ISSN 2312-1815

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА

ВІСНИК
ПРИКАРПАТСЬКОГО УНІВЕРСИТЕТУ

СЕРІЯ: ПОЛІТОЛОГІЯ

Випуск 15

Видається з 2006 р.

Видавничий дім
«Гельветика»
2023

УДК 32

Затверджено до друку вченою радою
Прикарпатського національного університету імені Василя Стефаника
(протокол № 11 від 22 грудня 2023 р.)

Адреса редакційної колегії:
76025, м. Івано-Франківськ, вул. Шевченка, 57
Факультет історії, політології і міжнародних відносин
Прикарпатського національного університету імені Василя Стефаника

Вісник Прикарпатського університету. Серія: Політологія / Прикарпатський національний університет імені Василя Стефаника. Одеса: Гельветика. 2023. Вип. 15. 70 с. ISSN 2312-1815. – Резюме укр., англ. мовами

У збірнику вміщено наукові статті, присвячені актуальним проблемам теорії та історії політичної науки, політичним інститутам і процесам, геополітиці й міжнародним відносинам і дослідженням молодих науковців.

ЗМІСТ

ПОЛІТИЧНІ ІНСТИТУТИ ТА ПРОЦЕСИ

ПОЛІТИЧНІ ПРОБЛЕМИ МІЖНАРОДНИХ СИСТЕМ ТА ГЛОБАЛЬНОГО РОЗВИТКУ

CONTENTS

POLITICAL INSTITUTIONS AND PROCESSES

POLITICAL PROBLEMS OF INTERNATIONAL SYSTEMS AND GLOBAL DEVELOPMENT

ПОЛІТИЧНІ ІНСТИТУТИ ТА ПРОЦЕСИ

УДК 316.46:32:27-587.6]17.022.1:32-059.1
DOI: https://doi.org/10.32782/2312-1815/2024-1-1

Назарій Баюрчак
ORCID: 0000-0001-8946-5493

ФОРМУВАННЯ ІМІДЖУ ПОЛІТИКА ЧЕРЕЗ КОНСТРУЮВАННЯ ОБРАЗУ ХАРИЗМАТИЧНОГО ЛІДЕРА

У статті досліджено сучасні проблеми харизматичного лідерства. В інформаційну епоху для створення харизматичного образу лідера використовуються технології формування іміджу. Інформаційні технології дають змогу створювати штучний образ політиків, що масово поширюється серед громадян. Для досягнення політичного лідерства, особливо під час виборчої кампанії, формується найпривабливіший для виборців імідж. Візуалізація політичного життя збільшує роль зовнішніх характеристик, які домінують над змістом політичної програми. Для досягнення політичного лідерства, що має, зокрема, харизматичний характер, потрібно керуватися політикою сприйняття й активно використовувати інформаційні технології.

Ключові слова: *політичний імідж, харизматичне лідерство, політичні технології, інформаційні технології, образ, виборча кампанія.*

Вступ. Проблема політичного лідерства належить до категорії питань, актуальність яких ніколи не ставиться під сумнів. Дослідження політичного лідерства носять як пізнавальний, так і прикладний характер, оскільки допомагають потенційним лідерам створювати механізми управління індивідами, а громадянам – розуміти ці механізми, розрізняти їх і в разі потреби їм протистояти. У ситуації сучасної політичної системи, що трансформується, відбувається суттєве розширення особистісної природи політики, що ставить перед дослідниками проблему розгляду явища «політичне лідерство» за нових методологічних підходів. Специфіка сучасного політичного процесу пов'язана з активізацією в ньому політичного лідера.

Мета та завдання. Мета статті – дослідити процес формування іміджу політика через конструювання елементів образу харизматичного лідера. Завдання – виокремити складові образу харизматичного лідера й навести конкретні способи застосування цих складових для формування іміджу політика.

Методологічною базою для дослідження слугували системний підхід, структурно-функціональний аналіз, метод синтезу, порівняльний аналіз, моделювання, семантичний аналіз та історичний підхід. Методологічна база статті спирається на вивчення чинників, характеру та напрямів стратегії щодо формування ефективного дієвого іміджу політичного лідера. Зважаючи на комплексний характер категорії харизматичний імідж, під час аналізу використаний системний підхід, що полягає в трактуванні іміджу як складної динамічної системи, яка розкривається через взаємодію внутрішніх і зовнішніх формоутворювальних чинників різних сфер соціально-політичного економічного та культурного життя. Для досягнення мети й поставлених завдань у роботі застосовані загальнонаукові та спеціальні методи соціально-політичних наук, зокрема методи теорії міжнародних відносин і політології. За допомогою використання загальнонаукових методів аналізу та синтезу виявлені закономірності формування харизматичного іміджу в політиці. Застосування історичного методу дало змогу розглянути еволюцію

концепцій іміджелогії з новітнього періоду. Застосування структурно-функціонального методу виявило складові харизматичного іміджу політичного лідера.

Виклад основного матеріалу дослідження. На цей час актуалізується проблема харизматичного лідерства, виникає потреба перегляду цього поняття відповідно до сучасних реалій та відокремлення особливостей і характеристик харизматичного лідера.

Р. Ітвел звертає увагу на цікавий феномен: потреба в харизматичних лідерах зростає не тільки у Східній Європі, а й у країнах Заходу. Він висуває низку гіпотез, що характеризують харизматичне лідерство [4, с. 15].

Гіпотеза 1. Положення про аномію. Стверджується, що харизматичні лідери привабливі, особливо для тих, хто, зазнаючи раптових змін, постраждав від втрати соціальної вкоріненості.

Гіпотеза 2. Положення про «довірчий контроль». Стверджується, що харизматичні лідери привабливі, оскільки вони дають нагоду людям, які відчувають безсилля, знову відчути свій вплив на політиків і події.

Гіпотеза 3. Положення про історичну легітимацію. Стверджується, що харизматики мають широке визнання, оскільки вони здатні уявити себе відповідними легітимній національній традиції.

Гіпотеза 4. Положення про авторитарність. Стверджується, що харизматичні лідери привабливі для тих, хто схильний до підпорядкування сильній владі.

Гіпотеза 5. Положення про низький рівень довіри до партій. Стверджується, що політики харизматичного типу набувають визнання, коли основним партіям не довіряють [8, с. 221].

Гіпотеза 6. Положення про «інституційну» харизму. Стверджується, що зайняття вищих постів, особливо виборного президентського, може принести додаткову харизму лідерові.

Гіпотеза 7. Харизматичний лідер викликає особливо інтенсивну ідентифікацію. Стверджується, що харизма є чимось більшим, ніж лише популярність чи повага: вона має на увазі сильне почуття ідентифікації з місією такого лідера.

Гіпотеза 8. Підтримка лідера іконного типу ґрунтується на раціональних факторах, таких як успіхи минулої кар'єри. Для іконного лідера типова демонстрація минулих успіхів, чи таланту, чи тісних зв'язків із важливими групами впливу [9, с. 131].

Отже, можна назвати такі риси харизматичних лідерів:

1. Особлива місія, яка полягає у проведенні радикальної зміни чи порятунку нації. Такі лідери можуть робити вибір між своїми обіцянками та компромісами, але вони керуються певною формою месіанського призначення. Ідея радикальної зміни не повинна висуватися у ясному, закінченому вигляді.

2. Особисте представництво. У ранніх роботах, присвячених харизмі, зазвичай виділялися ораторські здібності лідера. У пізніших – можливості створити правильний образ на телебаченні. Ця риса ґрунтується на візуалізації, хоч і не пов'язана безпосередньо із фізичною привабливістю.

3. Мачизм. Харизма зазвичай виступає чоловічою формою наративу – символізму, тоді як жінки можуть символізувати політичні ідеї, харизма більше асоціюється з дією, героїкою тощо (часто з війною чи кризою).

4. Наративи про жертовність і боротьбу [4, с. 120].

5. Цілі залучення або цілі ідентичності. Г. Гарднер щодо лідерства вважає, що «лідери та аудиторія перетинаються у багатьох історіях, але основна історія має справу з питаннями ідентичності. Той лідер, який досяг успіху у висловленні нової версії історії цієї групи, виявляється найбільш дієвим... Більшість лідерів надавали перевагу історіям, які мали ефект залучення, спонукали індивідів думати себе як частину ширшого співтовариства».

6. Категорії «друг – ворог». Хоча харизматичні лідери зазвичай прагнуть відтворення почуття спільності, важливою частиною їхнього озброєння виступає пошук ворогів.

В одних випадках це внутрішні вороги, які є елементом справжнього суспільства, в інших – зовнішні вороги.

7. Активізм прихильників. Харизматичні лідери також схильні чекати більшого від своїх прихильників, ніж іконні лідери.

Харизматичний образ лідера за доби інформаційних технологій формується за допомогою створення політичного іміджу. Імідж як форма відображення у свідомості людини предметного світу та соціальної дійсності існував на різних стадіях розвитку суспільства. У другій половині XX століття, коли інформаційні та телекомунікаційні технології посіли чільне місце у формуванні громадської думки, з'явилася іміджелогія як наука та навчальна дисципліна. Західна іміджелогія приділяє значну увагу дослідженню проблеми іміджу політика. Політична пропаганда і управління іміджем відіграють важливу роль у політичному процесі [6, с. 15].

Для створення відповідного публічного іміджу потрібний інформаційний контроль. Е. Гоффман називав такий феномен «навмисні жести» або «хибний крок». Розширення можливостей інформаційного суспільства призводить до того, що зростає імовірність невчасного вторгнення в життя політичного лідера. Отже, збільшується потреба протистояти таким ситуаціям із метою недопущення руйнування іміджу. Політикам доводиться боротися зі здатністю народу невідворотно підхоплювати й передавати інформацію. Політичні партії також замішані в цій діяльності, оскільки вони експлуатують бажання ЗМІ придбати сенсаційний контент і таким чином заохочують своїх прихильників шукати та розповсюджувати «випадкові» відео про своїх опонентів.

Контроль фахівців з іміджу над громадським сприйняттям їхніх клієнтів одночасно ізолює зовнішні ризики. Їхні методи передбачають рекламу й управління новинами за допомогою пресрелізів та інтерв'ю, постійне проведення кампанії з використанням усіх доступних ресурсів. Подібна ситуація сприяє тому, що публічні появи політиків розписані відповідно до сценарію, а політичний персонал не бажає допускати ЗМІ до контролю над кутом зйомки, вибором фотографій і структурою статті для політичного огляду. Для дослідження політичної обстановки відповідної підготовки політичного іміджу важливу роль відіграє моніторинг громадської думки [10, с. 15].

У західній науці цей феномен докладно аналізувався соціальними психологами, наприклад Дж. Алдерліхом і П. Гронки, відколи виникла потреба переглянути, яким чином виборці оцінюють кандидатів і формують переваги.

Далі, Р. Зайонц стверджував, що є дві системи незалежної політичної оцінки. Перша система передбачає швидку й поверхневу оцінку, друга система – більш повільну, деталізовану та глибоку. Інформація, яку мають виборці про кандидатів, дуже різноманітна. Така інформація стосується позиції, зовнішності, характеру, колишніх перемог і невдач. На основі даних відомостей виборець формує думку про імідж політичного лідера. Деякі дані можуть спонукати виборця більш глибоко й уважно досліджувати особливості політика. Інша частина інформації, що стосується, наприклад, зовнішності й характеристик характеру, викликає емоційну реакцію. Актуальним питанням залишається те, який із зазначених видів політичної оцінки переважає. Д. Редлоск і Р. Лоу відзначають, що пізнавальне сприйняття переважує афективне, хоча трапляються і зворотні ситуації. Як виняток наводяться вибори президента США у 2000 р., коли Е. Гор програв Дж. Бушу-молодшому, незважаючи на більш високу політичну компетентність. Проте його противнику вдалося привернути до себе виборців на емоційному рівні [7, с. 85].

Існує безліч факторів, які можуть визначити результат голосування за політичного лідера. Усі ці чинники разом становлять імідж кандидата. Детермінантами можуть стати групи тиску, політична історія сім'ї кандидата, економічні умови, особистий імідж чи партійна приналежність. Довгостроковими детермінантами є партійна ідентифікація та ідеологія,

короткостроковими – особисті якості кандидата і його позиція з актуальних питань. Виборець робить свій вибір, спираючись як на довгострокові, так і на короткострокові детермінанти.

Формування рішення виборця починається зі збору інформації. Пошук інформації може бути цілеспрямованим, або відомості можуть опинитися в полі зору виборця випадково. Як вказував Дж. Херштайн, «ця інформація може містити позицію кандидата з актуальних питань, минулі заслуги, зовнішність та інше». У. Нойман зазначає, що «політичні знання виборця фрагментарні, виборці не шукають специфічні факти про вибори, але збирають крихти інформації протягом передвиборних кампаній та формують загальне сприйняття основних питань та кандидатів». Частина виборців ґрунтує свої знання про кандидатів на виборчих бюлетенях. Більше зацікавлені виборці згадують образи та ідеї, які в них асоціюються з кандидатами. Частина виборців голосує лише з міркувань громадянського обов'язку, а інша частина оцінює кандидата та планує свій електоральний вибір [2, с. 134].

Позиція політика з актуальних питань важлива для виборця лише в таких випадках:

– виборці знають про такі питання та стурбовані ними;

– позиції кандидатів значно відрізняються одна від одної;

– виборці можуть порівнювати позиції кандидатів зі своїми власними.

Імідж політика формується поступово під час виборчої кампанії. Протягом цього часу сприйняття виборцем позиції кандидата перетворюється на сприйняття особистих характеристик політика. Отже, виборці оцінюють лідерський потенціал своїх майбутніх політичних лідерів.

Поза тим часто приписують людині певні властивості характеру, спираючись на фізичні особливості. Зовнішня привабливість виявляється значнішою характеристикою, ніж гідна поведінка. Непривабливі індивіди сприймаються негативно за низкою показників, вважаються менш соціально адаптованими, менш здоровими та менш розумними. Індивіди, що мають зайву вагу, часто розглядаються як ліниві, повільні й інтелектуально нерозвинені. Індивіди низького росту вважаються нижчими в професійному статусі та компетентності [4, с. 130].

З огляду на вищесказане можна дійти висновку, що зовнішність впливає на імідж політика. Політичні діячі та їх іміджмейкер розуміють важливість даних характеристик. За однією з версій, результати виборів можна передбачити, виходячи із зовнішніх даних кандидата. Такий висновок має велике значення для розуміння процесів прийняття рішень, розвитку демократії та політичного маркетингу.

Клас політиків приділяє пильну увагу управлінню репутацією, оскільки це є засобом для просування свого порядку денного та для перемоги на виборах. Вони усвідомлюють, що виборці наголошують на атрибутах лідера. Насправді, чим більше виборці схильні до впливу ЗМІ, тим більше цим фактом стурбовані політики. Іміджмейкери знають, що виборці часто покладаються на ненадійні сигнали, у тому числі візуальне сприйняття й особисті якості лідера. Наприклад, візуальні сигнали формують враження виборців про майстерність і компетентність лідера. Проте електоральна значимість іміджу політичного лідера може бути переоцінена [5, с. 111].

Б. Ньюман звертає увагу на маркетингові стратегії, які керують політичною системою. Ці стратегії дають змогу зробити образ важливішим, ніж сутність, особистість – важливішою, ніж актуальні питання політики та здатність до діалогу. Новинки починають сприйматись як розвага: вони повинні бути короткими, гострими і яскравими. Вважається, що це один з ефектів впливу телебачення на електоральний процес, особливо в Європі та США.

Для пересічного громадянина розрізнити імідж і реальність стає дедалі складніше. Політика «розчиняється» у ЗМІ, використовуючи механізми формування іміджу, що створюється на основі зовнішності та медійної обробки. Такі образи впроваджуються у свідомість громадян і визначають їх політичні уподобання, отже, вплив іміджу на результати політичних процесів не можна недооцінювати [3, с. 18].

За словами Б. Ньюмана, модернізація політики, що відбувається в останні десятиліття, повинна розумітися як комерціалізація, глобалізація та зростання ролі візуальної культури. Під час цих процесів ЗМІ відіграють визначальну роль. Отже, встановлюється нова динаміка політичної комунікації. Подібна тенденція, що характеризується узгодженням політики з логікою ЗМІ, називається політикою сприйняття.

Інформація, політика та розвага переплітаються й формують простір, у якому політики підкоряються правилам ЗМІ, перетворюючи політику на політику сприйняття. Стиль стає важливішим, ніж зміст, що призводить до потреби займатися управлінням політичних вражень. Отже, для управління політичними (особливо виборчими) процесами життєво важливо розуміти значення особистості, зовнішності та стилю для створення враження [9, с. 119].

Висновки і перспективи подальших досліджень. Таким чином, у цій статті було досліджено поняття політичного лідерства та політичного іміджу. Теоретично в політичному лідерстві одну з ключових позицій займає концепція харизматичного панування. Така концепція набуває нового формату в сучасних умовах, коли інформаційні технології дають змогу створювати штучний образ політиків, який масово поширюється серед громадян. ЗМІ стають ключовими гравцями в політичному процесі. Для досягнення політичного лідерства, особливо під час виборчої кампанії, потрібно сформувати найпривабливіший для виборців імідж і досягти його широкого поширення в масах. Через візуалізацію політичного життя збільшується роль зовнішніх, візуальних характеристик, які починають домінувати над змістом політичної програми. Отже, для досягнення політичного лідерства, що має, зокрема, харизматичний характер, слід застосовувати політику сприйняття та керувати враженнями громадян за допомогою інформаційних технологій.

Література:

1. Blondel J. Political Leadership: Towards a general analysis. London. 1987. 225 p.
2. Dowse R.E., & Hughes J.A. Political Sociology. London. 1986. 334 p.
3. Krech D. Individuals in Society. New York. 1962. 167 p.
4. McGraw K.M. Political impressions: Formation and Management. Oxford Hand-book of Political Psychology, 2003. 420 p.
5. Myron R. The New Leader: A revolutionary approach to effective leadership. New York, 1987. 307 p.
6. Parsons T. The Sociological Theory & Modern Society. New York, 1967. P. 225.
7. Hermann M.G.(Ed.) Political psychology. San Francisco: Jossey-Bass. 1986. P. 402.
8. Stogdill R. Handbook of Leadership: A Survey of Theory and Research. R.Stogdill. New York. 1974. 339 p.
9. Tucker R. The Theory of Charismatic Leadership. Daedalus. 1968. № 3. P. 731–756.
10. Weber M. Economy & Society. Los Angeles. 1978. P. 434.

References:

1. Blondel, J. (1987). *Political Leadership: Towards a general analysis*. London. P. 225.
2. Dowse, R.E., & Hughes, J.A. (1986). *Political Sociology*. London. P. 334.
3. Krech, D. (1962). *Individuals in Society*. New York. P. 167.
4. McGraw, K.M. (2003). *Political impressions: Formation and Management. Oxford Hand-book of Political Psychology*. P. 420.
5. Myron, R. (1987). *The New Leader: A revolutionary approach to effective leadership*. New York. P. 307.
6. Parsons, T. (1967). *The Sociological Theory & Modern Society*. New York. P. 225.
7. Hermann, M.G. (1986). *Political psychology*. San Francisko: Jossey-Bass. P. 402.
8. Stogdill, R. (1974). Handbook of Leadership: A Survey of Theory and Research. R.Stogdill. New York. P. 339.

9. Tucker, R. (1968). *The Theory of Charismatic Leadership. Daedalus*. № 3. P. 731–756.
10. Weber, M. (1978). *Economy & Society*. Los Angeles. P. 434.

Nazarii Baiurchak. Forming the image of a politician through constructing the image of a charismatic leader

This article explores contemporary issues of charismatic leadership. In the information age, image formation technologies are used to create a charismatic image of a leader. Information technologies make it possible to create an artificial image of politicians, which is widely distributed among citizens. To achieve political leadership, especially during an election campaign, the most attractive image for voters is formed. The visualization of political life increases the role of external characteristics that dominate the content of the political program. To achieve political leadership, which is especially charismatic, it is necessary to be guided by the politics of perception and actively use information technologies.

Key words: *political image, charismatic leadership, political technologies, information technologies, image, election campaign.*

УДК 321.01
DOI: https://doi.org/10.32782/2312-1815/2024-1-2

Олена Березовська-Чміль
ORCID: 0000-0002-3395-9141

ПОРІВНЯЛЬНИЙ АНАЛІЗ ДЕМОКРАТИЧНОГО ТА АВТОРИТАРНОГО ПОЛІТИЧНИХ РЕЖИМІВ

У статті здійснено порівняльний аналіз демократичного й авторитарного політичних режимів, їх характерних рис, особливостей і механізмів формування в сучасних державах.

Актуальність теми дослідження зумовлена дихотомією між двома найбільш поширеними в сучасному світі типами політичних режимів. Упродовж тривалого часу постійне протистояння між авторитарним і демократичним режимами породило безліч протиріч, що суттєво впливають на міждержавні відносини та розподіл сфер впливу на міжнародній арені.

На сучасному етапі у світовій політиці можемо спостерігати загострення конкурентної боротьби між демократією і диктатурою, між захистом прав людини і жорстким обмеженням цих прав, між свободою і всебічним контролем, між розвитком і стагнацією.

З'ясовано, що значна кількість держав вважають демократичний режим найбільш оптимальною моделлю управління завдяки принципам індивідуальної свободи, дотримання верховенства права, механізмам поділу влади та забезпечення прав людини. Основними характеристиками демократичного режиму є акцент на виборності та змінності представників влади, їх підзвітність народу, розвиток громадянського суспільства, свободи слова, незалежного суду, захист прав і свобод громадян, приватна власність та рівність можливостей для кожного.

Визначено, що авторитарний режим ґрунтується на жорсткій централізованій владі, обмеженні громадянських свобод, застосуванні репресій і контролю за населенням. Такий режим надає перевагу політичній стабільності та жорсткому управлінню, часто ціною гуманістичних принципів і прав людини. Авторитарні держави здійснюють контроль над ЗМІ, усувають лідерів опозиції та використовують цензуру як інструмент для зміцнення свого режиму.

Виявлено, що в деяких випадках авторитарний режим може маніпулювати й використовувати інструменти та фундаментальні принципи, пов'язані з демократією, спотворюючи та розмиваючи цінності, притаманні суспільству. Отже, громадська довіра до демократичного ідеалу може зруйнуватися, оскільки він стає інструментом маніпуляції представників влади.

Ключові слова: *політичний режим, права людини, свобода, демократія, авторитаризм, контроль.*

Вступ. Актуальність теми дослідження зумовлена тривалою дихотомією між двома найбільш поширеними в сучасному світі типами політичних режимів. Протягом тривалого часу постійне протистояння між авторитарним і демократичним режимами породило безліч протиріч, що суттєво впливають на міждержавні відносини та розподіл сфер впливу на міжнародній арені.

На сучасному етапі у світовій політиці можемо спостерігати загострення конкурентної боротьби між демократією і диктатурою, між захистом прав людини і жорстким обмеженням цих прав, між свободою і всебічним контролем, між розвитком і стагнацією.

Метою дослідження є порівняльний аналіз авторитарного та демократичного типів політичного режиму, їх становлення, характерних рис і особливостей функціонування в сучасних політичних системах.

Методи дослідження. У процесі наукового дослідження було використано порівняльний, системний та історичний методи.

Насамперед зауважимо, що політичний режим являє собою сукупність методів і способів здійснення влади державними органами, а також прояви форм і методів діяльності політичних партій, громадських організацій, рухів та інших структур громадянського суспільства.

Більшість класиків політичної думки виділяють три типи політичних режимів: демократичний, авторитарний і тоталітарний. Крім того, зустрічаються також гібридні (змішані) типи, що зазвичай формуються на етапі трансформацій і транзиту з одного типу політичної системи в інший.

Значна кількість держав вважають демократичний режим найбільш оптимальною моделлю управління завдяки принципам індивідуальної свободи, дотримання верховенства права, механізмам поділу влади та забезпечення прав людини. Основними характеристиками демократичного режиму є акцент на виборності та змінності представників влади, їх підзвітність народу, розвиток громадянського суспільства, свободи слова, незалежного суду, захист прав і свобод громадян, приватна власність та рівність можливостей для кожного.

На противагу демократичному авторитарний режим ґрунтується на жорсткій централізованій владі, обмеженні громадянських свобод, застосуванні репресій і контролю за населенням. Такий режим надає перевагу політичній стабільності й ефективному управлінню, часто ціною гуманістичних принципів і прав людини. Авторитарні держави часто здійснюють контроль над ЗМІ, усувають лідерів опозиції та використовують цензуру як інструмент для зміцнення свого режиму.

Аналіз останніх досліджень. Проблематиці політичних режимів присвячували свої праці такі українські вчені, як Головатий М. В., Кабанець О. С., Петришин О. В., Андрійчук Т. С., Колодій М. М., Швець В. Д., Долженков О. О., Бойчук М. А., Козьма В. В., Скрипнюк О. О. тощо.

Не менш значним є внесок міжнародних авторів, серед яких Дж. Браунлі, Ф. Ловенталь, С. Бітар, Н. Чізмен, М. Дероз'є, Н. Ліндштадт, Г. Прідам, Х. Арендт і багато інших дослідників.

Виклад основного матеріалу дослідження. Використовуючи сучасну методологію, автори досліджують формування та розвиток авторитарних і демократичних політичних режимів, насамперед зосереджуючись на двадцятому і двадцять першому століттях. Зокрема, особлива увага приділяється відмінним характеристикам і визначальним рисам, що демонструються кожним типом режиму.

На наш погляд, недостатньо вивченим є взаємний вплив авторитарних і демократичних політичних режимів один на одного, а також формування так званих гібридних режимів, що поєднують риси різних типів і важко піддаються визначенню. Також окремого дослідження, на нашу думку, потребує тоталітарний тип політичного режиму, що є перспективою подальших наукових розвідок.

Важливо визнати, що іноді авторитарний режим може маніпулювати й використовувати інструменти та фундаментальні принципи, пов'язані з демократією, спотворюючи та розмиваючи цінності, притаманні суспільству. Отже, громадська довіра до демократичного ідеалу може зруйнуватися, оскільки він стає інструментом маніпуляції представників влади. З метою уникнення такого розвитку подій потрібно очистити управлінські структури від недоброчесних чиновників, які заплуталися в корупції та керовані корисливими мотивами.

