

С. А. Дяченко,
д. держ. упр., доцент, доцент кафедри регіональної політики,
Навчально-науковий інститут публічного управління та державної служби
Київського національного університету імені Тараса Шевченка
ORCID ID: <https://orcid.org/0000-0002-5905-4607>
Ю. М. Узденюва,
державний експерт служби з питань воєнної безпеки,
Апарат Ради національної безпеки і оборони України
ORCID ID: <https://orcid.org/0000-0001-6236-9776>

DOI: 10.32702/2306-6814.2024.17.143

ІНФОРМАЦІЙНА СКЛАДОВА У КОНТЕКСТІ ВЕДЕННЯ ГІБРИДНОЇ ВІЙНИ: РЕТРОСПЕКТИВНИЙ АНАЛІЗ ТА СЬОГОДЕННЯ

S. Diachenko,
Doctor of Sciences in Public Administration, Associate Professor, Associate Professor of the Department
of Regional Policy, Educational and Scientific Institute of Public Administration
and Civil Service of Taras Shevchenko National University of Kyiv
Y. Uzdienova,
Public expert of the military security service, Apparatus of the National Security and Defense Council of Ukraine

INFORMATION COMPONENT IN THE CONTEXT OF HYBRID WARFARE: RETROSPECTIVE ANALYSIS AND TODAY

У статті розглянуто сутність гібридної війни, інформаційної війни, інформаційної зброї та визначено роль інформаційного впливу на суспільство. Проаналізовано основні етапи, методи і технології ведення гібридної війни, розкрито ознаки та характеристики її інформаційної складової. З'ясовано, що інформаційно-психологічний вплив має за мету формування у людей на-в'язаних відповідних ідей, поглядів, уявлень, переконань та спонукання до запрограмованих реакцій. Висвітлено ведення інформаційно-психологічної війни російською федерацією проти України, що триває з проголошення української незалежності, та спрямована на збільшення впливу на суспільні маси і суспільну свідомість; окреслено напрями впливу інформаційної зброї. Обґрунтовано, що основною метою гібридної війни є досягнення та утримання інформаційної переваги шляхом надання специфічного інформаційно-психологічного та інформаційно-технічного впливу на державну систему прийняття рішень. Проаналізовано чотири підходи до визначення інформаційної війни та узагальнено, що основними її цілями є широкомасштабне порушення роботи фінансових, транспортних і комунікаційних мереж і систем, руйнування економічної інфраструктури і підкорення населення країни, що зазнала атаки, волі країни-агресора. Наголошено, що архіважливим на сьогодні є розробка механізмів та інструментарію подолання наслідків, викликів і загроз цієї війни, методів протидії ворожим технологіям, а також способів упередження їх виникнення в майбутньому, після перемоги України.

The article examines the essence of hybrid war, information war, information weapons and defines the role of information influence on society. The main stages, methods and technologies of hybrid warfare are analyzed, the signs and characteristics of its informational component are revealed. It was found that informational and psychological influence has the purpose of forming appropriate ideas, views, perceptions, beliefs and encouraging programmed reactions in people. The information and psychological warfare conducted by the Russian Federation against Ukraine, which has been ongoing since the declaration of Ukrainian independence, and is aimed at increasing the influence on the public masses and public consciousness, is highlighted. Two leading directions of influence of information weapons are outlined: influence on enemy's information means and systems and influence on people's consciousness. It was found that the first direction is a cyber war, when technical equipment and its software systems are attacked; the second direction is methods of propaganda and agitation, counter-propaganda and counter-agitation. It is substantiated that the main goal of hybrid warfare is to achieve and maintain an informational advantage by providing a specific informational-psychological and informational-technical influence on the state decision-making system. Four approaches to the definition of information warfare are analyzed and it is summarized that its main goals are large-scale disruption of financial, transport and communication networks and systems, destruction of economic infrastructure and subjugation of the population of the attacked country to the will of the aggressor country. It is summarized that its main goals are large-scale disruption of financial, transport and communication networks and systems, destruction of economic infrastructure and subjugation of the population of the attacked country to the will of the aggressor country. It was emphasized that the development of mechanisms and tools for overcoming the consequences, challenges and threats of this war, methods of countering enemy technologies, as well as ways to prevent their occurrence in the future, after the victory of Ukraine, is of great importance today.

