УДК 81’42:355.01:316.776.23 (477)

https://doi.org/10.32689/2617-2224-2022-1(29)-17

Радченко Олександр Віталійович,
доктор наук з державного управління, професор, заслужений працівник освіти України, професор кафедри публічного управління на адміністрування, Національний авіаційний університет, 03680, м. Київ, просп. Гузара Любомира, 1, https://orcid.org/0000-0002-0437-6131

Radchenko Oleksandr Vitaliiovych,
Doctor of Science of the Public Administration, Professor, Honored Worker of Education of Ukraine, Professor at the Department of Public Administration, National Aviation University, 03680, Kyiv, Huzara Liubomyra Avenue, 1, https://orcid.org/0000-0002-0437-6131

Радченко Оксана Олександрівна,
кандидат наук з державного управління, доцент кафедри публічного врядування, Міжрегіональна Академія управління персоналом, 03039, м. Київ, вул. Фрометівська, 2, https://orcid.org/0000-0001-9286-0240

Radchenko Oksana Oleksandrivna,
PhD of Public Administration, Associate Professor at the Department of Public Administration, Interregional Academy of Personnel Management, 03039, Kyiv, Frometivska str., 2, https://orcid.org/0000-0001-9286-0240

ДЖЕРЕЛОЗНАВЧИЙ АНАЛІЗ ПРОБЛЕМАТИКИ ГІБРИДНИХ ВІЙН В СУЧАСНОМУ ДИСКУРСНОМУ ПРОСТОРІ УКРАЇНИ

Стаття пропонує авторську систематизацію наукових та експертних поглядів і підходів до проблематики гібридних війн та їх впливу на забезпечення інформаційного суверенітету держави в сучасному дискурсному просторі. Обґрунтовано нагальність дослідження інформаційних загроз, негатив-

них зовнішніх впливів на стан національної безпеки України, що особливо актуалізувалося після 2014 року, коли не в останню чергу завдяки успішному застосуванню інформаційних спецоперацій Росії вдалося анексувати Крим та розгорнути військове протистояння Сході України через забезпечення позитивного сприйняття частиною місцевого населення цих регіонів агресивних дій РФ.

Визначено, що кінцевою метою розв'язаної Росією гібридної геополітичної інформаційної війни є цивілізаційний вибір українського народу: рухатися в напрямку європейської інтеграції чи повертатися в лещата православно-російської цивілізації.

На основі сгенерованої в інтернет-сервісі *Word's* Хмарки тегів виокремлено 5 основних кластерів наукового розуміння проблематики феномену інформаційної війни. Розкрито основні підходи до наукового розуміння зазначеного соцієтального феномену в контексті: філософсько-онтологічної сутності інформаційної війни; понятійно-категоріального апарату; виокремлення ключових загроз національній безпеці держави; механізмів і технологій ведення гібридних війн; суб'єкт-об'єктної структуризації та практичних кейсів. Зроблено висновок про необхідність розгортання в Україні системної діяльності органів публічного врядування, насамперед, інституту Президента України, Кабінету Міністрів України, Збройних сил, СБУ та МВС з формування сучасної ефективної системи захисту національного інформаційного суверенітету, яка б включала підготовку фахівців сфери розпізнавання, запобігання й протидії проявам інформаційної війни, ведення контрпропагандистських інформаційних операцій тощо.

Ключові слова: держава, публічне управління, інформаційні війни, національна безпека держави.

SOURCE ANALYSIS OF THE PROBLEMS OF INFORMATION WARFARE IN MODERN DISCOURSE SPACE

The article offers the author's systematization of scientific and expert views and approaches to the problems of information warfare and their impact on ensuring the information sovereignty of the state in the modern discourse space. The urgency of the study of information threats, negative external influences on the national security of Ukraine, which became especially relevant after 2014, when thanks to the successful use of information special operations Russia managed to annex Crimea and deploy military confrontation in eastern Ukraine by ensuring a positive perception of aggressive actions of the Russian Federation.

It is determined that the ultimate goal of Russia's hybrid geopolitical information warning is the civilization choice of the Ukrainian people: to move towards European integration or return to the Orthodox-Russian civilization zone. On the basis of well-generated *Word's* Cluster Tags, 5 main clusters of scientific understanding of the phenomenon of information warfare are singled out. The main approaches to the scientific understanding of this societal phenomenon in the context of: philosophical and ontological essence of information warfare are revealed; conceptual and categorical apparatus; identification of key threats to national security; mechanisms and technologies of information warfare; subject-object structuring and practical cases. It is concluded that it is necessary to deploy systemic activities of public authorities in Ukraine, first of the Institute of the President of Ukraine, the Cabinet of Ministers of Ukraine, the Armed Forces, the Security Service and the Ministry of Internal Affairs to form a modern effective system of national information sovereignty manifestations of information warfare, conducting counter-propaganda information operations, etc.

