УДК 321.28
DOI: https://doi.org/10.32782/2312-1815/2024-1-4

Володимир Галіпчак
ORCID: 0009-0006-2501-0290

ІНФОРМАЦІЙНА ВІЙНА ЯК СКЛАДОВА ГІБРИДНОЇ ВІЙНИ В УМОВАХ РОСІЙСЬКОЇ АГРЕСІЇ

У статті досліджується роль інформаційної війни в контексті гібридної війни на прикладі російської агресії стосовно України та інших країн світу. Тема інформаційної війни залишається в центрі уваги науковців, політиків і громадськості, а її вивчення має важливе значення для розуміння та протидії сучасним викликам у геополітичному просторі. Проаналізовано основні цілі та методи впливу й ведення інформаційної війни в контексті як гібридної війни, так і повномасштабного вторгнення. Досліджено вплив кібер і мас-медіа на роль держави в умовах військових конфліктів.

Розглянуто важливість інформаційної війни як складової гібридної війни, оскільки інформаційна сфера відіграє ключову роль у формуванні громадської думки, впливає на настрої населення, має значний вплив на дипломатичні процеси та міжнародні відносини. Розуміння таких методів і прийомів інформаційної війни є важливим для країн, які стикаються з гібридною війною, особливо в контексті російської агресії. У статті також аналізуються можливі стратегії протидії інформаційній війні в умовах російської агресії, включно з розвитком кіберзахисту, підвищенням інформаційної грамотності суспільства та підтримкою незалежних ЗМІ. У контексті гібридної війни, де межа між військовим і цивільним впливом змішується, ця стаття розглядає важливість координації та співпраці між силами безпеки, правоохоронними органами й іншими зацікавленими сторонами для ефективного протидії інформаційній агресії. Крім того, у статті обговорюється важливість освіти та підвищення інформаційної грамотності суспільства, щоб громадяни були здатні розпізнавати й реагувати на дезінформацію. Особлива увага приділяється співпраці міжнародних партнерів у боротьбі з інформаційною війною та зміцненню кібербезпеки. Стаття також звертає увагу на потребу у створенні міжнародних стандартів і домовленостей, які регулювали б питання кібербезпеки й інформаційної війни.

Наголошено на необхідності глибокого розуміння й аналізу інформації, що надходить до суспільства, а також важливості критичного мислення та здатності розпізнавати дезінформацію. Важливо розробляти та впроваджувати стратегії інформаційної безпеки, співпрацювати з міжнародними партнерами й залучати громадськість до активної ролі в розпізнаванні та протидії інформаційній війні.

Ключові слова: *інформаційна війна, гібридна війна, російська агресія, цілі інформаційної війни, методи ведення інформаційної війни.*

Вступ. З початком повномасштабного російського вторгнення у 2022 році дедалі ширше постає питання та значення ролі інформаційної війни як однієї з провідних складових гібридної війни. Постановка проблеми полягає в розгляді впливу інформаційної війни на гібридну війну, яку Російська Федерація веде проти різних країн, зокрема проти України. Ця проблема виникає в контексті зростаючої важливості інформаційного простору та використання його для досягнення політичних і військових цілей. До основних аспектів проблеми належать: маніпуляція громадською думкою, завдання політичного й економічного тиску, наслідки для безпеки та стабільності. Розуміння й ефективна протидія інформаційній війні стають важливими завданнями для України та країн, які стикаються з російською агресією, з метою збереження безпеки, стабільності та демократичних цінностей.

Мета та завдання статті. Мета статті – проаналізувати важливість і вплив інформаційної війни як ключової складової гібридної війни, яку Російська Федерація веде проти різних країн, зокрема України. Головними завданнями статті є: дослідження сутності інформаційної війни, розуміння гібридної війни, роль інформаційної війни в російській агресії – наслідки

та виклики: протидія та захист. Мета статті полягає в освітленні та збагаченні розуміння щодо важливості інформаційної війни як складової гібридної війни в контексті російської агресії.

