думкою [2].

Важливу роль відіграє розвиток кібербезпеки, яка є однією з основних ланок захисту національної інформаційної інфраструктури. Кібератаки, спрямовані на державні установи та критично важливі об'єкти інфраструктури, можуть завдати серйозної шкоди економічній і політичній стабільності країни. Тому держава інвестує значні ресурси у розвиток сучасних технологій кіберзахисту, створення центрів оперативного реагування на кіберінциденти та підготовку спеціалістів з кібербезпеки. Наприклад, в Україні діють спеціалізовані структури, як-от Державна служба спеціального зв'язку та захисту інформації України, які займаються питаннями кібербезпеки та забезпеченням надійного захисту інформаційних систем.

Однією з ключових функцій держави є також підтримка та розвиток інформаційної грамотності населення. В умовах постійного впливу дезінформації та фейкових новин важливо навчити громадян критично мислити та розрізнити правдиву інформацію від спотворених фактів. Держава повинна ініціювати освітні програми, тренінги та медіаграмотність у школах і вищих навчальних закладах, а також сприяти популяризації незалежної журналістики та якісних медіа. Такі зусилля сприятимуть створенню суспільства, яке здатне адекватно оцінювати інформаційний простір та приймати зважені рішення на основі достовірних даних.

Не менш важливим є міжнародне співробітництво у сфері інформаційної безпеки. Україна активно співпрацює з Європейським Союзом, НАТО та іншими міжнародними організаціями з метою обміну досвідом, технологіями та ресурсами для протидії гібридним загрозам. Спільні зусилля в рамках таких ініціатив дозволяють покращувати національні стратегії захисту від кібератак, створювати більш надійні

системи захисту даних та посилювати колективну безпеку у сфері інформаційної політики.

Отже, роль держави у формуванні інформаційної політики полягає не лише у створенні нормативно-правових механізмів та захисті від зовнішніх загроз, але й у розбудові інформаційної інфраструктури, що забезпечує стійкість національного інформаційного простору. Держава повинна діяти як координаційний центр, який об'єднує зусилля різних інституцій, приватного сектору та громадянського суспільства для досягнення цілей інформаційної безпеки. Лише за таких умов можливо забезпечити захист від дезінформації, підтримувати національну єдність та сприяти розвитку стійкої демократичної держави [3].

Протидія гібридним загрозам вимагає комплексного підходу, який охоплює різноманітні стратегії для зменшення впливу дезінформації, підвищення стійкості інформаційного простору та захисту національних інтересів. Ці стратегії мають бути добре скоординованими між державою, громадянським суспільством і міжнародними партнерами. Ось детальний огляд ключових стратегій, які Україна використовує для протидії гібридним загрозам:

1. Інформаційна грамотність населення. Одним із найважливіших аспектів у боротьбі з дезінформацією є підвищення рівня інформаційної грамотності громадян. Це передбачає навчання навичкам критичного мислення та аналізу інформації, що дозволяє людям самостійно відрізнити правдиву інформацію від фейків і маніпуляцій. У рамках цієї стратегії в Україні проводяться освітні кампанії, що спрямовані на підвищення обізнаності про небезпеки дезінформації та важливість медіаграмотності. Такі ініціативи реалізуються як у навчальних закладах, так і через громадські організації та медіа-проекти, що працюють з широкою аудиторією.

2. Розвиток стратегічних комунікацій. Стратегічні комунікації – це систематичний підхід до координації повідомлень державних органів з метою досягнення єдиних інформаційних цілей. Українська держава активно працює над створенням ефективної системи стратегічних комунікацій, яка включає розробку єдиних інформаційних наративів, що підтримують національні інтереси та посилюють державну позицію у питаннях безпеки та міжнародної політики. Це також передбачає швидку і злагоджену реакцію на інформаційні атаки, щоб ефективно спростовувати фейкові новини та формувати позитивний образ країни.

3. Технологічні рішення та використання штучного інтелекту (AI). Сучасні технології, зокрема штучний інтелект та алгоритми

машинного навчання, відіграють важливу роль у виявленні та нейтралізації дезінформації. AI може допомагати автоматично ідентифікувати фейкові новини, боти у соціальних мережах та інші форми маніпуляцій. В Україні активно розвиваються технологічні рішення, які здатні аналізувати великий обсяг даних у режимі реального часу, що дозволяє швидше виявляти потенційні загрози і реагувати на них. Використання AI також дозволяє прогнозувати можливі інформаційні атаки і завчасно готувати відповідні контрзаходи.

4. Кібербезпека та захист критичної інфраструктури. Одним із ключових напрямків протидії гібридним загрозам є посилення кібербезпеки. Держава інвестує у розвиток захисних систем для критичної інфраструктури, таких як енергетичні об'єкти, фінансові установи та урядові платформи. Важливою частиною цього процесу є також підготовка фахівців з кібербезпеки та створення центрів моніторингу кіберзагроз, які працюють над швидким реагуванням на інциденти. Україна також співпрацює з міжнародними партнерами, такими як НАТО та Європейський Союз, для впровадження найкращих практик і технологій у сфері кіберзахисту.