Key words: state, public administration, information warfare, national security.

Вступ. Однією з головних загроз національній безпеці України, що постають у першій чверті XXI століття. є активне розгортання на нашій території гібридної геополітичної інформаційної війни, кінцевою метою якої є цивілізаційний вибір українського народу: рухатися в напрямку європейської інтеграції чи повертатися в лещата православно-російської цивілізації. Інформаційна війна стала для нас буденним явищем, інформаційна зброя застосовується в інформаційному просторі України щоденно тисячами інтернет-блогів і сервісів, телевізійних каналів, газет та журналів, чуток і фейків, дезінформаційних вкидань і вуличних акцій.

Технології гібридної війни розвиваються й поширюються настільки швидко, що експертно-наукове середовище не поспіває їх своєчасно осмислювати й систематизувати. «Якщо у мину-

лому, – зазначає С. Макдональд, – пропагандисти використовували грубі методи для зміни зображень реальних людей, подій та об'єктів, які зазвичай можна було легко виявити, то вже сьогодні комп'ютери дозволяють пропагандистам створювати будь-які уявні зображення, нерухомі або рухомі, з відповідним супровідним звуком. Й при цьому виявляти, що зображенням було піддано маніпулювання, стає надзвичайно важко, а Інтернет, телебачення та глобальні ЗМІ дають змогу майже миттєво поширювати змінені зображення й дезінформацію будь-якого іншого типу по всьому світу, підриваючи державний лад і політичний режим країни-конкурента» (Macdonald, 2006, с. 13). Тому виникає суспільна потреба й нагальне завдання проведення джерелознавчого аналізу наукового усвідомлення та систематизації сучасних підходів і трактувань сутності, механізмів та інструментарію гібридних війн та їх основної складової, що вже отримала самостійну назву – інформаційна війна.

Аналіз останніх досліджень і публікацій дає підстави стверджувати, що проблематика розгортання гібридних, та, зокрема, інформаційних війн в Україні надзвичайно активно обговорюється в публічному та науковому дискурсі, особливо після 2014 року, коли не в останню чергу завдяки успішному застосуванню інформаційних спецоперацій Росії вдалося анексувати Крим та розгорнути військове протистояння Сході України через забезпечення позитивного сприйняття частиною місцевого населення цих регіонів агресивних дій РФ. Так, он-лайн пошуковик національної бібліотеки імені В. Вернадського на ключові слова «інформаційна війна» видає 307 назв наукових статей, 257 джерел реферативної бази даних та 45 книжкових видань та компакт-дисків, причому 66 з них датовані 2018 роком, 71 – 2017 роком, 92 – 2016 роком і 82 – 2015 роком.

З усього загалу зазначених наукових публікацій в даній розвідці ми спиратимемося на таких сучасних вітчизняних дослідників, як І. Боднар, Г. Горпинич, Б. Калініченко, О. Курбан, О. Левченко, І. Парфенюк, Г. Почепцов, І. Проноза, С. Стародуб, А. Фісун, В. Шемчук, П. Шпига та Р. Рудник, А. Яфонкін та В. Шевчук. Серед закордонних науковців та експертів у галузі інформаційних війн відзначимо публікації Р. Бхана, Дж. ДерДеріана, М. Холловея, Н. Янкович, С. Макдональда, Б. Перрі, М. Піллсбері, Дж. Скотта, Р. Стенгеля, Д. Вентре.

Фокусуючи свою увагу на проблемах окремих сфер і напрямків інформаційного протистояння сучасних держав у глобальному інформаційному просторі та інформаційних загрозах цього простору системам національної безпеки держави, названі дослідники залишають поза полем зору **невирішені раніше** питання систематизації наукових підходів до проблематики інформаційних війн в публічно-політичному інформаційному просторі, що становитиме **мету даної публікації**.

1. Загальна візуалізація дискурсного простору інформаційних війн.

