ІНФОРМАЦІЙНА ВІЙНА ЯК КЛЮЧОВА ЗАГРОЗА ДЕМОКРАТИЧНОМУ ДЕРЖАВОТВОРЕННЮ УКРАЇНИ

Державно-управлінські студії № 10, 2019

УДК 35.078.1:001.102-049.5:316.32

Я. І. Чмир,
аспірант кафедри публічного адміністрування
Міжрегіональної академії управління персоналом

ІНФОРМАЦІЙНА ВІЙНА ЯК КЛЮЧОВА ЗАГРОЗА ДЕМОКРАТИЧНОМУ ДЕРЖАВОТВОРЕННЮ УКРАЇНИ

Ya. Chmyr,
graduate student of the Department of Public Administration
of the Interregional Academy of Personnel Management

INFORMATION WARFARE AS A KEY THREAT TO DEMOCRATIC STATE FORMATION OF UKRAINE

Анотація. *Стаття досліджує проблематику забезпечення інформаційної безпеки та національного суверенітету держави внаслідок розгортання інформаційних воєн. 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, що здатні завдати шкоду національним інтересам держави, сталому розвитку суспільства, благополуччю й здоров'ю кожного громадянина. З огляду на широкомасштабну інформаційну війну проти України та неминучість подальшого зростання загроз в сфері інформаційної безпеки обґрунтовується комплексна модель системи забезпечення інформаційної безпеки держави. Робиться висновок про необхідність активізації дій органів публічного врядування України в напрямку своєчасного виявлення й нейтралізації загроз та ризиків негативного впливу шкідливого контенту національного і світового інформаційного простору, забезпечення задоволення інформаційних потреб людини й суспільства, реалізації національних інтересів держави в глобальному інформаційному просторі та здійснення ефективного захисту національного інформаційного простору та інформаційного суверенітету держави.*

Abstract. *The article explores the issue of information security and national sovereignty of the state as a result of the deployment of information wars. 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.*

Given the large-scale information war against Ukraine and the inevitability of further growth of threats in the field of information security, a comprehensive model of the information 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 global information space, meeting the information needs of man and society, realization of national interests in the global information space. information space and information sovereignty of the state.

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

Keywords: *State, Information Warfare, Information Security, Information Sovereignty*

Постановка проблеми. Перехід людства до епохи інформаційного суспільства характеризується тим, що відбувається поступове переміщення в інформаційне середовище більшості геополітичних процесів та відносин між державами, народами чи окремими інституціями й людьми. В умовах, коли ядерні держави накопичили потенціал смертоносної зброї, здатний знищити саме людство й зруйнувати власну планету, міждержавна геополітична боротьба – дипломатична, політична, економічна, військова тощо – все 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 та інформаційні технології все більше перетворюються на головну зброю у міждержавному протиборстві, що спричинило появу й надзвичайно швидкий розвиток такого суспільно-політичного феномену як інформаційні війни. Рівень оволодіння інформаційно-комунікативними технологіями вже є визначальним чинником рівня розвитку будь-якої держави, й саме розуміння інформації як особливого виду зброї закріплена в 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, тощо описує, скільки потужних країн використовували інформаційну зброю та зловживали інформацією для дестабілізації політичного ладу й поширення негативних меседжів про ворожі нації та їх лідерів [16, с. 11].

Аналіз останніх досліджень і публікацій дає підстави стверджувати, що у вітчизняному науковому дискурсі все активніше піднімається проблематика забезпечення інформаційного суверенітету держави в умовах розгортання інформаційних воєн, формування та розвитку системи інформаційної безпеки як важливої складової національної безпеки країни в цілому. Зокрема, плідно працюють в зазначеному напрямку такі науковці як В. Богданович, Б. Ворович та Є. Марко [1], І. Боднар [2], З. Бржевська [3], У. Ільницька [4], Б. Калініченко [5], О.Курбан [6], Є. Мануйлов та Ю. Калиновський [8], І. Михальченко [9], І. Парфенюк [10], С. Стародуб [11], О. Бухтатий, О. Радченко та Г. Головченко

[12], А. Фісун [13], В. Шемчук [14], А. Яфонкін та В. Шевчук [15]. Водночас, все ще недостатнім є виявлення форм і чинників впливу інформаційної війни на стан і перебіг демократичних державотворчих процесів, особливості становлення системи національної безпеки держави в сучасних умовах, що й обумовлює формування ***мети статі та постановки завдання*** даного дослідження.