Ключові слова: гібридна війна, інформаційна війна, інформаційна зброя, інформаційна експансія, інформаційна операція, комунікативне забезпечення, комунікативні технології, маніпуляція, пропаганда, російсько-українська війна, публічне управління.

Key words: hybrid war, information war, information weapon, information expansion, information operation, communication support, communication technologies, manipulation, propaganda, Russia-Ukraine war, public administration.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Сучасний швидкий темп розвитку систем масової комунікації призводить до розмивання кордонів і збільшення можливостей здійснення маніпулятивного впливу на свідомість населення країни-агресора з пропагуванням власних ідей, підризу авторитету влади та розповсюдження ворожої інформації з метою абсолютного, тотального контролю над іншою країною. Сьогодні інформаційна зброя — це найпотужніший важіль для поширення дезінформації та впливу на свідомість населення. Важливим є ідентифікація інформаційної складової в контексті ведення гібридної війни, аналіз особливостей сучасного стану й характеристика етапів в історичній ретроспективі з метою визначення причин та наслідків її поширення, інструментарію подолання викликів і загроз, упередження їх виникнення в майбутньому.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Останнім часом значно зросла увага науковців до проблематики гібридної війни, її інформаційної складової, питань протидії російській інформаційній агресії в умовах повномасштабної російсько-української війни. Теоретичні та практичні аспекти інформаційного суспільства розглядаються в працях П. Бергера, З. Бжезінського, У. Ешбі, М. Постера, Е. Тоффлера та ін. Дослідженню особливостей інформаційної безпеки присвячені роботи О. Власюка, Н. Грицяк, Ю. Нестеряка, А. Семенченка та ін. Проблематика гібридної війни та інформаційного впливу на українське суспільство висвітлена у дослідженнях М. Гетьманчука, Н. Кравченко, Р. Марутян, К. Попович, І. Рущенка, Л. Чекаленко, П. Шпиги та ін. Аналізу сутності, проблем, ознак гібридної війни, шляхів її подолання присвячені напрацювання В. Горбуліна, Г. Почепцова, Г. Ситника, О. Суходолі, С. Телешуна та інших вчених.

Віддаючи належне проведенню дослідженням, потребує більш детального розгляду та вивчення питання інформаційної складової сучасної гібридної війни, яку розпочала російська федерація проти України. Доцільним є визначення методів здійснення маніпулювання свідомістю агресором, нав'язування ворожих поглядів та ідей з метою визначення шляхів протидії таким технологіям, розроблення механізмів їх подолання задля перемоги України.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Розкрити сутність поняття гібридної війни та інформаційної зброї; з'ясувати значення та роль інформаційного впливу на суспільство; проаналізувати основні етапи, методи та технології ведення гібридної війни; визначити напрями впливу інформаційної зброї; ідентифікувати ознаки та характеристики інформаційної складової гібридної війни з метою розробки механізмів подолання її наслідків, перемоги України та упередження виникнення загроз у майбутньому.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Ще з проголошення Незалежності України, російська федерація розпочала інформаційну війну проти України, спрямовану на громадян України та Європи, маючи на меті різні завдання й цілі та досягає своєї реалізації за допомогою психологічних і ментальних впливів на свідомість суспільства. Українське суспільство протягом всього періоду незалежності намагались роз'єднати і деморалізувати. Україна, в цілому перебувала в перманентному стані нестабільності, антагоністичності, невизначеності. Після офіційного проголошення незалежності, Україна, на жаль, не мала політичної спільності, об'єднаної ідеологічно, та не мала визначеної стратегії розбудови і розвитку держави. У свідомості частини населення спостерігалось нав'язане ворогом переконання безперспективності розвитку нашої країни.