У сфері політики та управління авторитаризм передбачає непохитне підкорення владі й обмеження свободи думки та дії особистості [11, с. 94]. Авторитарні режими характеризуються відсутністю чітко визначеного механізму передачі виконавчої влади та запереченням громадянських свобод і політичних прав громадян.

Влада зосереджена в руках лідера або невеликої елітної групи, що приймають рішення без урахування згоди або інтересів населення. Хоча термін авторитаризм часто використовується для охоплення будь-якого типу недемократичного правління, ми схиляємося до думки, що варто окремо виділяти як авторитарний, так і тоталітарний тип політичних режимів.

Режими, що використовують державні інституції для проникнення у свідомість населення, нав'язують тотальний ідеологічний конформізм і здійснюють всебічний контроль

над усіма сферами життя суспільства, класифікуються вченими як тоталітарні. Такі режими намагаються культивувати непохитну відданість серед своїх громадян як режиму загалом, так і лідеру [12]. Інакомислення в тоталітарних режимах жорстко придушується репресіями, стратою або ув'язненням. Поширеність політичної довіри є помітно низькою, оскільки громадян систематично заохочують стежити та звітувати один про одного, беручи на себе роль інформаторів режиму.

Після завершення холодної війни авторитарні та тоталітарні режими зазнали занепаду і вчені описували їх як застарілі й неефективні. В останні кілька десятиліть поява освіченого середнього класу в поєднанні з впливом студентських рухів і організованого робітництва сприяли поширенню демократії. Демократичні принципи набули поширення в різних регіонах світу, сприяючи тим самим утвердженню демократичних режимів.

Проте після світової фінансової кризи 2007–2008 рр. спостерігалася криза демократій і повернення до авторитарних тенденцій насамперед у сфері економіки.

Хоча багато з авторитарних держав усе ще проводять вибори, справедливість і конкурентоспроможність цих виборчих процесів скомпрометована, залишаючи чимало сумнівів щодо правдивості їх результатів [6].

У деяких випадках диктатори дозволяють опозиційним групам досягти успіху для створення ілюзії демократичного правління. Ілюстрацію цього можна спостерігати у Венесуелі, де Ніколас Мадуро дозволив опозиції отримати майже одну третину голосів у 2018 році [13, с. 5].

У більшості авторитарних режимів допускається існування символічної опозиції, але численним членам опозиції загрожує ув'язнення або переслідування. Крім того, виборці часто піддаються дезінформаційним кампаніям, спрямованим на підрив опозиційних кандидатів. Яскравим прикладом тут є РФ, де лідери опозиції в різні роки зазнавали переслідувань, ув'язнень і фізичного знищення.

Хоча більшість авторитарних режимів мають конституції, вони забезпечують обмежені свободи своїх громадян як у теорії, так і на практиці. Тоді як окремі особи можуть виражати свої думки з незначних питань, відкриті дискусії на багато тем суворо заборонені. Такі обмеження часто призводять до тяжких наслідків для тих, хто вважається загрозою для підриву стабільності режиму.

Сфера функціонування громадянського суспільства значно обмежена авторитарним режимом. ЗМІ не є повністю державною власністю, але журналісти та працівники ЗМІ стикаються з обмеженнями своєї свободи висловлювань і підлягають обмеженням щодо їх здатності критикувати уряд. Порушення цих обмежень можуть призвести до ув'язнення, переслідувань, погроз, штрафів або скасування їх ліцензії [10, с. 45]. Прикладами є такі країни, як РФ, КНР і КНДР, де ЗМІ є рупорами правлячої верхівки, і застосовують різноманітні методи й технології маніпуляції, дезінформації та пропаганди. Отже, як в авторитарних, так і в тоталітарних режимах здебільшого використовується вплив на масову свідомість і постійний контроль над настроями суспільства. Крім того, вагомими інструментами психологічного впливу на населення є формування офіційної ідеології та активна діяльність релігійних організацій, що теж може бути притаманно різним типам диктаторських режимів.

Авторитарні режими в сучасну епоху часто формують такі інститути, як законодавчі органи, політичні партії та судову систему, але їхні повноваження та вплив сильно обмежені. Влада може демонструвати видимість опозиції і політичного плюралізму, що слугують своєрідним фасадом демократії, стратегічно використаним для збереження внутрішньої влади режиму та міжнародної легітимності [4, с. 87].

В авторитарних режимах наявність суддів і судів не забезпечує їх незалежність від виконавчої влади. Ця несамостійність часто проявляється через практику, відому як «телефонне право», де авторитарні лідери інколи безпосередньо інструктують суддів через буквальні

телефонні розмови про те, як вирішувати політично делікатні справи. Така практика є характерною для авторитарних і гібридних режимів, що дає змогу заможним і впливовим особам обійти загальноприйняті правила та закони заради особистої вигоди [9, с. 20].

У двадцять першому столітті авторитарні режими вміло скористалися тривогою громадян як у сформованих демократіях, так і в країнах, що розвиваються, становлячи величезний виклик демократичним системам. Цей період став свідком появи такого явища, як «цифровий авторитаризм», за якого авторитарні режими використовують інформаційні технології як засоби збереження чи зміцнення свого авторитету і контролю. Ці режими використовують такі тактики, як розповсюдження інформації, що вводить в оману або відволікає увагу населення та накладає обмеження на доступ до інформації з джерел поза їх контролем [13].

Крім того, авторитарні країни ефективно використовували можливості Інтернету для поширення дезінформації та пропаганди, щоб посилити політичні розбіжності всередині демократичних суспільств і підривати довіру суспільства до демократичних інститутів.

На початку 2000-х років Китай розпочав роботу зі створення надійних цифрових технологій, які б дали змогу контролювати інформацію, доступну для населення. Було створено централізовану мережу точок перехоплення інтернет-трафіку. Таким чином, китайський уряд отримав можливість вибірково обмежувати доступ іноземних вебсайтів і доступність китайської мови для популярних онлайн-платформ [12].

Отже, такі платформи, як Twitter, Google, Facebook, YouTube, і віртуальні приватні мережі (VPN) було фактично заблоковано.

На відміну від жорстких обмежень і контролю, притаманних авторитарним режимам, демократичний режим являє собою систему управління, засновану на колективній волі та згоді керованих, відповідальності влади перед усіма членами суспільства, непохитної відданості верховенству права та непохитності дотримання основних прав і свобод людини.

Демократія часто породжує заплутану мережу взаємозалежних структур, у яких представники влади притягуються до відповідальності через сувору перевірку з внутрішніх і зовнішніх джерел, таких як автономна судова система, неупереджені ЗМІ й активне громадянське суспільство [2, с. 432]. Це створює справедливе середовище, яке дає змогу всім людям, незалежно від їх народження чи походження, активно брати участь у політичних справах і процесах прийняття рішень [3, с. 775].

Демократичні країни мають спільні інтереси у справедливій торгівлі та безпеці. Їхні інституційні структури та народна підтримка роблять їх більш передбачуваними як для державних, так і для приватних інвестицій.

Протягом двадцятого століття деяким країнам вдалося зберегти демократичні системи, навіть зіткнувшись зі значними дипломатичними, військовими, економічними чи політичними викликами.

Критики демократичного режиму стверджують, що більшість людей може перешкоджати політиці, з якою не погоджується, і ускладнювати процес формування урядів, прийняття законодавства. І навпаки, прихильники стверджують, що участь громадян у прийнятті політичних рішень посилює легітимність і значимість демократії.

Варто підкреслити, що демократія, на відміну від авторитаризму, має кілька найбільш важливих характеристик.

По-перше, демократія слугує запобіжником проти правління жорстоких автократів та узурпації влади.

По-друге, країни з демократичними режимами здебільшого демонструють вищий рівень добробуту порівняно з іншими режимами.

По-третє, демократія має властивість сприяти всебічному розвитку людини. Крім того, демократія дає людям змогу захищати себе та свої інтереси шляхом гарантування їхніх

основних прав і надання ширшого кола особистих свобод порівняно з альтернативними типами управління.

Разом із тим украй важливо визнати, що демократія накладає значну відповідальність як на окремих громадян, так і на суспільство щодо їхніх дій та рішень. Попри численні переваги, пов'язані з ринковою економікою, вона призвела до значних відмінностей в економічних і соціальних ресурсах, що охоплюють багатство, дохід, освіту та соціальний статус. Оскільки люди з більшими ресурсами часто використовують свої переваги, щоб впливати на політику системи на їхню користь, збереження такої нерівності є постійною проблемою для досягнення політичної рівності. Ці виклики стають більш вираженими в періоди економічного спаду, що посилює бідність і безробіття.

Незважаючи на ці виклики, існує загальна тенденція на користь демократизації. Демократія ґрунтується на принципах верховенства права, що передбачає рівність застосування законів до всіх осіб та установ, включно з урядом.

Демократичні держави віддають перевагу розподілу влади на виконавчу, законодавчу й судові гілки. Правова система підтримує це відокремлення шляхом реалізації системи стримувань і противаг для запобігання зловживанню владою. Крім того, закони полегшують доступ до інформації, заохочують участь громадськості та створюють механізми притягнення державних службовців до відповідальності за їхні дії.

На сучасному етапі у світі спостерігається посилення напруги між автократією та демократією, загострення цивілізаційних, релігійних, етнічних, расових і ціннісних протиріч, розгортання воєнних конфліктів, катаклізмів та екологічних катастроф. У таких умовах прогнозовано можуть зазнати занепаду ліберально-демократичні цінності й посилитися авторитарно-диктаторські методи управління.

Висновки. Підсумовуючи, варто зауважити, що в силу різних обставин в різних країнах можуть спостерігатися тенденції поступового переходу від авторитаризму до демократії, і навпаки. Крім того, у таких країнах, як КНР, РФ і КНДР, можемо спостерігати перехід від авторитарного до тоталітарного типу політичного режиму. Тоталітаризм, як найбільш жорсткий і найменш справедливий політичний режим, на наш погляд, може стати предметом подальших наукових досліджень із метою детального аналізу й уникнення його поширення у світі. Перспективами подальших досліджень є всебічний аналіз тоталітарного типу політичного режиму та його сучасних гібридних форм.

Література:

1. Андрійчук Т. Розвиток демократії в Україні: вплив політичних цінностей. *Наукові записки*. № 4. 2012. С. 266.

2. Арбластер Е. Ключові ідеї демократії. Демократія: антологія. Уклад. О. Проценко. Київ, XXVIII. 2005. С. 432.

3. Балл Т., Деггер Р. Демократичний ідеал: історія становлення. Демократія: антологія. уклад. О. Проценко. Київ, XXVIII. 2005. С. 775.

4. Бабанка М. Авторитаризм і тоталітаризм. *Подібність уявна і істотна різниця. Політичний менеджмент.* № 2, 2002. С. 87.

5. Данилюк Н. Визначальні ознаки авторитарного політичного режиму: роль «авторитарних послідовників» на її підтримку. *Освіта регіону*. № 4. 2009. С. 5.

6. Єгоров Г., Гур'єв С., Сонін К. Свобода ЗМІ, бюрократичні стимули та ресурс. Робота Центру демократії, розвитку та верховенства права (CDRL). № 71. 2006.

7. Петришин О. В. Демократія як основа правової, соціальної держави. *Закон України*. № 5. 2014. С. 79.

8. Шипунов Г. В. Авторитарний політичний режим. *Вісник Львівського університету*. № 5. 2014. С. 333.

9. Скрипнюк О. О. Сучасний авторитарний режим: характерні риси та прояви. *Юридичні науки*. № 2. 2020. С. 20.

10. Стоцький Я. Основи демократії. МАУП. № 3. 2011. С. 45.

11. Сухонос В. В. Сутність і функції державного авторитарного режиму в умовах переходу до демократії (теоретико-методологічний аналіз). *Юридичні науки*. 2. 2000. С. 94.

12. Brownlee J. Authoritarianism in an Age of Democratization. *New York: Cambridge Univ. Press*. 2007. P. 21.

13. Pridham G. EU Enlargement and Consolidating Democracy in Postcommunist States. Journal of Common Market Studies, 40, 2002. P. 5.

References:

1. Andriichuk, T. (2012). Rozvytok demokratii v Ukraini: vplyv politychnykh tsinnostei [The development of democracy in Ukraine: the influence of political values]. *Naukovi zapysky*. № 4. P. 266 [in Ukrainian].

2. Arblaster, E. (2005). Kliuchovi idei demokratii. Demokratiia: antolohiia [Key ideas of democracy. Democracy: an anthology]. Kyiv, XXVIII. P. 432 [in Ukrainian].

3. Ball T., & Dehher R. (2005). Demokratychnyi ideal: istoriia stanovlennia. Demokratiia: antolohiia [The democratic ideal: the history of formation. Democracy: an anthology]. Kyiv, XXVIII. P. 775 [in Ukrainian].

4. Babanka, M. (2002). Avtorytaryzm i totalitaryzm [Authoritarianism and totalitarianism]. *Podibnist uiavna i istotna riznytsia. Politychnyi menedzhment*. № 2, p. 87 [in Ukrainian].

5. Danyliuk, N. (2009). Vyznachalni oznaky avtorytarnoho politychnoho rezhymu: rol "avtorytarnykh poslidovnykiv" na yii pidtrymku [The defining characteristics of an authoritarian political regime: the role of "authoritarian followers" in its support]. *Osvita rehionu*. № 4. P. 5 [in Ukrainian].

6. Yehorov, H., Huriev, S., & Sonin, K. (2006). Svoboda ZMI, biurokratychni stymuly ta resurs. Robota Tsentru demokratii, rozvytku ta verkhovenstva prava (CDRL) [Media freedom, bureaucratic incentives and resources. Work of the Center for Democracy, Development and Rule of Law]. № 71 [in Ukrainian].

7. Petryshyn, O. V. (2014). Demokratiia yak osnova pravovoi, sotsialnoi derzhavy [Democracy as the basis of a legal, social state]. *Zakon Ukrainy*. № 5. P. 79 [in Ukrainian].

8. Shypunov, H. V. (2014). Avtorytarnyi politychnyi rezhym [Authoritarian political regime]. *Visnyk Lvivskoho universytetu.* № 5. P. 333 [in Ukrainian].

9. Skrypniuk, O. O. (2020). Suchasnyi avtorytarnyi rezhym: kharakterni rysy ta proiavy [Modern authoritarian regime: characteristic features and manifestations]. *Yurydychni nauky*. № 2. P. 20 [in Ukrainian].

10. Stotskyi, Ya. (2011). Osnovy demokratii [Basics of democracy]. MAUP. № 3. P. 45 [in Ukrainian].

11. Sukhonos, V. V. (2000). Sutnist i funktsii derzhavnoho avtorytarnoho rezhymu v umovakh perekhodu do demokratii (teoretyko-metodolohichnyi analiz) [The essence and functions of the state authoritarian regime in the conditions of the transition to democracy (theoretical and methodological analysis)]. *Yurydychni nauky.* 2. P. 94 [in Ukrainian].

12. Brownlee, J. (2007). Authoritarianism in an Age of Democratization. *New York: Cambridge Univ. Press*. P. 21.

13. Pridham, G. (2002) EU Enlargement and Consolidating Democracy in Postcommunist States. Journal of Common Market Studies, 40, P. 5.

Olena Berezovska-Chmil. Comparative analysis of democratic and authoritarian political regimes

The article provides a comparative analysis of democratic and authoritarian political regimes, their characteristic features, features and mechanisms of formation in modern states. In addition, the author studies the problems and challenges associated with digitalization, which can be used by autocrats as a tool to strengthen authoritarian regimes and control society.

The study shows that certain characteristics inherent in a democratic regime are undermined and fraudulently used to create the illusion of the value of citizens' opinions. This manipulation of public sentiment often occurs within countries led by authoritarian regimes. In addition, this study examines the specific features and underpinnings of the aforementioned political regimes, shedding light on the mechanisms through

which power is maintained within each system. At the current stage in world politics, we can observe the intensification of the competitive struggle between democracy and dictatorship, between the protection of human rights and the strict restriction of these rights, between freedom and comprehensive control, between development and stagnation.

The purpose of this study is a comparative analysis of authoritarian and democratic types of political regime, their formation, characteristic features and peculiarities of functioning in modern political systems. A significant number of states consider the democratic regime to be the most optimal model of governance, thanks to the principles of individual freedom, observance of the rule of law, mechanisms of separation of powers and the provision of human rights.

The main characteristics of a democratic regime are an emphasis on the electability and changeability of government representatives, their accountability to the people, the development of civil society, freedom of speech, an independent court, protection of the rights and freedoms of citizens, private property and equal opportunities for everyone. In contrast to a democratic one, an authoritarian regime is based on rigid centralized power, restrictions on civil liberties, repression and population control. Such a regime prioritizes political stability and effective governance, often at the cost of humanistic principles and human rights. Authoritarian states often control the media, remove opposition leaders, and use censorship as a tool to strengthen their regime.

The author concludes that democracy, in contrast to authoritarianism. includes several of the most important characteristics. First, democracy serves as a safeguard against the rule of brutal autocrats and the usurpation of power. Second, countries with democratic regimes tend to exhibit higher levels of welfare compared to other regimes. Thirdly, democracy has the property of promoting comprehensive human development. In addition, democracy gives people the opportunity to protect themselves and their interests by guaranteeing their basic rights and providing a wider range of personal freedoms compared to alternative forms of government.

Key words: *political regime, human rights, democracy, authoritarianism.*

УДК 327.7:355.01(477:470)
DOI: https://doi.org/10.32782/2312-1815/2024-1-3

Назар Воробець
ORCID: 0009-0003-8794-2243

ІНФОРМАЦІЙНА ВІЙНА РОСІЇ ПРОТИ УКРАЇНИ: ДИНАМІКА ВПЛИВУ НА СУСПІЛЬНУ СВІДОМІСТЬ І ВИКЛИКИ ДЛЯ НАЦІОНАЛЬНОГО СТАНОВЛЕННЯ

Проблема російської інформаційної агресії є дуже актуальною для України, особливо в умовах війни, яку Росія веде проти нашої держави з 2014 року. Російська пропаганда має на меті підривати суверенітет, територіальну цілісність, демократичні цінності та національну ідентичність України, а також розбивати єдність і солідарність українського суспільства. Російська інформаційна агресія також створює загрозу для європейської безпеки та міжнародного правопорядку, оскільки вона спрямована на руйнування довіри, співпраці й партнерства між Україною та її західними союзниками.

Досліджено вплив російської інформаційної війни на суспільну свідомість українців, а також охарактеризовано фактори, які визначають їхню стійкість або вразливість до російської пропаганди. У статті використовуються дані соціологічних опитувань, які показують, як змінювалися патріотичні настрої, довіра до ЗМІ, ставлення до Росії та її політики. Розглянуто, які заходи можуть бути вжиті для підвищення рівня інформаційної грамотності та критичного мислення громадян України.

Розглядається проблема у визначенні й аналізі впливу російської інформаційної агресії на суспільну свідомість українців, а також у розробці рекомендацій щодо підвищення рівня інформаційної безпеки, стійкості та резильєнтності України. Ця проблема є актуальною, складною, багатогранною та недостатньо дослідженою.

Ця стаття має на меті заповнити прогалину, використовуючи теоретичні, емпіричні та практичні методи дослідження. Результати цього дослідження можуть бути корисними в подальших дослідженнях із цієї проблематики, може використовуватися як методологічна база подальшого опрацювання проблем інформаційної безпеки, а також у навчальному процесі. Ці матеріали також можуть бути корисні для підвищення рівня інформаційної грамотності та критичного мислення громадян України, а також для формування патріотичних, демократичних і європейських цінностей.

Ключові слова: *інформаційна безпека, суспільна свідомість, інформаційна грамотність, протидія пропаганді, дезінформація і маніпуляція, громадянське суспільство.*

Вступ. Сучасна геополітична ситуація, зумовлена конфліктом між Україною та Росією, зробила інформаційну війну одним із найважливіших факторів, які впливають на суспільні процеси. Російська пропаганда має на меті підривати суверенітет, територіальну цілісність, демократичні цінності та національну ідентичність України, а також розбивати єдність і солідарність українського суспільства. Російська інформаційна агресія також створює загрозу для європейської безпеки та міжнародного правопорядку, оскільки вона спрямована на руйнування довіри, співпраці й партнерства між Україною та її західними союзниками.

Проблема полягає в тому, що російська інформаційна війна впливає на суспільну свідомість українців, а також на їхнє ставлення до Росії, до Заходу, до власної держави та до себе як нації. Російська пропаганда використовує різні канали, методи, технології та наративи для досягнення своїх цілей, враховуючи різні аудиторії, регіони, соціальні групи й індивідуальні особливості. Російська інформаційна війна також користується внутрішніми проблемами, суперечностями, слабкостями та вразливостями українського суспільства, політики, економіки, культури й історії.

Зазначена проблема потребує глибокого й комплексного дослідження, оскільки вона має велике значення для розуміння сучасної ситуації в Україні та в регіоні, а також для розробки ефективних стратегій і заходів для протидії російській інформаційній агресії та зміцнення інформаційної безпеки України.

Мета статті полягає в дослідженні аналізу та впливу російської інформаційної агресії на суспільну свідомість українців, а також в розробці рекомендації щодо підвищення рівня інформаційної безпеки, стійкості та резильєнтності України.

Зокрема, можна виокремити такі **завдання:**

1) проаналізувати динаміку впливу російської інформаційної війни на суспільну свідомість українців з 2014 року до сьогодні, використовуючи дані соціологічних опитувань;

2) вивчити та класифікувати основні методи, технології та наративи, які використовує Росія в інформаційній війні проти України, зокрема маніпуляції історичною пам'яттю, розповсюдження фейків і дезінформації через соціальні мережі, кібератаки та психологічні операції;

3) розробити рекомендації щодо підвищення рівня інформаційної безпеки, стійкості та резильєнтності України, а також зміцнення національної ідентичності, патріотизму й солідарності українського суспільства.

Аналіз останніх досліджень і публікацій. Проблема інформаційної безпеки привертає увагу багатьох науковців в українському науковому просторі, оскільки вона має як теоретичне, так і практичне значення. Українські дослідники активно вивчають цю проблематику, яка була та залишається актуальною в сучасних умовах. Зокрема, у численних роботах таких науковців, як Борисенко О., Почепцов Г., Курус Ю., Корсунський С., Романенко Є., Сенченко М., Литвиненко О. й інших, розглядаються різні аспекти інформаційної війни, як-от її сутність, особливості, механізми, наслідки та способи протидії. Проте, з огляду на складність і багатогранність дослідження функціонування інформаційної безпеки в країні, ця проблематика потребує подальшого розвитку.

Виклад основного матеріалу дослідження. У сучасному світі геополітичні конфлікти часто приймають форму гібридних воєн, де використання військової сили поєднується з іншими методами впливу на противника. Російська Федерація в останні роки стала активним учасником гібридної війни проти України, використовуючи різноманітні інструменти для досягнення своїх стратегічних цілей. Гібридна війна Росії проти України є одним із найбільш серйозних викликів для національної безпеки, суверенітету та територіальної цілісності України. Ця війна також має значний вплив на суспільну свідомість українців, які стикаються з різними формами російської агресії, пропаганди, дезінформації та маніпуляції.

Одним з аспектів впливу інформаційної війни на суспільну свідомість є зміна ставлення до радянського минулого й історичної пам'яті. За даними соціологічних опитувань, українці стали більш позитивно оцінювати розпад Радянського Союзу, засуджувати СРСР як тоталітарний режим, що здійснював державний терор, і переглядати своє ставлення до деяких знакових історичних особистостей, таких як Степан Бандера. Також українці стали більш патріотичними, довірливими до ЗМІ, критичними до Росії та її політики, а також готовими до захисту України від зовнішньої агресії [12].

Зокрема, за даними соціологічних опитувань від 5–12 серпня 2022 р. Фонду «Демократичні ініціативи» імені Ілька Кучеріва і соціологічної служби Центру Разумкова, переважна більшість опитаних громадян (67 %) позитивно оцінили розпад Радянського Союзу.

За результатами опитування, більшість українців (59 %) підтримують ідею засудження СРСР як комуністичного тоталітарного режиму, який проводив політику державного терору. Це на 25 % більше, ніж у 2020 році. Також зросла кількість тих, хто вважає, що Україна повинна відмовитися від спадщини СРСР: з 34 до 52 %. За той самий період, кількість тих, хто не

погоджується з цими твердженнями, зменшилася вдвічі – з 32 до 16 %. Отже, війна спричинила досить різкі зміни в оцінках українцями радянського минулого [9].

Ще одним аспектом впливу інформаційної війни на суспільну свідомість є зміна національної ідентичності та цінностей. Українці стали більше підтримувати європейський і євроатлантичний курс України, а також більше цінувати демократію, права людини, свободу слова, громадянське суспільство тощо. Також українці стали більш толерантними до різноманітності, у тому числі етнічної, мовної, релігійної, культурної тощо [4].

Інформаційна війна вплинула на суспільну активність та участь українців у різних сферах життя. Українці стали більш зацікавлені в політиці, волонтерстві, громадській діяльності, освіті, культурі тощо. Також українці стали більш відповідальними, солідарними, підтримуючими та співпрацюючими між собою, особливо у важкі часи [9].

Зі свого боку, російська інформаційна агресія використовує різні форми, методи, канали й повідомлення, щоб маніпулювати, дезінформувати, пропагувати, інтоксикувати, деморалізувати, розділяти, провокувати та травмувати українське суспільство. Україна вживає різних заходів, щоб протистояти російській інформаційній агресії, серед них – законодавчі, інституційні, комунікативні, освітні, громадські тощо. Однак ці заходи не завжди є достатніми, ефективними, координованими й системними.

