УДК 324(477):659.4
Андрій Нофенко,
аспірант кафедри політології,
Миколаївський національний університет ім. В. О. Сухомлинського
54030, м. Миколаїв, вул. Нікольська, 24, каб. 317,
https://orcid.org/0000-0002-2558-4749
nofenko@hotmail.com

ГІБРИДНА ВІЙНА РОСІЇ ПРОТИ УКРАЇНИ: ІНФОРМАЦІЙНИЙ НАСТУП ТА МЕХАНІЗМИ ПРОТИДІЇ

У статті детально розглянуто проблему інформаційної війни Росії проти Україні. Розкрито суть інформаційної війни, її трактування в межах різних підходів. На основі використання історичного, системного та структурно-функціональних методів з'ясовано основні недоліки інформаційної сфери України; виокремлено головні механізми її захисту. Серед механізмів протидії інформаційній війні Росії проти України виокремлено дві групи – нормативно-правові та інституційні. До першої групи відносяться законодавчі акти України, серед яких провідну роль у протидії інформаційній агресії Росії відіграє Доктрина інформаційної безпеки України. Серед другої групи механізмів виділяються державні й недержавні інституції, діяльність яких спрямовано на формування та реалізацію інформаційної безпеки України, а також міжнародні структури, діяльність яких націлено на нейтралізацію інформаційного впливу з боку Росії. Серед вітчизняних інституційних механізмів протидії російському інформаційному наступу важливе місце відведено Міністерству інформаційної політики України, Раді національної безпеки та оборони України, кіберполіції й ін.

Значну увагу звернуто на такі механізми протидії інформаційній війні Росії проти України, як заборона російських сайтів та соціальних мереж, а також запровадження квот на українську мову у мас-медіа. Зазначено, що дії України щодо нейтралізації інформаційних загроз з боку Росії потрібно здійснювати на різних рівнях – геополітичному, ресурсному, громадськості.

У ході проведеного дослідження сформовано рекомендації щодо протистояння інформаційній війні. Проведено аналіз факторів інформаційних впливів і протидії інформаційній зброї, у результаті чого вказано низку можливих дій для реалізації протидії російській інформаційній ескалації в Україні з метою створення гідної й адекватної відповіді на інформаційні виклики сучасності.

Зараз уже зрозуміло, що інформаційна боротьба стає тим фактором, що впливає на саму війну, її початок, хід і результат. Це підтверджується агресією Росії проти України. Тому досить актуальною проблемою безпеки України є розробка концепції захисту системи інформаційно-аналітичного забезпечення завдань інформаційної боротьби.

Ключові слова: *гібридна війна, російсько-українська війна, інформаційна війна, інформаційна безпека, інформаційна стратегія.*

1. ВСТУП

Постановка проблеми. Після Революції гідності, яка продемонструвала всьому світові бажання українців жити в демократичній європейській державі,

Україна стала жертвою російської збройної агресії, унаслідок чого відбулася анексія Криму та розпочалися військові дії на Донбасі, які тривають і досі. Учені характеризують діяльність Російської Федерації проти України як гібридну війну, що передбачає поєднання традиційних і нетрадиційних методів агресії, складність агресивних дій у багатьох сферах суспільного життя.

Інформація є однією зі складових частин російської агресії проти України, що дає змогу говорити про існування інформаційної війни між Україною й Росією. Це стосується активного поширення негативної, часто неправдивої чи спотвореної інформації про Україну з боку Російської Федерації для дискредитації нашої держави, кібератаки, пропаганди російських цінностей серед населення України тощо. Ця ситуація загрожує суверенітету та національній безпеці України, а також створює умови, у яких потрібна розробка механізмів протидії загрозам національній безпеці нашої країни загалом й інформаційній безпеці, зокрема.

Актуальність обраної проблеми для аналізу зумовлена також недостатнім рівнем наукового аналізу інформаційної війни як явища, властивого сучасним міжнародним відносинам. Досі не існує єдиного послідовного тлумачення поняття «інформаційна війна», її особливостей, структури й механізмів протидії в політичній науці. Більше того, дослідження інформаційної війни, як правило, проводяться на рівні журналістики чи політичної аналітики, що вимагає більш ретельного наукового вивчення сутності цього явища та розробки механізмів протидії російській інформаційній війні проти України на сучасному етапі.