Методи дослідження. Реалізація дослідницької мети може використовувати різні методи та підходи для збору й аналізу інформації, до основних можна віднести:

– **емпіричні дослідження:** збір та аналіз фактичних даних через спостереження, інтерв'ю, опитування або аналіз документів. Емпіричні дані можуть включати реакції суспільства на інформаційні кампанії або оцінку ефективності заходів протидії;

– **аналіз історичних подій:** вивчення історії російської агресії та попередніх прикладів інформаційної війни. Аналіз подій дає змогу виявити патерни та стратегії, використовувані в минулому;

– **кейс-стаді:** розгляд конкретних кейсів інформаційної війни в контексті російської агресії. Це може передбачати аналіз конкретних інцидентів, таких як кібератаки або маніпуляції інформацією;

– **аналіз кібернетичних аспектів:** дослідження впливу кібернетичних атак на інформаційну безпеку та гібридну війну. Аналіз технік, методів і інструментів, використовуваних у кіберпросторі;

– **геополітичний аналіз:** вивчення геополітичного контексту та впливу російської агресії на міжнародну політику й відносини. Розгляд аспектів міжнародної співпраці у протидії інформаційній агресії;

– **аналіз літератури:** рецензія на наявні теорії, концепції та дослідження, пов'язані з інформаційною війною та гібридною війною. Це може передбачати огляд академічних статей, книг, звітів із досліджень та інших джерел.

Ці методи можуть використовуватися окремо або комбінуватися для отримання комплексного розуміння теми та розкриття ключових аспектів інформаційної війни в умовах російської агресії.

Аналіз останніх досліджень. З часу початку російської агресії в Україні з'явилося чимало публікацій із цієї тематики, однак не всі вони несли прогностичний характер у своїх дослідженнях. До важливих вітчизняних доробок варто віднести праці Геращенка А. М. і Поліщука І. М., Степаненка В. В., Кириченка О. В., Демченка В. С., Войтенка О. Г., Рачковської Л. В.

У закордонній політичній науці до проблем вивчення інформаційних війн та військової стратегії в умовах гібридних війн спостерігається великий інтерес серед вчених: Рід Т. «Кібервійна не відбудеться», Джайлс К., Гофман Ф. Г. «Гібридна війна та виклики» розглядають гібридну війну, включно з інформаційною складовою, як сучасну стратегічну загрозу та виклик для національної безпеки та ін.

Виклад основного матеріалу дослідження. Інформаційна війна визначається як систематичне використання інформаційних ресурсів із метою впливу на громадську думку, створення сприятливих умов для досягнення власних політичних чи військових цілей. Інформаційна війна є важливою складовою гібридної війни, особливо в контексті російської агресії. Роль інформаційної війни в гібридних конфліктах є надзвичайно важливою і стратегічною.

Інформаційна війна виступає як одна з ключових складових гібридної війни, яка поєднує різні форми агресії та використовується з метою досягнення політичних, економічних і військових цілей.

Роль інформаційної війни в гібридних конфліктах полягає в тому, що вона допомагає створити незбалансовану інформаційну картину, підриває стабільність і довіру у суспільстві та може мати значний вплив на результати конфлікту.

Російська агресія справді має значний вплив на країни, зокрема Україну, яка є однією з основних жертв цього конфлікту. Цей вплив та агресію можна розглядати в різних аспектах:

1) політичний і територіальний вплив:

– окупація та анексія – російська агресія призвела до анексії Криму Росією та підтримки конфлікту на сході України в Донецькій і Луганській областях і, як наслідок, до початку повномасштабного вторгнення на територію нашої держави. Це призвело до змін в політичній картині та територіальній цілісності України;

2) економічний вплив:

– економічне виснаження – війна з Росією суттєво вплинула на економічні аспекти України, зокрема, через втрати територій і зниження рівня економічної активності;

3) інформаційна війна та дезінформація:

– маніпуляція інформацією – російська агресія супроводжується інтенсивною інформаційною війною, включно з дезінформацією та маніпуляціями для впливу на громадську думку та міжнародні відносини;

4) гуманітарні наслідки:

– внутрішні переселенці та біженці – конфлікт призвів до великої кількості внутрішніх переселенців і біженців, що створює гуманітарну кризу та викликає виклик для соціальної інфраструктури;

5) безпекові загрози:

– кібернетичні атаки – російська агресія спричиняє кібернетичні загрози, що можуть мати серйозний вплив на інформаційну безпеку та критичну інфраструктуру;

6) міжнародні відносини та санкції:

– ізоляція Росії – конфлікт призвів до ізоляції Росії на міжнародній арені через введення санкцій та обмежень, що впливають на її економіку та стосунки з іншими країнами [4].

