УДК 316.776:32 (477)
DOI https://doi.org/10.32782/apfs.v049.2024.36

С. М. Матвієнків
ORCID ID: https://orcid.org/0000-0002-7719-7791
кандидат політичних наук, доцент,
доцент кафедри політичних інститутів та процесів
Прикарпатського національного університету імені Василя Стефаника

Л. І. Братах
ORCID ID: https://orcid.org/0009-0005-8619-8576
аспірант кафедри політичних інститутів та процесів
Прикарпатського національного університету імені Василя Стефаника

ІНФОРМАЦІЙНІ ЗАГРОЗИ В УМОВАХ ПОВНОМАСШТАБНОЇ ВІЙНИ: СУЧАСНІ ВИКЛИКИ ДЛЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Постановка проблеми. В умовах сучасних міжнародних гібридних війна та конфліктів, де класичні військові дії супроводжуються інформаційними атаками, питання національної безпеки набуває нових форм. Особливо це стосується України, яка протягом останніх 10-ти років протистоїть гібридній агресії росії. Повномасштабне вторгнення рф у лютому 2022 року зумовило нові виклики та загрози для національної безпеки України, у зв'язку із суттєвою зміною інформаційного простору держави, вторгненням ворожих меседжів зокрема. Тому аналіз інформаційних загроз в умовах повномасштабної війни росії супроти України актуалізує розгляд інформаційної складової як невід'ємного елемента національної безпеки.

Метою цієї статті є аналіз сучасних інформаційних загроз в умовах повномасштабної війни росії проти України та визначення їхнього впливу на національну безпеку держави. Завданнями статті є: охарактеризувати поняття інформаційних загроз у контексті сучасної війни та визначити їх основні типи; проаналізувати вплив інформаційних загроз на національну безпеку України в умовах повномасштабної війни, включаючи внутрішні та зовнішні загрози; визначити наслідки інформаційних загроз для політичної стабільності, економічного розвитку та соціальної єдності України.

Аналіз останніх досліджень і публікацій з даної теми. Різні аспекти особливостей інформаційного простору України та його взаємозв'язку з національною безпекою держави є предметом досліджень таких вчених як Біловус Л., Грицай С., Залєвська І., Мазуренко Л., Матвієнків С., Цимбалюк В., Литвиненко О., Леоненко Н., Поступна О., Шмаленко Ю., Кольцов В., Руднєва А. та ряд інших дослідників. Відкритим для досліджень залишається аналіз інформаційних загроз, пов'язаних з повномасштабним вторгненням, які є одним із наймасштабніших викликів національній безпеці України.

Виклад основного матеріалу дослідження. В умовах сучасної війни, що розгортається не лише на полі бою, а й в інформаційному просторі, питання національної безпеки набуває нового виміру. Інформаційні загрози стали критичним фактором, який може впливати на соціальну стабільність, політичний лад та економічний розвиток країни. Україна, стикаючись із безпрецедентним інформаційним тиском під час повномасштабної війни росії проти нашої країни, вимушена протистояти дезінформації, пропаганді, кіберзагрозам та психологічним операціям, що мають на меті підрив національної безпеки.

Інформаційний простір – це сукупність усіх інформаційних ресурсів та інфраструктур, через які відбувається обмін інформацією між різними суб'єктами: державами, організаціями, суспільством і окремими індивідами. Він охоплює як традиційні засоби масової інформації (телебачення, радіо, преса), так і цифрові платформи (інтернет, соціальні мережі, блоги) та канали комунікації. Інформаційний простір є невід'ємною складовою сучасного суспільства, оскільки через нього відбувається формування світогляду, політичної культури, суспільної думки та комунікація на різних рівнях [1].