Аналіз останніх досліджень і публікацій. Питаннями російської інформаційної війни проти України цікавляться такі вітчизняні дослідники, як С. Демедюк, Н. Еляшевська, І. Лубкович, М. Сенченко. Такі іноземні вчені, як П. Дібб, М. Кофман, Х. Лемб і С. Расторгуєв, вивчають, аналізують та комплексно досліджують проблему інформаційної війни.

Згадані науковці аналізують суть й особливості інформаційної війни як явища, яке включає інформаційну війну Росії проти України; вивчають загрози, котрі вона несе як для України, так і для світової спільноти. Водночас недостатньо уваги приділено дослідженню та розробці механізмів протидії російській інформаційній війні на сучасному етапі. Відсутність усебічного вивчення російської інформаційної війни проти України, а також те, що агресія Росії проти нашої країни в інформаційній сфері триває й набуває нових форм, потребує більш ретельного вивчення в цій галузі.

Формулювання цілей статті. Мета роботи – проведення політичного аналізу російської інформаційної війни проти України та механізмів її протидії на сучасному етапі. На сьогодні вчені не сформували єдиної думки щодо науково-теоретичної концепції інформаційних воєн, а також щодо основних форм і методів їх ведення. Також зазначимо, що інформаційна війна – це неоднозначне поняття. Тому можна говорити про широке й вузьке значення цього терміна. Загалом інформаційну війну розуміємо як будь-який негативний інформаційний вплив на ворога. Суперником може бути будь-який суб’єкт:

фізична особа або група осіб, юридичні особи чи держава. Учасники таких воєн можуть діяти окремо або групами, спонтанно чи за домовленістю.

У вузькому розумінні інформаційна війна – це новий тип або метод збройного конфлікту, що не підлягає міжнародно-правовій кваліфікації. Однак серед науковців немає єдиної думки, оскільки більшість із них вважає, що інформаційна війна не може розглядатися як збройний конфлікт. Це тому, що хоча інформація діє як зброя, проте вона може перемогти ворога, не втрачаючи людських життів і без кровопролиття [7].

Загалом, найширшим та найповнішим визначенням інформаційної війни є таке: інформаційна війна – це відкритий або прихований цілеспрямований інформаційний вплив систем одна на одну для отримання певного виграшу в політичній, економічній чи ідеологічній сферах [3].

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Сьогодні для України під час інформаційного протистояння з Російською Федерацією захист власного інформаційного простору та національної інформаційної безпеки є однією з найважливіших цілей державного управління, а також першим кроком до формування позитивного іміджу держави на світовій арені, успішної європейської інтеграції й розвитку самодостатньої, національної самоідентичності.

Велика російська інформаційна війна проти України вийшла на новий етап на початку 2014 р., коли відбулися такі події, як Революція гідності, анексія Криму та початок війни на Сході України. У ході цього протистояння ми побачили, по-перше, усі вразливі сфери України в галузі інформаційної безпеки; по-друге – недостатню ефективність механізмів захисту інформації; по-третє – небажання несподіваних і непередбачуваних інформаційних контрзаходів.

Безперечно, український інформаційний сектор має багато недоліків у протидії інформаційній війні. Для визначення ефективності механізмів, які Україна використовує для протидії Росії в інформаційному просторі, ці негативні аспекти потрібно дослідити більш детально. За словами українського вченого І. Лубковича, вони включають: 1) непрацездатність – на рівні реакції на конкретну дезінформацію й інформацію, що надається російськими медіа-мережами, а також на рівні надання власних деталей про події і явища; 2) сила та обізнаність. Сила – це засіб ведення інформаційної війни, а обізнаність – ефективність їх застосування; 3) відсутність інформації проти державних органів; 4) фінанси означають, що більшість засобів масової інформації не відмовляються від трансляції російських телепередач, телесеріалів, фільмів через фінансову ситуацію й небажання втрачати гроші [2].