Ще під час ведення "холодної війни" між СРСР та США, метою якої було ідеологічне протистояння, шляхом перетворення війни з акту фізичного, агресивного, в новий вид та засіб досягнення поставлених цілей, спостерігались чіткі прояви інформаційної атаки. Класичне уявлення щодо ведення війни несе в собі масштабні вибухи, підривною діяльність, теракти, проте вона набула нових властивостей, значно ширших та завуальованих. На думку С. Смольця "холодна війна" включала два рівні ведення "бойових дій": видимий (явний) і невидимий (неявний). Явний полягав у використанні засобів, які можливо не були помітні для широкого загалу, проте про них всі все добре знали. Сюди відноситься: розвідка, міжнародне протистояння (в політичній, дипломатичній, економічній, військовій сферах), та зрештою, ідеологічне протистояння, що відображалось у науковій, публіцистичній полеміці і трансливалось на всі інші, без виключень, сфери людської життєдіяльності. Неявний — полягав у використанні інформаційно-психологічних технологій з впливу на масову свідомість, виконував функцію підтримки основних, в певній мірі, офіційних дій, в рамках цього геополітичного протис-

тояння. Іншими словами, його ціль — поглибити ефект "військових" дій, збільшити вплив на суспільні маси, суспільну свідомість, як на ворожі, так і на власні [10, с. 70].

Інформаційна війна, яку ведуть держави між собою, спрямовує інформаційно-психологічні впливи також на власних громадян. Вона є наймасштабнішою, оскільки за обсягом та кількістю жертв охоплює необмежений простір та необмежену кількість громадян. Її поширення та наслідки ми спостерігаємо сьогодні. Інформаційно-психологічна операція, яку проводить сьогодні росія проти України, — це попередньо спланований та послідовно реалізований вплив на погляди, настрої, світоглядні й політичні позиції людей з метою реалізації власних цілей.

Гібридна війна — це сукупність певних дій агресора по відношенню до потерпілої сторони, спрямованих на дискредитацію останнього в очах світового співтовариства, власного народу, розкол політичної еліти та суспільства в цілому, підриив авторитету влади, зневіру народу. Саме комплекс зазначених дій може нанести значно сильнішого удару ніж військове вторгнення, оскільки їх метою є формування певних стереотипів та установок масової свідомості через маніпулятивний вплив [11, с. 66].

Основою інформаційно-психологічної операції є маніпуляція свідомістю. Маніпуляція — це спонукання суб'єкта, яким управляють, уявно самостійно й добровільно приймати рішення, бажані для того, хто управляє, за допомогою спеціально підготовленої та певним чином поданої інформації. Саме інформаційна війна є дуже потужною та вигідною складовою гібридної війни, адже вона не потребує залучення значних фінансових ресурсів, крім того, вона не має меж, та не вимагає і не передбачає потужної підтримки держави. Ще однією ознакою такої війни є те, що для свого втілення вона потребує лише доступу до інформаційних мереж, систем, засобів масової інформації, вона географічно безмежна, має велику кількість використання різних шляхів для здійснення шпигунських дій, терористичних актів — а головне те, що її можна контролювати і вести з будь-якої віддаленої точки світу.

Саме поширення неправдивої та спотвореної інформації є основою ведення такої війни, головною ідеєю, розповсюдження якої є нав'язування позиції країни-агресора, нібито використовуючи патріотичну мету захисту корінних народів, прав та свобод людини, боротьби з пригніченням расової нерівності, тероризмом, проявами утисків щодо мовної політики тощо. Цілі інформаційної війни є дещо іншими, аніж війни у звичному розумінні: не фізичне знищення сторони і ліквідації його збройних сил, а широкомасштабне порушення роботи фінансових, транспортних і комунікаційних мереж та систем, руйнування економічної інфраструктури й підкорення населення країни, що зазнала атаки, волі країни-агресора.