Усі ці аспекти свідчать про комплексний вплив російської агресії на Україну, що охоплює політичні, економічні, соціальні та безпекові сфери. Це викликає потребу в ретельному дослідженні та розробці стратегій для протидії цьому впливу й відновлення стабільності в регіоні. Розглянемо детальніше саме інформаційні операції та інформаційну війну як засіб протидії російській агресії.

Основні цілі інформаційної війни можуть варіюватися залежно від конкретної ситуації і мети агресора. Однак основні цілі, які часто переслідуються в інформаційній війні, такі:

1. Маніпуляція громадською думкою. Одна з ключових цілей інформаційної війни – це маніпуляція громадською думкою з метою зміни уявлень, поглядів і поведінки людей. Це може передбачати поширення фейкових новин, дезінформацію, пропаганду та маніпулювання інформацією з метою впливу на переконання та вірування громадськості.

2. Створення хаосу та дезорієнтації. Інформаційна війна може мати за мету створення хаосу, паніки та дезорієнтації в цільовому суспільстві або країні. Шляхом поширення дезінформації, спотворення фактів та створення конфліктів можна збурити громадську стабільність і підривати довіру до влади.

3. Зниження морально-психологічного стану противника. Інформаційна війна може спрямовуватися на зниження морально-психологічного стану противника, створення паніки та нервової напруги. Це може передбачати психологічну дезорієнтацію, психологічний тиск і поширення загроз із метою впливу на рішення та поведінку противника.

4. Вплив на політичну ситуацію. Інформаційна війна може бути спрямована на вплив на політичну ситуацію в країні-жертві або вплив на політичні рішення зовнішніх держав. Це може передбачати дискредитацію політичних лідерів, спотворення інформації про політичні події та створення сприятливого політичного середовища для агресора.

5. Загроза кібербезпеці. У сучасному світі інформаційна війна часто супроводжується кібератаками та хакерськими діями. Одна із цілей інформаційної війни може полягати в порушенні кібербезпеки країни-жертви, зламі інформаційних систем, викраденні конфіденційної інформації та створенні хаосу в кіберпросторі [3].

Ці цілі відображають важливість інформаційної війни як стратегічного інструменту для досягнення політичних, економічних і військових цілей агресора. Говорячи про основні методи інформаційної війни, варто зазначити, що інформаційна війна передбачає різноманітні методи та підходи, що використовуються для досягнення відповідних цілей. До найбільш поширених методів інформаційної війни належать: пропаганда, дезінформація, кібератаки, використання соціальних мереж і медіа, штучного інтелекту й автоматизації, викрадення та злам.

Ці методи інформаційної війни використовуються з метою маніпулювання, дезорієнтації та впливу на суспільство, політику, економіку та безпеку цільових країн.

Говорячи про розвиток інформаційних воєн, варто сказати, що саме російська агресія несе чи не одну з найбільш руйнівних і деструктивних сил у світі в цьому контексті. Так, до основних рис інформаційної війни в контексті російської агресії відносимо такі елементи:

1. Психологічна операція. Інформаційна війна передбачає психологічні операції, спрямовані на вплив на свідомість та емоції людей. Це може бути психологічний тиск, створення страху, образи та злочини, щоб дискредитувати опонентів і збільшити підтримку власної агресії.

2. Пропаганда та дезінформація: російська агресія використовує пропаганду та дезінформацію для поширення спотвореної або фальшивої інформації. Це може передбачати поширення фейкових новин, маніпулювання фактами та створення негативного образу країни – жертви агресії.