З метою візуалізації дискурсного простору проблематики інформаційних війн піддамо програмній обробці текстовий загал публікацій зазначених вище авторів в інтернет-сервісі "Word's Cloud", що генерує відповідну Хмарку тегів (Рис. 1.). Така Хмарка тегів наглядно демонструю частоту використання та питому вагу окремих термінів і категорій, що описують феномен інформаційної війни. Як видно з Рис. 1., це, насамперед, війна, яка несе в собі загрози зовнішнього домінування через вплив на свідомість людей, внаслідок чого ця війна набуває ознак інформаційної, де основними інформаційними загрозами є операції обману, дезінформація та пропаганда, що підривають інформаційний суверенітет держави.

Проведений попередній джерельний аналіз публікацій закордонних та українських науковців і експертів дає нам можливість виокремити такі основні підходи до наукового розуміння зазначеного соцієтального феномену за кваліфікаційними ознаками фокусування на контексті: філософсько-онтологічної сутності інформаційної війни; виокремлення ключових загроз національній безпеці держави; понятійно-категоріального апарату; механізмів і технологій ведення інформаційних війн; суб'єкт-об'єктної структуризації та практичних кейсів (Рис. 2).

2. Кластер філософсько-онтологічної сутності інформаційної війни

Першим кластером визначаємо кластер філософсько-онтологічної сутності інформаційної війни. В цьому напрямку плідно працюють Р. Бхан, Г. Горпинич, І. Михальченко, Г. Почепцов, І. Проноза, В. Шемчук та інші дослідники. Зокрема, Г. Горпинич визначає онтологічну сутність інформаційної війни як «продукт розвитку суспільства, який ввібрав увесь можливий досвід людства, накоплений за роки протистоянь. Виникаюча на певному етапі інформаційного протиборства у наслідок науково-інформаційного прогресу і інформаційної інтеграції світового співтовариства, інформаційна війна стала самостійним контрольованим та неконтрольо-

Рис. 1. Хмарка тегів дискурсного простору проблематики інформаційних війн

Рис. 2. Систематизація дискурсного простору проблематики інформаційних війн

ваним засобом здійснення внутрішньої та зовнішньої політики у світі» (Горпинич, 2018, с. 37). У свою чергу, І. Михальченко фокусує увагу на тому, що філософською сутністю інформаційної війни як продукту постіндустріального суспільства є її технологічний характер та спрямування на досягнення гуманітарного поневолення одних груп людей іншими, що обумовлено неможливістю глобальних збройних конфліктів, які можуть знищити планету (Михальченко, 1998, с. 14).

У сутнісному плані В. Шемчук розглядає інформаційну війну як сучасну форму «продовження домінуючих ідеологічних засад державної політики, що здійснюється за допомогою комплексу засобів інформаційно-технологічної індустрії, механізмів інформаційно-психологічного впливу на суспільство всередині держави чи населення країн-конкурентів в умовах політичного (воєнно-політичного, економічного) конфлікту з метою формування в соціальному аспекті єдності суспільства, визначення його ідентичності та інформаційного захисту світоглядних цінностей, а також – деморалізації та фрагментації населення і силової компоненти держав-противників у межах глобального інформаційного простору» (Шемчук, 2019, с. 33).

З-поміж науковців, що представляють даний кластер найбільш, відомою фігурою виглядає Георгій Почепцов, праці якого стали вже класичними в теорії інформаційних війн та технологій комунікативного впливу на суспільну свідомість. Науковець стверджує, що «інформаційні війни давно зайняли належне місце у військовій парадигмі. Існує інфраструктура відповідної підготовки спеціалістів та їх місце у військовій ієрархії. Все це трапилося на наших очах, коли прийшло нове бачення війни, що було підказане новим інструментарієм – інформаційним. Це також співпало зі зміною парадигми війни в цілому, що реалізувалася в переході від суто військових і нелегальних видів зброї, до більш складної роботи з населенням. Причому сьогодні чітко стало зрозумілим, що важливим компонентом для виграшу є не лише населення ворожої сторони, а й власне населення, бо війни можуть вигравати на полі боя, а програватися в свідомості людей» (Почепцов, 2012).