На думку О. Саприкіна, поняття інформаційної експансії є технологією набагато ширшою, ніж інформаційної війни чи інформаційної атаки. Дослідник зауважує, що ці категорії можна вважати складовими інформаційної експансії [9]. В свою чергу, інформаційною експансією позначають діяльність із досягнення інтересів

методом безконфліктного проникнення в інформаційну сферу з метою поступової, планової, непомітної для суспільства зміни системи соціальних відносин за зразком системи джерела експансії; витіснення положень національної ідеології та національної системи цінностей і заміщення їх власними цінностями та ідеологічними настановами; збільшення ступеня свого впливу та присутності, введення контролю над стратегічними інформаційними ресурсами, інформаційно-телекомунікаційною структурою і національними ЗМІ; нарощування присутності власних ЗМІ в інформаційній сфері об'єкта проникнення для пропагандистського забезпечення певних геополітичних цілей та ін. Інформаційну експансію можуть створювати і поширювати як державні органи (за допомогою інформаційних установ і відповідних заходів), так і транснаціональні корпорації для досягнення власної вигоди: забезпечення ринку збуту, участі у великих міжнародних тендерах, доступу до дешевої сировини і робочої сили, політичних та військових цілей тощо.

Метою інформаційної експансії є [9, с. 40]:

- вплив на владу іншої країни для прийняття/скасування певних рішень, дій, інтеграційних намагань, демократизації тощо;

- контроль в укладенні міжнародних угод, формуванні міжнародних спілок;

- втручання в геополітичну, військову, економічну концепції країни;

- вплив на громадян країни для тиску на владу, а також з рекламно-пропагандистськими мирними цілями.

Серед ознак інформаційної експансії виокремлюють:

- монополізацію газет, журналів радіо і телебачення, а також засобів зв'язку спеціалізованими корпораціями;

- пряме підпорядкування засобів інформації та зв'язку олігархічному капіталу;

- відкрите втручання державних органів у сферу ЗМІ, заборону або позазаконне обмеження свободи слова;

- панування порівняно невеликої кількості засобів масової інформації й інформаційних агентств на ринку новин;

- монополізацію інформаційного простору країни або регіону;

- поглиблення диспропорцій у забезпеченні засобами інформації та зв'язку між країнами;

- використання друкованої преси, радіо, телебачення та інформаційними агентствами відповідних країн інформаційного забезпечення власної внутрішньої та зовнішньої політики на теренах інших країн;

- публікацію низки матеріалів, спрямованих на дискредитування політичної сили патріотичного налаштування; навмисне створення негативного іміджу політичній партії, руху чи певним державним діячам; спотворення визначних (національного історичного, культурного, релігійного та ін.) заходів чи подій в країні — об'єкти інформаційної експансії [9, с. 40].

Основною метою інформаційної війни є досягнення та утримання інформаційної переваги однією зі сторін над іншою шляхом надання специфічного інформацій-

но-психологічного та інформаційно-технічного впливу на державну систему прийняття рішень. Сучасні фахівці дійшли висновку, що існує декілька етапів інформаційних війн [14, с. 22]. На початковому етапі відбувається збільшення матеріалів та інших форм інформаційної активності із ціллю привернення уваги до "проблемної ситуації". На другому етапі інформаційного протистояння здійснюється пошук аудиторії, завоювання її прихильності та поступова консолідація споживачів інформаційного продукту довкола основного протиріччя. На третьому етапі проходить масовий інформаційний вплив на аудиторію, насичення інформаційного простору матеріалами та відомостями, які призводять до залучення широкої аудиторії на свою користь. Завершальним етапом слугує відповідна реакція аудиторії, яка впливає на забезпечення панування в інформаційному просторі конкретної сторони інформаційної війни [13, с. 468—470].

Найпоширенішою є думка, що поняття інформаційної війни з'явилося у 80-х роках ХХ століття, хоча задовго до цього вже були прояви ведення інформаційних війн у тій чи іншій формі. Вважається, що вперше термін "інформаційна війна" було введено у 1985 році в Китаї. В основі теоретичних підходів китайських спеціалістів в області інформаційного протистояння лежать погляди стратега і мислителя давнього Китаю Сунь-цзи. Він першим узагальнив досвід інформаційного впливу на супротивника. У трактаті про військову стратегію і тактику "Мистецтво війни" Сунь Цзи писав: "У будь-якій війні, як правило, найкраща політика зводиться до захоплення держави в цілому... Одержати сотні перемог у бою — це не межа мистецтва. Підкорити супротивника без бою — ось це вінець мистецтва".