3. Використання соціальних медіа та інтернету. Тут слід особливо звернути увагу на інформаційній грамотності населення. Вона означає здатність людей критично оцінювати, аналізувати та розуміти інформацію, яку вони споживають. До основних критеріїв інформаційної грамотності належать: критичне мислення (здатність аналізувати інформацію, розрізняти факти від дезінформації, визначати джерела й оцінювати їх достовірність – інформаційно грамотні люди вміють розпізнавати надійні джерела інформації від ненадійних; здатність до факт-чекінгу – інформаційно грамотні особи активно перевіряють факти, перш ніж довіряти чи поширювати інформацію, вони використовують різні джерела, провіряють факти, переконуються в їх достовірності та перевіряють контекст, у якому представлені; застосування критеріїв оцінки інформації – інформаційно грамотні люди використовують різні критерії для оцінки інформації, такі як джерело, авторитетність, доказова база, об'єктивність і контекст). Російські агенти активно використовують соціальні медіа та інтернет-платформи для поширення пропагандистського матеріалу та дезінформації. Це, зокрема, створення фейкових акаунтів, ботів і спеціальних коментаторів, які підтримують російську агресію та спотворюють дійсність [1].

4. Кібератаки та хакерські атаки: російська агресія також включає кібератаки та хакерські атаки, спрямовані на злам інформаційних систем, розповсюдження вірусів та крадіжку конфіденційної інформації. Це дає змогу викрадати важливі дані, перешкоджати роботі урядових структур і впливати на критично важливу інфраструктуру [10].

Геополітична ситуація Росії у веденні інформаційних воєн визначається комплексом факторів, що охоплюють політичні, економічні та соціокультурні аспекти. Росія використовує інформаційну війну як засіб досягнення своїх стратегічних цілей на міжнародній арені. Серед основних прикладів країн світу варто назвати такі:

• Грузія: Росія втручалася внутрішні справи Грузії, зокрема, шляхом військової інтервенції та визнання незалежності Абхазії та Південної Осетії. Інформаційна війна була використана для легітимізації цих дій та зміни громадської думки.

• Молдова: російська агресія також стосується Молдови, зокрема придністровського конфлікту, де Росія підтримує сепаратистські структури та військові сили. Інформаційна війна була використана для маніпулювання громадською думкою та створення незгоди серед населення.

• Балтійські країни: Литва, Латвія та Естонія також стикаються з впливом російської агресії, зокрема в енергетичному секторі, інформаційній сфері та військових провокаціях. Інформаційна війна використовується для створення напруженості та дезорієнтації в цих країнах.

• Сирія: Росія активно використовує інформаційну війну у своїй війні в Сирії. Вона поширює пропаганду та дезінформацію щодо своїх воєнних дій, зокрема стосовно цілей, методів і наслідків війни. Російські ЗМІ та інтернет-боти активно пропагують свою версію подій і впливають на громадську думку [7].

• Сполучені Штати Америки: втручання у вибори. Росія відома своїм втручанням у виборчі процеси у США через соціальні мережі та розповсюдження дезінформації [10].

Якщо говорити про нашу державу, слід сказати, що Україна зазнає найбільшого впливу російської агресії, активна фаза якої почалась у 2014 році з анексії Криму. Росія анексувала Крим, використовуючи комбінацію військових дій та інформаційної війни. Вона поширювала дезінформацію, фейкові новини та пропаганду, щоб створити непорозуміння та підтримку серед населення Криму для приєднання до Росії; підтримувала сепаратистські рухи на сході України, використовуючи інформаційну війну для маніпуляції громадською думкою. Вона поширює дезінформацію, пропаганду та використовує соціальні мережі для формування образу конфлікту та створення поділу в суспільстві [6].

Ці приклади свідчать про широкий спектр використання інформаційної війни Росією з метою досягнення своїх політичних та військових цілей. Вона використовує різні методи та засоби, щоб маніпулювати громадською думкою, створювати дезорієнтацію та досягати своїх стратегічних цілей [2].

Починаючи з 2022 року, з моменту початку повномасштабного російського вторгнення на територію України, Росія веде військові дії, порушуючи суверенітет і територіальну цілісність України, тим самим започатковуючи фазу відкритої, зокрема інформаційної, війни.