Інформаційна війна – це явище, яке виникло в сучасному світі внаслідок розвитку інформаційних технологій і збільшення ролі інформації в політичній, економічній, соціальній, культурній, ідеологічній сферах. Інформаційна війна означає відкритий або прихований цільовий інформаційний вплив систем одна на одну для досягнення певної перемоги в цих сферах [5, с. 64–66]. Інформаційна війна може включати поєднання традиційних і нетрадиційних методів агресії, складність агресивних дій у багатьох сферах громадського життя. Інформація виступає як зброя, яка може перемогти ворога без втрат людських життів і пролиття крові [6, с. 31–32].

На сьогодні вчені не сформували єдину домінуючу думку щодо науково-теоретичної концепції інформаційних воєн, а також основних методів, форм і способів їх проведення. Також слід зауважити, що інформаційна війна є неоднозначним поняттям. Тому можна говорити про широке та вузьке тлумачення цього терміна. У загальному розумінні інформаційна війна розглядається як будь-який негативний інформаційний вплив на ворога. Противник може бути будь-яким суб'єктом: індивідом чи групою осіб, юридичними особами чи державою. Учасники таких воєн можуть діяти індивідуально чи в групах, спонтанно чи за домовленістю. У вузькому розумінні інформаційна війна – це новий тип чи метод збройного конфлікту, який не підлягає міжнародним правовим кваліфікаціям.

Найбільш відомим фахівцем, що відносить інформаційну війну до інформаційних способів і засобів ведення протиборства, є український вчений Г. Почепцов. Так, він пише: «Інформаційна війна – це комунікативна технологія впливу на масову свідомість з короткочасними і довготривалими цілями» [8, с. 21–22].

Однак серед вчених немає єдиної думки, більшість із них вважає, що інформаційну війну не можна розглядати як збройний конфлікт.

На сьогодні для України під час інформаційної протистояння з Російською Федерацією захист власного інформаційного простору й національної інформаційної безпеки є однією з найважливішою метою державного управління, а також першим кроком до формування позитивного образу держави на світовій арені, успішної європейської інтеграції та розвитку самодостатньої, національної самосвідомості.

Велика російська інформаційна війна проти України перейшла на новий етап на початку 2014 року, коли відбулися події Революції Гідності, а також анексія Криму та повномасштабне вторгнення в Україну. Цей конфлікт ілюстрував, по-перше, усі вразливі сфери України

в інформаційній безпеці; по-друге, потребу в розробці механізмів протидії російській інформаційній агресії; по-третє, важливість формування суспільної свідомості українців як головного фактора національної безпеки.

Росія, мабуть, першою у світі почала використовувати інформаційний простір як зброю для реалізації своїх агресивних планів, спрямованих на підпорядкування інших держав і народів своїм інтересам. Ця інформаційна агресія в психологічній сфері має на меті впливати на свідомість громадян України, щоб спотворити їхнє сприйняття реальності, схилити їх до підтримки застосування зброї проти України й анексії її території. Росія почала активно та підло застосовувати деструктивні впливи інформаційно-психологічного характеру в рамках антиукраїнських операцій ще з моменту проголошення нашою державою незалежності. З того часу Росія системно проводить масштабні інформаційні кампанії проти нашої країни, метою яких є досягнення повного контролю над зовнішньою та внутрішньою політикою України й утримання її у сфері геополітичного впливу [7].

Російське керівництво з приходом до влади Володимира Путіна з кожним роком посилює атаки на Україну в інформаційному просторі, прагнучи відновлення великодержавності та створення нової російської імперії. РФ не може примиритися з тим, що Україна відірвалася від колишньої радянської імперії та обрала європейський шлях розвитку, прямуючи до Євросоюзу та НАТО. Тому Росія здійснює інформаційний тиск, поширюючи деструктивну, дезорієнтуючу, дезорганізуючу, деморалізуючу інформацію у вигляді фейків, перекручених тлумачень фактів і подій за допомогою Інтернет і медіа.

Успіхи російської пропаганди спираються на те, що їх пропагандисти першими усвідомили існування нового середовища існування людини – медіасередовища. Це місце, куди спрямовані наші час, гроші й думки. Воно таке ж реальне, як повітря, земля чи люди. Підпорядкувавши його досягненню цілей повного контролю й управління поведінкою людини, Росія визначила принципи, способи, форми та методи його організації, наповнила його відповідним змістом [13].

У цьому контексті для протидії інформаційній агресії і експансії російській пропаганді важливо постійно наголошувати, що зображення, яке ми бачимо на екрані телевізора чи монітора, не є реальністю, а є лише зображенням реальності. Зрозуміло, що російські пропагандисти, для того щоб спрямувати нашу свідомість у певному напрямку, використовують під час підготовки інформаційних матеріалів цілу низку маніпулятивних технік і прийомів. Змінюючи зображення реальності, вони таким чином змінюють і її саму в нашій свідомості [10]. Особливого значення в їх пропаганді набуває оціночна інформація, яку пропагандисти спеціально забарвлюють у чорні кольори для ініціювання у мас необхідних психологічних станів: занепокоєння, стурбованість, тривога, боязнь тощо. На їх фоні найфантастичніші фейки РФ повинні викликати в українців довіру й перешкоджати їх логічному аналізу. Звідси виникає проблема інформаційної грамотності та критичного мислення українського суспільства [9].

Ця проблема полягає в тому, що багато українців не мають достатніх знань, навичок, компетенцій і цінностей, щоб ефективно отримувати, аналізувати, оцінювати, створювати, використовувати та поширювати інформацію в різних формах, контекстах і ситуаціях. Це робить їх вразливими до російської пропаганди та дезінформації, які можуть маніпулювати їхніми емоціями, поглядами, поведінкою тощо. Для підвищення рівня інформаційної грамотності та критичного мислення українського суспільства потрібно вжити таких заходів:

– розробити та впровадити національну стратегію інформаційної грамотності, яка б визначала цілі, принципи, критерії, індикатори, механізми, ресурси, відповідальність тощо для підвищення рівня інформаційної грамотності та критичного мислення українського суспільства [3];

– забезпечити інтеграцію інформаційної грамотності та критичного мислення в освітні стандарти, програми, плани, методики, матеріали, оцінювання тощо на всіх рівнях і в усіх формах освіти;

– проводити постійні тренінги, курси, семінари, вебінари, конференції, фестивалі, конкурси, гранти тощо для підвищення рівня інформаційної грамотності та критичного мислення різних груп населення, особливо молоді, журналістів, вчителів, бібліотекарів, громадських активістів тощо;

– створити та підтримувати інформаційні ресурси, платформи, сервіси, інструменти, проєкти тощо, які б допомагали українцям отримувати, аналізувати, оцінювати, створювати, використовувати й поширювати якісну, об'єктивну, балансовану, різноманітну, перевірену, захищену інформацію в різних формах, контекстах та ситуаціях [3].

Також існує проблема інформаційної безпеки та захисту даних українських користувачів Інтернету. Ця проблема полягає в тому, що багато українців не знають, як захистити свої особисті, професійні, фінансові, медичні, соціальні, політичні тощо дані від російських кібератак, шпигунства, втручання та впливу. Це робить їх вразливими до російської кіберагресії, яка може красти, зламувати, змінювати, використовувати, поширювати, знищувати їхні дані для різних цілей [2]. Для забезпечення інформаційної безпеки та захисту даних українських користувачів Інтернету потрібно вжити таких заходів:

– розробити та впровадити національну стратегію інформаційної безпеки й захисту даних, яка б визначила цілі, принципи, критерії, індикатори, механізми, ресурси, відповідальність тощо для забезпечення інформаційної безпеки та захисту даних українських користувачів Інтернету;

– забезпечити дотримання законодавства, норм, стандартів, правил, рекомендацій, кодексів тощо, які регулюють інформаційну безпеку та захист даних українських користувачів Інтернету, а також застосовувати санкції, штрафи, покарання тощо за їх порушення.

Як уже зазначалося, інформаційна війна має на меті підірвати суверенітет, територіальну цілісність, демократію, національну ідентичність та євроінтеграцію України, а також зірвати її партнерство з НАТО й іншими західними країнами. Для досягнення цих цілей РФ використовує різноманітні засоби, форми та методи інформаційного впливу, а саме це:

– пропаганда, дезінформація, фейки, перекручення, маніпуляції, провокації, що поширюються через російські та проросійські ЗМІ, соціальні мережі, інтернет-тролі, боти, хакери тощо. Ці засоби мають на меті деморалізувати, дезорієнтувати, дезорганізувати, дискредитувати, розділити українське суспільство, сіяти сумніви, страх, ненависть, апатію, паніку тощо [11];

– збір, аналіз, блокування, знищення, заміна, підробка, викрадення інформації, що стосується державної безпеки, оборони, економіки, політики, культури, освіти, науки, медицини, екології тощо. Ці засоби мають на меті втрутитися в внутрішні справи, підірвати довіру до державних інституцій, зірвати стратегічні проєкти, зламати критичні інфраструктури, викликати параліч, хаос, кризу тощо [2];

– вплив на історичну пам'ять, культурну спадщину, духовні цінності, мовну політику, етнічну ситуацію, релігійну толерантність тощо. Ці засоби мають на меті підірвати національну ідентичність, змінити світогляд, сприяти асиміляції, сепаратизму, ревізіонізму, націоналізму, екстремізму тощо [11].

Наслідки інформаційної війни проти України є дуже серйозними та небезпечними, адже вони створюють ризики для національної безпеки, суверенітету, територіальної цілісності, демократії, євроінтеграції, міжнародного престижу, соціальної стабільності, економічного розвитку, культурної різноманітності, громадянського суспільства тощо. Інформаційна війна також впливає на свідомість українців, змінюючи їхнє ставлення до себе, до своєї держави, до

своєї історії, до своїх сусідів, до своїх партнерів, до своїх ворогів тощо. З одного боку, інформаційна війна може сприяти консолідації, патріотизму, самоорганізації, самовизначенню, самозахисту, самовдосконаленню українців, які виявляють опір, резистентність, критичне мислення, медіаграмотність, активну громадянську позицію тощо. З іншого боку, інформаційна війна може сприяти дезінтеграції, апатії, індиферентності, песимізму, фаталізму, депресії, травмі, страху, ненависті, ворожнечі, конфліктності, ізоляції, маргіналізації українців, які піддаються, пасивні, легковірні, маніпульовані, залежні, недостатньо освічені тощо [2].

Тому для протидії інформаційній війні проти України та її впливу на свідомість українців потрібно розробляти й реалізовувати комплексні заходи на рівні держави, суспільства, громадян, ЗМІ, експертів, освітян, науковців тощо. Ці заходи повинні бути спрямовані на зміцнення інформаційної безпеки, розвиток інформаційної культури, формування інформаційної свідомості українців.

Інформаційна свідомість є важливою умовою для успішної адаптації до сучасного інформаційного суспільства, захисту від інформаційної агресії, розвитку особистості, формування громадянської позиції, забезпечення національної безпеки тощо [9].

Для розвитку інформаційної свідомості українців потрібно здійснювати такі заходи:

– підвищення рівня медіаграмотності. Медіаграмотність допомагає виявляти й відхиляти маніпуляції, пропаганду, фейки, перекручення, провокації тощо;

– підвищення рівня інформаційної культури для здатності до етичного, відповідального, креативного, критичного ставлення до інформації, її джерел, авторів, одержувачів, контексту, змісту, форми тощо. Інформаційна культура допомагає виявляти й поважати авторські права, інтелектуальну власність, конфіденційність, приватність, безпеку, доступність, якість, релевантність, достовірність тощо [12];

– підвищення рівня інформаційної компетентності, що забезпечує здатність до ефективного, цілеспрямованого, свідомого, раціонального, оптимального відбору, пошуку, зберігання, обробки, аналізу, синтезу, оцінки, використання, створення, поширення інформації. Інформаційна компетентність допомагає вирішувати різні завдання, задачі, проблеми, проєкти, ситуації тощо.

Щоб ефективно відбити інформаційну атаку Росії на Україну та її вплив на суспільну свідомість, потрібно застосовувати комплексні заходи на всіх рівнях суспільства. Важливо виконувати заходи, які мають на меті посилення інформаційної безпеки, підвищення інформаційної культури та розвиток інформаційної свідомості серед українців.

Висновки. Отже, аналізуючи динаміку впливу інформаційної війни Росії на Україну, можна бачити, що цей конфлікт є не тільки випробуванням для держави, але й важливим фактором у формуванні суспільної свідомості. Пропаганда та медіаманіпуляції стали засобами воєнного конфлікту, а також впливають на розвиток суспільно-політичних процесів.

Суспільна свідомість українців, яка зазнає сильного тиску інформаційної війни, перебуває в стані зміни та адаптації. Це вимагає від нас розуміння й аналізу впливу інформаційних потоків на національну самосвідомість і громадянську позицію.

Викликом для національного становлення є не лише захист інформаційного простору, але й забезпечення інформаційної грамотності та критичного мислення серед громадян. Суспільство повинно вміти відрізняти дезінформацію від об’єктивних фактів, а також розуміти вплив медіа на світогляд і цінності.

Крім того, стикаючись із складнощами інформаційної війни, Україна має демонструвати світові важливість відстоювання інформаційної свободи, розвиток критичного мислення та створення резервів для забезпечення стійкості суспільства в умовах інформаційного напруження. Лише через це суспільство може сприймати виклики, пов’язані із зовнішньою інформаційною загрозою, як можливість для власного зростання та розвитку.

Література:

1. Божко В. Особливості та уроки гібридної війни Росії проти України. Національний університет «Києво-Могилянська академія». 2020. С. 1–15.

2. Борисенко О. Інформаційна війна проти України: сутність, особливості, наслідки. *Вісник Національної академії оборони України*, вип. 2 (53), 2017. С. 5–13.

3. Воробець Н. Р. Інституційні особливості формування та функціонування інформаційної безпеки в Україні: аналіз та перспективи розвитку. *Регіональні студії*, 2023 (34), с. 75–81.

4. Додонова Р. О. Гібридна війна: in verbo et in praxi : монографія / Донецький національний університет імені Василя Стуса / під. заг. ред. проф. Р. О. Додонова. – Вінниця : ТОВ «Нілан-ЛТД», 2017. 412 с.

5. Кирильчук Є. О. Інформаційна війна як дієвий феномен протистояння в суспільно-політичній боротьбі. *Наукові праці МАУП* 2013, вип. 4 (39), 2013. С. 58–61.

6. Маланчук Л. О. Посилення стійкості інформаційного суверенітету України в сучасних умовах. *Стратегія і тактика державного управління: збірник наукових праць*, вип. 1–2. 2017. С. 17–20.

7. Нофенко А. Особливості дискурсу політичної пропаганди в умовах інформаційно-психологічної війни. *Міжнародні відносини, суспільні комунікації та регіональні студії: збірник наукових праць*, вип. 2 (6), 2019. С. 68–77.

8. Почепцов Г. Г. Смислові та інформаційні війни. *Інформаційне суспільство*, вип. 18, 2013. С. 21–27.

9. Результати соціологічного опитування. Фонд «Демократичні ініціативи» імені Ілька Кучеріва із соціологічною службою Центру Разумкова з 5 по 12 серпня 2022 року. https://dif.org.ua/article/yak-transformuetsya-stavlennya-ukraintsiv-do-dekomunizatsii-upts-mp-ta-natsionalizmu-pid-chas-viyni-z-rosieyu?fbclid=IwAR3BAFLGcWGOz-Ivp3TRANTcNk-loGhwIjz3iJXjQ2lMXFDUQQuf1nrK9B4 (дата звернення: 13.10.2022).

10. Романюк В., Чуранова О. Україна в інформаційному просторі Росії та Білорусії: основні наративи. Інститут масової інформації. https://cutt.ly/sVcQ3sf (дата звернення: 22.09.2022).

11. Шевчук С. Інформаційна свідомість як фактор протидії інформаційній війні. Вісник Харківського національного університету ім. В. Н. Каразіна. *Серія «Питання політології»*, вип. 30, 2018. С. 87–94.

12. Як війна змінила суспільну свідомість українців: соціологічні дослідження. Національний інститут стратегічних досліджень (2022). https://niss.gov.ua/news/komentari-ekspertiv/yak-viyna-zminyla-suspilnu-svidomist-ukrayintsiv-sotsiolohichni (дата звернення: 2022).

13. Seib P. Information at War: Journalism, Disinformation, and Modern Warfare. Wiley. 2021.

References:

1. Bozhko, V. (2020). Osoblyvosti ta uroky hibrydnoi viiny Rosii proty Ukrainy [Peculiarities and lessons of Russia's hybrid war against Ukraine]. Natsionalnyi universytet "Kyievo-Mohylianska akademiia", pp. 1–15 [in Ukrainian].

2. Borysenko, O. (2017). Informatsiina viina proty Ukrainy: sutnist, osoblyvosti, naslidky [Information war against Ukraine: essence, features, consequences]. *Visnyk Natsionalnoi akademii oborony Ukrainy*, Vol. 2 (53), pp. 5–13 [in Ukrainian].

3. Vorobets, N. R. (2023). Instytutsiini osoblyvosti formuvannia ta funktsionuvannia informatsiinoi bezpeky v Ukraini: analiz ta perspektyvy rozvytku [Institutional features of the formation and functioning of information security in Ukraine: analysis and development prospects]. *Rehionalni studii*, 34, pp. 75–81 [in Ukrainian].

4. Dodonova, R. (2017). Hibrydna viina: in verbo et in praxi: *monohrafiia* [Hybrid war: in verbo et in praxi: *monograph*]. Donetskyi natsionalnyi universytet im. V. Stusa. Vinnytsia: TOV "Nilan-LTD", p. 412 [in Ukrainian].

5. Kyrylchuk, Ye. O. (2013). Informatsiina viina yak diievyi fenomen protystoiannia v suspilno politychnii borotbi [Information war as an effective phenomenon of confrontation in socio-political struggle]. *Naukovi pratsi MAUP*, Vyp. 4 (39), pp. 58–61 [in Ukrainian].

6. Malanchuk, L. O. (2017). Posylennia stiikosti informatsiinoho suverenitetu Ukrainy v suchasnykh umovakh [Strengthening the stability of Ukraine's information sovereignty in modern conditions]. *Stratehiia i taktyka derzhavnoho upravlinnia: zbirnyk naukovykh prats,* Vyp. 1–2, pp. 17–20 [in Ukrainian].

7. Nofenko, A. (2019). Osoblyvosti dyskursu politychnoi propahandy v umovakh informatsiino-psykholohichnoi viiny [Peculiarities of the discourse of political propaganda in the conditions of information and psychological warfare]. *Mizhnarodni vidnosyny, suspilni komunikatsii ta rehionalni studii: zbirnyk naukovykh prats*, Vyp. 2 (6), pp. 68–77 [in Ukrainian].

8. Pocheptsov, H. H. (2013). Smyslovi ta informatsiini viiny [Semantic and information wars]. *Informatsiine suspilstvo*, Vyp. 18, pp. 21–27 [in Ukrainian].

9. Rezultaty sotsiolohichnoho opytuvannia. (2022). Fond "Demokratychni initsiatyvy" imeni Ilka Kucheriva iz sotsiolohichnoiu sluzhboiu Tsentru Razumkova z 5 po 12 serpnia 2022 roku [Results of a sociological survey. Ilko Kucheriv Foundation "Democratic Initiatives" with the sociological service of the Razumkov Center from August 5 to 12, 2022]. URL: https://dif.org.ua/article/yak-transformuetsya-stavlennya-ukraintsiv-do-dekomunizatsii-upts-mp-ta-natsionalizmu-pid-chas-viyni-z-rosieyu?fbclid=IwAR3BAFLGcWGOz-Ivp3TRANTcNk-loGhwIjz3iJXjQ2lMXFDUQQuf1nrK9B4 [in Ukrainian].

10. Romaniuk, V., Churanova, O. (2022, 22 veresnia). Ukraina v informatsiinomu prostori rosii ta Bilorusii: osnovni naratyvy [Ukraine in the information space of Russia and Belarus: main narratives]. Instytut masovoi informatsii. URL: https://cutt.ly/sVcQ3sf [in Ukrainian].

11. Shevchuk, S. (2018). Informatsiina svidomist yak faktor protydii informatsiinii viini [Information consciousness as a factor of countering information war]. *Visnyk Kharkivskoho natsionalnoho universytetu im. V. N. Karazina. Seriia "Pytannia politolohii",* Vyp. 30, pp. 87–94 [in Ukrainian].

12. National Institute of Strategic Studies (2022). Yak viina zminyla suspilnu svidomist ukraintsiv: sotsiolohichni doslidzhennia Natsionalnyi instytut stratehichnykh doslidzhen [How the war changed the public consciousness of Ukrainians: sociological studies]. URL: https://niss.gov.ua/news/komentari-ekspertiv/yak-viyna-zminyla-suspilnu-svidomist-ukrayintsiv-sotsiolohichni [in Ukrainian].

13. Seib, P. (2021). Information at War: Journalism, Disinformation, and Modern Warfare. Wiley.

Nazar Vorobets. Information war of Russia against Ukraine: dynamics of influence on public consciousness and challenges for national formation

The problem of Russian information aggression is very relevant for Ukraine, especially in the conditions of the war that Russia is waging against our state since 2014. Russian propaganda aims to undermine the sovereignty, territorial integrity, democratic values and national identity of Ukraine, as well as to break the unity and solidarity of Ukrainian society. Russian information aggression also poses a threat to European security and international order, as it is aimed at destroying trust, cooperation and partnership between Ukraine and its Western allies. The article explores how the Russian information war affects the public consciousness of Ukrainians, as well as what factors determine their resilience or vulnerability to Russian propaganda.

The article uses data from sociological surveys, which show how patriotic moods, trust in the media, attitudes to Russia and its policies have changed. The article also considers what measures can be taken to increase the level of information literacy and critical thinking of Ukrainian citizens.

The problem of defining and analyzing the impact of Russian information aggression on the public consciousness of Ukrainians, as well as developing recommendations for increasing the level of information security, resilience and resilience of Ukraine is considered. This problem is relevant, complex, multifaceted and insufficiently researched. This article aims to fill the gap, using theoretical, empirical and practical methods of research. The results of this research can be useful in further studies on this issue, can be used as a methodological basis for further processing of information security problems, as well as in the educational process.

These materials may also be useful for improving the level of information literacy and critical thinking of Ukrainian citizens, as well as for forming patriotic, democratic and European values.

Key words: *information security, public awareness, information literacy, counter-propaganda, disinformation and manipulation, civil society.*

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.*

УДК 342-051:316.658
DOI: https://doi.org/10.32782/2312-1815/2024-1-5

Тарас Кобець
ORCID: 0009-0001-2179-321X

ПОРІВНЯЛЬНИЙ АНАЛІЗ ТЕХНОЛОГІЙ ПРОПАГАНДИ ТА ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ В УМОВАХ ВОЄННОГО СТАНУ

У сучасному геополітичному ландшафті ознаки військових конфліктів і криз збільшуються, а це робить актуальним питання впливу інформаційної боротьби на суспільство та міжнародні відносини. В умовах воєнного стану пропаганда й інформаційні операції стають надзвичайно важливими інструментами у веденні бойових дій. Аналіз порівняльних аспектів цих технологій дасть змогу глибше розуміти їхню роль у формуванні думок і поглядів громадян, вплив на міжнародну політику та безпеку держав. Дослідження цієї проблеми є важливим для розробки стратегій протидії маніпуляціям і дезінформації, сприяючи підвищенню стійкості та ефективності суспільства в умовах конфлікту.

Умови повномасштабної війни, ініційованої Російською Федерацією проти України, передбачають не лише військові дії, а й активне використання пропагандистських та інформаційних операцій з метою маніпулювання світовою громадськістю та створення власного образу конфлікту. Російська Федерація вдосконалила свою інформаційну стратегію, використовуючи різні засоби масової інформації, соціальні мережі, інтернет-ресурси та впливових агентів для поширення дезінформації, фейків і спотвореної інформації.

Це допомагає створити фальшивий інформаційний простір про конфлікт, виправдати власну агресію, дискредитувати українську владу та підтримати російські інтереси. Інформаційні операції РФ спрямовані на вплив на громадську думку та міжнародних партнерів, щоб зменшити підтримку України у світі та створити враження некоректності українського становища. У такій ситуації важливо ретельно аналізувати інформацію і підтримувати об'єктивність у сприйнятті подій.

Необхідність дослідження технологій пропаганди й інформаційних операцій у воєнних умовах край актуальна та важлива. Війна сьогодні – це не лише фізичний бій, але й інформаційна боротьба, де домінують стратегії маніпуляції, дезінформації та психологічного впливу. Дослідження пропаганди й інформаційних операцій дає змогу розуміти, як вони використовуються для формування громадської думки, дестабілізації ворога та збереження власної легітимності. Це також сприяє розробці ефективних стратегій контрпропаганди та захисту інформаційного простору. Важливо аналізувати й розкривати методи та технології, які використовуються для поширення фейкових новин та інших видів дезінформації. Дослідження цих технологій надає можливість розвинути системи попередження та реагування на інформаційну загрозу, підвищує інформаційну готовність і сприяє збереженню стабільності та безпеки в умовах війни.

Робота спрямована на визначення специфічних аспектів застосування інструментів пропаганди й інформаційних операцій у контексті військових конфліктів, а також їхнього впливу на суспільство, політику та безпеку.

Технології пропаганди й інформаційних операцій в умовах воєнного стану виявляють значний вплив на суспільство та міжнародну політику. Вони використовуються для маніпуляцій, формування громадської думки та можуть підірвати стійкість держав. Розуміння цих процесів стає ключовим для забезпечення національної та міжнародної безпеки.

Ключові слова: *пропаганда, інформаційні операції, війна, гібридна війна, воєнний стан.*

Вступ. Умови повномасштабного військового вторгнення Російської Федерації в Україну засвідчують надзвичайну актуальність досліджень у сфері пропаганди й інформаційних операцій. У такому конфліктному контексті інформаційні битви стають важливою складовою сучасних військових дій. Інформаційні агенти, керовані ворогом, спрямовують зусилля на

формування дезінформації та психологічного впливу на населення й міжнародну спільноту. Дослідження в цій сфері допомагають розкрити методи та технології, які ворог використовує для маніпуляцій і поширення пропаганди.

Розуміння цих процесів сприяє підвищенню інформаційної обізнаності, зміцненню стійкості суспільства й розробці стратегій протидії дезінформації в умовах військового конфлікту. Такі дослідження є важливими для національної та міжнародної безпеки і сприяють формуванню стратегічних відповідей на інформаційні загрози.