3. Кластер ключових загроз національній безпеці держави

Другий кластер – виокремлення ключових загроз національній безпеці держави – представляють публікації А. Аносова, З. Бржевської, Г. Гайдур, Н. Довженко, Р. Киричок, І. Боднар, В. Шевчука та А. Яфонкіна. Так, колектив авторів кафедри інформаційної та кібернетичної безпеки Державного університету телекомунікацій під керівництвом Галини Гайдур досліджує проблеми вразливості Української держави в умовах інформаційної війни. Науковці описують основні загрози, серед яких відзначають: руйнування єдиного інформаційного простору держави; маніпуляція суспільною, недостатня координація діяльності органів державної влади, слабкість системи освіти та виховання, протиправне застосування спеціальних засобів впливу на суспільну свідомість, загострення міжнародної конкуренції за володіння інформаційними технологіями та ресурсами; діяльність міжнародних терористичних організацій; недостатність нормативної правової бази, що регулює відносини в інформаційній сфері, а також недостатня практика застосування права (Бржевська та ін., 2019, с. 88). До цього переліку А. Яфонкін та В. Шевчук додають загрози тотальної безконтрольності комунікативної взаємодії віртуальних спільнот в соціальних мережах, адже це надає зловмисникам можливість «не тільки впливати на суспільну свідомість, збирати людей на масові акції і «кольорові революції», але й вербувати найманців в бандформування, планувати і координувати їх дії, організовувати теракти і диверсії, проводити масштабні операції, завдаючи ворожій державі неприйнятного збитку» (Яфонкін, Шевчук, 2017, с. 467).

І. Боднар виокремлює головну інформаційну загрозу національній безпеці – «це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості з метою нав'язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної і державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку» (Боднар, 2014, с. 69).

4. Кластер понятійно-категоріального апарату

Третій кластер понятійно-категоріального апарату містить наукові публікації Д. Вентре, О. Курбана, М. Піллсбері, Г. Почепцова, С. Стародуб, А. Фісуна, в яких розкриваються зміст і сутність понять та категорій, пов'язаних з інформаційною війною. Зокрема, А. Фісун пропонує інтегральне визначення терміну «інформаційна війна» як «комплексного, відкритого чи прихованого цілеспрямованого інформаційного впливу однієї сторони, чи взаємний вплив сторін одна на одну, який містить систему методів

і засобів впливу на людей, їхню психіку та поведінку, на інформаційні ресурси та інформаційні системи, з метою досягнення інформаційної переваги (в забезпеченні національної стратегії), що зумовлює прийняття сприятливих для ініціатора впливу рішень або знищення інформаційної інфраструктури противника, з одночасним зміцненням і захистом власної інформації та інформаційних систем» (Фісун, 2011, с. 538).

Більш вузьке, наближене до суто військової сфери тлумачення пропонують О. Курбан та С. Стародуб, на думку яких інформаційна війна – це «запобігання можливому військовому конфлікту, примус супротивника до відмови від участі у бойових діях через ослаблення морального духу особового складу збройних сил і цивільного населення супротивника» (Курбан, Стародуб, 2018, с. 96), та «порушення обміну інформацією в таборі супротивника, знищення не населення, а державного механізму, послаблюючи моральні й матеріальні сили супротивника або конкурента через цілеспрямовані заходи пропагандистського впливу на свідомість людини в ідеологічній та емоційній сферах» (Курбан, Стародуб, 2018, с. 28).

Найбільш узагальнююче розуміння феномену інформаційної війни пропонує Д. Вентре, який вбачає в останній інноваційний механізм відстоювання національних інтересів через досягнення ефективного контролю над інформаційним простором своєї та інших держав задля отримання економічних, політичних, дипломатичних та інших переваг (Ventre, 2016, с. 39).

Важливе зауваження в понятійному плані робить Г. Почепцов, який розводить суто ***інформаційну війну*** в класичному розумінні як діяльність, що прив'язана до традиційної війни у фізичному вимірі й націлену на інформаційні потоки, та ***війну смислову***, яка є більш прихованою та спрямованою на когнітивні процеси, коли відбувається захоплення й віртуального, й когнітивного просторів, внаслідок чого досягається цілеспрямоване програмування інформаційного простору навколо людини, що в заданому напрямку змінює її персональну свідомість та в цілому суспільну свідомість країни чи її окремих регіонів і територій. Так само принципове розведення двох понять інформаційної війни робить М. Піллсбері, який наголошує на розрізнення у англомовному дискурсі поняття "***Information war***" (як інформаційної війни у вигляді суто військових операцій, основними об'єктами ураження в яких стануть інформаційні системи супротивника) та "***Information warfare***" (як інформаційної війни у вигляді інформаційної діяльності, що застосовується державою, корпорацією або окремою політичною організацією задля послаблення чи знищення іншої держави, корпорації, політичної організації (Pillsbury, 1997, с. 227).