Виклад основного матеріалу. З входженням людства у постіндустріальну епоху роль інформаційних впливів на перебіг воєнних та політичних подій у світі тільки зростає. Глобальний інформаційний простір стає основним середовищем міжособистісних, групових та міжнародних контактів та основним місцем зіткнення національних інтересів і – як наслідок – полем битви за інформаційний суверенітет, за краще геополітичне місце країни в глобальному інформаційному суспільстві. З таких умов "поняття “мирний і воєнний стан” переплелося у віртуальному просторі, породивши страшне явище “інформаційна 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 в цілому. Поняття миру стало хитким, нестійким і концептуально розмитим, оскільки війни, крім реальних військових дій, які, на жаль, ще мають місце в суспільстві, перемістилися також у віртуальний простір, “військові” дії та події, відбуваються баталії за панування над масами і їх свідомістю. Основною зброєю в цій війні стають інформаційні та комунікаційні технології" [1, с. 45–46].

Існують різні підходи до визначення сутності та мети інформаційної війни. Сучасні дослідники і науковці вкладають у ці поняття різні сенси, зокрема визначаючи сутність і мету інформаційної 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 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 (Дж. Деріан [17, с. 46]);

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

– 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 (С. Стародуб [11,

с. 1128

– контроль інформаційного простору і забезпечення захисту своєї інформації від ворожих дій; використання контролю над інформаційним простором для проведення інформаційних атак на противника; підвищення загальної ефективності збройних інформаційних функцій (З. Бржевська [3, с. 90]);

– комплексний, відкритий чи прихований цілеспрямований інформаційний вплив 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 (А. Фісун [13, с. 538]);

– цілісна технологія, спрямована на досягнення гуманітарного поневолення одних груп людей іншими яка є продуктом постіндустріального суспільства і обумовлена неможливістю глобальних збройних конфліктів, які можуть знищити планету (І. Михальченко [9, с. 14–15]);

– 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 (О. Курбан [6, с. 96]);

– 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]);

– 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 (В. Шемчук [14, с. 33]).

Таким чином можемо зробити узагальнюючий висновок, що інформаційна війна являє собою 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 й задля її інформаційного

поневолення.

Оскільки будь-який процес або суспільне явище в системному вимірі завжди має свої суб'єкти та об'єкти, визначимо останніх для випадку інформаційної війни. Так, з урахуванням наведених в даному підрозділі наукових підходів, до основних суб'єктів інформаційної війни слід віднести:

− держави та їх інституції (серед світових держав беззаперечними лідерами в розробці та використанні інструментарію інформаційних воєн є Сполучені Штати Америки, Китай та Росія);

− міждержавні утворення, військово-політичні й оборонні союзи;

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

− віртуальні соціальні спільноти й 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 та 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 та особистісна свідомість громадян;

− національні цінності та національний менталітет;

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

− система підготовки та ухвалення публічно-управлінських рішень в політичній, економічній, безпековій сферах життєдіяльності держави;

− політична та адміністративна культура державно-управлінської еліти;

− інформаційна та інформаційно-комунікаційна інфраструктура держави;

− інституції національної оборони та безпеки, їх керівники та співробітники;

− інституції публічного врядування держави, їх керівники та службовці;

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

Як правило, інформаційну війну пов'язують, насамперед, з проведенням інформаційно-психологічних операцій та застосуванням різного роду інформаційної та інформаційно-психологічної зброї. Так, А. Манойло, А. Петренко та Д. Фролов підкреслюють, що "інформаційна війна – політична боротьба, виражена в формі інформаційно-психологічних операцій із

застосуванням інформаційної зброї і виступає неодмінним атрибутом політичного керівництва задля посилення зовнішньо- і внутрішньодержавних протирічь, проявів конфронтації з заданим рівнем інтенсивності і в свідомо певному організатором напрямку" [7, с. 81]. Є. Мануйлов та 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 в собі інформаційна зброя. Так, на думку І. Боднар головна інформаційна загроза 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 [2, с. 69]. А. Яфонкін та В. Шевчук вагомою загрозою вважають неконтрольованість соціальних мереж та віртуальних спільнот, оскільки "за допомогою соціальних мереж можна 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" [15, с. 467].