Інформаційний простір виконує кілька важливих функцій:

– комунікаційна функція – забезпечує обмін інформацією між людьми, соціальними групами, організаціями та державами. Завдяки цьому підтримується інформаційна взаємодія як на внутрішньому, так і на міжнародному рівнях;

– інформаційно-аналітична функція – сприяє збиранню, аналізу та поширенню інформації, необхідної для ухвалення рішень. Це стосується як державного управління, так і комерційної діяльності та суспільних ініціатив;

– культурно-виховна функція – через інформаційний простір формуються культурні цінності, етичні норми та світогляд громадян. ЗМІ та інші

джерела інформації впливають на формування національної ідентичності та суспільної свідомості;

– безпекова функція – інформаційний простір захищає суспільство від дезінформації, маніпуляцій і зовнішнього втручання в інформаційні процеси. Він також допомагає попереджати загрози, пов'язані з кіберзлочинністю та інформаційними атаками;

– маніпуляційна функція – в умовах конфлікту інформаційний простір може використовуватися для поширення пропаганди, дезінформації та маніпуляцій з метою досягнення політичних або військових цілей [1].

Інформаційний простір складається з кількох основних елементів, а саме інформаційні ресурси, інформаційні канали, інформаційні технології, інформаційні суб'єкти та об'єкти тощо. Інформаційні ресурси – це всі форми інформації, які існують у суспільстві: новини, аналітичні матеріали, культурні та освітні програми, рекламні повідомлення тощо. Вони можуть існувати в різних формах: текст, аудіо, відео, зображення. Інформаційні канали – засоби, через які інформація поширюється і сприймається. Це можуть бути ЗМІ, соціальні мережі, блоги, інтернет-портали, радіо, телебачення та інші. Кожен канал має свої специфічні характеристики і аудиторію. Інформаційні технології – інфраструктура, що забезпечує обробку, зберігання і передачу інформації [2, с. 28]. Це сервери, бази даних, платформи для обміну повідомленнями, інтернет-мережі та інші технічні засоби. Інформаційні суб'єкти – це всі учасники процесу обміну інформацією: держава, ЗМІ, громадські організації, політичні партії, комерційні структури та громадяни. Кожен суб'єкт виконує свою роль у створенні, розповсюдженні та споживанні інформації. Об'єктом є відповідно той, на кого спрямована інформація або той, кого вона стосується. Це можу бути як все суспільство, так і різні його сегменти [5].

Український інформаційний простір в умовах російської агресії зазнає серйозних викликів, які обумовлені тривалими і системними інформаційними атаками з боку росії. Основні специфічні особливості українського інформаційного простору в цей період можна описати наступним чином:

Дезінформація та пропаганда з боку росії. З початку конфлікту в 2014 році і особливо після повномасштабного вторгнення у 2022 році рф веде масштабну інформаційну війну проти України. Вона поширює дезінформацію як всередині України, так і на міжнародному рівні з метою дискредитації української влади, зниження морального духу населення та ослаблення підтримки України з боку її союзників. Так, наприклад, російські медіа зображують українську владу як «фашистську» або «неонацистську», стверджуючи, що в Україні відбувається репресія російськомовного населення. Цей наратив активно поширюється в міжнародних медіа та соціальних мережах для дискредитації України та виправдання російської агресії. Також, прикладом є пропагандистські заяви про «захист російськомовних» у Донецькій та Луганській областях [1].

Гібридне протистояння. московія активно поєднує класичні військові дії з інформаційними операціями. Це включає не лише поширення пропаганди, але й організацію кібератак на критичну інфраструктуру, втручання у вибори та інформаційні кампанії для маніпуляції громадською думкою. Особливо ці атаки зросли в останні кілька років в українських соціальних мережах та месенджерах [9].

Спроби підриву соціальної єдності. Ворожі інформаційні операції спрямовані на розкол українського суспільства, зокрема через акцентування на регіональних, мовних, політичних або релігійних розбіжностях. Мета таких операцій – послаблення внутрішньої єдності України в умовах воєнного стану. Наприклад, російська пропаганда активно експлуатує питання мовного поділу, стверджуючи, що російськомовні громадяни України зазнають утисків. Цей наратив просувається з метою розпалювання ворожнечі між україномовними і російськомовними громадянами. Наприклад, у східних і південних регіонах України пропагандисти намагалися переконати населення в тому, що «Київ» нібито проводить політику мовної дискримінації. російська пропаганда також намагається використовувати тему внутрішніх переселенців, підкреслюючи можливі соціальні та економічні проблеми, які вони створюють для приймаючих регіонів. Це має на меті викликати напруження між переселенцями і місцевим населенням, створюючи підґрунтя для соціальних конфліктів [8].