5. Кластер механізмів та технології ведення інформаційних війн

Четвертий кластер об'єднує широке коло науковців, котрі у своїх дослідженнях розкривають механізми та технології ведення інформаційних війн. Серед таких дослідників відзначимо Дж. ДерДеріана, Б. Калініченка, О. Левченко, С. Макдональда, І. Парфенюка, П. Шпигу та Р. Рудника. Зокрема, Дж. ДерДеріан головною технологічною особливістю інформаційної війни визначає її мережевий характер, здатний досягти військово-політичного домінування за рахунок комп'ютеризації військової техніки і формування мережевої організації збройних сил в ході проведення особливого виду військової операції, що виступає або самостійною формою, або частиною розширеного набору військових дій, що утворюють мережеві і кібервійни (Der Derian, 2009, с. 47).

Б. Калініченко виокремлює специфічні механізми та форми ведення інформаційної війни, до яких відносить: «тенденційне викладення фактів, упереджене висвітлення певної інформації, що стосується тих чи інших подій за допомогою цілеспрямовано підібраних (вирваних із контексту) правдивих даних; дезінформування «від зворотного», що відбувається шляхом надання правдивих відомостей спотвореному вигляді чи в ситуації, коли вони сприймаються об'єктом як неправдиві; термінологічне «мінування», яке полягає у викривленні первинної, правильної суті принципово важливих, базових термінів і тлумачень загальносвітоглядного та оперативно-прикладного характеру; «сіре» дезінформування, що передбачає використання синтезу правдивої інформації з дезінформацією та «чорне» дезінформування, яке передбачає використання переважно неправдивої інформації» (Калініченко, 2019, с. 69).

О. Левченко детально характеризує низку ключових видів інформаційно-психологічної зброї, яка впливає на психіку, свідомість, підсвідомість, морально-психологічний стан людини, соціальних груп та суспільства в цілому (пропагандистську, психофізичну, нейролінгвістичну, психотропну, психотронну, психогенну та психоаналітичну) (Левченко, 2014, с. 143).

Свій варіант переліку основних технологій інформаційної війни надають П. Шпига та

Р. Рудник: «порушення, пошкодження або модифікація інформаційних ресурсів і знань людей про самих себе та про середовище, яке їх оточує; здійснення впливу на суспільну думку та позицію політичної еліти; завдання шкоди протилежній стороні дипломатичними засобами; пропагандистські, психологічні та підривні акції у сфері культури й політики; дезінформація та чутки, створені навмисно; упровадження у ЗМІ своїх прибічників для проведення підривних акцій; проникнення в комп'ютерні мережі та системи управління базами даних, зараження комп'ютерних систем вірусами, навмисне введення різного роду помилок у програмне забезпечення об'єкта; інформаційна підтримка дисидентських та опозиційних рухів» (Шпига, Рудник, 2014, с. 332).

Свій погляд на інструментарій інформаційних війн демонструє І. Парфенюк, зараховуючи до такого інструментарію як традиційні літературу, театр, кінематограф, так і новітні е-книги, Інтернет, комп'ютерні ігри та медіавіруси (Парфенюк, 2019, с. 8–9). Проте, на нашу думку, зазначене вище є, скоріше, каналами доставки інформаційної зброї та ведення інформаційних операції спеціального впливу, а не власне такі інструменти.

6. Кластер суб'єкт-об'єктної структуризації та практичних кейсів інформаційної війни

П'ятий кластер містить наукові публікації, в яких, насамперед, розглядається суб'єкт-об'єктна структуризація інформаційної війни та наводяться численні практичні кейси застосування інструментарію та методів інформаційної війни в конкретних випадках протистояння сучасних держав на геополітичному рівні. Так, Дж. Скотт, до основних суб'єктів інформаційної війни відносить держави та їх політичні еліти, транснаціональні корпорації, релігійні, радикальні та фундаменталістські організації, політичні партії та рухи, внаслідок чого вже утворився «принципово новий світ навколо нас – світ, в якому йдуть щоденні всебічні битви за психологічне ядро світового населення, в якому Організація Об'єднаних Націй не має більшого значення, ніж Facebook, в якому операції оцифрованого впливу стали новою нормою контролю за виборчим процесом, громадською думкою та суспільною свідомістю в цілому. Боротьба суб'єктів у цьому геоінформаційному просторі є запеклою. І національні держави, і спеціальні групи інтересів у всіх можливих варіантах б'ються за найвищу позицію в контролі над публічною інформацією» (Scott, 2019, с. 7).

Р. Бхан наводить приклади застосування інформаційної зброї з боку найсильніших держав світу в ході інформаційно-політичного протистояння таких країн як США та Росія, Китай та Індія, Ізраїль та Палестина (Bhan, 2017).