5. Міжнародне співробітництво. Міжнародне співробітництво є важливим інструментом у боротьбі з гібридними загрозамі. Україна активно співпрацює з міжнародними організаціями та країнами-партнерами для обміну інформацією, технологіями та досвідом. Важливими партнерами є Європейський Союз, НАТО, США та інші країни, що підтримують Україну у протидії дезінформації та кіберзагрозам. Спільні навчання, участь у міжнародних форумах та розробка спільних стратегій допомагають Україні підвищити свою обороноздатність і покращити готовність до реагування на загрози [4].

6. Законодавчі ініціативи та регуляторні заходи. Важливим інструментом протидії гібридним загрозам є створення відповідної законодавчої бази, яка дозволяє ефективно регулювати інформаційний простір та протидіяти деструктивним впливам. В Україні було ухвалено низку законодавчих актів, спрямованих на боротьбу з пропагандою, поширенням фейкових новин та кіберзагрозами. Водночас держава працює над посиленням регулювання соціальних мереж та онлайн-платформ, щоб запобігати поширенню шкідливого контенту та дезінформації.

7. Підтримка незалежної журналістики та прозорих медіа. Державна підтримка незалежних медіа та високих стандартів журналістики є важливим компонентом у боротьбі з

дезінформацією. Якісні та прозорі медіа відіграють важливу роль у формуванні об'єктивного уявлення про реальність і слугують противагою маніпулятивним повідомленням, які розповсюджують пропагандистські ресурси. Українська держава підтримує ініціативи, спрямовані на розвиток незалежної журналістики, зокрема через грантову підтримку, навчальні програми та співпрацю з міжнародними медіаорганізаціями.

8. Підтримка громадських організацій та ініціатив протидії дезінформації. Громадські організації відіграють важливу роль у моніторингу інформаційного простору та викритті фейкових новин. Вони є джерелом незалежного аналізу та факт-чекінгу, що допомагає підвищити рівень довіри до інформації в суспільстві. Держава повинна активно співпрацювати з такими організаціями, підтримуючи їхні ініціативи та залучаючи до розробки національних стратегій протидії дезінформації [5].

Ефективні стратегії протидії гібридним загрозам повинні бути багатограними та інтегрованими. Вони мають охоплювати як технологічні аспекти захисту, так і соціально-політичні механізми для підвищення інформаційної стійкості суспільства. Комплексний підхід, що включає міжнародне співробітництво, розвиток стратегічних комунікацій, підтримку незалежної журналістики та інвестиції в кібербезпеку, дозволить Україні ефективніше захищатися від дезінформаційних атак та зміцнювати свою національну безпеку.

Перспективи вдосконалення інформаційної політики України є надзвичайно важливими в умовах сучасних викликів, з якими стикається країна. В умовах глобалізації та цифровізації інформаційний простір набуває особливого значення, що вимагає від держави активних дій у сфері формування та реалізації інформаційної політики.

Однією з ключових перспектив є інтеграція нових інформаційних технологій у державне управління. Це дозволить підвищити прозорість і доступність інформації для громадян, що, у свою чергу, зміцнить довіру до державних інститутів. Важливо розвивати електронні послуги, які спростять взаємодію між громадянами та державою, а також забезпечити захист особистих даних.

Другою важливою перспективою є розвиток медіаосвіти та критичного мислення серед населення. В умовах інформаційної війни та дезінформації важливо навчати громадян аналізувати та оцінювати інформацію, яку вони отримують. Це може бути досягнуто через освітні програми, що впроваджують навички критичного мислення в шкільній та вищій освіті.

Також необхідно сприяти розвитку національних медіа та підтримувати якісну журналістику. Державна підтримка незалежних медіа, які здатні протистояти дезінформації та маніпуляціям, стане важливим кроком у забезпеченні інформаційної безпеки країни.

Не менш важливим є вдосконалення законодавчої бази у сфері інформаційної політики. Україні потрібні чіткі норми, що регулюють інформаційні відносини, боротьбу з дезінформацією та захист прав журналістів. Розробка законів, які забезпечать захист інформаційного простору від зовнішніх загроз, є ключовою для зміцнення суверенітету України [6].

Таким чином, перспективи вдосконалення інформаційної політики України полягають у впровадженні нових технологій, розвитку медіаосвіти, підтримці незалежних медіа та вдосконаленні законодавства. Ці кроки допоможуть створити ефективну інформаційну систему, яка буде сприяти розвитку демократичних інститутів та підвищенню рівня життя населення.

Крім вищезазначених напрямків, важливо також зосередитися на міжнародній співпраці у сфері інформаційної політики. Україні слід активно співпрацювати з міжнародними організаціями, такими як ЮНЕСКО, ОБСЄ та іншими, які мають досвід у вирішенні проблем інформаційної безпеки та розвитку медіа. Участь у міжнародних проектах і ініціативах може сприяти отриманню нових знань і технологій, а також залученню фінансових ресурсів для реалізації внутрішніх програм.