Кіберзагрози. Україна постійно стикається з кібератаками на свої урядові системи, об'єкти критичної інфраструктури та ЗМІ. Ці атаки спрямовані на паралізацію роботи державних інститутів, створення паніки серед населення та поширення неправдивої інформації. Під час війни соціальні мережі стали одним з головних інструментів обміну інформацією та протидії пропаганді. Вони використовуються для мобілізації населення, розповсюдження правдивих новин і документування воєнних злочинів. Проте соціальні платформи також стали полем для дезінформаційних кампаній, що вимагає від користувачів критичного ставлення до інформації [6]. На початку 2022 року, незадовго до повномасштабного вторгнення Росії, українські урядові сайти, зокрема Міністерства оборони, Збройних сил та ПриватБанку, зазнали DDoS-атак. Це призвело до тимчасової втрати доступу до ресурсів, дезорганізуючи роботу державних органів і бан-

ківських установ. У тому ж 2022 році, під час повномасштабного вторгнення, російські хакери намагалися вразити телекомунікаційні системи України, зокрема мобільні оператори та інтернет-провайдери. Це могло призвести до зупинки роботи інформаційних ресурсів, обмежити доступ до новин та правдивої інформації, а також посіяти паніку серед населення [9].

Таким чином, інформаційні загрози можна визначити як будь-які дії чи кампанії, спрямовані на дестабілізацію суспільства або державних інституцій через маніпуляцію інформацією, спотворення фактів або створення дезінформації. У сучасній російсько-українській війні інформаційний простір став не менш важливим полем битви, ніж фізичні операції. Основні типи інформаційних загроз включають: дезінформацію – поширення неправдивих або маніпулятивних даних з метою впливу на громадську думку, створення паніки або недовіри до влади (це часто використовується для дискредитації української армії або для посилення розбіжностей у суспільстві; ворожа пропаганда – систематичне використання інформації для нав'язування певних політичних або ідеологічних поглядів (росія активно використовує пропаганду як на внутрішньому, так і на зовнішньому рівні для формування негативного іміджу України); атаки на інформаційну інфраструктуру, зокрема урядові сайти, банківську систему, електромережі та медіаплатформи; психологічні операції (психоопераційї) – кампанії, спрямовані на підрив морального духу громадян і військових, що можуть включати залякування, поширення фейкових новин про успіхи ворога або створення панічних настроїв [12].

Доктрина інформаційної безпеки України визнає інформаційну безпеку як важливу, самостійну складову національної безпеки держави. Указом Президента України № 685/2021 від 15 жовтня 2021 року була затверджена Стратегія інформаційної безпеки. Основна мета цієї стратегії полягає у нормативно-правовому врегулюванні питань інформаційної безпеки, зміцненні потенціалу для забезпечення інформаційної безпеки України, охорони її інформаційного простору, підтримці соціальної та політичної стабільності, оборони держави, захисті її суверенітету, територіальної цілісності, демократії, прав та свобод людини і громадянина за допомогою інформаційних засобів і заходів. Таким чином, було закладено основи для національної та інформаційної безпеки в інформаційній сфері [10].

Вітчизняні науковці звертали увагу на значущість цього питання для безпеки країни ще до його офіційного врегулювання на державному рівні. Наприклад, В. Цимбалюк визначає інформаційну безпеку України як стан захищеності державних інтересів у сфері інформації [13]. Л. Кочубей вважає, що інформаційна безпека відображає рівень захищеності життєво важливих інтересів, інформаційну підготовленість держави, суспільства та особистості тощо [5].

Повномасштабне вторгнення рф на територію України та руйнування українських міст і сіл подаються російськими масмедіа як так звана «військова операція». Це використовується для виправдання агресивних дій на внутрішньому та зовнішньому ринку. Тому в умовах повномасштабної війни з росією інформаційні загрози стають однією з головних проблем національної безпеки. Вони мають як внутрішній, так і зовнішній характер, впливаючи на різні аспекти життя країни [6].