Особливості застосування інформаційної зброї Росією у її геополітичному протистоянні зі Сполученими Штатами Америки, зокрема, на прикладі російського втручання в президентські вибори США, аналізують Р. Стенгель у книзі «Інформаційні війни: як ми програли глобальну битву проти дезінформації та що ми можемо з цим зробити» (Stengel, 2019) та Н. Янкович у книзі «Як програти інформаційну війну: Росія, фальшиві новини та майбутнє конфліктів» (Jankowicz, 2019). Експерти визнають, що Америка поки що програє глобальну битву проти дезінформації, війну, в якій «на кону» стоять не більше, не менше як «майбутнє громадянського дискурсу й демократії та цінність самої істини».

М. Холловей та Б. Перрі детально розбирають кейси застосування інформаційної зброї Російською Федерацією у її агресії проти України. Зокрема, М. Холловей описує, як уряд Росії створив спеціальні кібервійська у вигляді дописувачів у мережах Facebook, Vkontakte, Odnoklassniki, активність яких складала 5000 репостів на добу та в результаті чого Росія отримала суттєві переваги у інформаційному просторі для спрощення дій з анексії півострова, причому фінансування цієї підривної діяльності у соціальних інтернет-сервісах обійшлося у майже 20 мільйонів доларів (Holloway, 2017). У свою чергу, Б. Перрі зосередив увагу на подіях на Донбасі, зазначаючи, що захоплення Росією частини Луганської та Донецької областей стало значним чином результатом успішних попередніх тривалих інформаційних операцій серед населення Південно-Східних регіонів України, в ході яких досягався контроль над ескалацією ситуації. Внаслідок успішної російської пропаганди населення Донбасу позитивно сприйняли відповідні наративи та формування проросійської ініціативної більшості, яка стала основою для консолідації сепаратистів та підтримки інтервенції збройних формувань (Perry, 2015).

Запропонована нами систематизація дискурсного поля проблематики інформаційної війни, очевидно, є одним з багатьох можливих варіантів і не претендує на абсолютизацію, проте вона як і будь-яка інша наукова модель дозволяє розкрити окремі принципово важливі аспекти обраного предмету дослідження.

Висновки та перспективи подальших досліджень.

Проведене в даній розвідці дослідження засвідчило, що в сучасному світі інформаційні війни стають буденним явищем та новою формою просування національних інтересів держав з одночасним захистом власного інформаційного суверенітету. Полем ведення інформаційних війн стають як національні, так і глобальний інформаційний простір, в якому держави, уряди та політики на практиці намагаються реалізувати широковідомий вислів: «Той, хто володіє інформацією – володіє світом».

