УДК 35.078.1:001.102-049.5:316.32
DOI https://doi.org/10.32851/tnv-pub.2021.3.14

ГІБРИДНА ВІЙНА ЯК КЛЮЧОВА ЗАГРОЗА НАЦІОНАЛЬНОМУ СУВЕРЕНІТЕТУ УКРАЇНИ

Радченко О.В. *– доктор наук державного управління, професор,*
заслужений працівник освіти України,
професор кафедри публічного управління на адміністрування
Національного авіаційного університету
ORCID: 0000-0002-0437-6131
Scopus Author ID: 57219931612
Чмир Я.І. *– кандидат наук державного управління,*
доцент кафедри публічного адміністрування
Міжрегіональної академії управління персоналом
ORCID: 0000-0002-4476-6687

Стаття досліджує проблематику забезпечення національного суверенітету держави внаслідок розгортання гібридних воєн, насамперед у глобальному інформаційному просторі. Це зумовлює необхідність створення ефективної системи забезпечення інформаційної безпеки людини, суспільства та держави. Інформаційна безпека розглядається як система, що забезпечує необхідний рівень стабільності та захищеності політичної, соціально-економічної, військово-оборонної, духовно-культурної та інших сфер і галузей життєдіяльності суспільства від небезпечних, дестабілізуючих негативних деструктивних загроз, здатних завдати шкоду національним інтересам держави, сталому розвитку суспільства, благополуччю та здоров'ю кожного громадянина.

Визначається, що гібридна війна становить якісно нову радикальну форму геополітичних і внутрішньополітичних конфліктів латентного й асиметричного характеру, універсальний засіб безкровного забезпечення інтересів суб'єктів ведення інформаційної війни, де основною зброєю виступає інформація, інтернет-мережа та канали масової комунікації, цілеспрямовані на бажану зміну суспільної свідомості, базових цінностей і політичних орієнтації громадян, політичної еліти та вищих керівних кадрів протиборствуючої держави та задля її інформаційного поневолення.

З огляду на широкомасштабну гібридну війну проти України та неминучість подальшого зростання загроз у сфері інформаційної безпеки обґрунтовується комплексна модель системи забезпечення національної безпеки держави. Робиться висновок про необхідність активізації дій органів публічного врядування України у напрямку своєчасного виявлення й нейтралізації загроз і ризиків негативного впливу шкідливого контенту національного і світового інформаційного простору, забезпечення задоволення інформаційних потреб людини й суспільства, реалізації національних інтересів держави у глобальному інформаційному просторі та здійснення ефективного захисту інформаційного суверенітету держави.

Ключові слова: *держава, гібридна війна, інформаційна безпека, інформаційний суверенітет.*

Radchenko O.V., Chmyr Ya.I. Hybrid war as a key threat to the national sovereignty of Ukraine

The article explores the issue of ensuring and national sovereignty of the state due to the deployment of hybrid wars, primarily in the global information space. This necessitates the creation of an effective system of information security of man, society and the state Information security is seen as a system that provides the necessary level of stability and protection of political, socio-economic, military-defense, spiritual, cultural and other spheres and spheres of society from dangerous, destabilizing negative destructive threats that can harm the national interests of the state. development of society, well-being and health of every citizen.

It is determined that hybrid war is a qualitatively new radical form of geopolitical and domestic conflicts of latent and asymmetric nature, a universal means of bloodless security of the interests of the subjects of information warfare, where the main weapon is information, Internet

and mass communication channels, targeted public consciousness, basic values and political orientations of citizens, political elite and senior management of the opposing state and for its information enslavement.

Given the large-scale hybrid war against Ukraine and the inevitability of further growth of threats in the field of information security, a comprehensive model of the national security system of the state is substantiated. It is concluded that it is necessary to intensify the actions of public authorities of Ukraine in the timely detection and neutralization of threats and risks of negative impact of harmful content of national and world information space, meeting the information needs of man and society, realization of national interests in the global information space. sovereignty of the state.