Окрім того, слід приділити увагу розвитку інформаційної інфраструктури. Це включає в себе модернізацію існуючих інформаційних систем, забезпечення доступу до інтернету в усіх регіонах, зокрема у віддалених і сільських територіях. Вдосконалення технічної бази сприятиме покращенню якості послуг, що надаються державою, а також забезпечить рівний доступ до інформації для всіх громадян.

Необхідно також враховувати специфіку інформаційного простору України, де є багато мовних і культурних різноманітностей. Розробка політики, яка враховує потреби різних мовних груп, стане запорукою інклюзивності та забезпечення інформаційної справедливості. Створення контенту українською, російською та іншими мовами, а також підтримка регіональних ЗМІ можуть допомогти забезпечити доступ до інформації для всіх верств населення.

Значну увагу варто звернути на боротьбу з кібератаками та інформаційними загрозами. Створення ефективних механізмів кібербезпеки, розвиток національних стратегій захи-

сту інформаційних систем, а також навчання спеціалістів у цій сфері є необхідними кроками для забезпечення надійності інформаційної інфраструктури.

Важливою складовою вдосконалення інформаційної політики є також залучення громадськості до її формування. Активне залучення громадян до процесів прийняття рішень, обговорень та ініціатив допоможе створити більш адаптивну і чутливу до потреб суспільства інформаційну політику. Розвиток платформ для громадських консультацій та електронних петицій може сприяти залученню широких верств населення до інформаційної політики.

Загалом, вдосконалення інформаційної політики України вимагає комплексного підходу, що охоплює як технологічні, так і соціально-культурні аспекти. Співпраця з міжнародними партнерами, розвиток інфраструктури, боротьба з інформаційними загрозами та залучення громадськості до процесів формування політики є ключовими елементами, які забезпечать успішну реалізацію інформаційної стратегії країни. Ці дії сприятимуть не лише покращенню інформаційного середовища, але й загальному розвитку демократії та зміцненню суспільної згуртованості в Україні.

Висновки. В умовах зростаючих гібридних загроз та активної інформаційної війни роль держави у забезпеченні інформаційної безпеки України є критично важливою. Держава повинна активно втручатися в захист інформаційного простору, розробляючи та впроваджуючи ефективні стратегії протидії дезінформації та кібератакам. Вдосконалення законодавчої бази є необхідним кроком для адаптації до сучасних викликів, що забезпечить правові механізми для захисту інформаційної безпеки та притягнення до відповідальності за інформаційні правопорушення. Розвиток медіаграмотності населення є ключовим фактором у зменшенні впливу пропаганди та дезінформації. Держава повинна сприяти підвищенню

рівня освіти громадян у цій сфері, що дозволить їм критично оцінювати інформацію. Інвестиції в сучасні технології та розвиток кібербезпеки є необхідними для захисту державних інформаційних систем та інфраструктури. Міжнародна співпраця з партнерами та організаціями дозволяє обмінюватися досвідом та ресурсами в боротьбі з гібридними загрозами на глобальному рівні. Прозора та відкрита комунікація держави з громадянами зміцнює довіру та зменшує вразливість до дезінформації. Створення спеціалізованих органів, відповідальних за моніторинг та реагування на інформаційні загрози, підвищує ефективність протидії. У підсумку, комплексний підхід, що поєднує законодавчі ініціативи, технологічний розвиток, освіту та міжнародну співпрацю, дозволить Україні ефективно захищати свій інформаційний простір та забезпечувати національну безпеку в умовах гібридних загроз та інформаційної війни.

ЛІТЕРАТУРА:

1. Шульга О. І., Мельник Л. М. Забезпечення інформаційної безпеки України: сучасні виклики та шляхи вирішення. Інформаційні технології та кібербезпека. 2020. Т. 18. № 2. С. 112–120.
2. Шабунін С. М., Ємельянова О. В. Протидія російській дезінформації: аналіз стратегій та механізмів впливу. Журнал соціальних комунікацій. 2019. № 4. С. 38–45.
3. Дубровська О. П., Лисенко І. А. Міжнародна співпраця України з ЄС та НАТО у сфері кібербезпеки. Сучасні проблеми міжнародних відносин. 2021. № 27. С. 102–109.
4. Офіційний сайт Міністерства цифрової трансформації України. URL: <https://thedigital.gov.ua>
5. Кучеренко Л. Г. Інформаційні технології в державному управлінні: європейські стандарти та український контекст. Вісник Київського національного університету ім. Тараса Шевченка. Серія: Державне управління. 2020. № 17(1). С. 22–33.
6. Сидоренко Ю. В. Регулювання інформаційного простору в країнах ЄС: уроки для України. Європейська інтеграція і міжнародні відносини. 2019. № 5(2). С. 91–102.