Мета та завдання. Метою роботи є визначення специфічних аспектів застосування інструментів пропаганди й інформаційних операцій у контексті військових конфліктів, а також їхнього впливу на суспільство, політику та безпеку.

Відповідно до цієї мети були сформовані такі завдання:

– розкрити сутність категорії пропаганда;

– розкрити сутність категорії інформаційна війна;

– здійснити розкриття технології пропаганди;

– розкрити технологію інформаційних операцій;

– здійснити порівняльний аналіз технологій пропаганди та інформаційних операцій.

Методи дослідження. У рамках цієї наукової статті використовувалися такі методи дослідження, як аналіз, синтез і порівняння.

Виклад основного матеріалу. Підрив Каховської ГЕС 6 червня 2023 року російськими окупаційними військами вкотре на перше місце інформаційного порядку денного поставив питання протидії пропаганді сусідньої держави та її впливу на ухвалення рішень у рамках світових політичних інституцій. Після підриву, який спричинив екологічну, гуманітарну, економічну катастрофу в басейні річки Дніпро в Херсонській, Миколаївський, Запорізькій, Одеській областях та у Криму, міжнародні ЗМІ в перший день трагедії вийшли з неоднозначними матеріалами про те, що винуватець поки що неочевидний. Міжнародні медіа, намагаючись балансувати на межі журналістських стандартів, поширили суперечливі матеріали. Дехто навіть ставив під сумнів винуватість Російської Федерації [3].

Події показали, яким чином протягом великої війни в Україні російська пропаганда впливає на міжнародні ЗМІ, а через них – на уряди їхніх країн. Після підриву Каховської ГЕС Росія використовувала різні елементи пропаганди для досягнення своїх політичних цілей. Зокрема, відразу ж видала кілька варіантів, чому це сталося, згодом вийшла зі спростуванням усіх, згодом звинуватила Україну в підриві, навіть почала розповсюджувати фейкові знімки нібито ракетного обстрілу. Але ключовим є те, що це спотворення призвело до перекручування фактів про винуватців цієї трагедії [3].

Пропаганда в умовах війни становить серйозну загрозу, оскільки вона має потенціал маніпулювати масовою свідомістю й переконаннями громадян. Це може призвести до формування агресивних або нетерпимих поглядів, змінити сприйняття реальності та стимулювати насильство.

Пропагандистські засоби, такі як дезінформація і психологічний тиск, використовуються для підриву міжнародної стабільності та суспільного спокою. Тому важливо вивчати й розробляти стратегії протидії пропаганді в рамках геополітичних конфліктів.

Відповідно до дослідницької проблематики цієї наукової статті існує потреба в розкритті категорії «пропаганда» в наукових працях сучасних науковців, для чого скористаємося нижченаведеною таблицею (таблиця 1), у якій наочно відображені дані трактування як вітчизняних, так і іноземних науковців.

Отже, на основі вищенаведених тверджень можна визначити, що пропаганда – це складний і багатогранний термін, який визначається як систематичний процес впливу на громадську думку, переконання та ставлення індивідів чи груп з метою досягнення певних стратегічних

Таблиця 1

Трактування категорії «пропаганда» в працях сучасних науковців

№	Автор	Визначення
1	Некрасов А. О. [1]	Пропаганда – це спрямована система впливу, що передбачає використання комунікативних методів і засобів для формування певних переконань, ставлень та дій аудиторії
2	Заболотний А. Г. [2]	Пропаганда – це специфічний вид комунікації, який має на меті переконати та вплинути на інших шляхом представлення інформації з метою досягнення певної мети чи підтримки певної ідеї
3	Кухоцька Т. [3]	Пропаганда – це масовий, організований і систематичний процес, спрямований на маніпуляцію суспільною свідомістю та вплив на неї
4	Городнича К. В. [4]	Пропаганда – це інженерія згоди, спрямована на створення сприятливого настроювання аудиторії та вплив на її поведінку через ретельне керування інформацією
5	Шевців М. Б., Гончарук К. А. [5]	Пропаганда – це створення ілюзії, сприяючи формуванню інтерпретацій і подій з метою зміни думок та дій громадськості
6	Mattingly D. C., Yao E. [6]	Пропаганда – це здійснення систематичного та прихованого впливу на маси за допомогою розроблених і вивчених технологій комунікації
7	Malhan M., Dewani P. P. [7]	Пропаганда – це масштабна, організована спроба вплинути на громадську думку та переконання, зазвичай через поширення односторонньої та вибіркової інформації

цілей. Цей вплив може здійснюватися через різні засоби комунікації, зокрема ЗМІ, соціальні мережі, радіо, телебачення, публічні виступи, графічні матеріали й інші канали інформації. Пропаганда нерідко має масовий характер, оскільки її метою є вплив на велику кількість осіб.

Ця форма комунікації може бути пов'язана з різними ідеологічними, політичними чи соціальними поглядами та цілями й використовується для підтримки чи поширення конкретних ідей, ставлень чи цілей. Пропаганда може мати інформаційний і психологічний виміри й передбачати елементи маніпуляції та дезінформації з метою впливу на сприйняття та поведінку аудиторії.

Вона часто використовується в політичних, військових чи геополітичних контекстах для досягнення стратегічних цілей і потребує критичного аналізу та реакції для забезпечення якості інформаційної обстановки та збереження національної і міжнародної безпеки.

Пропаганда в розумінні систематичної інформаційної діяльності для впливу на громадську думку і сприйняття індивідів стала невід'ємною складовою конфлікту між Російською Федерацією і Україною. Російська Федерація регулярно застосовує різні інформаційні методики для досягнення своїх політичних і воєнних цілей у цьому конфлікті. Ці методи передбачають поширення дезінформації, створення маніпулятивних новин, формування образу ворога й інші прийоми психологічного впливу. Пропагандистські зусилля Росії мають на меті деморалізацію та дестабілізацію суспільства в Україні, а також руйнування підтримки міжнародного співтовариства для України. Така стратегія інформаційної війни викликає серйозні виклики для національної і міжнародної безпеки України та потребує постійного аналізу.

Аналогічним чином здійснимо порівняння трактувань визначень категорії «інформаційна операція» в працях сучасних вчених, для чого скористаємося нижченаведеною таблицею (таблиця 2), у якій наочно відображені дані трактування як вітчизняних, так і іноземних науковців.

Отже, можна визначити, що інформаційна операція – це складне та багатоаспектне поняття, що визначається як координована діяльність, спрямована на збір, обробку, аналіз, створення й поширення інформації з метою впливу на свідомість, сприйняття та поведінку

Таблиця 2

Трактування категорії «інформаційна операція» в працях сучасних науковців

№ з/п	Автор	Визначення
1	Верголяс О. О. [8]	Систематична стратегічна діяльність для досягнення стратегічних цілей шляхом контролю над інформаційною обстановкою
2	Ділай А., Кротченко В. [9]	Використання інформації та комунікації для впливу на інших з метою досягнення стратегічних цілей
3	Сніцаренко П. М. [10]	Систематична діяльність зі створення, поширення й керування інформацією для впливу на сприйняття та поведінку цільових аудиторій
4	Ehrett C., Linvill D. L., Smith H., Warren P. L., Bellamy L., Moawad M., Moody M. [11]	Комплекс дій зі збору, аналізу, обробки, поширення та контролю інформації для досягнення стратегічних цілей, включно зі впливом на громадську думку
5	Linvill D. L., Warren P. L. [12]	Інтегрована система комунікації та впливу для маніпуляції інформацією та враженнями для досягнення політичних чи військових цілей

цільових аудиторій. Ця діяльність може передбачати використання різних засобів комунікації, зокрема медіа, соціальні мережі, інтернет, радіо, телебачення, газети, а також спеціалізовані інформаційні платформи та технології.

Інформаційні операції можуть мати різноманітні цілі, такі як вплив на громадську думку, маніпуляція інформаційною обстановкою, створення або руйнування образів, сприяння або перешкоджання специфічним подіям або процесам.

Цей термін широко використовується в різних контекстах, включно з політичною, військовою, комерційною, а також громадською сферами. Він передбачає не тільки обмін інформацією, але й психологічний вплив на цільові аудиторії з використанням різноманітних технік і стратегій.

Важливим аспектом інформаційних операцій є їх вплив на національну та міжнародну безпеку, а також здатність змінювати хід політичних подій і конфліктів. Із ц цим урахуванням аналіз, контроль і реагування на інформаційні операції стають надзвичайно важливими завданнями в сучасному інформаційному віці.

Слід розуміти, що, незважаючи на те що пропаганда та інформаційні операції є поняттями, які характеризуються певними відмінностями, вони використовуються разом в інформаційній війні (у тому числі і сьогодні в умовах повномасштабного вторгнення РФ в Україну) і мають певні схожі риси.

Відповідно до дослідницької проблематики цієї науково-дослідної роботи здійснимо розкриття й аналіз ключових спільних рис технологій пропаганди та інформаційних операцій, для чого скористаємося нижченаведеною блок-схемою (рис. 1), на якій наочно відображено цю системність структурних елементів.

Розглянемо більш детально ці сходні риси у сфері технологій пропаганди й інформаційних операцій:

– медійні платформи – технології пропаганди й інформаційних операцій використовують медійні платформи, такі як телебачення (наприклад, колишні телеканали Медведчука, радіо, соціальні мережі, вебсайти й інші канали для поширення інформації (значного розповсюдження в умовах повномасштабного вторгнення отримали проросійські телеграм канали) і повідомлень для населення території;

– кіберпростір – обидві сфери активно використовують інтернет і кіберпростір для поширення пропаганди й інформаційних повідомлень. Це передбачає створення вебсайтів, інтернет-форумів, спеціальних ботів та інші види;

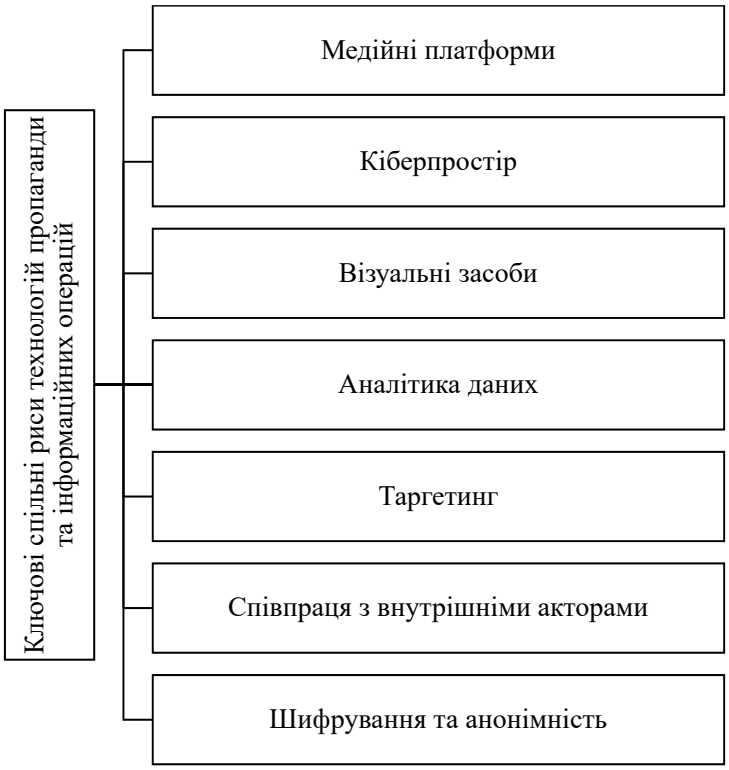

Рис. 1. Ключові спільні риси технологій пропаганди й інформаційних операцій

Джерело: побудовано автором на основі [1, 4–7, 10–11, 13, 15]

– візуальні засоби – обидві технології передбачають використання візуальних засобів, таких як фотографії, відео та графіка, для створення впливових матеріалів;

– аналітика даних – ці сфери використовують аналіз даних для визначення ефективності своєї діяльності та впливу на аудиторію;

– таргетинг – і пропаганда, і інформаційні операції дають змогу точно націлювати повідомлення на конкретні аудиторії та враховувати їхні індивідуальні характеристики й інтереси;

– співпраця з внутрішніми акторами – у деяких випадках технології передбачають співпрацю зі спільнотами, групами або особами всередині країни для підтримки пропаганди й інформаційних операцій;

– шифрування й анонімність – і пропаганда, і інформаційні операції можуть використовувати шифрування й анонімність для захисту ідентичності та джерел інформації, що дає змогу зберігати конфіденційність діяльності.

Незважаючи на існуючі спільні риси в технологіях пропаганди та інформаційних операцій, також слід розуміти, що існують значні відмінності в цих сферах.

Відповідно до дослідницької проблематики цієї науково-дослідної роботи здійснимо розкриття й аналіз ключових відмінностей технологій пропаганди та інформаційних операцій, для чого скористаємося нижченаведеною блок-схемою (рис. 2), на якій наочно відображена ця системність структурних елементів.

Пропаганда й інформаційні операції мають певні відмінності у своїх цілях, методах і контексті застосування:

1. Ціль і спрямованість:

– головною метою пропаганди є переконання аудиторії в правильності певних ідей або підтримка конкретних інтересів або поглядів;

Рис. 2. Ключові відмінності технологій пропаганди та інформаційних операцій

Джерело: побудовано автором на основі [1–3, 6–9, 12, 14–18]

– ціль інформаційних операцій може передбачати не лише переконання, але й збирання інформації, поширення дезінформації, психологічний вплив тощо. Основна мета – змінити інформаційну обстановку або створити певний ефект.

2. Масштаб і амплітуда:

– пропаганда переважно має масовий характер і спрямована на велику кількість осіб;

–інформаційні операції можуть бути спрямовані на обмежену аудиторію або мати менший масштаб.

3. Легітимність і конфіденційність:

– пропаганда може бути відкритою і легальною діяльністю;

– водночас інформаційні операції часто мають елементи конфіденційності та можуть бути прихованими або іноді навіть незаконними.

4. Контекст і застосування:

– пропаганда використовується в різних сферах, включно з політикою, культурою, релігією тощо;

– інформаційні операції частіше виникають у військовому або геополітичному контексті, а також у сферах кібербезпеки та розвідки.

5. Засоби комунікації:

– пропаганда використовує різні засоби комунікації, зокрема ЗМІ, соціальні мережі, радіо, телебачення і публічні виступи;

– при цьому інформаційні операції можуть передбачати кібератаки, збір інформації за допомогою розвідувальних засобів, дезінформацію і психологічний вплив.

6. Підтримка з боку влади:

– пропаганда може мати офіційну підтримку від держави або партійної структури;

– водночас інформаційні операції можуть виконуватися як державними структурами, так і недержавними акторами або навіть кримінальними групами.

7. Ефективність і результати:

– ефективність пропаганди може бути важко виміряти, до того ж вона залежить від реакції аудиторії;

– інформаційні операції можуть бути спрямовані на конкретні цілі, такі як кібератаки або збір конфіденційної інформації, і їх результати можуть бути більш кількісно виміряні.

Висновки. Як підсумок цієї наукової статті можна зробити такі висновки:

1. Технології пропаганди й інформаційних операцій мають декілька ключових спільних рис, які свідчать про їхню суттєву взаємодію. Обидві сфери використовують медійні платформи, кіберпростір і візуальні засоби для поширення інформації та впливу на аудиторію. Вони також можуть використовувати аналітику даних, спеціалізовані таргетингові стратегії та сприймати важливість співпраці зі спільнотами або внутрішніми акторами. Крім того, технології обох сфер можуть застосовувати шифрування й анонімність для забезпечення конфіденційності.

2. Технології пропаганди й інформаційних операцій, хоча і мають певну спільність у використанні комунікаційних засобів, відрізняються значущими характеристиками та метою. Пропаганда передбачає систематичний вплив на громадську думку, спрямований на переконання аудиторії в певних ідеях або поглядах. З іншого боку, інформаційні операції можуть передбачати різноманітні завдання, такі як збір інформації, психологічний вплив, дезінформацію та кібератаки, а їх мета – зміна інформаційної обстановки або досягнення конкретних стратегічних цілей. Інформаційні операції також часто відзначаються більшою конфіденційністю та можуть виконуватися не лише державними структурами, але й недержавними або кримінальними акторами. З огляду на ці відмінності розуміння обох явищ стає важливим завданням для реагування на сучасні виклики у сфері інформаційної безпеки та геополітики.

Література:

1. Некрасов А. О. Пропаганда як предмет дослідження. Міністерство освіти і науки України, Київський національний університет культури і мистецтв, Київський університет культури, факультет післядипломної освіти рада молодих вчених КНУКіМ, 2021 .С. 116.

2. Заболотний А. Г. Пропаганда: визначення, основні елементи та види. Актуальні проблеми технічних та соціально-гуманітарних наук у забезпеченні діяльності служби цивільного захисту : матеріали Всеукраїнської науково-практичної конференції (4 квітня 2014 року, м. Черкаси). Черкаси : ЧІПБ імені Героїв Чорнобиля НУЦЗ України, 2014. 304 с., с. 216.

3. Кухоцька Т. Російська пропаганда в політичній комунікації під час війни. *Collection of scientific papers «ΛΟΓΟΣ»,* (June 23, 2023; Oxford, UK), 2023. С. 193–194.

4. Городнича К. В. Пропаганда як технологія політичного маніпулювання. Міжнародні наукові дослідження: інтеграція науки та практики, 2018. С. 82–84.

5. Шевців М. Б., Гончарук К. А. Пропаганда як соціально-політичне явище: проблеми розуміння. Південноукраїнський правничий часопис. Випуск 1. 2019. С. 119–122.

6. Mattingly D. C., Yao E. How soft propaganda persuades. *Comparative Political Studies*, 55 (9), 2022. P. 1569–1594.

7. Malhan M. & Dewani P. P. Propaganda as communication strategy: Historic and contemporary perspective. *Academy of Marketing Studies Journal*, 24 (4). 2020. P. 1–15.

8. Верголяс О. О. Спеціальні інформаційні операції в системі засобів протидії загрозам національній безпеці України. *Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки».* Випуск 4. 2019. С. 7–16.

9. Ділай А., Кротченко В. Війна за Україну: від інформаційних операцій до прямого вторгнення. *Вісн. Львів. ун-ту. Серія: Журналістика*, 2019. С. 13–20.

10. Сніцаренко П. М. Інформаційна операція Збройних Сил України як інтегруюча форма воєнних дій в інформаційному просторі. *Наука і оборона*. 2020. № 1. С. 37–42.

11. Ehrett C., Linvill D. L., Smith H., Warren P. L., Bellamy L., Moawad M., ... & Moody M. Inauthentic newsfeeds and agenda setting in a coordinated inauthentic information operation. Social Science Computer Review, 40 (6), 2022. P. 1595–1613.

12. Linvill D. L. & Warren P. L. Engaging with others: How the IRA coordinated information operation made friends. Harvard Kennedy School Misinformation Review, 1 (2). 2020.

13. Вітюк Н. Особливості дискурсу політичної пропаганди в умовах інформаційно-психологічної війни. *Збірник наукових праць: психологія. 2019. Вип. 24*. С. 29–38.

14. Герасименко О. Політична пропаганда як засіб інформаційної війни. *Scientific Collection "InterConf",* 2022. № 120, с. 102–104.

15. Ділай А., Кротченко В. Війна за Україну: від інформаційних операцій до прямого вторгнення. *Вісн. Львів. ун-ту. Серія: Журналістика*, 2019. С. 13–20.

16. Мєлєкєсцев К. І. Про трактування інформаційної війни: від технічно-кібернетичної до історико-психологічної парадигми. *Південний архів (історичні науки)*, 2022. № 38, с. 62–67.

17. Bjola C. & Papadakis K. Digital propaganda, counterpublics, and the disruption of the public sphere: The Finnish approach to building digital resilience. In The World Information War. Routledge, 2021. P. 186–213.

18. Bahar H. M. Social media and disinformation in war propaganda: how Afghan government and the Taliban use Twitter. Media Asia, 47 (1–2), 2020. P. 34–46.

References:

1. Nekrasov, A. O. (2021). Propaganda yak predmet doslidzhennya [Propaganda as a subject of research]. Ministerstvo osvity i nauky Ukrayiny, Kyiv National University of Culture and Arts, Kyiv University of Culture, Faculty of Postgraduate Education, Council of Young Scientists of KNUCA, p. 116 [in Ukrainian].

2. Zabolotnyi, A. G. (2014). Propaganda: vyznachennya, osnovni elementy ta vidy [Propaganda: Definition, Key Elements, and Types]. Aktualni problemy tekhnichnykh ta sotsialno-humanitarnykh nauk u zabezpechenni diyalnosti sluzhby tsyvilnoho zakhystu: Materialy Vseukrayinskoi naukovo-praktychnoi konferentsii (4 kvitnia 2014 roku, m. Cherkasy). Cherkasy: ChIPB imeni Heroiv Chornobylia NUTsZ Ukrainy. P. 216 [in Ukrainian].

3. Kukhotska, T. (2023). Rosiiska propahanda v politychnii komunikatsii pid chas viiny [Russian Propaganda in Political Communication During the War]. *Collection of scientific papers «ΛΟΓΟΣ»*, (June 23, 2023; Oxford, UK), p. 193–194 [in Ukrainian].

4. Horodnycha, K. V. (2018). Propahanda yak tekhnolohiia politychnoho manipuliuvannia [Propaganda as a Technology of Political Manipulation]. *Mizhnarodni naukovi doslidzhennia: intehratsiia nauky ta praktyky*, p. 82–84 [in Ukrainian].

5. Shevtsiv, M. B., & Honcharuk, K. A. (2019). Propahanda yak sotsialno-politychne yavyshche: problemy rozuminnia [Propaganda as a Social-Political Phenomenon: Understanding Issues]. *Pivdennoukrainskyi pravnychyi chasopys*, (1), p. 119–122 [in Ukrainian].

6. Mattingly, D. C., & Yao, E. (2022). How soft propaganda persuades. *Comparative Political Studies*, 55 (9), pp. 1569–1594.

7. Malhan, M., & Dewani, P. P. (2020). Propaganda as communication strategy: Historic and contemporary perspective. *Academy of Marketing Studies Journal,* 24 (4), pp. 1–15.

8. Verholias, O. O. (2019). Spetsialni informatsiyni operatsiyi v systemi zasobiv protydiyi zahrozam natsional'niy bezpeky Ukrayiny [Special Information Operations in the System of Counteracting Threats to National Security of Ukraine]. *Mizhnarodnyi naukovyi zhurnal "Internauka". Seriya: "Yurydychni nauky*," (4), p. 7–16 [in Ukrainian].

9. Dilay, A., & Krotchenko, V. (2019). Viyna za Ukrayinu: vid informatsiynykh operatsiy do pryamoho vtorgnennya [War for Ukraine: From Information Operations to Direct Invasion]. *Visnyk Lviv. un-tu. Seriya: Zhurnalistyka*, p. 13–20 [in Ukrainian].

10. Snitsarenko, P. M. (2020). Informatsiyna operatsiya Zbroinykh Sil Ukrayiny yak intehruyucha forma voyennykh dii v informatsiynomu prostori [Information Operation of the Armed Forces of Ukraine as an Integrating Form of Warfare in the Information Space]. *Nauka i oborona*, (1), p. 37–42 [in Ukrainian].

11. Ehrett, C., Linvill, D. L., Smith, H., Warren, P. L., Bellamy, L., Moawad, M., ... & Moody, M. (2022). Inauthentic newsfeeds and agenda setting in a coordinated inauthentic information operation. Social Science Computer Review, 40 (6), p. 1595–1613.

12. Linvill, D. L., & Warren, P. L. (2020). Engaging with others: How the IRA coordinated information operation made friends. *Harvard Kennedy School Misinformation Review*, 1(2).

13. Vitiuk, N. (2019). Osoblyvosti dyskursu politychnoi propahandy v umovakh informatsiino-psykholohichnoi viiny [Features of Political Propaganda Discourse in the Context of Information-Psychological Warfare]. *Zbirnyk naukovykh prats: psykholohiia*, (24), p. 29–38 [in Ukrainian].

14. Herasymenko, O. (2022). Politychna propahanda yak zasib informatsiinoi viiny [Political Propaganda as a Means of Information Warfare]. *Scientific Collection "InterConf,"* (120), p. 102–104 [in Ukrainian].

15. Dilay, A., & Krothenko, V. (2019). Viyna za Ukrayinu: vid informatsiinykh operatsiy do pryamoho vtorgnennia [War for Ukraine: From Information Operations to Direct Invasion]. *Visnyk Lviv. un-tu. Seriya: Zhurnalistyka*, p. 13–20 [in Ukrainian].

16. Meliakievtsev, K. I. (2022). Pro traktuvannia informatsiinoi viiny: vid tekhnichno-kibernetychnoi do istoriko-psykholohichnoi paradyhmy [On the Interpretation of Information Warfare: From Technical-Cybernetic to Historical-Psychological Paradigm]. *Pivdennyi arkhiv (istorychni nauky),* (38), p. 62–67 [in Ukrainian].

17. Bjola, C., & Papadakis, K. (2021). Digital propaganda, counterpublics, and the disruption of the public sphere: The Finnish approach to building digital resilience. In The World Information War (pp. 186-213). Routledge.

18. Bahar, H.M. (2020). Social media and disinformation in war propaganda: how Afghan government and the Taliban use Twitter. Media Asia, 47 (1–2), p. 34–46.

Taras Kobets. Comparative analysis of propaganda and information operations techniques under martial law

In today`s geopolitical landscape, signs of military conflicts and crises are increasing, which makes the issue of the impact of information warfare on society and international relations relevant. Under martial law, propaganda and information operations become extremely important tools in the conduct of hostilities. Analyzing the comparative aspects of these techniques will allow us to better understand their role in shaping the opinions and views of citizens, and their impact on international politics and state security. The study of this issue is important for developing strategies to counter manipulation and disinformation, contributing to the resilience and effectiveness of society in situations of conflict.