Key words: *state, hybrid war, information security, information sovereignty.*

Постановка проблеми. Перехід людства до епохи інформаційного суспільства характеризується тим, що відбувається поступове переміщення в інформаційне середовище більшості геополітичних процесів і відносин між державами, народами чи окремими інституціями й людьми. В умовах, коли ядерні держави накопичили потенціал смертоносної зброї, здатний знищити саме людство та зруйнувати планету, міждержавна геополітична боротьба – дипломатична, політична, економічна, військова тощо – дедалі більше зміщується в інформаційну площину, де шляхом активного впливу на суспільство, владні структури, вище керівництво та лідерів нації-конкурента держави намагаються отримати перевагу та просувати власні національні інтереси. Інформація й інформаційні технології дедалі більше перетворюються на головну зброю у міждержавному протиборстві, що спричинило появу й надзвичайно швидкий розвиток такого суспільно-політичного феномену, як гібридні війни. Рівень оволодіння інформаційно-комунікативними технологіями вже є визначальним чинником рівня розвитку будь-якої держави, і саме розуміння інформації як особливого виду зброї закріплена у Доктринах національної безпеки провідних країн, адже «той, хто володіє інформацією, володіє світом». Американський дослідник індійського походження Рамеш Хан переконаний, що саме інформація вирішить долю майбутніх воєн. У своїй однойменній книзі він на прикладі протистоянь США – Росія, Ізраїль – Палестина, Китай – Індія описує, скільки потужних країн використовували інформаційну зброю та зловживали інформацією для дестабілізації політичного ладу та поширення негативних меседжів про ворожі нації та їхніх лідерів [16, с. 11].

Аналіз останніх досліджень і публікацій дає підстави стверджувати, що у вітчизняному науковому дискурсі дедалі активніше піднімається проблематика забезпечення інформаційного суверенітету держави в умовах розгортання гібридних воєн, формування та розвитку системи інформаційної безпеки як важливої складової частини національної безпеки країни загалом. Зокрема, плідно працюють у зазначеному напрямі такі науковці, як В. Богданович, Б. Ворович і Є. Марко [1], О. Барна [2], С. Запорожець [3], У. Ільницька [4], Б. Калініченко [5], О. Кріслата [6], О. Левантовис [8], П. Парфенюк [10], Ю. Радковець [11], А. Фісун [13], В. Шемчук [14], А. Яфонкін, В. Шевчук [15] та ін. Водночас усе ще недостатнім є виявлення форм і чинників впливу гібридної війни на стан і перебіг демократичних державотворчих процесів, особливості становлення системи національної безпеки держави у сучасних умовах, що й зумовлює формування мети статі та постановки завдання дослідження.

Виклад основного матеріалу. Із входженням людства у постіндустріальну епоху роль інформаційних впливів на перебіг воєнних і політичних подій у світі тільки зростає. Глобальний інформаційний простір стає основним середовищем міжособистісних, групових і міжнародних контактів та основним місцем

зіткнення національних інтересів і – як наслідок – полем битви за інформаційний суверенітет, за краще геополітичне місце країни у глобальному інформаційному суспільстві. Як зазначає О. Левантович: «Так чи інакше світова карта сьогодення переповнена гібридними протистояннями, мова і про невеликі конфлікти, і про масштабні війни, з'являється потреба розробляти асиметричну, гібридну відповідь. Система безпеки, яку розробило міжнародне право після 1945 р., сьогодні не може відповісти на загрозу нового виклику» [7, с. 53].

За таких умов «поняття "мирний і воєнний стан" переплелося у віртуальному просторі, породивши страшне явище "гібридна війна", яка, на переконання В. Богдановича, Б. Воровича та Є. Марко, здатна втягнути в ареал воєнно-інформаційних дій мільйони людей за стислий період часу. Відстані, кордони, часові та інші перешкоди миру реального у віртуальному просторі нічого не значать, тому інформаційна зброя стала могутньою зброєю XXI ст., під прицілом якої знаходиться як окремий індивід, так і людство загалом. Поняття миру стало хитким, нестійким і концептуально розмитим, оскільки війни, крім реальних військових дій, які, на жаль, ще мають місце у суспільстві, перемістилися також у віртуальний простір, "військові" дії та події, відбуваються баталії за панування над масами та їх свідомістю. Основною зброєю у цій війні стають інформаційні та комунікаційні технології» [1, с. 45–46].