На сьогодні даний термін використовується у двох площинах:

- у широкому розумінні — для визначення протистояння в інформаційній сфері у засобах масової інформації для досягнення різних політичних цілей;

- у вузькому розумінні — для визначення воєнного протистояння, у військовій інформаційній сфері для досягнення односторонніх переваг в отриманні, зборі, обробці та використанні інформації на полі бою (в операції, битві) [2].

В. Ліпкан [2] дотримується позиції, відповідно до якої інформаційне протистояння — це форма боротьби сторін в інформаційному просторі з використанням політичних, економічних, дипломатичних, військових та інших методів, способів та засобів для впливу на інформаційне поле супротивника та захисту власного інформаційного поля в інтересах досягнення поставлених цілей. Ураховуючи таке визначення можна зазначити, що інформаційне протистояння включає в себе три незмінні складові: вплив, аналіз, протистояння.

Усвідомлено інформаційна зброя почала застосовуватися саме від 70-х років ХХ ст., коли людство почало вступати до інформаційної ери, яка характеризується визнанням пріоритету за знанням, інформацією та інформаційними технологіями. У гуманітарному сенсі інформаційна війна становить собою активні методи трансформації інформаційного простору, що знаходить свій вираз у системі нав'язування моделей світу, які покликані забезпечити бажані типи поведінки, атаках на

структури породження інформації — процеси міркувань. У той же час технічне трактування даного поняття полягає у тому, що за допомогою спеціальних програм руйнується обладнання, програмне забезпечення тощо [2].

Науковці П. Шпиґа та Р. Рудник виділяють чотири підходи щодо визначення інформаційних війн [12]. Перший підхід трактує інформаційну війну як сукупність політико-правових, соціально-економічних, психологічних дій, що передбачають захоплення інформаційного простору, витіснення ворога з інформаційної сфери, знищення його комунікацій, позбавлення засобів передачі повідомлень. Інформаційні війни визначаються як відкриті чи приховані цілеспрямовані взаємодії інформаційних систем з метою отримання певної переваги в матеріальній сфері. Під час протистояння інформаційні системи постійно використовують інформаційну зброю, яка має запустити програми самознищення ворожої інформаційної системи (для людини інформаційним впливом, що здатний привести до запуску таких програм, є активізація бажань, думок і провокування вчинків, скерованих на самознищення).

Другий підхід визначає інформаційну війну як найгострішу форму протистояння в інформаційному просторі. Акцент переноситься на характер протистояння опонентів. У даному випадку першочергового значення набувають такі якості інформаційної взаємодії, як безкомпромісність, висока інтенсивність суперечки та короткотривалість гострого суперництва. Для позначення агресивності сторін застосовується поняття інформаційної зброї. При такому трактуванні інформаційної війни, коло учасників інформаційного протиборства значно розширюється. Ними вже є не лише дві сторони, але й всі ті, хто так чи інакше є присутніми в інформаційному просторі в даний проміжок часу, а саме: громадськість, особи, які відповідають за прийняття рішень, бізнес, ЗМІ та ін. За такої інтерпретації інформаційних війн до них часто відносять будь-які форми ідейного протистояння різних доктрин, релігій і навіть напрямів мистецтва. Ідейні суперечності та різниця в думках визначаються формами інформаційного протистояння.

Третій підхід полягає у розгляді інформаційної війни як форми забезпечення та ведення військово-силових дій за допомогою найсучасніших електронних засобів, наприклад, цифрових випромінювачів, супутникових передавачів та інших аналогічних інструментів і засобів, які застосовуються для виконання військових завдань. Четвертий підхід ототожнює інформаційні війни з кібернетичними війнами. Під останніми розуміють протистояння між технічними системами [12, с. 3—4].