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

– 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 та 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 інформаційній війні проти нашої держави Російська Федерація. Причому попри явну гібридну війну РФ проти України, анексію Криму та 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 нарративу і формування проросійської ініціативної більшості, яка стала основою для консолідації сепаратистів та 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 мільйонів 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 та міжнародній суспільній думці враження про підтримку місцевим населенням анексії, дискредитації місцевої опозиції, поширення серед населення чуток, почуттів страху й ненависті. Причому швидкість поширення контенту складала 5 тисяч 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 і 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, що у своїй найвищій критичній фази інформаційного протиборства набули рис феномену "інформаційної війни". В сучасних умовах використання інформаційної зброї все більше поширюється в практиці міжнародних відносин, оскільки надає можливість отримати інформаційну перевагу і домінування в інформаційному просторі світу. Відтак загострюється необхідність активізації дій органів публічного врядування України в напрямку своєчасного виявлення й нейтралізації загроз та ризиків негативного впливу шкідливого контенту національного і світового інформаційного простору, забезпечення задоволення інформаційних потреб людини й суспільства, реалізації національних інтересів держави в глобальному інформаційному просторі та здійснення ефективного захисту національного інформаційного простору та інформаційного суверенітету держави. Особливо важливим є протистояння

проявам інформаційної війни для України, що вимагає від нашої держави проведення відповідних заходів реагування, зокрема:

– 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 існуючих 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 в суспільстві демократичної інформаційно-комунікативної культури, здатності розбиратися в достовірності інформації тощо.

Список використаних джерел:

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. Боднар І. Інформаційна безпека як основа національної безпеки. *Mechanism of Economic Regulation*. 2014. № 1. С. 68-75.

3. Бржевська З., Довженко Н., Киричок Р., Гайдур Г., Аносов А. Інформаційні війни: проблеми, загрози та протидія. *Кібербезпека: освіта, наука, техніка*. 2019. № 3. С. 88-96.

4. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Humanitarian vision*, 2016. 2(1), 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. Курбан О. Теорія інформаційної війни: базові основи, методологія та понятійний апарат. *Scientific Journal «ScienceRise»*. 2015. №11/1(16). С. 95 – 100.

7. Манойло А. Петренко А., Фролов Д. Государственная информационная

политика в условиях информационно-психологической войны. 3-е изд. Москва: Горячая линия–Телеком, 2018. 541 с.

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. Михальченко И. А. Информационные войны на рубеже XXI века. *Безопасность информационных технологий*. 1998. № 3. С. 14-15.

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

11. Стародуб С. Інформаційні війни та системи захисту в умовах глобалізаційних процесів. *Держава та регіони. Серія : Соціальні комунікації*. 2018. № 3. С. 27-31.

12. Україна медійна : на порозі інформаційної революції : моногр. [Олександр Бухтатий, Олександр Радченко, Гліб Головченко; За науковою редакцією д. держ. упр., проф. Радченка О. В.]. Київ: Видавець СВС Панасенко, 2015. 208 с.

13. Фісун А. Ґенеза поняття «інформаційна війна». *Гілея*. 2011. № 49. С. 534–538.

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, No.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 Chernyakhovskoho. Vol.3. Pp. 44-48. In Ukraine.

2. Bodnar I. (2014). Informatsiyna bezpeka yak osnova natsional′noyi bezpeky [Information security as a basis of national security]. *Mechanism of Economic Regulation*. Vol.1. Pp. 68-75. In Ukraine.

3. 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*. Vol.3. Pp. 88-96. 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), Pp. 27–32. In Ukraine.

5. Kalinichenko B. (2019). Vyznachalni 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. Pp. 61-73. In Ukraine.

6. 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). Pp. 95 – 100. In Ukraine.

7. Manoilo A. Petrenko A., Frolov D. (2018). Gosudarstvennaya informatsion-naya politika v usloviyakh informatsionno-psikhologicheskoy voyny [State information policy in the conditions of information-psychological war]. 3rd ed. Moscow: Telecom Hotline, 541 p. in Russian.

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

9. Mikhalchenko I.A. (1998). Informatsionnyye voyny na rubezhe XXI veka [Information warfare at the turn of the XXI century]. *Bezopasnost' informatsionnykh tekhnologiy*. Vol.3. Pp. 14-15. in Russian.

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

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.* Vol.3. Pp. 27-31. 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. Fisun A. (2011). Geneza ponyattya «informatsiyna viyna» [Genesis of the concept of "information warfare "]. *Hileya*. Vol.49. Pp. 534–538. 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]. *Kontseptual'ni pidkhody do rozuminnya informatsiynoyi viyny v suchasnomu sviti*. T. 30(69), Vol.3. Pp. 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. Pp. 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. *RealClear Media Group Newsletters.* May 10, 2017. URL: https://www.Realclearde-fense. 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.