Існують різні підходи до визначення сутності та мети гібридної війни у глобальному інформаційному просторі, що вже отримала відносно самостійну назву – «інформаційна війна». Сучасні дослідники вкладають у ці поняття різні сенси, зокрема визначаючи сутність і мету такої війни як:

– контроль над інформаційним простором задля отримання економічних, політичних, дипломатичних та інших переваг (Д. Вентре [20, с. 39]);

– домінування за рахунок комп'ютеризації військової техніки та формування мережевої організації збройних сил у ході проведення особливого виду військової операції, що виступає або самостійною формою, або частиною розширеного набору військових дій, які утворюють мережеві та кібервійни (Дж. Деріан [17, с. 46]);

– широкомасштабна інформаційна боротьба із застосуванням комплексу заходів, операцій та інструментів дії на психіку людей як цілеспрямований інформаційний вплив на масову свідомість, систему державного та військового управління протиборчої сторони (І. Парфенюк [10, с. 7]);

– найефективніший засіб ведення політичного протиборства, який не потребує людських жертв, надзвичайних матеріальних затрат і є в деякому сенсі більш швидким і прихованим засобом досягнення політичної мети, ніж звичайна війна (Б. Калініченко [5, с. 4]);

– війна без правил, яка спрямована на руйнування духовного світу націй і народів, проти яких ведеться, та вирізняється агресією, використанням сучасних технологій і сучасних методів мобілізації. Серед трьох її складових частин (інформаційної, психологічної, ідеологічної) найважливішою є інформаційна (О. Кріслата [6, с. 197]);

– війна, що виходить за рамки традиційних понять про неї та набуває комбінованого характеру, перетворюючись на клубок політичних інтриг, запеклої боротьби за політико-економічне домінування над країною, за території, ресурси та фінансові потоки. Сторони вдаються до всіх можливих засобів і будь-яких, навіть найбезчесніших, прийомів і дій – як силових, так і несилових. Жертвами ведення такої війни зазвичай стають мирні жителі, передусім найбеззахисніші категорії населення (Ю. Радковець [11, с. 36]);

– цілісна технологія, спрямована на досягнення гуманітарного поневолення одних груп людей іншими, яка є продуктом постіндустріального суспільства і зумовлена неможливістю глобальних збройних конфліктів, що можуть знищити планету (В. Бебик та ін. [9, с. 14–15]);

– 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 у соціальному аспекті єдності суспільства, визначення його ідентичності й інформаційного захисту світоглядних цінностей, а також деморалізації та фрагментації населення та силової компоненти держав-противників у межах глобального інформаційного простору (В. Шемчук [14, с. 33]).

Таким чином, можемо зробити узагальнюючий висновок, що гібридна війна становить якісно нову радикальну форму геополітичних і внутрішньополітичних конфліктів латентного й асиметричного характеру, універсальний засіб безкровного забезпечення інтересів суб'єктів ведення інформаційної війни, де основною зброєю виступає інформація, інтернет-мережа та канали масової комунікації, спрямовані на бажану зміну суспільної свідомості, базових цінностей і політичних орієнтації громадян, політичної еліти та вищих керівних кадрів протиборствуючої держави й задля її інформаційного поневолення.

Оскільки будь-який процес або суспільне явище у системному вимірі завжди має свої суб'єкти й об'єкти, визначимо останніх для інформаційної війни як ключової складової частини війни гібридної. Так, до основних суб'єктів інформаційної війни слід віднести:

– держави та їхні інституції (серед світових держав беззаперечними лідерами у розробці та використанні інструментарію інформаційних воєн є Сполучені Штати Америки, Китай і Росія);

– міждержавні утворення, військово-політичні й оборонні союзи;

– транснаціональні медіа-корпорації та транснаціональні фінансово-промислові корпорації;