Висновки. Отже, варто зазначити, що в контексті війни між Україною та Росією рівень інформаційної війни від української сторони значно менший порівняно з російським. Однак Україна також використовує інформаційні інструменти для впливу на громадську думку та сприяння своїм цілям, тим самим успішно здійснюючи як внутрішню, так і зовнішню політику протидії російській агресії. Узагальнюючи основні методи ведення інформаційної війни нашої держави, варто ще раз підкреслити такі:

– посилення медійної присутності – Україна звернула більше уваги на засоби масової інформації, які підтримують українську позицію та розповсюджують правдиву інформацію щодо конфлікту. Українські медіа, які діють в умовах конфлікту, намагаються донести свої повідомлення до міжнародного співтовариства та громадськості;

– активне використання соціальних мереж – Україна активно використовує соціальні мережі для поширення своєї позиції та висвітлення ситуації в районах, що постраждали від конфлікту. Створюються ресурси та групи, які розповсюджують новини, факти та переконують у своїй правоті;

– міжнародна комунікація – Україна використовує дипломатичні канали, міжнародні організації та співробітництво з партнерами для розповсюдження інформації про російську агресію та впливу на формування світової думки.

Також на прикладі інших країн світу виявлено, як Росія використовує інформаційні технології для досягнення своїх стратегічних цілей. Дезінформація, втручання у виборчі процеси, підтримка проросійських рухів та інші методи стають частою практикою для забезпечення впливу на рішення та настрої суспільств.

Висновки статті підкреслюють потребу в розвитку стратегій протидії інформаційній війні, зокрема, в умовах російської агресії. Такі заходи, як кіберзахист, підвищення інформаційної грамотності суспільства та співпраця міжнародних партнерів, визначаються як ключові

для зміцнення обороноздатності та резистентності країн перед інформаційними загрозами. Визначено необхідність активного залучення громадськості до розпізнавання та протидії інформаційній війні. Глибоке розуміння та критичне мислення стають ключовими елементами успішного протистояння цьому складному виклику.

Підсумовуючи вищесказане, варто зазначити, що масштаб інформаційної війни з боку України значно менший порівняно з Росією, оскільки Росія володіє значними ресурсами, контролює засоби масової інформації та використовує широку мережу агентурних структур. Україна стикається з необхідністю захищатися від російської пропаганди й інформаційних атак, намагаючись зберегти свою суверенність та стабільність, і, слід зазначити, з гідністю проходить це випробування.

Література:

1. Войтенко О. Г., Рачковська Л. В. Інформаційна війна Російської Федерації проти України: методи, засоби, наслідки. Київ : Державний інститут керівних кадрів. 2018. С. 16–22.

2. Геращенко А. М., Поліщук І. М. Інформаційна війна: сучасні виклики та загрози національній безпеці. Київ : Кондор. 2016. С. 155.

3. Єрмак О. М., Шевченко С. М. Інформаційна війна в контексті гібридної війни Росії проти України. Київ : Інститут національної безпеки. 2017. С. 12–21.

4. Мацегора О. Інформаційна війна в контексті гібридної війни проти України. Вісник Черкаського державного технологічного університету. *Серія: Економічні науки.* 2019. № 1 (3), с. 99–106.

5. Мороз О. В. Інформаційна безпека держави в умовах гібридної війни. Київ : Національна академія державного управління при Президентові України. 2016.

6. Степаненко В. В., Кириченко О. В., Демченко В. С. Гібридна війна: загроза національній безпеці України. Київ : Інститут національної безпеки. 2015. С. 24–35.

7. Чубарова Е., Шадур А. Інформаційна гібридна війна Росії проти України: особливості та наслідки. *Політологічні читання.* 2017. № 1, с. 202–207.

8. Giles K. Russia's "Hybrid Warfare": How the Kremlin is Reinventing War in the 21st Century. The Atlantic Council. 2015.

9. Hoffman F.G. Hybrid Warfare and Challenges. Joint Force Quarterly. 2011.

10. Rid T. Cyber War Will Not Take Place. Oxford University Press. 2013.

11. Watts C. Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News. Harper Collins. 2018.

References:

1. Voytenko, O. G., & Rachkovska, L. V. (2018). Informatsiyna viyna Rosiyskoyi Federatsiyi proty Ukrayiny: metody, zasoby, naslidky [Information war of the Russian Federation against Ukraine: methods, means, consequences]. Kyiv: Derzhavnyy instytut kerivnykh kadriv. P. 16–22 [in Ukrainian].