Існує думка, що вперше термін "інформаційна війна" вжив американський фахівець, експерт Томас Рон у звіті "Системи зброї й інформаційна війна" у 1976 році. Він науково обґрунтував, що саме інформація є найслабшою ланкою будь-якої армії [3, с. 300]. Відтоді починається розуміння неймовірного впливу за допомогою маніпуляції на свідомість населення з насаджування власних поглядів та ідей, виникає чітке усвідомлення, що інформація може бути зброєю.

Сучасні дослідники й науковці виділяють два провідні напрями впливу інформаційної зброї: 1) вплив на інформаційні засоби і системи супротивника; 2) вплив

на свідомість людей. Перший напрям ще має назву кібервійна, коли атакам піддається технічне обладнання і системи його програмного забезпечення. Другий напрям — це давні способи пропаганди та агітації, контрпропаганди і контрагітації, що досягли небувалих результатів по витонченості і масовості впливу на свідомість людей.

Д. Присяжнюк трактує інформаційні війни як вид конфлікту, при якому завданнями протиборчих сторін є захист власної інформації та інформаційних систем, маніпулювання інформацією противника або її спотворення, а також обмеження можливостей протиборчої сторони в доступі і обробці інформації [7, с. 3].

П. Шпиґа та Р. Рудник зазначають, що інформаційна зброя — це інформація (дані), які є засобом ведення інформаційних війн і призначення яких полягає в зміні системних якостей об'єкта інформаційного впливу за допомогою прихованих установок на здійснення задуманих користувачем інформаційної зброї дій [12].

Серед основних напрямів і прикладів використання інформаційної зброї виокремлюють:

- 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;
- чутки, які створені навмисно;
- введення у ЗМІ своїх прибічників для проведення підривних акцій;
- проникнення в комп'ютерні мережі та системи управління базами даних, зараження комп'ютерних систем вірусами, навмисне впровадження різного роду помилки у програмне забезпечення об'єкта;
- інформаційна підтримка дисидентських та опозиційних рухів тощо [12, с. 330—331].

Зрозуміло, що російська федерація ще задовго до повномасштабного вторгнення на територію України розпочала вести інформаційну стратегічну операцію в нашій державі. Серед ключових аспектів такої операції 2013-2014 років, спрямованих на соціум Півдня і Сходу нашої країни через культурні впливи, що сприяло поширенню російських культурно-світоглядних цінностей та нав'язування російської ідентичності, Н. Кравченко виокремлює [4]:

- 1) тиражування російської поп-культури через телеканали, радіостанції, концертні зали, ресторани, кафе, дискотеки, транспортні засоби;
- 2) за сприяння фонду "Русский мир" (2007 р.) пропагування сприйняття російської мови як рідної для всіх українців та формування громадської думки про надання їй статусу державної;
- 3) насаджування переконань про спільне історичне коріння, братську єдність та взаємозалежність двох народів;
- 4) використання інтернет-ресурсів: русифікація інтернет-сайтів в Україні, популяризація російських ме-

режевих ресурсів, активізація діяльності блогерів у необхідному контенті;

5) захоплення національного медіа-простору шляхом трансляції та поширення російських засобів інформації, а також трансляцією російського інформаційного продукту на українських телеканалах (Інтер, СТБ, ТРК "Україна"). До початку повномасштабної російсько-української війни в Україну транслювали понад 80 телеканалів з рф [15] особлива увага в цей період зверталась на роз'яснення переваг інтеграції України з росією та участі України в Митному союзі;

6) формування позитивного іміджу росії та негативного іміджу України і Заходу, пропагування атрибутів російської державності, російських спецслужб, силових структур через фільми російських кіностудій;

7) агентурна діяльність ФСБ при підтримці проросійських сил (бізнесових, політичних еліт, громадських організацій) в інформаційному полі України, зокрема, через Всеукраїнський союз радянських офіцерів, Кримський козацький союз "Возрождение", Єкатеринославське козацтво, Об'єднану раду Українського закордонного козацтва, Координаційну раду російських організацій "Руське віче" та ін., які активно співпрацювали з автономною некомерційною організацією "Центр-Кремлівська стратегія";

8) релігійний чинник в особі УПЦ МП та Союзу православних громадян України [4, с. 108-109].