Загалом, механізми захисту інформаційної безпеки України можна розділити на дві групи – законодавчі та інституційні. Розглядаючи законодавчі механізми, зазначимо, що в Україні розроблено достатню кількість правових документів стосовно інформації й інформаційного простору з часів

незалежності. Серед них – такі закони, як «Про інформацію», «Про інформаційні агентства», «Про Концепцію національної програми інформатизації», «Про захист інформації в інформаційно-комунікаційних системах», «Про пресу в Україні» та ін.

Нещодавно введено в дію Доктрину інформаційної безпеки України – один із законодавчих документів, що стосуються інформаційної безпеки України. Екс-президент України П. Порошенко затвердив його 25 лютого 2017 р. після затвердження Радою національної безпеки та оборони в грудні 2016 р.

Наступний тип механізмів забезпечення інформаційної безпеки – інституціональні механізми, що охоплюють державні та недержавні установи, діяльність яких спрямовано на формування та реалізацію інформаційної безпеки. Сьогодні до предметів формування й реалізації політики в інформаційній сфері в нашій країні належать Рада національної безпеки і оборони України, Міністерство інформаційної політики України, Міністерство закордонних справ, Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації, Департамет кіберполіції національної поліції України.

Розглядаючи механізми протидії російській інформаційній війні, також звертаємо увагу на указ екс-президента України П. Порошенка про заборону російських соціальних мереж і сайтів, який набув чинності 17 травня 2017 р.

Думки щодо заборони російських сайтів та соціальних мереж розділили науковців й аналітиків на тих, хто негативно відреагував на заборону, і тих, хто вважає цю заборону великим успіхом України в протидії російській інформаційній війні. Також важливою є реакція міжнародних акторів на указ екс-президента. Наприклад, Генеральний секретар Ради Європи Турбйорн Ягланд висловив стурбованість рішенням, пояснивши, що ця заборона протистоїть свободі вираження поглядів і свободі ЗМІ. Таку саму позицію має Таня Купер, представниця Human Rights Watch, яка прирівнює указ Президента України до бажання контролювати політичний дискурс у країні зі свого боку. Усупереч цим позиціям, Генеральний секретар Північноатлантичного альянсу Єнс Столтенберг зазначив, що блокування українським урядом соціальних мереж і сайтів Росії – це питання виняткового національної безпеки держави, а не свободи слова в ньому.

Потрібно також звернути увагу на закон про введення квот на українську мову на телебаченні, який підписаний Президентом України 6 червня 2014 р. Відповідно до цього нормативного акта, частка різних програм, передач, фільмів – українською мовою має бути не менше ніж 75 % на телебаченні. Зазначимо, що заборона російських соціальних мереж і сайтів, а також цитування української мови на телебаченні – це певні кроки до ізоляції України від Росії. Ці дії керівництва нашої держави показують не лише Росії, а й усьому світові те, що Україна є незалежною державою з єдиною державною мовою. Однак ці рішення мають і конкретні негативні сторони. Міжнародна спільнота може вважати заборону російських соціальних мереж і сайтів точним показником недемократичності нашої держави. Зі свого боку, цитування

української мови на телебаченні не лише створює вигляд дискримінації російськомовного населення в Україні, у якому Російська Федерація переконує весь світ, але й провокує державу-агресора на виконання певних дій у відповідь.

Також зазначимо, що, крім законодавчих механізмів, недержавні суб'єкти в Україні також беруть активну участь у протидії інформаційній війні з боку Російської Федерації. До структур неурядового сектору відносимо, насамперед, міжнародні організації, такі як ООН та її спеціалізовані агенції, а також ОБСЄ, Рада Європи й ін., а також вітчизняні організації громадянського суспільства, які активно протидіють інформаційній війні Росії проти України.