За таких умов можемо зробити висновок про необхідність нагального розгортання в Україні системної діяльності органів публічного врядування, насамперед, інституту Президента України, Кабінету Міністрів України, Збройних сил, СБУ та МВС з формування сучасної ефективної системи захисту національного інформаційного суверенітету, яка б включала підготовку фахівців сфери розпізнавання, запобігання й протидії проявам інформаційної війни, ведення контрпропагандистських інформаційних операцій тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Боднар І. Інформаційна безпека як основа національної безпеки. *Mechanism of Economic Regulation*. 2014. № 1. С. 68–75.
2. Бржевська З., Довженко Н., Киричок Р., Гайдур Г., Аносов А. Інформаційні війни: проблеми, загрози протидія. *Кібербезпека: освіта, наука, техніка*. 2019. № 3. С. 88–96.
3. Горпинич Г.І. Інформаційні війни як об'єкт наукової рефлексії. Поліпарадигмальний підхід. *Габітус*. 2018. Вип. 5. С. 36–41.
4. Калініченко Б. Визначальні напрями формування стратегії протистояння інформаційній війні *Держава і право. Серія : Політичні науки*. 2019. Вип. 83. С. 61–73.
5. Курбан О. Теорія інформаційної війни: базові основи, методологія та понятійний апарат. *Scientific Journal «ScienceRise»*. 2015. № 11/1(16). С. 95–100.
6. Левченко О. Класифікація інформаційної зброї за засобами ведення інформаційної боротьби. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2014. № 2(20). С. 142–146.
7. Михальченко И.А. Информационные войны на рубеже XXI века. *Безопасность информационных технологий*. 1998. № 3. С. 14–15.
8. Парфенюк І. Інструментарій інформаційних війн: традиційні та новітні засоби. *Вісник Книжкової палати*. 2019. № 1. С. 7–10.
9. Почепцов Г.Г. Інформаційні війни: тенденції та шляхи розвитку. *Інтернет-сайт MS. Detector. Media*. URL: https://ms.detector.media/manipulyatsii/post/6479/2012-08-12-informatsiini-viini-tendentsii-ta-shlyakhi-rozvitku/.
10. Проноза І. Інформаційна війна: сутність та особливості прояву. *Актуальні проблеми політики*. 2018. Вип. 61. С. 76–84.
11. Стародуб С. Інформаційні війни та системи захисту в умовах глобалізаційних процесів. *Держава та регіони. Серія : Соціальні комунікації*. 2018. № 3. С. 27–31.
12. Фісун А. Ґенеза поняття «інформаційна війна». *Гілея*. 2011. № 49. С. 534–538.
13. Шемчук В. Концептуальні підходи до розуміння інформаційної війни в сучасному світі. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Юридичні науки*. 2019. Т. 30(69), № 3. С. 29–35.
14. Шпига П., Рудник Р. Основні технології та закономірності інформаційної війни. *Проблеми міжнародних відносин*. 2014. Вип. 8. С. 326–339.
15. Яфонкін А., Шевчук В. Інформаційна війна проти держави та інформаційна безпека України. *Форум права*. 2017. № 5. С. 466–472.
16. Bhan Ramesh. Information War: (Dis)information will Decide Future Wars. Educreation Publishing, 2017. 200 p.
17. Der Derian J. Virtuous War: Mapping The Military-Industrial-media-entertainment Network. London: Routledge, 2009. 330 p.
18. Holloway M. How Russia Weaponized Social Media in Crimea. RealClear Media Group Newsletters. May 10, 2017. URL: https://www.realcleardefense.com/articles/2017/05/10/how_russia_weaponized_social_media_in_crimea_1.
19. Jankowicz Nina. How to Lose the Information War: Russia, Fake News, and the Future of Conflict. Bloomsbury Publishing, 2019. 288 p.
20. Macdonald Scot. Propaganda and Information Warfare in the Twenty-First Century: Altered Images and Deception Operations. Routledge, 2006. 224 p.
21. Perry Bret. Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations. Small Wars Journal. 2015. Vol.11, No. 8. URL: http://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-andspecial-opera11352.html.
22. Pillsbury Michael. Chinese Views of Future Warfare. Washington DC: DIANE Publishing, 1997. P. 330.
23. Scott James. Information Warfare: The Meme Is the Embryo of the Narrative Illusion. Amazon Digital Services LLC – KDP Print US, 2019. P. 7
24. Stengel Richard. Information Wars: How We Lost the Global Battle Against Disinformation and What We Can Do About It. Atlantic Books, 2019. 303 p.
25. Ventre Daniel. Information Warfare. John Wiley & Sons, 2016. 352 p.