– віртуальні соціальні спільноти та соціальні інтернет-сервіси (напр. Facebook, Vkontakte, Odnoklassniki тощо);

– засоби масової інформації та комунікації (супутникові, інтернет та ефірні телеканали, традиційні газети та журнали й інтернет-видання);

– лідери суспільних думок, виразники національних цінностей і менталітету народу, нації;

– спецслужби та спецпідрозділи системи національної оборони й безпеки;

– агенти впливу (п'ята колона) – громадяни певної держави, їх організації, рухи та партії, які на ідеологічний або фінансовій основі здійснюють інформаційні операції на користь іноземної держави;

– недержавні радикальні, екстремістські, фундаменталістські, терористичні та інші ідеологічно-радикальні та релігійно-радикальні організації і формування.

Серед об'єктів інформаційних воєн основними є:

– суспільна й особистісна свідомість громадян;

– національні цінності та національний менталітет;

– система суспільно-політичних та інформаційно-комунікаційних відносин відповідної країни та її суспільства;

– система підготовки й ухвалення публічно-управлінських рішень у політичній, економічній, безпековій сферах життєдіяльності держави;

– політична й адміністративна культура державно-управлінської еліти;

– інформаційна й інформаційно-комунікаційна інфраструктура держави;

– інституції національної оборони та безпеки, їхні керівники та співробітники;

– інституції публічного врядування держави, їх керівники та службовці;

– критично важлива економічна інфраструктура держави, банківські установи, підприємства військово-промислового комплексу тощо.

Зазвичай гібридну війну пов'язують насамперед із проведенням інформаційно-психологічних операцій і застосуванням різної інформаційної та інформаційно-психологічної зброї. Так, С. Запорожець наголошує, що «провідна роль у гібридній війні відводиться інформаційно-психологічному й економічному впливу на противника. Застосування непрямих асиметричних дій і способів ведення війни дозволяє позбавити протиборчу сторону фактичного суверенітету без захоплення території держави військовою силою» [3, с. 21]. М. Туранський підкреслює, що «однією з особливостей воєнних дій сьогодення є проведення у їхньому ході комплексу заходів з інформаційно-психологічного впливу на населення та війська противника, де особливий акцент припадає на такі складові частини, як інформаційно-психологічне й інформаційно-пропагандистське забезпечення. Якісно новий підхід до ведення воєнних кампаній бачимо у гібридній війні РФ проти України, у якій ключовим моментом стала психологічна й інформаційна обробка місцевого населення, що надало Росії змогу здійснити анексію Криму» [13, с. 111].

Є. Мануйлов і Ю. Калиновський додають, що «інформаційна зброя особливо ефективно діє проти тієї країни, яка знаходиться у кризовому стані, у суспільній свідомості якої панує ціннісна амбівалентність, соціально-політична невизначеність. Застосування інформаційної зброї стає особливо ефективним, коли у державі спостерігається протистояння між політичними силами, наявною є криза моральної та правової свідомості, є слабкою патріотично налаштована еліта у всіх сферах суспільного життя» [8, с. 149].

Варто окреслити основні загрози інформаційному суверенітету держави та процесам демократичного державотворення, що несе у собі інформаційна зброя. Так, на думку О. Барни, такою загрозою національній безпеці є «відсутність державної ідеології, спільних ціннісних орієнтацій розвитку суспільства, чіткої соціально-економічної політики, критичне майнове розшарування суспільства, які призвели до поляризації світоглядних засад щодо перспектив розвитку Української держави й активізували споживацьку мотивацію політичної поведінки громадян» [2, с. 371]. А. Яфонкін і В. Шевчук вагомою загрозою вважають неконтрольованість соціальних мереж і віртуальних спільнот, оскільки «за допомогою соціальних мереж можна не тільки впливати на суспільну свідомість, збирати людей на масові акції та "кольорові революції", але й вербувати найманців у бандформування, планувати і координувати їх дії, організовувати теракти і диверсії, проводити масштабні операції, завдаючи ворожій державі неприйнятного збитку» [15, с. 467].