Розглянувши механізми забезпечення інформаційної безпеки та протидії інформаційним загрозам України, акцентуємо увагу на тому, що з 2014 р. Україна почала робити конкретні кроки для вдосконалення й забезпечення ефективності цих механізмів. Затвердження Доктрини інформаційної безпеки України у 2017 р. дало поштовх до систематизації повноважень державних органів у сфері інформаційної політики та відповідальності за їх недотримання. Інституційні механізми розширилися з 2014 р. завдяки Міністерству інформаційної політики України та кіберполіції. Однак цього в сучасному глобалізованому інформаційному суспільстві явно недостатньо. Саме тому Україні потрібно проаналізувати, розробити, створити й оновити механізми протидії російській інформаційній війні та захисту її інформаційної безпеки.

Російська агресія в Україні аж ніяк не завершена. Більше того, вона перебуває в процесі ескалації. Росія щодня накопичує свої сили, удосконалює свої навички та застосовує нові технології й методи, щоб завдавати інформаційний удар знову та знову. Отже, російська інформаційна війна розвиватиметься й, імовірно, буде посилена шляхом використання дедалі ефективнішої тактики. Не можна сказати, що Україна вже програла цю війну, але для запобігання їй потрібно ще багато зробити. Безперечно, в Україні вже існує чимало нааявних механізмів протидії інформаційній війні, але їх потрібно вдосконалити, розвинути та зробити ефективнішими.

Відсутність достатніх державних інструментів для ведення інформаційної війни є актуальним питанням війни з Росією. Український учений М. Сенченко зазначає, що Україні для ефективного протистояння інформаційній війні з боку Росії потрібно мати хоча б: 1) ефективну систему ведення інформаційної війни; 2) ефективну концепцію інформаційної війни; 3) стратегію ведення інформаційної війни [4].

Стратегія інформаційної війни України повинна містити оборонну й наступальну політику. Щодо першого компонента, то він стосується дій, спрямованих на фізичний і психологічний захист населення, військ, уряду, інформаційної інфраструктури та супутників у космосі. Оборонна політика повинна включати організацію діяльності структури формування оборонних систем і співпрацю з іншими державами задля протидії інформаційній війні; оперативну протидію діяльності, впливам та проявам інформаційно-політичної агресії, операцій інформаційно-психологічної війни; приведення засобів

масової інформації й асоціацій віртуальних громад до готовності ефективно протидіяти та реагувати на інформаційну агресію.

В умовах, коли держава веде відкриту агресію та інформаційну війну, як наприклад Російська Федерація, украй важлива оперативна здатність реагувати на різні типи інформаційних атак і загроз, які постійно наступають на Україну з боку північно-східного сусіда.

Дії держави у вищезазначених умовах можна розділити на три рівні: перший – геополітичний, або вплив на інформаційного агресора та обмеження інтенсивності й сили його нападу; другий – умова, що включає захист цілісності, ефективності та спроможності системи управління, інформаційної інфраструктури, інформаційних ресурсів; третій – громадський, який спрямований на захист стабільності та послідовності розвитку суспільно-політичних відносин, свідомості громадян.

Інструменти інформаційної політики першого рівня повинні включати: 1) залучення світової спільноти й світової громадської думки для виявлення агресора та його руйнівних наслідків; 2) інформування світової спільноти про атаки противника й об'єктивний стан у власній країні; 3) посилення контрпропаганди, національного інформаційного простору, формування оперативних інформаційних центрів; 4) заборону на засоби масової інформації на своїй території, що належать до інформаційного простору агресора, із метою уникнення пропагандистського й руйнівного впливу на громадян; 5) підтримку стабільного статусу держави, позитивного іміджу України та характеру стабільної держави; 6) співпрацю й обмін досвідом із міжнародними організаціями щодо протидії кібератакам та інформаційним загрозам [6].