REFERENCES

1. Bodnar I. (2014). Informatsiyna bezpeka yak osnova natsional'noyi bezpeky [Information security as a

basis of national security]. *Mechanism of Economic Regulation*. Vol.1. 68-75. [in Ukrainian]
2. Brzhevskaya Z., Dovzhenko N., Kirichok R., Gaidur G., Anosov A. (2019). Informatsiyni viyny: problemy, zahrozy ta protydiya [Information warfare: problems, threats and counteraction]. *Kiberbezpeka: osvita, nauka, tekhnika – Cybersecurity: Education, Science, Technology*. Vol.3. 88-96. [in Ukrainian]
3. Gorpynych G. I. (2018). Informatsiyni viyny yak ob'yekt naukovoyi refleksiyi. Poliparadyhmal'nyy pidkhid [Information warfare as an object of scientific reflection. Polyparadigmatic approach]. *Habitus*. Vol.5. 36- 41[in Ukrainian]
4. Kalinichenko B. (2019). Vyznachal'ni napryamy formuvannya stratehiyi protystoyannya informatsiyniy viyni [Determining directions of formation of strategy of counteraction to information warfare]. *Derzhava i pravo. Seriya :* Politychni nauky – State and law. Series: Political sciences. Vol.83. 61-73. [in Ukrainian]
5. Kurban O. (2015). Teoriya informatsiynoyi viyny: bazovi osnovy, metodolohiya ta ponyatiynyy aparat [The theory of information warfare: basic principles, methodology and conceptual apparatus]. *Scientific Journal «ScienceRise»*. Vol.11/1(16). 95 – 100. [in Ukrainian]
6. Levchenko O. (2014). Klasyfikatsiya informatsiynoyi zbroyi za zasobamy vedennya informatsiynoyi borot'by [Classification of information weapons by means of information warfare]. *Suchasni informatsiyni tekhnolohiyi u sferi bezpeky ta oborony – Modern information technologies in the field of security and defense*. Vol.2 (20). 142–146. [in Ukrainian]
7. Mikhalchenko I.A. (1998). Informatsionnyye voyny na rubezhe XXI veka [Information warfare at the turn of the XXI century]. *Bezopasnost' informatsionnykh tekhnologiy – Impassion of information technologies*. Vol.3. 14-15. [in Russian].
8. Parfenyuk I. (2019). Instrumentariy informatsiynykh viyn: tradytsiyni ta novitni zasoby [Tools of information warfare: traditional and modern tools]. *Visnyk Knyzhkovoyi palaty – Bulletin of the Book Chamber*. Vol.1. 7-10. [in Ukrainian]
9. Pocheptsov G. G. (2017). Informatsiyni viyny: tendentsiyi ta shlyakhy rozvytku [Information warfare: tendencies and ways of development]. *Website MS. Detector.Media*. URL : http://www.rossia.in/modules/sections/index.php7op–viewarticle&artid=11. [in Ukrainian]
10. Pronoza I. (2018). Informatsiyna viyna: sutnist' ta osoblyvosti proyavu Information warfare: the essence and features of manifestation]. *Aktual'ni problemy polityky – Actual policy problems*. Vol.61. 76-84. [in Ukrainian]
11. Starodub S. (2018). Informatsiyni viyny ta systemy zakhystu v umovakh hlobalizatsiynykh protsesiv [Information warfare and defense systems in the context of globalization processes]. *Derzhava ta rehiony. Seriya : Sotsial'ni komunikatsiyi – State and regions. Series: social communications*. Vol.3. 27-31. [in Ukrainian]
12. Fisun A. (2011). Geneza ponyattya «informatsiyna viyna» [Genesis of the concept of "information warfare "]. *Hileya – Gilaya*. Vol.49. 534–538. [in Ukrainian]
13. Shemchuk V. (2019). Kontseptual'ni pidkhody do rozuminnya informatsiynoyi viyny v suchasnomu sviti [Conceptual approaches to understanding information warfare in the modern world]. *Vcheni zapysky Tavriys'koho natsional'noho universytetu imeni V. I. Vernads'koho. Seriya : Yurydychni nauky – Scientists of the Tauride National University named V. I. Vernadsky. Series: Legal sciences*. T. 30(69), Vol.3. 29-35. [in Ukrainian]
14. Shpiga P., Rudnik R. (2014). Osnovni tekhnolohiyi ta zakonomirnosti informatsiynoyi viyny [Basic technologies and patterns of information warfare]. *Problemy mizhnarodnykh vidnosyn – Problems of international relations*. Vol.8. 326–339. [in Ukrainian]
15. Yafonkin A., Shevchuk V. (2017). Informatsiyna viyna proty derzhavy ta informatsiyna bezpeka Ukrayiny [Information warfare against the state and information security of Ukraine]. *Forum prava – Forum right*. Vol. 5. 466–472. [in Ukrainian]
16. Bhan Ramesh. (2017). Information War: (Dis)information will Decide Future Wars. Educreation Publishing, 200 p.
17. Der Derian J. (2009). Virtuous War: Mapping The Military-Industrial-media-entertainment Network. London: Routledge, 330 p.
18. Holloway M. (2017). How Russia Weaponized Social Media in Crimea. RealClear Media Group Newsletters. May 10. URL : https://www.realcleardefense.com/articles/2017/05/10/how_russia_weaponized_social_media_in_crimea_1
19. Jankowicz Nina. (2019). How to Lose the Information War: Russia, Fake News, and the Future of Conflict. Bloomsbury Publishing. 288 p.
20. Macdonald Scot. (2006). Propaganda and Information Warfare in the Twenty-First Century: Altered Images and Deception Operations. Routledge. 224 p.
21. Perry Bret. (2015). Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations. Small Wars Journal. Vol.11, No.8. URL : http://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-andspecial-opera11352.html
22. Pillsbury Michael. (1997). Chinese Views of Future Warfare. Washington DC: DIANE Publishing. 421 p.
23. Scott James. (2019). Information Warfare: The Meme Is the Embryo of the Narrative Illusion. Amazon Digital Services LLC – KDP Print US. 160 p.
24. Stengel Richard. (2019). Information Wars: How We Lost the Global Battle Against Disinformation and What We Can Do About It. Atlantic Books. 303 p.
25. Ventre Daniel. (2016). Information Warfare. John Wiley & Sons, 352 p.