Внутрішні загрози: підрив суспільної єдності – дезінформація та пропаганда спрямовані на розкол у суспільстві, підвищення рівня недовіри до влади та державних інституцій. Це може створювати розбіжності між різними соціальними та політичними групами, послаблюючи національну єдність і підтримку воєнних зусиль; деградація морального стану населення – психологічні операції, що поширюють страх та невпевненість, можуть знижувати бойовий дух як серед військових, так і серед цивільного населення. Постійні інформаційні атаки підривають віру в успіх України на полі бою [9].

Зовнішні загрози: міжнародна дискредитація – інформаційні атаки росії спрямовані не тільки на внутрішню аудиторію, а й на міжнародне співтовариство. Мета – викликати сумніви щодо легітимності дій України або спотворити факти про конфлікт для зменшення міжнародної підтримки; атаки на критичну інфраструктуру можуть призводити до дестабілізації важливих державних систем (енергетика, фінанси, транспорт), що ускладнює не тільки ведення оборони, але й підтримку економічної та соціальної стабільності всередині країни. російська федерація протягом багатьох років не змінює своїх наративів щодо України, поширюючи антиукраїнські тези по всьому світу та щорічно витрачаючи на міжнародні медіа близько 4,5 млрд доларів. Про це заявив виконавчий директор Інституту інформаційної безпеки Артем Біденко. Він зазначив, що основні російські наративи залишаються незмінними: Україна зображується як неспроможна держава з корупцією, українці – як росіяни, а української мови не існує. Одночасно росія поширює ідеї, що вона не є імперіалістичною державою, а потерпає від західних агресивних амбіцій, використовуючи Україну як інструмент. Біденко наголосив, що російські медіа, такі як Sputnik і Russia Today, є потужним інструментом пропаганди, спрямованим не лише проти України, але й проти сусідів – країн Балтії та Польщі. Метою цієї пропаганди є створення інформаційного хаосу для досягнення військових цілей [3].

Інформаційні атаки в умовах війни можуть мати руйнівні наслідки для всіх основних аспектів життя держави. Постійна дезінформація та пропаганда можуть викликати політичну нестабільність, коли влада втрачає підтримку населення через зниження довіри до її дій. російські інформаційні операції спрямовані на підрив легітимності українського керівництва, що може призводити до політичних криз і зниження здатності держави ефективно управляти ситуацією під час війни. Інформаційні загрози також негативно впливають на економіку. Кібератаки на фінансові системи можуть паралізувати економічні процеси, викликаючи паніку на ринках. Дезінформація щодо стану економіки або майбутніх подій здатна зменшити довіру інвесторів і партнерів до українського ринку, що уповільнює його розвиток.

Вплив інформаційних атак на суспільство призводить до підвищення напруги між різними соціальними групами. Розповсюдження фейкових новин, що спрямовані на маніпуляцію національними або релігійними почуттями, може посилити розкол у суспільстві, що ускладнює консолідацію населення перед лицем спільного ворога. ля поширення фейкової інформації зазвичай використовуються месенджери (WhatsApp, Viber, Telegram), соціальні мережі (Facebook, Twitter, Instagram) та онлайн-платформи. Основні типи фейків включають: фейк-реклама, яка просуває продукти або послуги (інформацію слід перевіряти на офіційних сайтах); фейк-псевдоексперт, що посилається на неперевірених осіб, без надання достовірних джерел або доказів; фейк-конспірологія, заснований на теоріях змови, які легко спростовуються; фейк-клікбейт, що привертає увагу сенсаційними заголовками, які не відповідають змісту. Для поширення фейків активно використовуються ботоферми та «фабрики Інтернет-тролів». Крім того, під час російсько-української війни фейки відіграють ключову роль у боротьбі наративів, зокрема через поширення таких ворожих меседжів, як «Україна – фашистська держава» або «звільнення українців від націоналістів» [1].

Висновки з дослідження і перспективи подальших пошуків у даному науковому напрямку. Інформаційний простір відіграє ключову роль у національній безпеці України, особливо в умовах російської агресії. Сучасні виклики вимагають постійного моніторингу інформаційних загроз і розвитку ефективних механізмів протидії дезінформації та кіберзагрозам. Водночас важливою є консолідація зусиль держави, суспільства та міжнародних партнерів для зміцнення інформаційної стійкості та підвищення рівня інформаційної грамотності серед громадян.