Другий рівень, зі свого боку, досить обширний і поєднує систему державного управління та національну інформаційну інфраструктуру, загальну обороноздатність країни, її спроможність протистояти агресивним атакам і підтримувати інформаційну, територіальну, економічну, соціально-політичну, культурну цілісність держави. Основні механізми інформаційної політики повинні включати: 1) створення координаційного органу, центру прийняття рішень, управління інформаційною політикою та безпекою, створення єдиної ефективної системи з вертикальною лінією органів та інститутів; 2) підготовку фахівців у галузі інформаційної війни й реалізацію державної інформаційної стратегії: політологи, аналітики, спеціалісти з інформаційних технологій, інформаційно-психологічної безпеки, практичні психологи щодо допомоги жертвам інформаційної агресії; 3) навчання державних службовців принципів та методів захисту інформації, інформаційної грамотності й основ інформаційної безпеки, психологічного захисту свідомості та зміцнення «інформаційного імунітету»; 4) створення спеціалізованого органу з питань кібербезпеки й протидії хакерським атакам із залученням фахівців з інформаційних технологій; 5) управління та контроль внутрішнього й постійний аналіз зовнішніх інформаційних полів; удосконалення інституціонального складника моніторингу інформації та консолідації законодавства відповідної діяльності, а також відповідальності за дії в цій

галузі; 6) створення єдиного науково-інформаційного центру для обробки новин на визначений період для виявлення джерел інформації, ринку новин і державних джерел розвідки противника; посилення інформаційних ресурсів політичних організацій; 7) підвищення юридичної відповідальності засобів масової інформації за поширення руйнівної інформації, агресивних закликів, кола ворожих ідей тощо; 8) інформаційно-психологічний захист військового командування й армії від пропаганди деморалізації; методи навчання захисту інформації, принципи наступальних та оборонних дій у відповідь на інформаційну війну, особливості використання інформаційної зброї [6].

Щодо третього рівня – рівня громадськості, то тут важливою є діяльність, спрямована на підтримку стабільності суспільно-політичного розвитку, консолідації й психологічної безпеки громадян та масової свідомості взагалі. Тому серед механізмів третього рівня політичної опозиції держави відзначимо: 1) надання громадянам необхідної інформації, інформування громадськості про інформаційну небезпеку й інформаційну зброю, як технічну, так і психологічну; 2) розвиток незалежних соціальних медіа; 3) залучення віртуальних громадських об'єднань та засобів масової інформації до захисту національного інформаційного простору, створення віртуальної системи колективної безпеки й зменшення соціальної напруги; 4) захист духовного потенціалу суспільства від нав'язування ворожих цінностей, підвищення стійкості свідомості дітей і молоді; 5) посилення символізму та ідеології, яка ґрунтується на принципах поваги, єдності та солідарності. Створення соціальних роликів і реклами, які повинні бути спрямовані на психологічний захист громадян [6].

Особливу увагу треба приділяти засобам масової інформації під час планування та впровадження ефективних механізмів інформаційної безпеки й протидії російській інформаційній війні в Україні. Утрати України в інформаційній війні з Росією певним чином пов'язані з вразливістю засобів масової інформації України до інформаційних атак і дезінформації з боку Росії. Загалом можна виокремити такі причини слабкості українських ЗМІ: 1) поява багатьох нових електронних ресурсів, котрі спрямовані на антиукраїнську політику та є пропагандистськими. Проблема для України в цій ситуації полягає у відсутності контролю за появою таких електронних ресурсів й оперативному реагуванні на такі явища; 2) активна поява в ЗМІ, соціальних мережах та інших інформаційних об'єктах агітаційних матеріалів і відсутність контролю за поширенням цієї інформації; 3) недостатня ефективність протистояння вірусам та шкідливому російському програмному забезпеченню, що займається поширенням російських пропагандистських і дезінформаційних матеріалів; 4) ефективність Російської Федерації в розробці систем, які беруть участь у маніпулюванні свідомістю громадян та розповсюдженні дезінформації. Водночас Україна лише починає розвивати такі системи; у нас немає засобів для стовідсоткової протидії інформаційним сигналам з російської сторони; 5) неналежна підготовка фахівців ведення інформаційної війни та забезпечення інформаційної безпеки держави. В Україні недостатня кількість вищих навчальних закладів, які готують фахівців із захисту інформації й кіберзахисту;

6) незначна кількість джерельної бази, яка б забезпечувала інформацію про специфіку, засоби, методи, особливості інформаційної війни та тактику її ведення. Якщо проаналізувати доступність такої літератури, то її кількість недостатня, а чисельність сучасних фахівців із цих питань – ще менша [1].