The conditions of a full-scale war initiated by the Russian Federation against Ukraine include not only hostilities, but also active use of propaganda and information operations to manipulate the world community and create its own image of the conflict. The Russian Federation has improved its information strategy by using various media, social networks, Internet resources and influential agents to spread disinformation, fakes and distorted information.

This helps to create a false information space about the conflict, justify its own aggression, discredit the Ukrainian government and support russian interests. Information operations of the Russian Federation are aimed at influencing public opinion and international partners to reduce support for Ukraine in the world and create the impression that Ukraine's situation is incorrect. In such a situation, it is important to carefully analyze information and perceive the events objectively.

It is extremely relevant and important to study propaganda and information operations techniques under martial law. The war today includes not only physical combat, but also information warfare, which is dominated by strategies of manipulation, disinformation, and psychological influence. The study of propaganda and information operations allows us to understand how they are used to shape public opinion, destabilize the enemy, and preserve our own legitimacy. It also contributes to the development of effective strategies for counterpropaganda and protection of the information space. It is important to analyze and reveal the methods and techniques used to spread fake news and other types of disinformation. The study of these techniques provides an opportunity to develop systems for preventing and responding to information threats, enhances information awareness, and contributes to maintaining stability and security in wartime conditions.

The study aims to determine specific aspects of the use of propaganda and information operations tools in the context of military conflicts, and their impact on society, politics and security.

Propaganda and information operations techniques under martial law have a significant impact on society and international politics. They are used to manipulate and shape public opinion, and can undermine the stability of the states. Understanding these processes is becoming key to ensuring national and international security.

Key words: *propaganda, information operations, war, hybrid warfare, martial law.*

УДК 355.021
DOI: https://doi.org/10.32782/2312-1815/2024-1-6

Андрій Міщук
ORCID: 0000-0002-2585-7110

Мар'яна Міщук
ORCID: 0000-0002-2589-6582

ЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ: ДІЯЛЬНІСТЬ УПЦ (МП)

Стаття розглядає вплив діяльності Української православної церкви (далі – УПЦ (МП)), підконтрольної Московському патріархату, на національну безпеку України, зокрема, досліджуються проблема загроз національній безпеці України в контексті діяльності УПЦ (МП). Стаття аналізує вплив московського центру на функціонування її структурних одиниць і духовенство. Подано факти співпраці представників цієї церкви із російським агресором як безпосередньо через участь у коригуванні вогню, забезпеченні окупантів провіантом, інформацією, так і через пропагування ідей так званого русского міра. Звертається увага на можливі аспекти інформаційної війни, у якій релігійна сфера може використовуватися для формування певного образу країни та сприяння розпалюванню конфліктів. Аналізуються можливі загрози, які виникають із залежності церкви від російських церковних структур та її вплив на формування національної ідентичності. Наведено спроби розпалювання міжнаціональної та міжконфесійної ворожнечі, відкритої підтримки агресії РФ, яка нібито «захищає» істинних українських православних від загроз Європи.

Ключові слова: *національна безпека, релігія, політика, колабораціонізм, церква, агресія.*

Вступ. Релігія має значний вплив на політику в багатьох країнах і регіонах світу та залежить від багатьох факторів, включно з культурними, історичними та правовими особливостями кожної конкретної держави.

Вплив релігійного осередку однієї держави на іншу може мати різні аспекти та проявлятися в різних сферах, зокрема, дипломатичні відносини (духовні особи, глави церков і релігійні організації можуть виступати як посередники, впливати на розвиток дипломатичних відносин між державами, сприяючи діалогу між країнами або досягненню взаємного порозуміння); гуманітарна допомога та місіонерська діяльність (релігійні організації можуть надавати гуманітарну допомогу та проводити місіонерську діяльність в інших країнах, що, зі свого боку, може впливати на соціальні й економічні аспекти життя в країнах). Але, крім цих позитивних факторів, можна конкретизувати й негативну роль релігійного чинника, яка проявляється у впливі на політичні процеси в інших країнах через представництво, політичні зв'язки та лобіювання. До того ж усупереч морально-етичним засадам християнства окремі релігійні організації розпалюють міжнаціональні конфлікти, несуть загрозу державному суверенітету й освячують військову агресію, виправдовуючи терористичну діяльність та порушуючи одну із Заповідей Божих («Не вбий!»).

Мета та завдання статті. Метою статті є дослідити факти, що вказують на загрозу національної безпеки України з боку діяльності духовенства та функціонування ієрархій УПЦ (МП).

Методи. Для аналізу фактів використано такі загальнонаукові методи, як аналіз, синтез, порівняння. Дослідженні базувалося переважно на використанні методологічних засад інституціоналізму.

Аналіз останніх досліджень. Серед сучасних дослідників варто виділити праці О. Хмільовської [23], В. Олійника [14], Я. Конощука [8].

Виклад основного матеріалу дослідження. Саме російська православна церква (далі – РПЦ) намагається використовувати релігійну ідеологію для виправдання агресивної політики російської влади на чолі з Путіним. РПЦ та її патріарх Кирил відкрито підтримують війну проти України та ще й розглядають її як священну в реалізації концепту так званого *русского міра*. Це невипадково, адже в РФ державний апарат і церква нерозривно пов'язані між собою (ця традиція, беручи свій початок ще з імперських часів, набула значного поширення в період функціонування СРСР та особливо активізувалася в сучасних умовах).

Дослідники вказують на таке несумісне для істинних християнських церков явище, як мілітаризація російської церкви. Релігієзнавиця, професорка Інституту філософії імені Г. С. Сковороди Національної академії наук України Людмила Філіпович у цьому контексті наводить такі факти: «По-перше, будівництво відомого військового храму у Підмосков'ї – це дуже яскрава демонстрація того, що змінюється сама суть християнства. Того, що ця релігія зі світотворчої (це основне призначення християнства) перетворюється на таку войовничу, дуже агресивну релігію, яка освячує війну… По-друге, священики РПЦ беруть безпосередню участь у військових діях. Ми неодноразово бачили, наприклад, тих самих священиків, які в руках тримають зброю… з боку Росії це агресивний, віроломний напад на суверенну державу, якою була Україна і є …» [25].

У цьому ж контексті Служба безпеки України повідомила про викриття керівництва РПЦ в організації на території РФ власних приватних військових компаній для війни проти нашої держави: «За вказівками Московського патріархату їхні ПВК займаються вербуванням та бойовою підготовкою найманців для війни проти України. Задокументовано, що одна з таких приватних військових компаній під назвою «Андріївський хрест» діє на базі Кронштадтського Морського собору в Санкт-Петербурзі. У стінах релігійної установи її представники вербують прихожан для подальшого включення до складу окупаційних угруповань РФ, які задіяні на передовій... Після зарахування найманців до лав ПВК московської церкви вони проходять курс військово-тактичної та вогневої підготовки під керівництвом інструкторів з російських спецслужб» [1; 5].

Ще в 2014 р. **на засіданні XVIII Всесвітнього російського народного собору, який відбувся в Москві, було прийнято декларацію, у якій зазначалося: «…**росіянин – це людина, яка вважає себе росіянином; не має інших етнічних уподобань; говорить і думає російською мовою; визнає православне християнство основою національної духовної культури; відчуває солідарність з долею російського народу» [26]. Не випадково особлива роль у декларації відводиться православній вірі, адже РПЦ як безпосередньо, так і через їй підвладну структурну одиницю – Українську православну церкву московського патріархату (далі – УПЦ (МП)), активно вроваджувала ідеологічну конструкцію «русского міра».

Саме ідеологеми «русского міра», на думку О. Хмільовської, Московський патріархат тривалий час в ході так званого духовно-патріотичного виховання віруючих, прищеплював їм. Дослідниця констатує: «…на жаль, протягом 25 років незалежності України релігійному чиннику було відведено периферійне місце в системі національної безпеки держави. Ігнорування саме цієї безпекової складової і спричинило російську релігійну експансію на південних та східних територіях України… Саме ці території зазнали найбільшого впливу УПЦ МП, і саме тут московський патріархат став організатором ідеологічної пропаганди агресора» [23].

Стаття 7 Закону України «Про основи національної безпеки України» від 19 червня 2003 року (зі змінами та доповненнями 2015 р.) серед потенційних загроз національній безпеці України вказує на «можливість… радикалізації та проявів екстремізму в діяльності деяких об'єднань національних меншин та релігійних громад» [3].

Ось головні аргументи, які вказують на пряму загрозу УПЦ (МП) національній безпеці України:

Зв'язок із Росією: УПЦ (МП) є афілійованою з російською православною церквою і отримує підтримку з боку Московії. Це може створювати ситуацію, де церква вважається інструментом впливу Росії в Україні. І навіть Собор УПЦ (МП) 27 травня 2022 р., незважаючи на те, що, з одного боку, познімав у Статуті всі згадки про московський центр, з іншого – не змінив її канонічного та організаційного статуус, як констатує М. Княжицький. Глава УПЦ (МП) є членом Синоду РПЦ, представники духовенства УПЦ (МП) входять до різноманітних структурних підрозділів РПЦ. І навіть богослов Кирило Говорун (у минулому керівник відділу зовнішніх зв'язків УПЦ (МП) відзначає той факт, що, попри спробу дистанціюватись від Москви, «… вони залишаються в Московському патріархаті через те, що ввели туди згадку про грамоту від патріарха Олексія від 1990 року. Там говориться, що УПЦ є частиною світового православ'я через РПЦ» [24]. 25 листопада 2022 р. після обшуку в Чернівцях СБУ оприлюднила листування митрополита Мелетія Буковинського (керівника відділу зовнішніх зв'язків УПЦ) з митрополитом Марком з Російської православної церкви за кордоном, у якому Мелетій пише, що УПЦ і далі є частиною РПЦ [19].

Співробітництво з російськими органами влади: значна частина духовенства УПЦ (МП) виражають повну підтримку російської окупації. Факти, наведені *в Реєстрі Зрадників Руху ЧЕСНО (40 із них – представники УПЦ (*МП*)),* свідчать про те, що «московська «церква» становить загрозу національній безпеці України та діє не як релігійна організація, а як важлива організаційна та адміністративна структура російської церкви та агентурна мережа окупаційних спецслужб» [14].

Український релігієзнавець, завідувач відділення релігієзнавства Інституту філософії імені Г. Сковороди НАН України, професор Олександр Саган стосовно зазначеного питання відзначає: «Діяльність московського патріархату в Україні об'єктивно є загрозою національній безпеці нашої країни. Чому об'єктивно? Тому що ще наприкінці 90-х років минулого століття московська патріархія уклала договори співпраці зі всіма силовими структурами російської федерації. Як показала війна Росії проти України, ця співпраця лише посилюється. Тому абсолютно справедливо ще у 2014 році було ухвалене рішення не співпрацювати з УПЦ (МП) у сфері підготовки і діяльності військових капеланів. Адже вже тоді були непоодинокі випадки колабораціонізму і відвертої праці на ворога кліриків саме цієї церкви» [10].

Підтримка російської агресії суттєво змінила ставлення значної частини українського суспільства до московського патріархату та викликала відповідні рішення органів місцевого самоврядування. Уже 16 вересня 2022 р. на сесії Івано-Франківської облради депутати підтримали одноголосно та скерували до Президента, Верховної Ради та СБУ звернення, у якому просили «керівництво держави заборонити Українську православну церкву Московського патріархату в країні, ініціювати розслідування її діяльності та покарати винних за колабораціонізм», адже представники УПЦ (МП), за твердженням депутатів, всіляко уникають засудження російської агресії проти України, відкрито співпрацюють з Росією на окупованих територіях, більше того, допомагають військовим формуванням агресора та зберігають у храмах зброю, власне через це «на теренах України не може існувати антиукраїнська структура ворожої країни, та ще й під час війни. Незалежність від Росії має бути у всьому, в релігії та вірі також» [22].

Львівська облрада ухвалила заборонити УПЦ Московського патріархату 29 листопада 2022 року. На Хмельниччині подібне рішення значною мірою було викликано побиттям 2 квітня 2023 р. священиками хмельницького Свято-Покровського кафедрального собору військового Збройних сил України, а тому вже на позачерговій сесії 4 квітня депутати Хмельницької обласної та міської рад одностайно висловилися проти УПЦ (МП). За заборону діяльності Української православної церкви (МП) 10 квітня 2023 р. проголосували депутати Рівненської обласної ради та Рівненської міської ради (підтримали рішення про припинення права користування УПЦ (МП) земельними ділянками на території громади). А мер Рівного Олександр Третяк із цього

приводу зазначив: «Неприпустимо, щоб під час війни в державі функціонувала церква, яка благословляє російських солдатів на вбивства українців» [9]. 11 квітня за заборону УПЦ (МП) одноголосно проголосували депутати Волинської обласної ради, 17 квітня – Тернопільської міської ради. У Вінницькій області Московський патріархат заборонили ще в листопаді 2022 р,. однак відповідне рішення Вінницька облрада ухвалила 28 квітня 2023 р. (54 голоси із 60 присутніх депутатів). Депутати ухвалили документ під назвою «Про забезпечення зміцнення національної безпеки у сфері свободи совісті та діяльності релігійних організацій на території Вінницької області», у якому констатували «припинення договорів оренди нерухомого майна, земельних ділянок і заборону будь-якого користування майном, що є спільною власністю територіальних громад, сіл, селищ, міст Вінницької області, з релігійними організаціями Української православної церкви в єдності з Московським патріархатом та іншими релігійними організаціями, афілійованими із центрами впливу релігійних організацій, керівні центри яких розташовані в державі-агресорі» [12]. 27 квітня діяльність УПЦ (МП) заборонили Житомирська обласна та Чернівецька міська ради. 1 червня депутати Закарпатської облради підтримали рішення «Про забезпечення зміцнення національної безпеки у сфері діяльності громадських та релігійних організацій на території Закарпатської області», відповідно до якого передбачається заборона на території області діяльності **релігійних, церковних, громадських та інших організацій,** які співпрацюють або мають зв'язки з Росією. 9 червня депутати Київської обласної ради, констатуючи той факт, що саме Кремль контролює УПЦ (МП), тому це загрожує національній безпеці України, прийняли також відповідне рішення про заборону. 12 липня 2023 р. (усупереч твердженням прихильників УПЦ (МП), що рішення про заборону їх церкви приймалися лише владними органами Західної України) на 19-й сесії Запорізької міської ради восьмого скликання депутати проголосували за припинення взаємовідносин Запорізької міської територіальної громади з релігійними організаціями Української православної церкви Московського патріархату.

Кожна з перелічених обласних рад також надіслала звернення щодо перегляду відповідно до наявної суспільно-політичної ситуації та якнайшвидшого ухвалення законопроєктів № 8371 «Про внесення змін до деяких законів України щодо діяльності в Україні релігійних організацій» (від 19 січня 2023 р.) і № 8221 «Про забезпечення зміцнення національної безпеки у сфері свободи совісті та діяльності релігійних організацій» (від 23 листопада 2022 р.).

У деяких областях частково заборонили УПЦ (МП), тобто рішення схвалили окремі громади чи населені пункти: 27 квітня 2023 року – Броварська міськрада (Київської області), 3 травня 2022 року – Конотопська міська рада (Сумської області) [12]. Так, за словами міського голови Конотопа А. Семеніхіна, «між ворогом і його аґентом немає різниці. А у випадку моспархату це є два в одному. Тому я прийняв рішення заборонити на території мого міста діяльність цієї аґентурної мережі ФСБ» [20].

Відразу ж після 23 лютого 2022 р. з'являлися повідомлення про сприяння священниками УПЦ (МП) російським окупаційним військам та подальшу пропаганду ними «русского міра». Неодноразово священики УПЦ (МП) в різних регіонах України відмовлялися проводити заупокійну літургію за загиблими воїнами ЗСУ.

РНБО ввела санкції щодо 21 церковника РПЦ. Серед них, зокрема, протоієрей, письменник, проповідник **Артемій Владіміров (**виправдовує агресію РФ проти України та висловлює надію на поглинання Росією країн колишнього СРСР), митрофорний протоієрей, проповідник, телеведучий, популярний YouTube-блогер **Андрій Ткачов (**російську агресію розглядає як покарання українцям за Майдан, до того ж закликає російських військових продовжувати вбивати українців**)** [6].

СБУ у жовтні 2022 р. розпочала обшуки в окремих єпархіях УПЦ (МП). Усі ці дії проходили в межах «системної роботи СБУ з протидії підривній діяльності російських спецслужб в Україні» та в межах чинного законодавства.

Василь Малюк 27 жовтня назвав УПЦ (МП) «ідеальним полем для функціонування ворожої резидентури» та заявив, що від початку війни СБУ відкрила 23 кримінальні провадження щодо діячів УПЦ, а вже 33 церковників є підозрюваними – «від класичних агентів збору глибинної інформації до банальних коригувальників вогню в рясах» [4].

Працівники СБУ викривали факти проросійської діяльності окремих священиків та й навіть єпископів.

Деякі священнослужителі УПЦ (МП) складали списки колишніх учасників АТО, державницьки налаштованих осіб. Так, Віктор Талько (настоятель Свято-Михайлівського храму в Бородянці Київської області) під час окупації Бородянки, незважаючи на всі ті звірства російської армії, прийняв агресорів і забезпечував її штаб усім необхідним. До того ж він сприяв взяттю у полон та примусовому вивезенню мешканців Бородянки та сусідніх селищ на територію Білорусі, а також брав участь у коригуванні вогню по Гостомелю та підступах до Києва [25].

Саме тому, враховуючи всі ці факти, співробітники СБУ проводили обшуки в ієрархіях УПЦ (МП) у різних областях та, незважаючи на територіальне розташування, знаходили фактично всюди речі, пов'язані з російською пропагандою: рублі, російські паспорти, пропагандистську літературу та навіть сухпайки армії агресорів. Так, зокрема, уже 12 жовтня співробітники СБУ повідомили про викриття на Вінниччині митрополита Тульчинського і Брацлавського УПЦ (МП) Іонафана (Анатолій Єлецьких), якого на проросійських чатах називали «послідовно проросійським Тульчинським митрополитом», «відданим Патріарху Кирилу, Російській Церкві, Росії», який «ненавидить українізацію» [15]. Він виправдовував агресію РФ, працював в інтересах агресора, сприяв поширенню друкованих матеріалів зі зверненням до громадян України Путіна і Кирила, а також закликав до визнання «ЛНР» і «ДНР». Протиправний характер дій було підтверджено експертизою, проведеною з ініціативи СБУ.

Під час оперативної операції в Кіровоградській та Олександрійській єпархіях було проведено обшуки в митрополитів Кіровоградського і Новомиргородського Іоасафа і митрополита Олександрійського та Світловодського Боголєпа, за результатами яких виявлено «листування митрополита Кіровоградського і Новомиргородського з патріархом московським Кирилом та вилучено велику кількість виготовлених у РФ антиукраїнських матеріалів. У їх текстах містяться ознаки вчинення кримінальних правопорушень, передбачених двома статями ККУ», – йдеться в повідомленні СБУ. Було виявлено також, що окремі представники цих громад церковних були причетні до розповсюдження інформації, що посягала на територіальну цілісність України [19].

У Чернівецько-Буковинській єпархії УПЦ (МП) було «викрито листування керівників єпархії зі своїми московськими кураторами, у яких вони отримують «методички» щодо «особливостей» проведення церковних літургій після повномасштабного вторгнення» [17]. Було знайдено також прокремлівську літературу, що містила заклики підтримки окупантів і фотокопії посвідчень росіян, які брали участь у бойових діях проти українських військ (на компютерах).

На бік Росії відкрито перейшли та втекли туди два єпископи УПЦ (МП) – митрополит Роменський і Буринський Іосиф та митрополит Ізюмський і Куп'янський Єлисей.

Під час контррозвідувальних заходів СБУ 7 грудня 2022 р. на Черкащині (обшук проходив у 10 культових приміщеннях УПЦ (МП), у тому числі і в Красногірському Свято-Покровському жіночому монастирі) було знайдено прокремлівську агітаційну літературу, листування з московським патріархом, молитви за патріарха та молитва-гімн «Боже, царя храни» і навіть символіку терористичного об'єднання «Новоросія», що є свідченням прямого зв'язку з російськими агресорами [**11].**

Служба безпеки України проводила контррозвідувальні заходи також на території Свято-Успенської Києво-Печерської лаври в Києві [18]. І це не випадково, адже, як стверджує

керівник Центру стратегічних комунікацій та інформаційної безпеки Ігор Соловей, цитуючи книгу «Спецслужби світу за 500 років», ще чотири століття тому російська розвідка перебувала в лаврі: «Москва мала в Україні сильну таємну агентуру в обличчі українського православного духовенства, яке надавало московській владі цінну інформацію про стан справ в Польщі і настрої української козацької старшини. Центр російської агентурної розвідки в Україні знаходився в Києві, в Києво-Печерській лаврі» (йдеться про 1662 р.). До того ж навіть в умовах агресивної війни РФ проти України в одному з храмів Києво-Печерської лаври під час духовних піснеспівів звучала пісня «Звон плывёт, плывёт над Россиею, пробуждается матушка-Русь» [18]. На що керівник СБУ В. Малюк відповів таким чином: «Ті, хто в умовах повномасштабної війни, яку розв'язала Росія проти України, чекає на пробудження *«матушки-Руси»*, мають розуміти, що це шкодить безпеці та інтересам України та наших громадян. І ми не допустимо таких проявів» [21]. Під час обшуків у Лаврі було виявлено коло осіб з паспортами та військовими квитками СРСР або підробленими українськими паспортами. Попри спробу начебто дистанціюватися від РПЦ, реальний стан речей продемонстрував сам Кремль, адже речник президента РФ Д. Пєсков назвав обшуки в лаврі «діями проти російського православ'я». Та, зрештою, і сам Онуфрій (глава УПЦ (МП)) приймав у Києво-Печерській лаврі (2022 р.) російських полонених окупантів, де провів спільну молитву, проспівав «Многая літа» та побажав окупантам здоров'я**.** Настоятель Свято-Успенської Києво-Печерської Лаври Петро Лебідь перебуває під слідством у справі щодо розпалювання релігійної ворожнечі та ненависті [14].

Зважаючи на кримінальні провадження стосовно членів УПЦ (МП) (за даними СБУ, з початку повномасштабної агресії РФ відкрито 68 кримінальних проваджень щодо представників УПЦ (МП) (з яких 16 – стосовно митрополитів церкви; з – поміж викритих злочинів – 20 фактів держзради та колабораціонізму. 26 фігурантам – представникам УПЦ (МП) повідомлено про підозру, а ще 19 уже отримали судові вироки), що несуть загрозу національній безпеці. 19 жовтня 2023 р. Верховна Рада України проголосувала (267 депутатів) у першому читанні за урядовий законопроєкт № 8371 про заборону релігійних організацій, що пов'язані з РФ. Він був зареєстрований у парламенті ще 19 січня 2023 року, а 12 квітня Всеукраїнська Рада Церков і релігійних організацій рекомендувала схвалити його в першому читанні. Відповідно до законопроєкту, в Україні **«не допускається діяльність релігійних організацій, які афілійовані із центрами впливу релігійної організації (об'єднання), керівний центр (управління) якої знаходиться за межами України в державі, яка здійснює збройну агресію проти України»** [2].

Оскільки законопроєктом передбачається припинення діяльності релігійної організації через рішення суду за адміністративним позовом центрального органу виконавчої влади, що реалізує державну політику у сфері релігії, або прокурора, то, очевидно, що це не означає негайного припинення функціонування УПЦ (МП) [8].

Як відзначає народний депутат України М. Княжицький, «на превеликий жаль, незважаючи на дії української влади, керівництво УПЦ МП може почуватися у відносній безпеці. Згідно з урядовим законопроєктом, тривалість судової процедури заборони її діяльності вимірюється роками. Знайомий правник оцінив, що на рішення апеляційного суду (а апелювати напевно будуть) можна чекати до 2025 р. Згодом, коли рішення українських судів буде негативним для УПЦ МП, вона звернеться до Європейського суду з прав людини. А він окремі справи розглядає роками. Упродовж цього часу московська церква діятиме вільно, транслюватиме свою пропаганду» [7]. Власне тому, на його думку, «для захисту української незалежності та демократії необхідно якомога скоріше ухвалити законопроєкт «Про забезпечення зміцнення національної безпеки у сфері свободи совісті та діяльності релігійних організацій» (№ 8221)» [7].

Висновки. Продовження діяльності УПЦ (МП) афілійованої з російською православною церквою впливатиме на подальші загрози національній безпеці України, адже, навіть нібито

відмежовуючись від РПЦ, ця церква у своїй структурі має багато прихильників так званого *русского міра*, які у своїх проповідях (через сепаратистські заяви) орієнтуються на московський центр і жодним чином не визнають акт агресії проти нашої держави, до того ж розпалюють міжнаціональну та міжконфесійну ворожнечу, надаючи цим самим ідейне підґрунтя для конфліктів, і відкрито підтримують агресію РФ, яка нібито «захищає» істинних українських православних (маючи на меті посилення впливу на населення, яке використовується та використовуватиметься як додаткове знаряддя війни) від загроз Європи.

Література:

1. Васьків О. РПЦ створює «православні ПВК» для війни проти України – СБУ. URL: https://suspilne.media/597689-rpc-stvorue-pravoslavni-pvk-dla-vijni-proti-ukraini-sbu/ (дата звернення 10.11.2023).

2. Депутати попередньо підтримали заборону релігійних організацій, пов'язаних із РФ. Законопроєкт направлений на припинення діяльності УПЦ (МП). URL: https://chas.news/news/deputati-poperedno-pidtrimali-zaboronu-religiinih-organizatsii-povyazanih-iz-rf (дата звернення 09.11.2023).

3. Закон України «Про основи національної безпеки України». URL: https://zakon.rada.gov.ua/laws/show/964-15#Text (дата звернення 15.10.2023).

4. Керівник СБУ Малюк розповів про Кримський міст, «кротів» і загрозу від УПЦ МП. URL: https://www.bbc.com/ukrainian/news-63410973 (дата звернення 13.10.2023).

5. Київ звинуватив РПЦ у створенні «православних ПВК» для війни в Україні. URL: https://www.radiosvoboda.org/a/news-rpts-pvk viyna/32645187.html (дата звернення 15.11.2023).