Інформаційні загрози в умовах повномасштабної війни росії проти України є одним із найважливіших викликів для національної безпеки. Вони впливають на політичну стабільність, економічний розвиток та соціальну єдність країни, послаблюючи її обороноздатність та позиції на міжнародній арені. Для протидії цим загрозам необхідно впроваджувати комплексні стратегії, що включають як зміцнення інформаційної безпеки, так і підвищення рівня медіаграмотності населення. Відкритим для дослідження є пошук конкретних кроків та рішень, якими Україна посилювала б свою інформаційну стійкість, розвиваючи відповідні державні інституції та співпрацюючи з міжнародними партнерами для забезпечення ефективної протидії інформаційним загрозам.

Література

1. Біловус Л. Український інформаційний простір: сьогодення та перспективи. Український інформаційний простір: *Науковий журнал Інституту журналістики і міжнародних відносин КНУКІМ*. Число 1. – У 2-х ч. Ч. 1. 2013. URL: http://dspace.wunu.edu.ua/handle/316497/8741.

2. Грицай С. Архітектоніка сучасного медіапростору. *Вісник Книжкової палати*. 2012. № 5. С. 26–29.

3. «Два роки повномасштабної війни: загрози нацбезпеці, інформаційні виклики, оборонні тренди». 2024. Укрінформ. URL: https://www.ukrinform.ua/rubric-presshall/3832380-dva-roki-povnomasstabnoi-vijni-zagrozi-nacbezpeci-informacijni-vikliki-oboronni-trendi.html

4. Залєвська І., Удренас Г. Інформаційна безпека України в умовах російської військової агресії. *Південноукраїнський правничий часопис* 2016. № 1–2. С. 20–26.

5. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки*. 2016. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf

6. Леоненко Н., Поступна О. Інформаційна безпека України : механізми, сучасні виклики та загрози в умовах інформаційного глобалізму. *Вісник Національного університету цивільного захисту України Серія «Державне управління»*. 2022. URL: http://repositsc.nuczu.edu.ua/handle/123456789/16883

7. Литвиненко О. Інформаційний простір як чинник забезпечення національних інтересів України: ІМВКУ ім. Т. Шевченка. 1998. 145 с.

8. Мазуренко Л. Інформаційна безпека в умовах російсько-української війни: виклики та загрози. *Вісник Харківського національного університету імені В. Н. Каразіна, серія «Питання політології»*. 2022. Вип. 42.

9. Осмоловська А. Інформаційний простір України: національний та зовнішньо-політичний виміри. URL: file:///C:/Users/Natalya/Downloads/10382-Текст% 20статті-20654-1-10-20210625.pdf

10. Про Доктрину інформаційної безпеки України: Указ Президента України №47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL: https://www.president.gov.ua/documents/472017- 21374

11. Про рішення Ради національної безпеки і оборони України 2021: Указ Президента України № 685/2021 від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://www.president.gov.ua/documents/6852021-41 069

12. Скочиляс-Павлів О. Сучасні загрози інформаційній безпеці України в умовах правового режиму воєнного стану. *Юридичний науковий електронний журнал*. 2023. URL: http://lsej.org.ua/9_2023/65.pdf

13. Цимбалюк В. Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики. *Адміністративне право і процес* №2(8). 2014. С. 22–30.

Анотація

Матвієнків С. М., Бартах Л. І. **Інформаційні загрози в умовах повномасштабної війни: сучасні виклики для національної безпеки України.** – Стаття.