Більш детальне розкриття загроз національній безпеці України в інформаційній сфері подає У. Ільницька:

– прояви обмеження свободи слова та доступу до інформації;

– викривлення, спотворення, блокування, замовчування, упереджене та тенденційне висвітлення інформації;

– несанкціоноване її поширення;

– відкрита дезінформація;

– інформаційна експансія з боку інших держав і руйнівне інформаційне вторгнення у національний інформаційний простір;

– виникнення і функціонування у національному інформаційному просторі держави непідконтрольних інформаційних потоків;

– поширення засобами масової інформації культу насильства, жорстокості;

– повільність входження України у світовий інформаційний простір;

– невиваженість державної інформаційної політики та відсутність необхідної інфраструктури в інформаційній сфері;

– розміщення дезінформації в Інтернеті [4, с. 30].

Всі ці та інші проблеми України доволі активно використовує у гібридній війні проти нашої держави Російська Федерація. Причому, попри явну гібридну війну РФ проти України, анексію Криму й агресію на Донбасі, саме інформаційні операції визначаються відомим західним експертом безпекового сектору Бредом Перрі як найбільш ефективні. Б. Перрі визначає, що «контроль над ескалацією ситуації досягався завдяки активній тривалій проросійській пропаганді серед населення Південно-Східних регіонів України. Наслідками таких дій стали сприйняття населенням відповідного наративу і формування проросійської ініціативної більшості, яка стала основою для консолідації сепаратистів і підтримки інтервенції збройних формувань» [19].

Цю тезу у статті «Як Росія озброювала соціальні медіа в Криму» підтримує й інший американський аналітик Майкл Холловей, за даними якого уряд Російської Федерації витратив 19 млн доларів для фінансування діяльності 600 спеціально залучених дописувачів Facebook, Vkontakte, Odnoklassniki. Діяльність цих авторів полягала у публікації статей і коментарів до них з метою формування в українській і міжнародній суспільній думці враження про підтримку місцевим населенням анексії, дискредитації місцевої опозиції, поширення серед населення чуток, почуттів страху та ненависті. Причому швидкість поширення контенту становила 5 тис. репостів за добу. Крім того, у Криму російськими військами інформаційних операцій створювався інформаційний вакуум шляхом блокування урядових сайтів, здійснення кібератак на сайти ЗМІ. Результатом таких дій стало отримання суттєвих переваг у інформаційному просторі для спрощення дій з анексії півострова. Таким чином, анексія Криму послужила дослідним майданчиком для проведення інформаційних операцій проти інформаційної безпеки держави та продемонструвала, що соціальні інтернет-сервіси є ефективним інструментом управління суспільством [18].

Висновки. Таким чином, підсумовуючи проведене дослідження, можемо зробити висновок, що з формуванням глобального інформаційного простору до нього перемістилися й різноманітні політичні процеси міждержавної геополітичної боротьби, які у своїй найвищій критичній фази інформаційного протиборства набули рис феномену «гібридної війни». У сучасних умовах використання інформаційної зброї дедалі більше поширюється у практиці міжнародних відносин, оскільки надає можливість отримати інформаційну перевагу і домінування в інформаційному просторі світу. Загострюється необхідність активізації дій органів публічного врядування України в напрямку своєчасного виявлення й нейтралізації загроз і ризиків негативного впливу шкідливого контенту національного і світового інформаційного простору, забезпечення задоволення інформаційних потреб людини й суспільства, реалізації національних інтересів держави у глобальному інформаційному просторі та здійснення ефективного захисту національного інформаційного простору й інформаційного суверенітету держави. Особливо

важливим є протистояння проявам гібридної війни для України, що вимагає від нашої держави проведення відповідних заходів реагування, таких як:

– захист інформаційно-комунікативної командної інфраструктури комп'ютерних та інформаційних мереж і баз даних державного та військового управління;

– створення спеціальних підрозділів і служб системи захисту від несанкціонованого доступу до інформаційних ресурсів, хакерських атак;

– боротьба з фейками, поширенням тенденційного викривлення фактів, упередженим висвітленням проблем тощо;