6. Кізілов Є., Гундяєв і Ко: РНБО вводить санкції щодо 21 церковника РПЦ. URL: https://www.pravda.com.ua/news/2023/01/23/7386192/ (дата звернення 20.10.2023).

7. Княжицький М. Національна безпека – підстава для заборони російської церкви в Україні. URL: https://espreso.tv/natsionalna-bezpeka-pidstava-zaboroni-rpts-v-ukraini (дата звернення 21.10.2023).

8. Конощук Я. Важкий процес: чи позбавлять депутати Україну від чортів у рясах. URL: https**:**// www.unian.ua/society/vazhkiy-proces-chi-pozbavlyat-deputati-ukrajinu-vid-chortiv-u-ryasah-12416781.html (дата звернення 25.10.2023).

9. Ланцюгова реакція: облради України одна за одною забороняють Московську церкву. URL: https://lb.ua/society/2023/04/30/553488_lantsyugova_reaktsiya_oblradi_ukraini.html. (дата звернення 28.10.2023).

10. Лемеха С. Діяльність моспатріархату в Україні об'єктивно є загрозою нацбезпеці нашої країни – професор Олександр Саган. URL: https://armyinform.com.ua/2023/04/13/diyalnist-mospatriarhatu-v-ukrayini-obyektyvno-ye-zagrozoyu-naczbezpeczi-nashoyi-krayiny-profesor-oleksandr-sagan/ (дата звернення 03.11.2023).

11. Масненко В. В американському виданні «Свобода» опублікована стаття науковця НУ. URL: htps://cdu.edu.ua/news/v-amerykanskomu-vydanni-svoboda-opublikovana-stattia-naukovtsia-nu.html (дата звернення 05.11.2023).

12. Музика О. Де в Україні вже заборонили діяльність УПЦ МП: перелік областей. URL: https://24tv.ua/de-zaboronili-upts-mp-ukrayini-spisok-oblastey-de-ne-bude-moskovskogo_n2292769 (дата звернення 09.11.2023).

13. Національна безпека – підстава для заборони російської церкви в Україні. URL: https://espreso.tv/natsionalna-bezpeka-pidstava-zaboroni-rpts-v-ukraini (дата звернення 11.11.2023).

14. Олійник В. Скільки «московських попів» у Реєстрі Zрадників? URL: https://www.chesno.org/post/5750 (дата звернення 13.11.2023).

15. Працював на Росію? СБУ каже, що викрила митрополита УПЦМП. URL: https://www.bbc.com/ukrainian/news-63228632 (дата звернення 13.11.2023).

16. Рада в першому читанні підтримала законопроєкт про заборону УПЦ МП. URL: https://prm.ua/rada-v-pershomu-chytanni-pidtrymala-zakonoproiekt-pro-zaboronu-upts-mp/ (дата звернення 13.11.2023).

17. СБУ обшукала єпархію на Буковині. Кажуть – знайшли громадянство РФ у митрополита. URL: https://www.bbc.com/ukrainian/news-63758847 (дата звернення 15.11.2023).

18. СБУ прийшла в Києво-Печерську лавру. Шукають осередок «русского міра». URL: https://www.bbc.com/ukrainian/news-63713328 (дата звернення 15.11.2023).

19. СБУ проти УПЦ МП. Ще у двох митрополитів знайшли антиукраїнські матеріали. URL: https://www.bbc.com/ukrainian/news-63460868 (дата звернення 15.11.2023).

20. Тищенко К. У Конотопі заборонили УПЦ МП: загроза нацбезпеці. URL: https://www.pravda.com.ua/news/2022/05/4/7344042/ (дата звернення 17.11.2023).

21. У Києво-Печерській лаврі «молилися за Росію». СБУ почала розслідування. URL: https://www.bbc.com/ukrainian/news-63615831 (дата звернення 27.10.2023).

22. Франківська облрада просить заборонити в Україні московський патріархат. URL: https://www.ukrinform.ua/rubric-regions/3572848-frankivska-oblrada-prosit-zaboroniti-v-ukraini-moskovskij-patriarhat.html (дата звернення 27.10.2023).

23. Хмільовська О. Діяльність московського патріархату як загроза національній безпеці Української Держави. URL: https://ukrnationalism.com/publications/2611-diialnist-moskovskoho-patriarkhatu-iak-zahroza-natsionalnii-bezpetsi-ukrainskoi-derzhavy.html (дата звернення 27.10.2023).

24. Хоменко С., Червоненко В. СБУ проти УПЦ. Як і чому Зеленський та спецслужби взялись за (не) московську церкву. URL: https://www.bbc.com/ukrainian/features-63802715 (дата звернення 17.11.2023).

25. Чому влада України вважає УПЦ МП загрозою для національної безпеки? URL: https://antikor.com.ua/articles/619782pochemu_vlasti_ukrainy_schitajut_upts_mp_ugrozoj_natsionaljnoj_bezopasnosti (дата звернення 23.11.2023).

26. Щур М. Російська церква визначила, хто може бути росіянином. URL: https://www.radiosvoboda.org/a/26691614.htm (дата звернення 19.11.2023).

References:

1. Vaskiv, O. (2023). RPTs stvoriuie “pravoslavni PVK” dlia viiny proty Ukrainy – SBU [The Russian Orthodox Church is creating “Orthodox PMCs” for the war against Ukraine – Security Service of Ukraine]. Retrieved from: https://suspilne.media/597689-rpc-stvorue-pravoslavni-pvk-dla-vijni-proti-ukraini-sbu/ [in Ukrainian].

2. Chas News (2023). Deputaty poperedno pidtrymaly zaboronu relihiinykh orhanizatsii, poviazanykh iz rf. Zakonoproiekt napravlenyi na prypynennia diialnosti UPTs (MP) [Deputies previously supported the ban on religious organizations associated with the Russian Federation. The bill is aimed at ending the activities of the Ukrainian Orthodox Church (MP). Retrieved from: https://chas.news/news/deputati-poperedno-pidtrimali-zaboronu-religiinih-organizatsii-povyazanih-iz-rf [in Ukrainian].

3. Verkhovna Rada of Ukraine (2018). Zakon Ukrainy “Pro osnovy natsionalnoi bezpeky Ukrainy” [Law of Ukraine “On the Basics of National Security of Ukraine”]. Retrieved from: https://zakon.rada.gov.ua/laws/show/964-15#Text [in Ukrainian].

4. BBC News Ukraine (2022). Kerivnyk SBU Maliuk rozpoviv pro Krymskyi mist, “krotiv” i zahrozu vid UPTs MP [Head of the Security Service of Ukraine Malyuk talked about the Crimean bridge, “moles” and the threat from the UOC (MP)]. Retrieved from: https://www.bbc.com/ukrainian/news-63410973 [in Ukrainian].

5. Radio Svoboda (2023). Kyiv zvynuvatyv RPTs u stvorenni “pravoslavnykh PVK” dlia viiny v Ukraini [Kyiv accused the Russian Orthodox Church of creating “Orthodox PMCs” for the war in Ukraine]. Retrieved from: https://www.radiosvoboda.org/a/news-rpts-pvk viyna/32645187.html [in Ukrainian].

6. Kizilov, Ye. (2023). Hundiaiev i Ko: RNBO vvodyt sanktsii shchodo 21 tserkovnyka RPTs [Gundyaev and Co.: NSDC imposes sanctions on 21 churchmen of the Russian Orthodox Church]. Retrieved from: https://www.pravda.com.ua/news/2023/01/23/7386192/ [in Ukrainian].

7. Kniazhytskyi, M. (2023). Natsionalna bezpeka – pidstava dlia zaborony rosiiskoi tserkvy v Ukraini [National security is the reason for banning the Russian Church in Ukraine]. Retrieved from: https://espreso.tv/natsionalna-bezpeka-pidstava-zaboroni-rpts-v-ukraini [in Ukrainian].

8. Konoshchuk, Ya. (2023). Vazhkyi protses: chy pozbavliat deputaty Ukrainu vid chortiv u riasakh [A difficult process: will the deputies rid Ukraine of devils in robes]. Retrieved from: https://www.unian.ua/society/vazhkiy-proces-chi-pozbavlyat-deputati-ukrajinu-vid-chortiv-u-ryasah-12416781.html [in Ukrainian].

9. LB.ua (2023). Lantsiuhova reaktsiia: oblrady Ukrainy odna za odnoiu zaboroniaiut Moskovsku tserkvu [Chain reaction: regional councils of Ukraine ban the Moscow Church one by one]. Retrieved from: https://lb.ua/society/2023/04/30/553488_lantsyugova_reaktsiya_oblradi_ukraini.html [in Ukrainian].

10. Lemekha, S. (2023). Diialnist mospatriarkhatu v Ukraini obiektyvno ye zahrozoiu natsbezpetsi nashoi krainy – profesor Oleksandr Sahan [The activities of the Mospatriarchy in Ukraine are objectively a threat to the national security of our country – Professor Oleksandr Sagan]. Retrieved from: https://armyinform.com.ua/2023/04/13/diyalnist-mospatriarhatu-v-ukrayini-obyektyvno-ye-zagrozoyu-naczbezpeczi-nashoyi-krayiny-profesor-oleksandr-sagan/ [in Ukrainian].

11. Masnenko, V. (2023). V amerykanskomu vydanni "Svoboda" opublikovana stattia naukovtsia NU [An article by a NU scientist was published in the American publication Svoboda]. Retrieved from: https://cdu.edu.ua/news/v-amerykanskomu-vydanni-svoboda-opublikovana-stattia-naukovtsia-nu.html [in Ukrainian].

12. Muzyka, O. (2023). De v Ukraini vzhe zaboronyly diialnist UPTs MP: perelik oblastei [Where in Ukraine the activities of the UOC MP have already been banned: a list of regions]. Retrieved from: https://24tv.ua/de-zaboronili-upts-mp-ukrayini-spisok-oblastey-de-ne-bude-moskovskogo_n2292769 [in Ukrainian].

13. Kniazhytskyi, M. (2023). Natsionalna bezpeka – pidstava dlia zaborony rosiiskoi tserkvy v Ukraini [National security is the reason for banning the Russian Church in Ukraine]. Retrieved from: https://espreso.tv/natsionalna-bezpeka-pidstava-zaboroni-rpts-v-ukraini [in Ukrainian].

14. Oliinyk, V. (2023). Skilky "moskovskykh popiv" u Reiestri Zradnykiv? [How many "Moscow priests" are in the Register of Treasoners?]. Retrieved from: https://www.chesno.org/post/5750 [in Ukrainian].

15. BBC News Ukraine (2022). Pratsiuvav na Rosiiu? SBU kazhe, shcho vykryla mytropolyta UPTsMP [Did you work for Russia? The SBU says it has exposed the metropolitan of the UOCMP]. Retrieved from: https://www.bbc.com/ukrainian/news-63228632 [in Ukrainian].

16. Direct TV channel (2023). Rada v pershomu chytanni pidtrymala zakonoproiekt pro zaboronu UPTs MP [In the first reading, the Council supported the draft law on banning the UOC MP]. Retrieved from: https://prm.ua/rada-v-pershomu-chytanni-pidtrymala-zakonoproiekt-pro-zaboronu-upts-mp/ [in Ukrainian].

17. BBC News Ukraine (2022). SBU obshukala yeparkhiiu na Bukovyni. Kazhut – znaishly hromadianstvo RF u mytropolyta [The Security Service of Ukraine searched the diocese in Bukovyna. They say – they found Russian citizenship in the metropolitan]. Retrieved from: https://www.bbc.com/ukrainian/news-63758847 [in Ukrainian].

18. BBC News Ukraine (2022). SBU pryishla v Kyievo-Pechersku lavru. Shukaiut oseredok "russkoho mira" [The Security Service of Ukraine came to the Kyiv-Pechersk Lavra. They are looking for a cell of the "Russian world"]. Retrieved from: https://www.bbc.com/ukrainian/news-63713328 [in Ukrainian].

19. BBC News Ukraine (2022). SBU proty UPTs MP. Shche u dvokh mytropolytiv znaishly antyukrainski materialy [The Security Service of Ukraine against UOC MP. Two more metropolitans were found with anti-Ukrainian materials]. Retrieved from: https://www.bbc.com/ukrainian/news-63460868 [in Ukrainian].

20. Tyshchenko, K. (2022). U Konotopi zaboronyly UPTs MP: zahroza natsbezpetsi [The UOC MP was banned in Konotop: a threat to national security]. Retrieved from: https://www.pravda.com.ua/news/2022/05/4/7344042/ [in Ukrainian].

21. BBC News Ukraine (2022). U Kyievo-Pecherskii lavri "molylysia za Rosiiu". SBU pochala rozsliduvannia ["They prayed for Russia" in the Kyiv-Pechersk Lavra. The SBU started an investigation]. Retrieved from: https://www.bbc.com/ukrainian/news-63615831 [in Ukrainian].

22. Ukrinform (2022). Frankivska oblrada prosyt zaboronyty v Ukraini moskovskyi patriarkhat [The Frankiv Regional Council asks to ban the Moscow Patriarchate in Ukraine]. Retrieved from: https://www.ukrinform.ua/rubric-regions/3572848-frankivska-oblrada-prosit-zaboroniti-v-ukraini-moskovskij-patriarhat.html [in Ukrainian].

23. Khmilovska, O. (2017). Diialnist moskovskoho patriarkhatu yak zahroza natsionalnii bezpetsi Ukrainskoi Derzhavy [The activities of the Moscow Patriarchate as a threat to the national security of the Ukrainian State]. Retrieved from: https://ukrnationalism.com/publications/2611-diialnist-moskovskoho-patriarkhatu-iak-zahroza-natsionalnii-bezpetsi-ukrainskoi-derzhavy.html [in Ukrainian].

24. Khomenko, S., Chervonenko, V. (2022). SBU proty UPTs. Yak i chomu Zelenskyi ta spetssluzhby vzialys za (ne)moskovsku tserkvu [The Security Service of Ukraine against UOC. How and why did Zelenskyi and the special services take on the (non)Moscow church]. Retrieved from: https://www.bbc.com/ukrainian/features-63802715 [in Ukrainian].

25. Antikor (2023). Chomu vlada Ukrainy vvazhaie UPTs MP zahrozoiu dlia natsionalnoi bezpeky? [Why do the authorities of Ukraine consider the UOC MP a threat to national security?]. Retrieved from:

https://antikor.com.ua/articles/619782pochemu_vlasti_ukrainy_schitajut_upts_mp_ugrozoj_natsionaljnoj_bezopasnosti [in Ukrainian].

26. Shchur, M. (2023). Rosiiska tserkva vyznachyla, khto mozhe buty rosiianynom [The Russian Church defined who can be a Russian]. Retrieved from: https://www.radiosvoboda.org/a/26691614.htm [in Ukrainian].

Andrii Mishchuk, Marianna Mishchuk. Threats to Ukraine's national security: activities of the UOC (MP)

Religion has a significant influence on politics in many countries and regions worldwide and is dependent on various factors, including the cultural, historical, and legal specifics of each particular state. The impact of a religious center of one state on another can have various aspects and manifest in different spheres. The article explores the issue of threats to Ukraine's national security in the context of the activities of the Ukrainian orthodox church (MP). The article analyzes the influence of the moscow center on the functioning of its structural units and clergy. It presents facts of cooperation between representatives of this church and the russian aggressor, both directly through involvement in fire correction, providing provisions to occupiers, and sharing information, as well as through the promotion of the ideas of the so-called "russkiy mir". Attempts to fuel interethnic and interconfessional hostility are outlined, along with open support for кussian aggression, which supposedly "protects" true Ukrainian Orthodox believers from European threats.

Key words: *national security, religion, politics, collaborationism, church, aggression.*

ПОЛІТИЧНІ ПРОБЛЕМИ МІЖНАРОДНИХ СИСТЕМ ТА ГЛОБАЛЬНОГО РОЗВИТКУ

УДК 327.88:327.7 (061.1ЄС)
DOI: https://doi.org/10.32782/2312-1815/2024-1-7

Голуб'як Наталія
ORCID: 0000-0001-6021-5482

Голуб'як Ігор
ORCID: 0009-0008-3999-1864

ГІБРИДНІ ЗАГРОЗИ ЯК ВИКЛИКИ БЕЗПЕКОВІЙ ПОЛІТИЦІ ЄС

Стаття присвячена питанням стійкості ЄС до гібридних загроз з інституційної, правової та соціальної точок зору. Автори намагаються окреслити особливості загальноєвропейського підходу до протидії гібридним загрозам і наголошують на потребі в лідерстві ЄС у встановленні стандартів інформаційної безпеки.

Основна мета дослідження полягає у з'ясуванні способів і методів ЄС із запобігання гібридним загрозам із метою забезпечення інформаційної безпеки. Серед поставлених завдань виокремлюються такі: розглянути особливості формування інформаційної безпеки в ЄС; виокремити понятійну специфіку «гібридних загроз» і зосередити увагу на аналізі інституційної спроможності ЄС щодо протидії гібридним викликам.

У першій частині статті розглядається стан формування інформаційної політики Європейського Союзу, а саме загальноєвропейські підходи та спеціалізовані структури захисту.

Друга частина дослідження присвячена визначенню поняття «гібридні загрози» та «протидія гібридним загрозам». Автори вказують на переважання «м'якого підходу» в межах політики ЄС, зосередженого на взаємодії та діалозі. Окремо звернено увагу на становлення інституційно-правової бази протидії гібридним загрозам і напрацюванню міжінституційної взаємодії із НАТО.

За результатами підсумовано актуальні критичні фактори вразливості, що підкреслюють необхідність проактивної політичної участі та виділення ресурсів з боку ЄС із метою реагування та попередження гібридних викликів і загроз.

Ключові слова: *інформаційне суспільство, інформаційна безпека, гібридні загрози, гібридні виклики, протидія гібридним загрозам, Європейський Союз.*

Вступ. На сучасному етапі важливе значення для міжнародної політичної системи мають такі фактори, як зміна геополітичного середовища після закінчення холодної війни; технологічна і правова вразливість, притаманна глобалізації та спільному ринку; постісторичний дух часу Європи, який не сприймає підривну діяльність, не кажучи вже про пряму військову агресію. У 1990-х роках Європа була здебільшого оточена країнами, що реформувалися або молодими демократіями, заклопотаними власними трансформаціями. Тепер же континент сусідить з амбітними потугами, які прагнуть поширювати як жорстку, так і м'яку силу в Європу. Багато з них співпрацюють з антисистемними силами в Європі, які можуть мати різні цілі, у тому числі поширення репресивних інстинктів і популістських ідеологій серед держав ЄС.

Отже, тоді як ворожі державні й недержавні державні суб'єкти вже давно застосовують гібридні методи проти ЄС, тривала гібридна війна Росії в Україні, а також її втручання у президентські вибори в США у 2016 році стали переломним моментом, викривши неготовність

і вразливість західних країн до цих загроз. Останніми роками ми стали свідками численних інших випадків втручання Росії у внутрішні справи країн ЄС, включно із втручанням у референдум щодо Brexit 2016 року, фінансуванням правих партій та ультраправих політичних партій у Франції, Угорщині та Німеччині; проведенням цілеспрямованих замахів на вбивство у Великій Британії та Німеччині тощо.

Технологічні зміни, оцифрування економіки та повсякденного життя в країнах ЄС, формування відкритого і взаємопов'язаного суспільства – усе це надало ворожим іноземним суб'єктам широкий спектр для впливу та втручання. Тож **актуальним** постає питання інформаційної безпеки, яка в Європейському Союзі вибудовується на наддержавному, національному й індивідуальному рівнях. Загалом важливість вивчення цього досвіду вагома для безпечного використання інформації в Україні та відповідності стандартам і вимогам *acquis communautaire*.

Основна **мета дослідження** полягає у з'ясуванні способів і методів ЄС із запобігання гібридним загрозам із метою забезпечення інформаційної безпеки. Серед поставлених **завдань** виокремлюються такі: розглянути особливості формування інформаційної безпеки в ЄС; виокремити понятійну специфіку «гібридних загроз» і зосередити увагу на аналізі інституційної спроможності ЄС щодо протидії гібридним викликам.

У науковій сфері ця проблематика знайшла відображення у працях як вітчизняних, так й іноземних учених, серед них варто відзначити напрацювання О. Твердохліб, С. Троян, Є. Таран, М. Копійки, Є. Тихомирової, Kalniete S. & Pildegovičs T., Gresse G.

Виклад основного матеріалу дослідження. Об'єднана Європа створила абсолютно нову, раніше не існуючу організаційну форму – мережеву державу (*network state*), яка намагається відповідати на сучасні виклики процесів глобалізації та регіоналізації. Формування єдиного інформаційного простору, інформаційна інтеграція європейських держав у межах ЄС здійснюються на основі концепції єдиної загальної інформаційної політики, що втілена в ідеології європейського співробітництва у сфері інформації та комунікацій [1, с. 431]. Виходячи із цього, була сформована так звана європейська специфічність політики [2], закладена в організаційній формі самого ЄС як наднаціонального рівня, побудованого на спільності інтересів держав-членів з урахуванням принципу субсидіарності.

На сучасному етапі європейські фахівці в галузі інформаційних систем, безпеки і стратегічного планування активно обговорюють проблеми, що виникають в умовах можливості застосування інформаційної зброї, тобто засобів спрямованого впливу на інформаційні ресурси ймовірного супротивника у військовий і мирний час. Для цього на практиці реалізуються плани організаційного та технічного забезпечення національної інформаційної безпеки, створюються підрозділи, призначені для відбиття «інформаційної агресії». Уряди беруть на себе роль координаторів міжвідомчих зусиль у цій сфері [3, с. 29].

Вирішуючи проблеми інформаційної спільноти щодо мережевої та інформаційної безпеки, Європейське Співтовариство розробило тристоронній підхід, що передбачає конкретні заходи інформаційної безпеки; захист конфіденційності інформації та даних; боротьбу з кіберзлочинністю й гібридними викликами. Отже, розуміючи важливість єдиної системи інформаційної захисту, Європейський Союз намагається організувати колективний і широкомасштабний підхід до забезпечення інформаційної безпеки як окремих держав – членів ЄС, так й об'єднання загалом [4]. Для цього створені спеціалізовані структури захисту: Європейське агентство з питань мережевої та інформаційної безпеки (ENISA); у структурі Європейського поліцейського офісу (Європол) був утворений Європейський центр боротьби з кіберзлочинністю; Група співпраці NIS; мережа CSIRTS та інші.

Натомість конкретні цілі та заходи інформаційної безпеки формулюються у програмах і робочих планах інститутів ЄС, які передбачають необхідність пошуку спільних рішень

об'єднання європейських країн щодо інформаційного протиборства та визначають потребу в трансформації програми європейської інформаційної безпеки [5].

Однією з характерних особливостей останніх років є активне використання цілого спектра викликів і загроз міжнародній безпеці й інформаційному суспільству, яке має принципово нову якість і об'єднується поняттям «гібридні загрози». Обговорення навколо проблеми гібридних війн пов'язані з тим, що поряд із використанням звичайного комплексу загроз національній безпеці зростає роль невійськових викликів. Давайте звернемося до поняття «гібридні загрози», за яким закріпилися різні визначення і з яким конкурують інші терміни, такі як «нелінійна війна», «асиметричний конфлікт» і «підривна діяльність». Але, якщо коротко, «гібридні загрози» означають використання спонсорованих державою, але не офіційно афілійованих акторів, які не вдаються до фізичного насильства. Отже, основна мета – примусити об'єкт загрози до втілення стратегічних інтересів агресора.

Гібридні «трюки» використовувалися протягом всієї історії, починаючи з троянського коня, винайденого Одіссеєм, до шкідливого програмного забезпечення Trojan, написаного хакерами. Вважається, що навіть періоди миру є «гібридними», оскільки вони перериваються вбивствами, корупцією, шпигунством, дезінформацією, маніпуляціями й економічним тиском. Основині прояви гібридних загроз втілюються у фейкових новинах, інформаційній війні та маніпуляціях у соціальних мережах, але засоби використання державами нерозкритих і неатрибутованих активів для послаблення своїх супротивників виходять далеко за межі цих елементів [6].

Цифрова інфраструктура – від військового зв'язку, передавачів 5G і машин для голосування – дає змогу ворожим суб'єктам успішно отримувати доступ до все більшої кількості даних і розвідувальної інформації. Тож виникнення нових гібридних сутичок і постійне притягнення країн до інформаційної боротьби характеризують кібербезпеку як одну з невід'ємних елементів колективної безпеки країн і міжнародного суспільства.

Отже, «гібридні загрози» розглядаються як загальний термін, що охоплює цілу низку дестабілізувальних і синхронізованих цивільних і військових дій. Ці дії можуть передбачати кампанії з дезінформації, кібератаки, підбурювання до політичної або економічної корупції, впровадження агентів впливу, тиск на незалежні ЗМІ та скуповування критично важливої інфраструктури [7].

Крім того, із самого початку слід уточнити, що протидія гібридним загрозам є передусім компетенцією та відповідальністю країн-членів. На відміну від ЄС чи інших міжнародних організацій, національні уряди мають відповідний інструментарій, а саме «розвідувальні та контррозвідувальні органи (як цивільні, так і військові), силові служби (забезпечення громадського порядку та безпеки), засоби зв'язку з громадянами та можливості реагування на кіберінциденти. Водночас, хоча національна безпека належить до сфери життєво важливих інтересів кожної держави-члена, гібридні загрози часто виходять за межі кордонів, що залишає за ЄС важливу роль у підтримці стійкості держав-членів у тих випадках, коли їх реакція на національному рівні є недостатньо адекватною [8].

Старший політичний радник Європейської ради з міжнародних відносин Густав Грессел відзначає, що підвищена вразливість Європи до гібридних атак не є ризиком, притаманним технологічному прогресу і глобалізації: це питання вибору. Європа зупинилася на підході *laissez-faire* до цих питань, тобто залишається такою, що прагне до вирішення проблем через діалог, а не конфронтацію. Варіант рішучої відповіді є дуже незручним для громадськості та політиків у більшості країн ЄС. На думку дослідника, деякі країни – члени ЄС, які визнають гібридні загрози одним із головних пріоритетів, створили спеціальні підрозділи в уряді або міністерствах закордонних справ для координації реагування на гібридні загрози (це Швеція, Фінляндія, Польща, Литва та Іспанія). Цей список свідчить про особливе занепокоєння щодо Росії.