Як бачимо, український медіа-простір надзвичайно вразливий до інформаційних атак і дій Російської Федерації й значно програє в цьому протистоянні. Безперечно, ключем до ефективної протидії російській інформаційній війні проти України є не лише державна спроможність України реагувати на російські інформаційні атаки, а й міжнародна допомога провідних міжнародних акторів, таких як США і ЄС. Інформаційна війна Росії, як показує міжнародна практика, ведеться не лише проти України. Російські хакери також утручаються в інформаційні системи інших країн, уключаючи США [5].

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Підбиваючи підсумки, зазначимо, що, незважаючи на існування в Україні бази законодавчих механізмів захисту інформації та протидії інформаційній війні Росії проти України, вона належно не сформована. Війна і її складник, особливо важливі для нас, інформаційна війна в Україні аж ніяк не закінчуються. Росія знову й знову нагромаджує сили для удару. Отже, вона продовжуватиме вчитися та, імовірно, придумає більш досконалі інформаційні тактики. Росія намагатиметься продовжувати інформаційну війну в майбутньому, напевно, за допомогою потенційно більш тонких засобів, хоча стратегія не змогла досягти деяких своїх цілей. Сучасна інформаційна епоха швидко трансформується й призводить до появи нових засобів і методів ведення війни. І Росія випереджає Україну на кілька кроків у розвитку її механізмів та технологій. Ось чому найважливішими для Української держави є формування справді ефективної системи дій в інформаційній війні, а також методу протидії інформаційним впливам із боку держави-агресора; розробка стратегії інформаційної війни за участю вчених, політологів й аналітиків, котрі спеціалізуються в інформаційній сфері; підтримка іміджу держави, покращення ефективного висвітлення достовірної інформації в ЗМІ та покращення їхньої роботи в цілому.

Визнання обмеженості російської гібридної війни так само важливо, як і визнання її сильних сторін. Її успіх сильно залежить від певних умов, які панують у свідомості противника. Якби Захід рішуче протистояв руйнуванню Української держави, то зростання впливу кремлівського інформаційного порядку – мало б набагато менший маштаб. Гібридна стратегія завжди ставить перед Україною значні виклики – і вона повинна бути набагато пильнішою щодо показників російських спроб інформаційного наступу. Але Україна не є безпорадною перед такою стратегією. Насправді вона може й повинна розробити власну теорію та доктрину, щоб протистояти їй.

Водночас, ураховуючи продовження інформаційного протистояння між Росією та Україною, цей аналіз не можемо вважати повноцінним, зважаючи на

мінливість його об'єкта. Перспективним подальшим дослідженням у цьому напрямі може бути аналіз рівня ефективності протидії російській інформаційній війні проти України в майбутньому, а також вивчення міжнародного досвіду боротьби в інформаційній війні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Еляшевська, Н. (2015). Вразливість України до інформаційної війни. *Теле- та радіожурналістика,* Vol. 14, 165—169.

2. Лубкович, І. М. (2014). Місце українських медій в інформаційній війні 2013–2014 рр. *Наукові записки інституту журналістики,* № 56, 182—187.

3. Расторгуев, С. П. (1997). Информационная война как целенаправленное информационное воздействие информационных систем. *Информационное общество,* № 1, 64–66.

4. Сенченко, М. (2014). Запорука національної безпеки в умовах інформаційної війни. *Вісник Книжкової палати,* № 6, 3–9.

5. Dibb, P. (2016). Why Russia is a threat to the international order. Access: https://www.aspi. org.au/publications/why-russia-is-a-threat-to-the-internationalorder/Russia.pdf

6. Kofman, M., Rojansky, M. (2015). A Closer look at Russia's «Hybrid War». Access: https://www.wilsoncenter.org/sites/default/files/7KENNAN%20CABLEROJANSKY%20KOFMAN.pdf

7. Lamb, Ch. J. (1997). The impact of information age technologies on operations other than war. *In War in the information age: new challenges for U. S. security policy* (ed. by Robert L Pfaltzgraff; Richard H Shultz). Washington: D. C.: Brassey's, 256–268.