У статті досліджується комплексний вплив ключових загроз національній безпеці України через уразливість її інформаційного простору в умовах російсько-української гібридної війни. Гібридний характер цього конфлікту передбачає поєднання традиційних військових дій із широкомасштабними інформаційними та кібератаками, що робить захист інформаційного простору критично важливим для забезпечення стабільності держави. Особлива увага приділена дослідженню сучасних інструментів інформаційної війни, таких як дезінформація, фейкові новини, пропаганда, інформаційні маніпуляції та психологічні операції. Ці інструменти використовуються для підриву суспільної довіри, поглиблення політичних та соціальних розколів у суспільстві, а також для зменшення міжнародної підтримки України. У статті розглянуто такі загрози, як масові дезінформаційні кампанії, спрямовані на дискредитацію українських органів влади, посів розбрату між регіонами та етнічними групами в Україні, а також вплив на електоральні процеси. Досліджено роль кіберзагроз у цьому контексті, зокрема хакерські атаки на критичну інфраструктуру, урядові установи та засоби масової інформації, що підривають не лише внутрішню безпеку, а й міжнародний імідж України. Окремий акцент зроблено на інформаційних стратегіях росії, спрямованих на розпалювання мовних та культурних конфліктів, маніпуляцію історичною пам'яттю та створення фальшивих наративів для виправдання агресії. Проаналізовано конкретні приклади успішних і неуспішних інформаційних операцій з боку росії, що мали на меті деморалізацію українського суспільства та зниження його опору агресії. У статті також розглядаються механізми протидії цим загрозам, включаючи вдосконалення законодавства у сфері інформаційної безпеки, посилення спроможностей державних органів у боротьбі з кібератаками та інформаційними впливами. Окрема увага приділяється необхідності підвищення рівня медіаграмотності населення, що дозволить громадянам краще розпізнавати фейкову інформацію та не піддаватися маніпуляціям. Важливою складовою стратегій протидії є міжнародне співробітництво України з західними партнерами, спрямоване на обмін досвідом та ресурсами у сфері кібербезпеки та інформаційної оборони. Автори доходять висновку, що для ефективної протидії гібридній війні необхідно впроваджувати комплексний підхід до захисту інформаційного простору, що передбачає як технічні заходи кібербезпеки, так і підвищення стійкості суспільства до інформаційних атак. Створення стійкого, захищеного інформаційного середовища є запорукою зміцнення національної безпеки України та її позицій на міжнародній арені.

Ключові слова: національна безпека, інформаційний простір, інформація, держава, Україна, російсько-українська війна, повномасштабне вторгнення.

Summary

Matvienkiv S. M., Bartakh L. I. **Information threats in the context of a full-scale war: modern challenges for the national security of Ukraine.** – Article.

The article examines the complex impact of key threats to Ukraine's national security due to the vulnerability of its information space in the context of the russian-Ukrainian hybrid war. The hybrid nature of this conflict involves a combination of traditional military operations with large-scale information and cyber attacks, which makes the protection of the information space critical to ensuring the stability of the state. Particular attention is paid to the study of modern tools of information warfare, such as disinformation, fake news, propaganda, information manipulation, and psychological operations. These tools are used to undermine public trust, deepen political and social divisions in society, and reduce international support for Ukraine. The article examines such threats as massive disinformation campaigns aimed at discrediting Ukrainian authorities, sowing discord between regions and ethnic groups in Ukraine, and influencing electoral processes. The role of cyber threats in this context is analyzed, including hacker attacks on critical infrastructure, government agencies, and media, which undermine not only internal security but also Ukraine's international image. A special emphasis is placed on russia's information strategies aimed at fomenting linguistic and cultural conflicts, manipulating historical memory, and creating false narratives to justify aggression. The article analyzes specific examples of successful and unsuccessful information operations by russia aimed at demoralizing Ukrainian society and reducing its resistance to aggression. The article also discusses the mechanisms for countering these threats, including improving information security legislation, strengthening the capabilities of government agencies to combat cyberattacks and information influences. Special attention is paid to the need to increase the level of media literacy of the population, which will allow citizens to better recognize fake information and avoid manipulation. An important component of counteraction strategies is Ukraine's international cooperation with Western partners aimed at exchanging experience and resources in the field of cybersecurity and information defense. The authors conclude that in order to effectively counter hybrid warfare, it is necessary to implement a comprehensive approach to protecting the information space, which includes both technical cybersecurity measures and increasing the resilience of society to information attacks. Creating a stable, secure information environment is the key to strengthening Ukraine's national security and its position in the international arena.

Key words: national security, information space, information, state, Ukraine, Russian-Ukrainian war, full-scale invasion.