Однак найбільші країни ЄС, Франція та Німеччина, ще не зовсім засвоїли поняття гібридних загроз, але обидві країни шукають шляхи реагування на них, а такі країни, як Австрія, Угорщина та Італія, загалом не надто переймаються гібридними загрозами [6].

Якщо говорити про наднаціональний рівень, то частини апарату ЄС дуже активно працюють над питаннями протидії гібридним загрозам, але все ще бракує цілісного підходу до цих питань. За останні роки з'явилися нові комунікації, закони, стратегії, цільові групи, фінансування та робочі групи країн-членів спрямовані на посилення безпеки та стійкості ЄС.

Інституційний вимір стійкості ЄС до гібридної війни має вирішальне значення для сигналізації про наявність політичної волі сприймати гібридні загрози серйозно. Тому потрібно спочатку розглянути кроки, які інституції ЄС зробили для розбудови своєї спроможності протидіяти гібридним загрозам.

Починаючи з 2014 року, ЄС ухвалив низку законодавчих актів у цій сфері, у тому числі в таких сферах політики, як енергетична безпека, захист критичної інфраструктури, захист даних, перевірка іноземних інвестицій і прозорість політичного фінансування.

Серед ключових ініціатив варто виділити схвалення Європейською Комісією ще у 2016 р. «Спільних принципів протидії гібридним загрозам – відповідь Європейського Союзу» (*Joint Framework on countering hybrid threats a European Union response*). До принципів, що стосуються механізмів реалізації стратегічних комунікацій для протидії дезінформації та публічного викриття гібридних загроз належать такі: захист об'єктів критичної інфраструктури, оскільки гібридні атаки можуть призвести до серйозних економічних або соціальних порушень; тісна взаємодія з НАТО, яка дасть змогу більш ефективно реагувати на гібридні загрози; служби зовнішніх зв'язків ЄС, спираючись на діяльність оперативних робочих груп, зобов'язані оптимізувати роботу лінгвістів, фахівців із соціальних медіа, які можуть проводити моніторинг інформації не з ЄС; забезпечити цілеспрямовану комунікацію для реагування на дезінформацію [9].

У тому ж році прийнято Резолюцію «Стратегічні комунікації Європейського Союзу як протидія пропаганді третіх сторін» (*EU strategic communication to counteract propaganda against it by third parties*), яка виділяє перелік ключових проблем, а саме: стратегічні комунікації та інформаційна війна є не лише зовнішнім аспектом ЄС, але й внутрішнім; дезінформація та пропаганда трактуються як складові частини гібридної війни; «позитивні меседжі ЄС повинні бути наступальними (*offensive*), а не захисними (*defensive*)»; окремі аспекти інформаційного впливу Росії стосуються, зокрема, роботи окремих фундацій та органів (наприклад, «Росспівпраця»), телеканалів (RT), мультимедійних сервісів («Супутник»); проблему інформаційної війни з ІДІЛ та протидії дезінформації й радикалізації; потреба в моніторингу джерел фінансування антиєвропейської пропаганди; «розпалювання ненависті, насильства або війни не може ховатися за ширмою свободи висловлення думок» [9].

У червні 2018 року Комісія опублікувала Спільне повідомлення про підвищення стійкості та посилення спроможності протистояти гібридним загрозам. У подальшому новий стратегічний порядок денний ЄС на 2019–2024 роки чітко підкреслює стійкість до гібридних загроз і дезінформації як один із ключових напрямів майбутньої роботи. Нарешті, у грудні 2019 року Європейська Рада оприлюднила Висновки щодо протидії гібридним загрозам, які стали історичними завдяки тому, що в них є посилання на «можливість для держав-членів посилатися на положення про солідарність» (стаття 222 ДФЄС) (стаття 222 Договору про заснування Європейського Союзу) для вирішення серйозної кризи, спричиненої гібридною діяльністю [8].

Крім створення інституційних рамок і політико-правової основи для гібридної стійкості ЄС, кілька інституційних ініціатив принесли відчутні результати. У масштабах ЄС працюють два найбільш відомі центри протидії дезінформації – Оперативна робоча група зі стратегічних комунікацій ЄС (East StratCom Task Force) та Європейський центр передового досвіду для протидії гібридним загрозам (European Centre of Excellence for Countering Hybrid Threats) [10].

Важливим компонентом щодо стримування та протидії гібридним загрозам стало функціонування трьох сил StratCom під егідою Європейської служби зовнішньої діяльності (EEAS) – одна з них зосереджена на регіоні Східного партнерства, друга – на Західних Балканах, третя – на Південному сусідстві. Робота спецпідрозділів EEAS з викриття дезінформації, спрямованої проти ЄС у цих регіонах, є критично важливою, оскільки, надаючи допомогу країнам-кандидатам на вступ у розбудові стійкості, ЄС не лише зміцнює демократичні інститути, але й безпосередньо просуває власні безпекові інтереси [8].

Окремо слід відзначити міжінституційну співпрацю в розбудові стійкості до гібридних загроз, зокрема, на прикладі взаємодії між ЄС і НАТО, які є природними партнерами і діють на основі схожих стратегічних перспектив, оцінки ризиків та інтересів у протидії гібридним загрозам, особливо з боку Росії. Так, у липні 2016 року президент Європейської Ради, президент Європейської комісії і генеральний секретар НАТО підписали спільну декларацію, у якій окреслили сім сфер співпраці, у тому числі зусилля з протидії гібридним загрозам.

Помітним зрушенням стало створення Європейського центру передового досвіду для протидії гібридним загрозам (European Centre of Excellence for Countering Hybrid Threats). Засновниками Центру стали 12 країн: Фінляндія, Швеція, Норвегія, США, Франція, ФРН, Велика Британія, Іспанія, Польща, Естонія, Латвія і Литва. Ця структура під гібридними загрозами має на увазі, зокрема, поширення неправдивої інформації, атаки проти інформаційних систем, а також інші види атак за допомогою сучасних технологій. Загалом це ворожі дії, спрямовані на дестабілізацію держави без формального оголошення війни. Такі дії є скоординованими, синхронізованими та свідомо спрямованими на вразливість демократичних держав й інституцій. Нині Центр має три активні спільноти – гібридний вплив (на чолі з Великою Британією), уразливості та стійкості (на чолі з Фінляндією), стратегії та оборони (на чолі з Німеччиною) [9].

Крім інституційної адаптації до зростаючого потенціалу гібридних загроз, ЄС намагається використовувати регуляторні інструменти для обмеження поширення дезінформації, яка підриває стійкість суспільства, сприяючи поляризації та радикалізації, а також підриває довіру до державних інституцій. Розвиток онлайн-платформ ускладнив контроль потоків неправдивої інформації, тому в цифровому просторі досить актуальним питанням на сьогодні також є проблема наростаючої дезінформації, головним джерелом «виробництва» від інституційних джерел якої є Інтернет.

Під зростаючим тиском щодо протидії цій загрозі ЄС уперше випустив Кодекс практики для боротьби з дезінформацією у вересні 2018 року, який був визнаний першою світовою рамкою для саморегулювання, спрямованого на боротьбу з дезінформацією. Кодекс практики підписали соціальні мережі та партнери з рекламної індустрії. У грудні 2018 року цей крок було доповнено Планом дій ЄС щодо дезінформації, який був задуманий як проактивний захід для «захисту демократичних систем Союзу та боротьби з дезінформацією, у тому числі в контексті майбутніх європейських виборів» [9].

Висновки. У світі є необхідність загального розуміння визначення гібридної загрози, що потребує періодичної співпраці, ефективної політики в межах ЄС, так і налагодженої співпраці між ЄС і НАТО. Тож усім державам слід визначити їхні вразливі сторони, щоб усвідомити, які гібридні загрози апріорі могли бути використані їхніми противниками. Обмін наявним досвідом кожної з країн потрібно сформувати так, щоб співпраця принесла якомога більше продуктивних рішень із питань гібридних загроз і кібербезпеки.

Загалом політика ЄС у сфері кібербезпеки, незважаючи на явний прогрес, досягнутий останніми роками, усе ще не є повністю узгодженою, і їй бракує прозорості. Це проявляється як на регулятивному, так і на інституціональному рівні. У традиційному вимірі (так звана жорстка сила) бачення повної стратегічної автономії, пов'язаної з наявністю власних можливостей кіберзахисту, залишається нереалізованою. Держави-члени визнають необхідність зміцнення

своїх ресурсів, але не хочуть ділитися своїми можливостями. ЄС спрямований більшою мірою на так звану м'яку безпеку: посилення зовнішнього виміру політики, підвищення стійкості мереж і систем ІКТ до кіберзагроз, розробку можливостей та інструментів для реагування на кібератаки, ефективну співпрацю в боротьбі з кіберзлочинністю, просування стандартів і цінностей у кіберпросторі.

Отже, стійкість до гібридних загроз неможливо досягти без загальноєвропейського набору норм, які б забезпечували стандарти підзвітності та прозорості. Роль ЄС полягає у зміцненні стійкості до гібридної війни, має охоплювати все суспільство, а також сприяти міжнародному та міжвідомчому співробітництву і встановленню спільних стандартів для зменшення вразливостей.

Література:

1. Угрин Л. Інформаційна політика. Політологія: навч. енцикл. слов.-довід. для студентів ВНЗ I–IV рівнів акредитації / за наук. ред. д-ра політ. наук Н. М. Хоми [В. М. Денисенко, О. М. Сорба, Л. Я. Угрин та ін.]. Львів : Новий Світ-2000, 2014. С. 270.

2. Твердохліб О. С. Європейський підхід до розроблення інформаційної політики держави актуальні проблеми. *Економіка*. 2016. № 3 (177). С. 429-435. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/ape_2016_3_51.pdf.

3. Троян С. Інформаційно-безпекова політика Європейського Союзу. Зовнішні справи : суспільно-політичний журнал. 2019. № 2/3. С. 28–32.

4. Таран Є. Політика забезпечення інформаційної безпеки у США та ЄС: досвід для України. Вісник Львівського університету. *Серія: Філософсько-політологічні студії. 2019*. Вип. 25. С. 170–175. URL: http://fps-visnyk.lnu.lviv.ua/archive/25_2019/25.pdf.

5. Копійка М. В. Стратегічні ризики інформаційної безпеки європейських країн. *Міжнародні та політичні дослідження*. 2019. Вип. 32. С. 85–102. URL: https://doi.org/10.18524/2304-1439.2019.32.173847.

6. Gresse G. Protecting Europe against hybrid threats. 2019. URL: https://ecfr.eu/wp-content/uploads/6_Protecting_Europe_against_hybrid_threats.pdf.

7. Hybrid COE. Countering disinformation: News media and legal resilience. Hybrid CoE Papers. 2019. URL: https://www.hybridcoe.fi/wp-content/uploads/2020/07/News-Media-and-Legal-Resilience_2019_HCPaper-ISSN.pdf.

8. Kalniete S., & Pildegovičs T. Strengthening the EU's resilience to hybrid threats. European View. 2021. 20 (1). P. 23–33.

9. Міжнародний досвід протидії гібридним загрозам: законодавче регулювання та організації з питань стратегічних комунікацій. *Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром*. URL: https://infocenter.rada.gov.ua/uploads/documents/29377.pdf.

10. Тихомирова Є. ЄС: проекти з протидії сфабрикованим новинам. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2019. № 1 (5). URL: https://relint.vnu.edu.ua/index.php/relint/article/view/90.

References:

1. Uhryn, L. (2014). Informatsiina polityka. Politolohiia: navch. entsykl. slov.-dovid. dlia studentiv [Information policy. Political science: a textbook.] VNZ I–IV rivniv akredytatsii/za nauk. red. d-ra polit. nauk N. M. Khomy; [V. M. Denysenko, O. M. Sorba, L. Ya. Uhryn ta in.]. Lviv: Novyi Svit-2000. P. 270 [in Ukrainian].

2. Tverdokhlib, O. S. (2016). Yevropeiskyi pidkhid do rozroblennia informatsiinoi polityky derzhavy aktualni problemy [European approach to state information policy-making] *Ekonomika.* № 3 (177). P. 429–435. Retrieved from: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/ape_2016_3_51.pdf [in Ukrainian].

3. Troian, S. (2019). Informatsiino-bezpekova polityka Yevropeiskoho Soiuzu [European Union policy in the field of information security]. *Zovnishni spravy : suspilno-politychnyi zhurnal*. № 2/3. P. 28–32 [in Ukrainian].

4. Taran, Ye. (2019). Polityka zabezpechennia informatsiinoi bezpeky u SShA ta YeS: dosvid dlia Ukrainy [Policy of providing information security in the US And EU: experience for Ukraine]. *Visnyk Lvivskoho universytetu. Seriia: Filosofsko-politolohichni studii.* №. 25. P. 170–175. Retrieved from: http://fps-visnyk.lnu.lviv.ua/archive/25_2019/25.pdf [in Ukrainian].

5. Kopiika, M. V. (2019). Stratehichni ryzyky informatsiinoi bezpeky yevropeiskykh krain [Strategic risks of information security of the european countries]. *Mizhnarodni ta politychni doslidzhennia*. № 32. P. 85–102. Retrieved from: https://doi.org/10.18524/2304-1439.2019.32.173847 [in Ukrainian].

6. Gresse, G. (2019) Protecting Europe against hybrid threats. Retrieved from: https://ecfr.eu/wp-content/uploads/6_Protecting_Europe_against_hybrid_threats.pdf.

7. Hybrid COE (2019). Countering disinformation: News media and legal resilience. Hybrid CoE Papers. Retrieved from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/News-Media-and-Legal-Resilience_2019_HCPaper-ISSN.pdf.

8. Kalniete S., & Pildegovičs T. (2021) Strengthening the EUs resilience to hybrid threats. European View. 20 (1). P. 23–33.

9. Parshikova, A. (n.d.). Mizhnarodnyi dosvid protydii hibrydnym zahrozam: zakonodavche rehuliuvannia ta orhanizatsii z pytan stratehichnykh komunikatsii [International experience in countering hybrid threats: legislative regulation and strategic communications organisations]. *Informatsiina dovidka, pidhotovlena Yevropeiskym informatsiino-doslidnytskym tsentrom*. Retrieved from: https://infocenter.rada.gov.ua/uploads/documents/29377.pdf [in Ukrainian].

10. Tykhomyrova, Ye. (2019). YeS: proekty z protydii sfabrykovanym novynam [EU: prospects for combated news]. *Mizhnarodni vidnosyny, suspilni komunikatsii ta rehionalni studii*. № 1 (5). Retrieved from: https://relint.vnu.edu.ua/index.php/relint/article/view/90 [in Ukrainian].

Nataliia Holubiak, Ihor Holubiak. Hybrid threats as a challenge for EU security policy

This article focuses on the EU's resilience to hybrid threats from an institutional, legal and societal perspective. The authors try to outline the characteristics of a pan-European approach to countering hybrid threats and emphasise the need for EU leadership in setting information security standards.

The main objective of the study is to identify ways and means for the EU to prevent hybrid threats in order to ensure information security. Among the tasks set are: to consider the peculiarities of information security formation in the EU; to highlight the conceptual specificity of "hybrid threats"; and to focus on the analysis of the EU's institutional capacity to face hybrid challenges.

The first part of the article examines the state of formation of the European Union's information policy, namely common European approaches and specialised protection structures.

The second part of the study is devoted to the definition of "hybrid threats" and "countering hybrid threats". The authors point to the prevalence of a "soft approach" within EU policy, focusing on interaction and dialogue. Particular attention is paid to the establishment of an institutional and legal framework for countering hybrid threats and the development of inter-institutional cooperation with NATO.

As a result, authors summarise the current critical vulnerabilities that underline the need for proactive political engagement and resource allocation by the EU to respond to and prevent hybrid challenges and threats.

Key words: *information society, information security, hybrid threats, hybrid challenges, countering hybrid threats, European Union.*

УДК 327.8
DOI: https://doi.org/10.32782/2312-1815/2024-1-8

Михайло Савлюк
ORCID: 0009-0001-9870-8343

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті йдеться про перехід України від постіндустріального суспільства до інформаційного, що ставить перед країною нові виклики та загрози. Російська Федерація використовує в Україні гібридну війну, яка передбачає інформаційні атаки шляхом поширення неправдивої або частково правдивої інформації, маніпулювання фактами, сіяння паніки та розбрату. Метою роботи є дослідження алгоритму інформаційної атаки противника та розробка програми протидії агресору. Використані методи дослідження – аналіз, синтез, емпіричне пізнання та порівняння. За результатами дослідження було розроблено алгоритм визначення достовірності поширюваної інформації та виявлення інформаційних атак противника. Цей алгоритм допомагає відрізнити справжню інформацію від результату ворожих інформаційних операцій.

Ключові слова: *ІПСО, інформаційна безпека, кібербезпека, соціальні мережі пропаганда, інформаційні операції, війна, гібридна війна, історія, інформаційні атаки, національна безпека.*

Вступ. Уже понад півтора року як розгорнулася повномасштабна війна між та Російською Федерацією та Україною. Бойові дії тривають не тільки безпосередньо на полі бою, а й на інформаційному фронті – так звана гібридна війна. Ворог намагається знищити авторитет України на міжнародній арені, поширюючи інформацію, яка несе репутаційні ризики для України. Ворог щоразу, хвиля за хвилею, просуває все нові етапи своїх ІПСО, намагаючись посіяти зневіру серед українців і міжнародних партнерів України. Ворожа пропаганда й інформаційні атаки стосовно України розпочалися не 24 лютого 2022 року чи навесні 2014 року. Усе це має набагато довшу історію і почало діяти набагато швидше, ніж почалися безпосередні збройні зіткнення.

Мета та завдання. Метою роботи є визначення специфічних аспектів застосування інструментів ворожої пропаганди й інформаційних психологічних спеціальних операцій у контексті російської агресії, а також їхнього впливу на суспільство й пересічних громадян, політику та національну безпеку.

Відповідно до цієї мети були сформовані такі **завдання**:

– визначення категорії «інформаційна безпека»;

– дослідження історії інформаційної безпеки;

– з'ясування, якою має бути політика інформаційної безпеки держави;

– визначення інформаційної стратегії держави під час воєнного стану.

Методи дослідження. У рамках цієї наукової статті використовувалися такі методи дослідження, як аналіз, синтез, емпіричний метод і порівняння.

Аналіз останніх досліджень. Серед вітчизняних науковців, які б досліджували тему національної безпеки крізь призму інформаційної безпеки, насамперед слід відзначити Боднар І., Фурашева В., Архипова О. та Довганя О. Ці вітчизняні науковці наразі розробили досить ґрунтовний теоретичний аналіз проблем національної безпеки, проєктуючи її на інформаційне поле. Ними були визначені основні проблеми, структура та методи вивчення зазначеної проблематики.

Виклад основного матеріалу. Прихід до влади в Російській Федерації керівника авторитарного типу породив нові виклики та загрози для всього цивілізованого світу. Реваншистські

настрої та імперські погляди серед більшості населення, а особливо серед політичного та силового керівництва Росії, викликали черговий виток інформаційної війни, про яку вже почали забувати після завершення Холодної війни. У зв'язку зі стрімким розвитком інформаційних технологій і переходом більшості сучасних держав від постіндустральних до інформаційних суспільств стали можливими швидкі та надійні способи поширення інформації [1]. Цим не могли не скористатися авторитарні та тоталітарні режими, які намагаються протистояти так званому колективному Заходу. Зокрема, це стосується Російської Федерації, яка завдяки тому, що на світових ринках стрімко дорожчали ціни на енергоносії (зокрема, на нафту та газ), почала отримувати надприбутки до державного бюджету, але замість того щоб покращувати соціально-економічний стан своїх громадян і працювати над розвитком інфраструктури всередині власної країни, почала працювати над відновленням колишнього СРСР (нової країни в її територіальних межах).

На початку такої експансії, поки йшло відновлення російського військово-промислового комплексу, про якусь збройну агресію не йшлося. Проте наявні ресурси дали змогу російським пропагандистам розпочати роботу над створенням міфу про «вставання з колін» та історії про другу за силою армію світу. Насправді така робота принесла дуже хороші плоди, адже переважна більшість росіян, які пам'ятали голодні та холодні 90-ті роки (відразу після розпаду СРСР), у таку пропаганду охоче вірила. Така пропагандистська робота мала й успіх поза межами Російської Федерації. Адже за валюту куплялися публікації в провідних європейських і світових засобах масової інформації, що дало змогу поширювати пропагандистські матеріали про економічну могутність Росії та силу й непереможність російської армії.

Основною загрозою для національної безпеки є можливість впливу інших сил на інформаційну структуру країни, її інформаційні ресурси та суспільство загалом. Це вплив може бути спрямований на нав'язування державі інших цінностей, переконань, інтересів і рішень, які вигідні для інших сил [10]. Суть цієї загрози полягає в тому, щоб керувати поведінкою та розвитком країни у важливих сферах її суспільного та державного життя в напрямі, який вигідний іншим силам. Це може загрожувати суверенітету України в ключових галузях суспільного та державного життя, і ця загроза реалізується через інформаційні впливи. Стратегічне інформаційне протистояння є новим типом конфлікту, здатним вирішувати суперечності без застосування традиційних засобів ведення війни [3].

Отже, російська пропаганда почала впливати на інформаційну безпеку простих громадян. А з розвитком соціальних мереж і глобалізацією інформаційного простору російська пропаганда прийшла персонально до кожної людини, яка має акаунт у соціальних мережах. Це почало нести додаткові загрози для світової стабільності, адже, як ми бачили з початком повномасштабного вторгнення РФ до України (24 лютого 2022 року), усі світові найпрогресивніші розвідки давали Україні часу від трьох днів до двох тижнів. За їхніми розрахунками, російська армія мала б бути настільки високооснащеною та сильно тренованою, що Збройні сили України фактично не мали б шансів на опір загарбникам. Тому українській армії на початку не надавалися сучасні зразки озброєнь, які стоять на озброєнні армій країн НАТО. Командування НАТО побоювалося, що в разі стрімкого контрнаступу російської армії таке сучасне озброєння могло легко потрапити до рук російських, китайських та іранських інженерів, які б в подальшому могли відтворити такі сучасні зразки озброєння для своїх авторитарних режимів.

Із цього ми можемо побачити, що жертвами російської пропаганди та ІПСО стали не тільки пересічні громадяни, а й досвідчені офіцери світових розвідок, які так само повірили у міф про непереможність та силу «другої армії світу». Тож можна зробити висновки, що гібридні війни – це не вигадка, вони дійсно мають дуже важливий вплив на проведення бойових дій на лінії фронту. Інформаційна безпека є важливим фактором, що впливає на національну безпеку держави. А доступність і популярність соціальних мереж роблять вплив ворожої пропаганди

особливо дієвим. Тому для України, яка наразі перебуває у стані війни (у тому числі й гібридної) з Російською Федерацією, інформаційна безпека дорівнює національній безпеці, і нам треба навчитися її ефективно обороняти, маючи значно менші ресурси, ніж наш ворог [1].

Що таке інформаційна безпека. Інформаційна безпека є актуальною і важливою проблемою в сучасному світі, де інформація стала однією з найцінніших ресурсів. Ця стаття присвячена теоретико-методологічним засадам дослідження інформаційної безпеки, які допоможуть краще зрозуміти сутність цього поняття й визначити його відмінності від кібербезпеки [3].

Інформаційна безпека – це комплекс заходів, стратегій і політик, спрямованих на захист інформації від загроз, які можуть призвести до її втрати, руйнування або незаконного доступу (наразі ми бачимо, як ворог намагається активно втручатися в персональний (конфіденційний) простір українських споживачів інформації та активно впливати на нього своїми наративами та прихованою пропагандою) [1].

Це поняття містить декілька важливих аспектів:

1. Конфіденційність. Збереження конфіденційності інформації – це один із головних аспектів інформаційної безпеки. Інформація повинна бути доступною лише тим, кому вона потрібна, і не повинна потрапляти в руки несанкціонованих осіб (про що вказувалось вище).

2. Цілісність. Цілісність інформації визначається її станом, у якому вона зберігається й передається. Інформація повинна залишатися незмінною та недоторканою щодо будь-яких вторгнень або маніпуляцій (наразі російською пропагандою активно застосовується політтехнологічний метод напівправди, коли кінцевому споживачу інформації подається тільки та частина інформації, яка вигідна агресору (але вона часто вирвана з основного контексту і втрачає свою цілісність).

3. Доступність. Інформація повинна бути доступною тим, хто має на це право і потребує її для виконання своїх обов'язків. Недоступність інформації може призвести до порушення роботи організацій і завдати шкоди їх діяльності (щодо російського медіаполя, то ми бачимо тут власне зворотну ситуацію, коли цілий ряд інформаційних ресурсів і популярних соціальних мереж перебувають під тривалою державною забороною (фактично введена цензура), через це кінцевий споживач перебуває в «інформаційній бульбашці» і може сприймати за чисту правду все, що йому подає державна пропагандистська машина).

Чим відрізняється інформаційна безпека від кібербезпеки. Інформаційна безпека та кібербезпека часто сприймаються як синоніми, але вони мають важливі відмінності. Кібербезпека – це підгалузь інформаційної безпеки, яка спеціалізується на захисті інформації в цифровому середовищі. У вказаній статті нас більше цікавитиме саме напрям інформаційної безпеки, адже саме завдяки «атакам» на особистий інформаційний простір відбувається вплив на споживачів, що в кінцевому підсумку може вплинути на національну безпеку держави [12].

Основні відмінності між цими поняттями такі:

– Сфера застосування. Інформаційна безпека охоплює захист інформації в будь-якому форматі, включно з паперовими документами та фізичними носіями інформації (що є дуже важливим для нашого дослідження). Кібербезпека, з іншого боку, стосується виключно цифрової інформації і потребує спеціалізованих засобів і технологій для її зламу [13].