RUSSIA'S HYBRID WAR AGAINST UKRAINE: INFORMATION ATTACK AND MECHANISMS OF COUNTERING

The article deals with the problem of Russian information war against Ukraine. The authors explain the primary sense of the information war, its interpretation in the framework of wide and narrow approaches. Basing on the use of historic, systemic and structural-functional methods, the main disadvantages of the information sphere of Ukraine and the central mechanisms of its protection are identified. The tools of counteraction to the Russian information war against Ukraine are divided into two groups: legislative and institutional. To the first group there are referred the legislative acts of Ukraine, among which the Doctrine of Information Security of Ukraine that plays a leading role in counteracting Russian information aggression. Among the second group of mechanisms there are state and non-state institutions, whose activities are aimed at the formation and implementation of Ukraine's information security, as well as international structures whose actions are aimed at neutralizing the information influence from Russia. According to the authors, among the domestic institutional mechanisms of counteracting the Russian information war, the important place is taken by the Ministry of Information Policy of Ukraine, the National Security, and Defense Council of Ukraine, the Cyber Police, and others. Considerable attention in the article is paid to such mechanisms of counteraction to Russian information war against Ukraine as the prohibition of Russian sites and social networks, as well as the introduction of quotas on the Ukrainian language in the mass media. The authors note that Ukraine's actions on the neutralization of information threats from Russia should be carried out at different levels: geopolitical, resource level, the level of the public.

In the course of the research, recommendations were made on the confrontation with the information warfare. The analysis of the factors of informational influence and counteraction of information weapons was conducted, as a result of which a number of possible actions

were taken to counter the Russian information escalation in Ukraine in order to create a decent and adequate response to the information challenges of our time.

It has now become clear that the information fight is becoming a factor affecting the very war itself, its beginning, course and outcome. This is confirmed by Russia's aggression against Ukraine. Therefore, a very urgent problem of Ukraine's security is the development of a concept for the protection of the information and analytical framework for information control tasks. In the course of the study, recommendations were drawn up on the confrontation in the information warfare.

Key words: hybrid warfare; Russian-Ukrainian war; information warfare; information security; information strategy.

REFERENCES

1. Eliashevska, N. (2015). Vrazlyvist Ukrainy do informatsiynoi viyny. *Tele- ta radizhurnalistyka,* Vol. 14, 165–169.

2. Lubkovitch, I. M. (2014). Mistse ukrainskyh mediy v informatsiyniy viyni 2013–2014 rr. *Naukovi zapysky instytutu zhurnalistyky,* № 56, 186–187.

3. Rastorguev, S. P. (1997). Informatsionnaya voyna kak tselenapravlennoe informatsionnoe vozdeystvie informatsionnyh sistem. *Informatsionnoe obschestvo,* № 1, 64–66.

4. Senchenko, M. (2014). Zaporuka natsionalnoi bezpeky v umovah informatsiynoi viyny. *Visnyk Knyzhkovoi palaty,* № 6, 3–9.

5. Dibb, P. (2016). Why Russia is a threat to the international order. Access: https://www.aspi.org.au/publications/why-russia-is-a-threat-to-the-internationalorder/Russia.pdf

6. Kofman, M., Rojansky, M. (2015). A Closer look at Russia’s «Hybrid War». Access: https://www.wilsoncenter.org/sites/default/files/7KENNAN%20CABLEROJANSKY%20KOFMAN.pdf

7. Lamb, Ch. J. (1997). The impact of information age technologies on operations other than war. *In War in the information age: new challenges for U. S. security policy* (ed. by Robert L Pfaltzgraff; Richard H Shultz). Washington: D. C.: Brassey’s, 256–268.

Матеріал надійшов до редакції 10.10.2019 р.