Головною метою російської пропаганда є дискредитація української влади, збройних сил та загалом суспільства [6, с. 87]. Розуміючи силу інформаційного впливу на суспільство і водночас можливі критичні наслідки, в результаті активної української протидії, рф визначає інформаційну складову пріоритетним напрямом безпекової політики [1]. Ведення сучасної інформаційної війни — це елемент глобальнішого воєнного протистояння між агресором (росією) та Україною, яка безсумнівно переможе.

На думку І. Рущенка "гібридна війна" — це ланцюг запланованих агресором подій, які крок за кроком ведуть до загарбання чужих територій чи встановлення фактичного контролю над частинами країни-жертви [8]. Серед основних характеристик гібридної війни Г. Почепцов у праці "Від покемонів до гібридних війн: нові комунікативні технології XXI століття" [5] виокремлює такі її визначальні риси: військові дії в гібридній війні пригніщені, а інформаційні, навпаки, різко посилені.

На думку науковця інформаційні операції спрямовані на [5, с. 195—196]:

а) масову свідомість у тактичному аспекті, коли вирішуються завдання близького плану;

б) масову свідомість у стратегічному аспекті, коли вирішується проблема досягнення цілей далекого плану;

в) структури управління, алгоритми прийняття рішень, що має за мету зміну цінності популяції.

Таким чином, сутність інформаційної складової гібридної війни полягає в створенні перешкод нападникам, щоб вони не могли адекватно реагувати у відповідь. Головне завдання інформаційного інструментарію — впливати на центри прийняття рішень супротивника. Ця війна може постійно змінювати правила гри і задіяні типи сил, оскільки одночасно оперує як військовими, так і

цивільними складовими, причому, цивільна є фундаментом для військової. Гібридна війна працює не тільки з атакованим населенням, а й зі своїм власним. Завдяки Інтернету відбувається зв'язок не з одиницями, як це було з друкованими інформаційними потоками, а з масами.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

На підставі викладеного необхідно підкреслити, що специфікою інформаційної війни є те, що вона ведеться, на відміну від збройної боротьби, як у мирний, так і у воєнний час. Вона націлена на всі можливості та фактори ураженості, які неминуче виникають при зростанні залежності від інформації, а також на використання інформації у найрізноманітніших конфліктах. Об'єктом уваги стають інформаційні системи (включаючи відповідні лінії передач, центри обробки та людський фактор цих систем), а також інформаційні технології, які використовуються в системах озброєння. Тому сферами інформаційного протистояння є: світоглядна, політична, дипломатична, воєнна, науково-технологічна, соціальна та гуманітарна, ідеологічна, екологічна. Крім того, ще однією з головних цілей та завдань інформаційної складової в контексті гібридної війни, є придушення в людині морального творчого початку, зміна світогляду та підірив авторитету влади.

Ідентифікувавши інформаційну складову гібридної війни, визначивши ризики, охарактеризувавши її етапізацію та особливості сучасного стану, виявлено цілі, методи та технології, що призвели до трагічних наслідків її поширення. Архіважливим на сьогодні є розробка механізмів та інструментарію подолання наслідків, викликів і загроз цієї війни, методів протидії ворожим технологіям, а також способів упередження їх виникнення в майбутньому, після перемоги України.

Література:

1. Дуцик Д. Українська інформаційна політика в умовах війни: критичні зауваження. Протидія російській інформаційній агресії: спільні зусилля задля захисту демократії. Аналітичний звіт. Київ.: Телекритика, 2015. 77 с.
2. Ліпкан В.А. Теоретичні основи та елементи національної безпеки України: Монографія. Київ, 2003. 600 с.
3. Короход Я. Д. Інформаційно психологічні війни — зброя XXI Актуальні проблеми політики. 2013. Вип. 50. С. 299—307.
4. Кравченко Н. Інформаційна складова як ключовий аспект гібридної війни. Acta de Historia & Politica: Saeculum XXI, 2022. Т. IV. С. 106—118.
5. Кріслата О. Гібридна війна та її інформаційна складова. Збірник праць Науково-дослідного інституту пресознавства. 2018. Вип. 8. С. 190—199.
6. Патлашинська І. В. Сучасна російсько-українська інформаційна війна: завдання, методи та особливості використання. Регіональні студії. 2022. № 28. С. 84—87.
7. Присяжнюк Д.М. Застосування маніпулятивних технологій з боку Росії в ЗМІ України (на прикладі Криму). Вісник Київського національного університету імені