– Загрози. Інформаційна безпека стосується загроз, які можуть бути як фізичного, так і цифрового характеру (що, власне, ми зараз і спостерігаємо в українському медіаполі). Кібербезпека здебільшого зосереджена на цифрових загрозах, таких як хакерські атаки, віруси й інші онлайн-загрози.

– Заходи. Для забезпечення інформаційної безпеки використовуються різноманітні заходи, включно з фізичними засобами безпеки, контролем доступу і політиками безпеки, а також постійний моніторинг, зокрема, з боку органів влади та фахівців спецслужб. Кібербезпека

вимагає спеціалізованих технологій, включно з файрволами, антивірусами і криптографічними рішеннями [12].

У цій частині ми розглянули теоретико-методологічні засади дослідження інформаційної безпеки, визначили сутність поняття інформаційної безпеки та відмінності від кібербезпеки. Важливо зазначити, що інформаційна безпека є складною та багатогранною проблемою, яка потребує комплексного підходу та постійного вдосконалення заходів з її забезпечення, адже розвиток інформаційного поля (зокрема, соціальних мереж) ніколи не стоїть на місці [5]. Соціальні платформи постійно розвиваються та збагачуються. І якщо 15 травня 2017 року, згідно з указом п'ятого Президента України, у рамках введення додаткових санкцій України щодо Росії було введено заборону на популярні російські соціальні мережі «Одноклассники» та «Вконтакті» (що істотно зменшило вплив російської пропаганди на українських споживачів інформації), то зараз виникають нові популярні соціальні мережі, такі як «Тік Ток» [11].

Ця популярна соціальна мережа теж несе певну загрозу, оскільки до її баз даних має доступ уряд Китаю, який опосередковано підтримує Росію (не запроваджує проти неї економічних санкцій через її агресію щодо України, а, навпаки, активно розвиває економічно-торгівельні відносини з нею). У США від початку зростання популярності цієї соцмережі військовим було заборонено мати там свої акаунти, бо це могло викликати, як наслідок, витік персональних даних і потрапляння їх до рук не дружніх до США розвідок і спецслужб. У 2023 році саме через цей аспект у деяких американських штатах вже введено повну заборону на використання «Тік Ток» [14]. В Україні на цей час такої заборони немає, а тому російська пропаганда має додаткове інформаційне поле для поширення своїх наративів.

Щоб детально дослідити порушення та наслідки впливу на інформаційну безпеку, слід вивчити її історичну еволюцію від найдавніших часів і до тепер. Так ми зможемо краще зрозуміти ті виклики, з якими стикалась інформаційна безпека в різні епохи, і вивчити, як саме в ті чи інші часи протидіяли чи намагалися протидіяти інформаційним загрозам, які тоді виникали.

Для початку пропонується розглянути, як розвивалася та для чого створювалася інформаційна безпека від найдавніших часів і до XIX століття, оскільки цей період є відносно менш конфліктним, ніж інформаційні війни, які відбуваються в новітні часи.

Початки інформаційної безпеки. Започаткування інформаційної безпеки помічається ще в античній Греції та Римській імперії, де використовувалися методи шифрування для захисту секретної інформації. Наприклад, відомий шифр Скитала використовувався в античному Римі для шифрування повідомлень. Уже тоді люди зрозуміли, наскільки важливими для соціуму є інформаційна безпека й інформаційна гігієна [4].

Середньовіччя та Ренесанс. Середньовіччя відзначається використанням шифрувальних пристроїв, таких як шифратори та коди, для забезпечення безпеки дипломатичних спілкувань. Ренесансний період призвів до розвитку криптографії та поширення її в армії і державних структурах. В цю епоху ми бачимо створення уже чогось схожого на те, що є в сучасному світі та сучасних арміях.

Епоха промислової революції. З появою промислової революції зросла важливість захисту технічних і комерційних інформаційних ресурсів. Багато інноваційних методів і технологій було використано для захисту виробничих секретів та патентів. На цьому етапі ми бачимо заходи, якими людство користується і досі. Це, зокрема, патенти та захист банківської і комерційної таємниці. На цьому етапі людство все чіткіше починає розуміти переваги інформаційної гігієни й інформаційної безпеки, адже саме ці заходи допомагають сталому розвитку й економічному прогресу, до якого прагне все людство [7].

XIX століття. На початку XIX століття розвивалася телеграфія, що вимагала нових методів захисту інформації від небажаного втручань і посягань на конфіденційну передачу

інформаційних повідомлень. У 1854 році було створено кодекс, який став відомий як код Морзе для передачі повідомлень через телеграф.

Загальна тенденція розвитку інформаційної безпеки в цей період полягала в пошуку й застосуванні нових методів шифрування та зберігання інформації. Зокрема, бажання посилити інформаційну безпеку певною мірою спонукало людство до розвитку та прогресу, адже способи шифрування та передачі інформації, які виникали в попередні епохи, призвели до розвитку нових технологій і винаходів [12].

Інформаційна безпека у XX–XXI століттях. Далі слід розглянути період, який є значно коротшим у часі, ніж ті історичні періоди, які розглядалися вище. Але цей період тривалістю трохи менше півтора століття став найбільш інтенсивним відрізком часу стосовно розвитку та поширення інформаційних технологій і засобів для їх передавання на великі відстані та для масової аудиторії.

Ера кібернетики. XX століття відзначається різким розвитком науки, а саме комп'ютерів і кібернетики. Із цим розвитком з'явилися нові можливості для зберігання, обробки та передачі інформації, а також нові загрози для інформаційної безпеки. Кожен винахід у цій галузі ставав доступнішим і дешевшим для широкого загалу, що, зі свого боку, потягнуло за собою масові зловживання та використання їх у злочинних і протизаконних діях [12].

Важливим етапом стало створення Еніака – першого електронного комп'ютера, який використовувався для розшифрування різноманітних ворожих кодів під час кровопролитної Другої світової війни. Це відкриття вперше показало, що комп'ютери можуть бути використані як для захисту, так і для порушення інформаційної безпеки. Тобто інформаційне протистояння та боротьба за інформаційну безпеку вийшли на абсолютно новий рівень. Тож почали виникати нові виклики й загрози для інформаційної безпеки та належного поводження з конфіденційною інформацією для її розпорядників. Це знову ж таки сприяло стрімкому прогресу й розвитку всіх подальших інформаційних систем і способів поширення масової та конфіденційної інформації [7].

Кібернетична ера. У другій половині XX століття і на початку XXI століття інформаційна безпека стала викликати все більший інтерес через поширення комп'ютерів, Інтернету та цифрових технологій. Кіберзагрози, такі як хакерські атаки, віруси та фішинг, стали повсюдними явищами. Вони стали новими викликами для розпорядників інформації та правоохоронних органів. Різноманітні розробки й винаходи зловмисників ніколи не залишаються на місці та постійно розвиваються [15]. Злочинці щоразу вигадують нові способи поширення фейкових і неправдивих новин або ж намагаються видурити конфіденційну банківську інформацію, щоб отримати із цього фінансовий зиск.

Саме на цей час припадає розквіт інформаційних воєн, поширення пропаганди та створення спеціальних підрозділів приватних фірм або ж підрозділів армій світу (так званих ботоферм). Основним завданням таких підрозділів є саме поширення неправдивої інформації та потрібних їхньому керівництву наративів. Такі заходи допомагають деморалізувати противника та пришвидшують перемогу [12].

На замовлення урядів створюються інформаційні ресурси (такі як інформаційні вебсайти чи телеканали) або ж навіть цілі соціальні мережі, які в подальшому дають змогу військовим розвідкам і спецслужбам цих держав конфіденційно отримувати персональну інформацію про зареєстрованих користувачів [15].

Такі виклики майже миттєво зумовлюють створення протидії. Однією з таких важливих подій в історії інформаційної безпеки стало створення стандарту криптографічного захисту інформації – шифру AES. Цей стандарт став основою для захисту важливої інформації на державному й корпоративному рівнях.

XXI століття також відзначається розробкою та впровадженням стратегій і політик інформаційної безпеки на рівні держав та організацій. Наразі це є один з основних чинників,

який у подальшому може впливати на стабільну національну безпеку та боротися з викликами й загрозами, які оточують людство в сучасному інформаційному та кібернетичному глобалізованому світі [7].

Із цього можна зробити цілий ряд висновків, які в подальшому допоможуть більш конкретно зрозуміти суть досліджуваної проблематики. Історія інформаційної безпеки свідчить про постійний розвиток і адаптацію заходів і методів для захисту інформації протягом століть. Від античних методів шифрування до сучасних кіберзаходів – інформаційна безпека завжди залишалася актуальною та важливою проблемою. Вона ніколи не стоїть на місці, і на нові виклики завжди потрібно шукати якусь протидію [1]. А оскільки прогрес і людство не стоять на місці, то на кожен їхній винахід знаходяться ті негативні сили, які намагаються це використати на свою не зовсім законну користь.

Далі пропонується розглянути те, що на сучасному етапі повинна мати кожна держава та поважна установа, йдеться про політику інформаційної безпеки.

Інформаційна безпека є важливим елементом сучасного світу, особливо в контексті збільшення обсягу інформації та швидкості її передачі. Політика інформаційної безпеки є ключовим аспектом управління цією проблемою [8]. Далі розглядатимемо політику інформаційної безпеки держави та її особливості в умовах війни, а саме вивчатимемо алгоритм дій для протидії ворожим інформаційним атакам.

Політика інформаційної безпеки держави – це сукупність стратегій, методів і механізмів, спрямованих на захист національних інформаційних ресурсів і забезпечення їх надійності та цілісності. Вона передбачає такі аспекти:

Створення інфраструктури інформаційної безпеки. Держава повинна розробити інфраструктуру та мати висококваліфікованих фахівців для зберігання, обробки та передачі інформації з врахуванням сучасних вимог щодо безпеки [6].

Законодавство та регулювання. Для забезпечення інформаційної безпеки держава повинна приймати та застосовувати відповідне законодавство, включно із законами про кібербезпеку, захист персональних даних та іншими нормативними актами. Це повинен бути сукупний кодекс сучасних законів (про які два десятиліття тому навіть ніхто б і не думав), завдяки якому можна якісно регулювати інформаційне поле держави [5].

Розвиток і підтримка кадрів. Держава має забезпечити підготовку та підтримку висококваліфікованих фахівців у сфері інформаційної безпеки, зокрема кіберспеціалістів та аналітиків. Такі люди мають першими виявляти загрози інформаційній безпеці держави (навіть, якщо вони носять прихований характер). Вони повинні бути вмотивованими, навченими та мати відповідне обладнання й забезпечення (як фінансове, так і технічне), щоб на високому рівні конкурувати з опонентами [4].

Міжнародне співробітництво. Здійснення політики інформаційної безпеки також передбачає співпрацю з іншими країнами та міжнародними організаціями для обміну інформацією і спільної боротьби з кіберзагрозами та сучасними інформаційними викликами [8]. Така співпраця дасть змогу попереджувати небезпечні ситуації та навіть війни (як це сталося 24 лютого 2022 року в Україні та 7 жовтня 2023 року в Ізраїлі), «оскільки попереджений, значить озброєний».

Створення культури інформаційної безпеки. Політика інформаційної безпеки повинна сприяти формуванню свідомого підходу до безпеки інформації серед громадян та організацій, адже «не стільки небезпечний ворог, як дурень з ініціативою». Інформаційна політика держави має також бути спрямована на освіту населення поводження з інформацією, зокрема в соціальних мережах [4], адже сьогодні соцмережами користується чимало людей похилого віку й осіб без відповідної освіти, які запросто підхоплюють і поширюють ворожі наративи.

На завершення пропонується розглянути актуальну проблематику для сучасного стану України, а саме політику інформаційної безпеки держави під час війни та воєнного стану.

В умовах війни політика інформаційної безпеки набуває особливо важливого та критичного значення, оскільки інформація може бути використана відверто або приховано для досягнення військових і політичних цілей. Нижче розглянемо основні аспекти політики інформаційної безпеки держави під час війни.

Кібервійна. У сучасних конфліктах інформаційна безпека стає одним з основних аспектів бойових дій, оскільки так звані хакерські атаки можуть істотно впливати на роботу критичної інфраструктури держави, роботу транспорту, освітнього процесу й інших не менш важливих для перемоги компонентів. Держава повинна бути готовою до відповіді на ворожі кібератаки та захист своєї критичної інфраструктури [7]. Коли якісно «контратакувати» й «оборонятися» на кіберполі, то противник може відмовитися від своїх планів у цьому напрямі. І всі свої сили залучатиме до відбиття саме «кіберконтратак».

Пропаганда та психологічна війна. Інформація може бути використана для маніпулювання громадською думкою та зміни ставлення до війни. Ворог у доступний спосіб може поширювати власні наративи та пропаганду і, використовуючи політтехнології та психологічні маніпуляції, домогтися того, що громадяни держави, яка піддається нападу, самостійно поширюватимуть таку неправдиву та відверту дезінформацію серед власних друзів (це стосується власне соціальних мереж і пліток). Така робота буде відвертим підіграванням ворогу та його спецслужбам. Держава повинна мати стратегію протидії таким впливам і розвивати контрпропаганду. Для цього потрібна відповідна стратегія та кваліфіковані фахівці з досвідом роботи в інформаційному полі [6].

Захист інформації. У військових операціях держава повинна забезпечити захист конфіденційної інформації від ворожих розвідувальних дій. Конфіденційність і захист такої інформації сприятиме успішним наступальним і контрнаступальним операціям [2]. Саме так, як це було з контрнаступом Збройних сил України на харківському напрямку восени 2022 року (що дало змогу звільнити значну частину окупованих територій) чи успішною атакою на Кримський міст восени того ж року (завдяки чому вдалося порушити логістичні ворожі ланцюжки на півдні України).

Міжнародне співробітництво. Під час війни міжнародне співробітництво в галузі інформаційної безпеки набуває важливого значення для обміну розвідувальною інформацією та координації заходів. Така співпраця є особливо корисною, коли держава істотно поступається ворогам у плані технічного та матеріального забезпечення. І якщо мати добрі стосунки з іноземними державами, у яких є сучасне обладнання й оснащення, то це буде важливим фактором у протидії ворогові [2].

Гуманітарні аспекти. Держава повинна також враховувати гуманітарні аспекти інформаційної безпеки, забезпечуючи доступ до гуманітарної інформації та дотримання прав людини під час конфлікту. На жаль, відкритістю джерел гуманітарної інформації може скористатися ворог, щоб створювати провокації та поширювати небезпечну для всіх громадян дезінформацію.

Політика інформаційної безпеки держави є важливим інструментом управління інформаційними ресурсами й забезпечення національної безпеки в сучасному світі. Вона має враховувати як нормальні умови, так і специфічні аспекти під час війни, щоб забезпечити надійний захист інформації та інтересів держави. На жаль, на сучасному етапі політика інформаційної безпеки України не є на досконалому рівні, що викликає загрози та напади з боку ворога [5].

Саме розробка й дослідження наявної проблематики має всебічно сприяти покращенню інформаційної безпеки нашої держави. Написання та створення методичних інформаційних

посібників для спецслужб і пересічних громадян має стати наріжним каменем в роботі з витіснення ворожих наративів і ворожої пропаганди з українського інформаційного поля [4]. Люди повинні навчитися вирізняти ворожі потоки інформації серед тих численних повідомлень, які їх оточують. Особливо це стосується користувачів соціальних мереж, адже саме там зустрічаються величезні масиви неперевіреної та невідфільтрованої інформації. А це, зі свого боку, зміцнить бойовий дух армії та всіх громадян і наблизить перемогу України.

Література:

1. Архипов О. Є., Архипова Є. О. Особливості розуміння понять «інформаційна безпека» та «безпека інформації». *Інформаційні технології та безпека: основи забезпечення інформаційної безпеки (ІТБ-2014): Матеріали XIV Міжнародної науково-практичної конференції*. Київ : ІПРІ НАН України, 2014. С. 18–30.

2. Богданович В. Ю., Ворович Б. О., Марко Є. І. Інформаційна безпека як основа воєнної безпеки держави та суспільства. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського,* 2018. № 3, с. 44–48.

3. Боднар І. Р. Інформаційна безпека як основа національної безпеки. *Mechanism of Economic Regulation,* 2014. № 1, с. 68–75.

4. Булаєв В. П. Теоретико-методологічні засади дослідження адміністративно-правового регулювання діяльності інформаційних служб системи МВС України. Laws and Administrative Measures on Information Services of the Ministry of Internal Affairs of Ukraine. 2018.

5. Довгань О. Д., Ткачук Т. Ю. Система інформаційної безпеки України: онтологічні виміри. Інформація і право. № 1 (24). 2018. С. 89–103.

6. Колгатин А. Г. Інформаційна безпека в системах відкритої освіти. *Освітні технології та суспільство*. 2014. Т. 17, № 1. С. 417–425.

7. Лисенко Сергій. Історія досліджень інформаційної безпеки як об'єкта правовідносин. *Supremația Dreptului*. № 2 (2016), с. 34–44.

8. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України. *Політичний менеджмент.* 2008.

9. Рішення РНБО України від 28 квітня 2017 року. URL: https://zakon.rada.gov.ua/laws/show/n0004525-17#Text.

10. Троянський О. А. Інформаційна безпека в Україні: сучасний стан та перспективи розвитку. 2021.

11. Указ Президента України № 133/2017. URL: https://www.president.gov.ua/documents/1332017-21850

12. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право,* 2012. № 2 (5), с. 162–169.

13. Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and national security*. Potomac Books, Inc., 2009.

14. Kumar, Anilesh. State nationalism or popular nationalism? Analysing media coverage of TikTok ban on mainstream Indian TV news channels. *Media Asia*, 2023. P 1–17.

15. Miller, Daniel, et al. *How the world changed social media*. UCL press, 2016.

References:

1. Arkhipov, O. E., & Arkhipova, Ye. O. (2014). Osoblyvosti rozuminnia poniat "informatsiina bezpeka" ta "bezpekainformatsii" [Features of Understanding the Notions of "Information Security" and "Security of Information"]. *Information Technologies and Security: Basics of Ensuring Information Security (ITS-2014): Proceedings of the XIV International Scientific and Practical Conference.* Kyiv: IEP NAPS of Ukraine. P. 18–30 [in Ukrainian].

2. Bohdanovych, V. Yu., Vorovych, B. O., & Marko, Ye. I. (2018). Informatsiina bezpeka yak osnova voiennoi bezpeky derzhavy ta suspilstva [Information Security as the Basis of State and Society Military Security]. *Collection of Scientific Papers of the Center for Military-Strategic Research of the Ivan Chernyakhovsky National Defense University of Ukraine*, 3. P. 44–48 [in Ukrainian].

3. Bodnar, I. R. (2014). Informatsiina bezpeka yak osnova natsionalnoi bezpeky [Information Security as the Basis of National Security]. *Mechanism of Economic Regulation*, 1. P. 68–75 [in Ukrainian].

4. Bulayev, V. P. (2018). Teoretyko-metodolohichni zasady doslidzhennia administratyvno-pravovoho rehuliuvannia diialnosti informatsiinykh sluzhb systemy MVS Ukrainy [Theoretical and Methodological Foundations of Research on Administrative and Legal Regulation of the Activities of Information Services in the Ministry of Internal Affairs of Ukraine]. *Laws and Administrative Measures on Information Services of the Ministry of Internal Affairs of Ukraine* [in Ukrainian].

5. Dovhan, O. D., & Tkachuk, T. Yu. (2018). Systema informatsiinoi bezpeky Ukrainy: ontolohichni vymiry [The Information Security System of Ukraine: Ontological Aspects]. *Information and Law,* 1 (24). P. 89–103 [in Ukrainian].

6. Kolhatin, A. G. (2014). Information Security in Open Education Systems [Informatsiina bezpeka v systemakh vidkrytoi osvity]. *Educational Technologies and Society*, 17.1. P. 417–425 [in Ukrainian].

7. Lysenko, S. (2016). Istoriia doslidzhen informatsiinoi bezpeky yak obiekta pravovidnosyn [The History of Research on Information Security as an Object of Legal Relations]. *Supremacy of Law,* 2. P. 34–44 [in Ukrainian].

8. Ostroukhov, V., Petryk, V. (2008). Do problemy zabezpechennia informatsiinoi bezpeky Ukrainy [On the Issue of Ensuring Information Security of Ukraine]. *Political Management* [in Ukrainian].

9. Verkhovna Rada of Ukraine (2017). Resolution of the National Security and Defense Council of Ukraine, April 28, 2017. Retrieved from https://zakon.rada.gov.ua/laws/show/n0004525-17#Text [in Ukrainian].

10. Troyansky, O. A. (2021). "Information Security in Ukraine: Current State and Development Prospects" [in Ukrainian].

11. Decree of the President of Ukraine No. 133/2017. Retrieved from https://www.president.gov.ua/documents/1332017-21850 [in Ukrainian].

12. Furashev, V. M. (2012). Kiberprostir ta informatsiinyi prostir, kiberbezpeka ta informatsiina bezpeka: sutnist, vyznachennia, vidminnosti [Cyberspace and Information Space, Cybersecurity and Information Security: Essence, Definitions, Differences]. *Information and Law,* 2 (5). P. 162–169 [in Ukrainian].

13. Kramer, Franklin D., Stuart H. Starr, Larry K. Wentz, eds. (2009). Cyberpower and National Security. *Potomac Books,* Inc.

14. Kumar, Anilesh. (2023). State Nationalism or Popular Nationalism? Analyzing Media Coverage of the TikTok Ban on Mainstream Indian TV News Channels. *Media Asia*. P. 1–17.

15. Miller, Daniel, et al. (2016). How the World Changed Social Media. UCL Press.

Mykhailo Savlyuk. Theoretical and methodological basis of information security research

The article discusses Ukraine's transition from a post-industrial society to an information society, which poses new challenges and threats to the country. The Russian Federation is using hybrid warfare in Ukraine, which includes information attacks by spreading false or partially true information, manipulating facts, and sowing panic and discord. The purpose of the study is to investigate the algorithm of the enemy's information attack and to develop a programme of counteraction to the aggressor. The research methods used are analysis, synthesis, empirical knowledge and comparison. The study resulted in the development of an algorithm for determining the reliability of disseminated information and detecting enemy information attacks. This algorithm helps to distinguish genuine information from the result of enemy information operations.

Key words: *IPSO, information security, cybersecurity, social media propaganda, information operations, war, hybrid warfare, history, information attacks, national security.*

ВІДОМОСТІ ПРО АВТОРІВ

Баюрчак Назарій – аспірант кафедри політичних інститутів та процесів Факультету історії, політології і міжнародних відносин, Прикарпатський національний університет імені Василя Стефаника.

Березовська-Чміль Олена Борисівна – кандидат політичних наук, доцент кафедри політичних інститутів та процесів, Прикарпатський національний університет імені Василя Стефаника.

Воробець Назар – аспірант кафедри політології Факультету історії, політології і міжнародних відносин, Прикарпатський національний університет імені Василя Стефаника.

Галіпчак Володимир – аспірант кафедри політичних інститутів та процесів Факультету історії, політології і міжнародних відносин, Прикарпатський національний університет імені Василя Стефаника.

Головчук Юрій – аспірант кафедри політичних інститутів та процесів Факультету історії, політології і міжнародних відносин, Прикарпатський національний університет імені Василя Стефаника.

Голуб'як Ігор – аспірант кафедри політичних інститутів та процесів Факультету історії, політології і міжнародних відносин, Прикарпатський національний університет імені Василя Стефаника.

Голуб'як Наталія – кандидат політичних наук, асистент кафедри міжнародних відносин, Прикарпатський національний університет імені Василя Стефаника.

Дукач Наталія – аспірант кафедри політології Факультету історії, політології і міжнародних відносин, Прикарпатський національний університет імені Василя Стефаника.

Івасюк Іван – аспірант кафедри політичних інститутів та процесів Факультету історії, політології і міжнародних відносин, Прикарпатський національний університет імені Василя Стефаника.

Кирничний Себастьян – магістрант Факультету історії, політології і міжнародних відносин, Прикарпатський національний університет імені Василя Стефаника.

Кобець Тарас – аспірант кафедри політичних інститутів та процесів Факультету історії, політології і міжнародних відносин, Прикарпатський національний університет імені Василя Стефаника.

Кобець Юлія – кандидат політичних наук, доцент кафедри політичних інститутів та процесів, Прикарпатський національний університет імені Василя Стефаника.

Матвієнків Світлана – кандидат політичних наук, доцент кафедри політичних інститутів та процесів, Прикарпатський національний університет імені Василя Стефаника.

Міщук Андрій – кандидат історичних наук, доцент кафедри історії України, Прикарпатський національний університет імені Василя Стефаника.

Міщук Мар'яна – кандидат політичних наук, доцент кафедри політичних інститутів та процесів, Прикарпатський національний університет імені Василя Стефаника.

Никорович Юрій-Андрій – аспірант кафедри політичних інститутів та процесів Факультету історії, політології і міжнародних відносин, Прикарпатський національний університет імені Василя Стефаника.

Савлюк Михайло – аспірант кафедри політичних інститутів та процесів Факультету історії, політології і міжнародних відносин, Прикарпатський національний університет імені Василя Стефаника.

Шлемкевич Тетяна – кандидат політичних наук, асистент кафедри журналістики, Прикарпатський національний університет імені Василя Стефаника.

ВІСНИК ПРИКАРПАТСЬКОГО УНІВЕРСИТЕТУ
СЕРІЯ: ПОЛІТОЛОГІЯ

Випуск 15, 2023

Головний редактор *Василь МАРЧУК*
Літературний редактор *Руслана БОДНАР*
Комп'ютерна верстка *Вікторія ГАЙДАБРУС*
Коректор *Надія ГРИЦІВ*

Підписано до друку 26.12.2023 р.
Формат 60×84/8. Гарнітура Times New Roman.
Папір офсет. Цифровий друк. Ум. друк. арк. 8,14. Зам. № 0224/170

Наклад 100 прим.

Видавничий дім «Гельветика»
65101, Україна, м. Одеса, вул. Інглезі, 6/1
Тел.: +38 (095) 934 48 28, +38 (097) 723 06 08
E-mail: mailbox@helvetica.ua
Свідоцтво суб'єкта видавничої справи
ДК № 7623 від 22.06.2022 р.