2. Herashchenko, A. M., & Polishchuk, I. M. (2016). Informatsiyna viyna: suchasni vyklyky ta zahrozy natsionalniy bezpetsi [Information warfare: modern challenges and threats to national security]. Kyiv: Kondor, pp. 155 [in Ukrainian].

3. Yermak, O. M., & Shevchenko, S. M. (2017). Informatsiyna viyna v konteksti gibrydnoyi viyny Rosiyi proty Ukrayiny [Information warfare in the context of Russia's hybrid war against Ukraine]. Kyiv: Instytut natsionalnoyi bezpeky, pp. 12–21 [in Ukrainian]

4. Matsehora, O. (2019). Informatsiyna viyna v konteksti gibrydnoyi viyny proty Ukrayiny [Information warfare in the context of a hybrid war against Ukraine]. *Visnyk Cherkaskoho derzhavnoho tekhnolohichnoho universytetu. Seriya: Ekonomichni nauky*, no 1 (3), pp. 99–106 [in Ukrainian].

5. Moroz, O. V. (2016). Informatsiyna bezpeka derzhavy v umovakh gibrydnoyi viyny [Information security of the state in conditions of hybrid warfare]. Kyiv: Natsionalna akademiya derzhavnoho upravlinnya pry Prezydentovi Ukrayiny [in Ukrainian].

6. Stepanenko, V. V., Kyrychenko, O. V., & Demchenko, V. S. (2015). Gibrydna viyna: zahroza natsionalniy bezpetsi Ukrayiny [Hybrid war: a threat to the national security of Ukraine]. Kyiv: Instytut natsionalnoyi bezpeky. P. 24–35 [in Ukrainian].

7. Chubarova, E., & Shadur, A. (2017). Informatsiyna gibrydna viyna Rosiyi proty Ukrayiny: osoblyvosti ta naslidky [Hybrid information war of Russia against Ukraine: features and consequences]. *Politolohichni chytannya*, no 1, pp. 202–207 [in Ukrainian].

8. Giles, K. (2015). Russia's "Hybrid Warfare": How the Kremlin is Reinventing War in the 21st Century. The Atlantic Council.

9. Hoffman, F.G. (2011). Hybrid Warfare and Challenges. Joint Force Quarterly.

10. Rid, T. (2013). Cyber War Will Not Take Place. Oxford University Press.

11. Watts, C. (2018). Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News. Harper Collins.

Volodymyr Halipchak. Information warfare as a component of hybrid warfare under conditions of Russian aggression

This article examines the role of information warfare in the context of hybrid warfare using the example of Russian aggression against Ukraine and other countries of the world. The topic of information warfare remains in the center of attention of scientists, politicians and the public, and its study is important for understanding and countering contemporary challenges in the geopolitical space.

The article examines the importance of information warfare as a component of hybrid warfare, as the information sphere plays a key role in shaping public opinion, influences the mood of the population, and has a significant impact on diplomatic processes and international relations. Understanding such methods and techniques of information warfare is important for countries facing hybrid warfare, especially in the context of Russian aggression.

The article also analyzes possible strategies for countering information warfare in the face of Russian aggression, including the development of cyber defense, increasing information literacy of society, and supporting independent mass media. In the context of hybrid warfare, where the line between military and civilian influence is blurred, this article examines the importance of coordination and cooperation between security forces, law enforcement agencies, and other stakeholders to effectively counter information aggression.

In addition, the article discusses the importance of education and increasing the information literacy of society so that citizens are able to recognize and respond to disinformation. Particular attention is paid to the cooperation of international partners in the fight against information warfare and strengthening cyber security. The article also draws attention to the need to create international standards and agreements that would regulate issues of cyber security and information warfare.

The article highlights the need for in-depth understanding and analysis of information coming to society, as well as the importance of critical thinking and the ability to recognize misinformation. It is important to develop and implement information security strategies, collaborate with international partners, and involve the public in an active role in recognizing and countering information warfare.

Key words: *information war, hybrid war, Russian aggression, goals of information war, methods of conducting information war.*