– протиборство інформаційній експансії Російської Федерації та руйнівному інформаційному впливу інформаційної зброї РФ на національний інформаційний суверенітет України;

– формування стратегічної інформаційно-комунікативної політики України щодо запобігання, протидії та нейтралізації шкідливого інформаційно-психологічного впливу на суспільну свідомість на загальнодержавному, регіональному та місцевому рівнях;

– формування стратегічної політики України щодо покращення свого міжнародного іміджу в глобальному інформаційному просторі світу;

– проведення заходів інформаційної просвіти населення формування у суспільстві демократичної інформаційно-комунікативної культури, здатності розбиратися у достовірності інформації тощо.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. 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.

2. Барна О.С. Інформаційний простір України як чинник суспільної консолідації в умовах гібридної війни. *Держава і право. Юридичні і політичні науки.* 2019. Вип. 86. С. 365–376.

3. Запорожець С.А. Стан забезпечення інформаційної безпеки України у воєнній сфері в умовах гібридної війни. *Politology bulletin*. 2019. Iss. 83. С. 16–25.

4. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Humanitarian vision.* 2016. № 2 (1). С. 27–32.

5. Калініченко Б. Визначальні напрями формування стратегії протистояння інформаційній війні. *Держава і право. Серія : Політичні науки.* 2019. Вип. 83. С. 61–73.

6. Кріслата О. Гібридна війна та її інформаційна складова. *Збірник праць Науково-дослідного інституту пресознавства*. 2018. Вип. 8. С. 190–199.

7. Левантович О. Гібридні війни XXI століття: нові виклики для медіапростору. *Вісник Львівського університету. Серія Журналістика*. 2019. Вип. 45. С. 52–59.

8. Мануйлов Є.М., Калиновський Ю.Ю. Аксіологічний вимір інформаційної безпеки української держави. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія : Філософія, філософія права, політологія, соціологія.* 2017. № 3. С. 13–30.

9. Національна безпека в умовах інформаційних та гібридних війн : монографія / В.С. Куйбіда та ін. ; за заг. ред. В. Куйбіди і В. Бебика. Нац. акад. держ. упр. при Президентові України. Київ : НАДУ, 2019. 380 с.

10. Парфенюк І. Інструментарій інформаційних війн: традиційні та новітні засоби. *Вісник Книжкової палати.* 2019. № 1. С. 7–10.

11. Радковець Ю.І. Ознаки технологій «гібридної війни» в агресивних діях Росії проти України. *Наука і оборона.* 2014. № 3. С. 36–42.

12. Україна медійна : на порозі інформаційної революції : монографія / О. Бухтатий, О. Радченко, Г. Головченко ; за наук. ред. Радченка О.В. Київ : Видавець СВС Панасенко, 2015. 208 с.

13. Туранський М.О. Інформаційно-психологічні операції в гібридній війні: історіографічний аспект. *Вісник Черкаського університету. Серія : Історичні науки.* 2018. № 1. С. 111–121.

14. 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.

15. Яфонкін А.О., Шевчук В.А. 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. Perry Bret. Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations. *Small Wars Journal.* 2015. Vol. 11, № 8. URL: http://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-andspecial-opera11352.html

20. Ventre Daniel. Information Warfare. John Wiley & Sons, 2016. 352 p.

REFERENCES:

1. Bogdanovich V., Vorovich B., Marko E. (2018). Informatsiyna bezpeka yak osnova voyennoyi bezpeky derzhavy ta suspil'stva [Information security as the basis of military security of the state and society]. *Zbirnyk naukovykh prats' Tsentru voyenno-stratehichnykh doslidzhen' Natsional'noho universytetu oborony Ukrayiny imeni Ivana Chernyakhovs'koho*, Vol.3, 44–48 [In Ukraine].

2. Barna O.S. (2019). Informatsiynyy prostir Ukrayiny yak chynnyk suspil'noyi konsolidatsiyi v umovakh hibrydnoyi viyny [Information space of Ukraine as a factor of social consolidation in the conditions of hybrid war]. *Derzhava i pravo. Yurydychni i politychni nauky*. Vol. 86. Pp. 365–376. [In Ukraine].

3. Zaporozhets S.A. (2019). Stan zabezpechennya informatsiynoyi bezpeky Ukrayiny u voyenniy sferi v umovakh hibrydnoyi viyny [The state of information security of Ukraine in the military sphere in a hybrid war]. *Politology bulletin*, Iss. 83, 16–25 [In Ukraine].

4. Ilnytska U. (2016). Informatsiyna bezpeka Ukrayiny: suchasni vyklyky, zahrozy ta mekhanizmy protydiyi nehatyvnym informatsiyno-psykholohichnym vplyvam [Information security of Ukraine: modern challenges, threats and mechanisms for counteracting negative information and psychological influences]. *Humanitarian vision*, Vol. 2 (1), 27–32 [In Ukraine].

5. 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*, Vol. 83, 61–73 [In Ukraine].

6. Krislata O. (2018). Hibrydna viyna ta yiyi informatsiyna skladova [Hybrid war and its information component]. *Zbirnyk prats' Naukovo-doslidnoho instytutu presoznavstva*, Vol. 8, 190–199 In Ukraine.

7. Levantovych O. (2019). Hibrydni viyny XXI stolittya: novi vyklyky dlya mediaprostoru [21st Century Hybrid Wars: New Challenges for the Media Space]. *Visnyk L'vivs'koho universytetu. Seriya Zhurnalistyka*, Vol. 45, 52–59 [In Ukraine].

8. Manuilov E., Kalinovsky Y. (2017). Aksiolohichnyy vymir informatsiynoyi bezpeky ukrayins'koyi derzhavy [Axiological dimension of information security of the Ukrainian state]. *Visnyk Natsional'noho universytetu "Yurydychna akademiya Ukrayiny imeni Yaroslava Mudroho". Seriya : Filosofiya, filosofiya prava, politolohiya, sotsiolohiya*, Vol. 3, 13–30 [In Ukraine].

9. Kuybida V., Bebyk V. ta in. (2019). Natsional'na bezpeka v umovakh informatsiynykh ta hibrydnykh viyn [National security in terms of information and hybrid wars] : monohrafiya. Kyyiv : NADU, 2019. 380 p. [In Ukraine].

10. Parfenyuk I. (2019). Instrumentariy informatsiynykh viyn: tradytsiyni ta novitni zasoby [Tools of information warfare: traditional and modern tools]. *Visnyk Knyzhkovoyi palaty*, Vol. 1, 7–10 [In Ukraine].

11. Radkovets Y.I. (2014). Oznaky tekhnolohiy "hibrydnoyi viyny" v ahresyvnykh diyakh Rosiyi proty Ukrayiny [Signs of "hybrid war" technologies in Russia's aggressive actions against Ukraine]. *Nauka i oborona*, Vol. 3, 36–42 [In Ukraine].

12. Buhtatiy O., Radchenko O., Golovchenko G. (2015). Ukrayina mediyna : na porozi informatsiynoyi revolyutsiyi [Media Ukraine: on the threshold of the information revolution]: monograph. Kyiv: Publisher SVS Panasenko, 208 p. [In Ukraine].

13. Turansky M. O. (2018). Informatsiyno-psykholohichni operatsiyi v hibrydniy viyni: istoriohrafichnyy aspekt [Information-psychological operations in hybrid warfare: historiographical aspect]. *Visnyk Cherkas'koho universytetu. Seriya : Istorychni nauky*, Vol. 1, 111–121 [In Ukraine].

14. 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* T. 30 (69), Vol. 3, 29–35 [In Ukraine].

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*, Vol. 5, 466–472 In Ukraine.

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. *Real Clear Media Group Newsletters.* May 10, 2017. URL: https://www.realcleardefense.com/articles/2017/05/10/how_russia_weaponized_social_media_in_crimea_1

19. Perry Bret. (2015). Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations. *Small Wars Journal.* Vol. 11, № 8. URL: http://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-andspecial-opera11352.html

20. Ventre Daniel. (2016). Information Warfare. John Wiley & Sons, 352 p.