Тараса Шевченка: Військово-спеціальні науки / Київ. нац. ун-т ім. Тараса Шевченка. — Київ: Київський університет 2011. Вип. 26. С. 96—99.

8. Рущенко І. П. Російсько-українська гібридна війна: погляд соціолога: Монографія. Харків, 2015. 268 с.

9. Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро-2012. Вісник Книжкової палати. 2013. № 1. С. 40—43.

10. Смолюк С. П. Інформаційна війна як чинник формування суспільного буття. Вісник НТУУ "КПІ". Філософія. Психологія. Педагогіка: збірник наукових праць. 2011. № 3 (33). С. 70—74.

11. Феськов І. В. Основні методи ведення гібридної війни в сучасному інформаційному суспільстві. Актуальні проблеми політики. 2016. Вип. 58. С. 66—76.

12. Шлига П. С., Рудник Р. М. Основні технології та закономірності інформаційної війни. Проблеми міжнародних відносин. 2014. Вип. 8. С. 326—339.

13. Яфонкін А., Шевчук В. Інформаційна війна проти держави та інформаційна безпека України. Форум права. 2017. № 5. С. 466—472.

14. Bhan R. Information War: (Dis)information will Decide Future Wars. New York: Educreation Publishing, 2017. 200 p. URL: https://books.google.de/books?id=8_xDDwAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

15. The information portal "All-Ukrainian News". URL: <https://vv.org.ua/poslednienovosti/nacrada-iz-tb-zaboronila-transljaciju-na-teritorii-ukraini-shhe-troh-rosijskih-telekanaliv/>

References:

1. Dutsyk, D. (2015), Ukrains'ka informatsijna polityka v umovakh vijny: krytychni zauvazhennia. Protydiia rosijs'kij informatsijnij ahresii: spil'ni zusyllia zadlia zakhystu demokratii [Ukrainian information policy in the conditions of war: critical remarks. Countering Russian Information Aggression: Joint Efforts to Protect Democracy], Telekrytyka, Kyiv, Ukraine.

2. Lipkan, V.A. (2003), Teoretychni osnovy ta elementy natsional'noi bezpeky Ukrainy [Theoretical foundations and elements of national security of Ukraine], Kyiv, Ukraine.

3. Korokhod, Ya.D. (2013), "Information and psychological warfare is a XXI weapon", Aktual'ni problemy polityky, vol. 50, pp. 299—307.

4. Kravchenko, N. (2022), "The information component as a key aspect of hybrid warfare", Acta de Historia & Politica: Saeculum XXI, vol. IV, pp. 106—118.

5. Krislata, O. (2018), "Hybrid war and its information component", Zbirnyk prats' Naukovo-doslidnoho instytutu presoznavstva, vol. 8, pp. 190—199.

6. Patlashyn's'ka, I.V. (2022), "Modern Russian-Ukrainian information war: tasks, methods and features of use", Rehional'ni studii, vol. 28, pp. 84—87.

7. Prysiazhniuk, D.M. (2011), "The use of manipulative technologies by Russia in the mass media of Ukraine (on the example of Crimea)", Visnyk Kyivs'koho natsional'noho

universytetu imeni Tarasa Shevchenka: Vijs'kovo-spetsial'ni nauky, vol. 26, pp. 96—99.

8. Ruschenko, I.P. (2015), Rosijs'ko-ukrains'ka hibrydna vijna: pohliad sotsiolooha [Russian-Ukrainian hybrid war: a sociologist's view], Kharkiv, Ukraine.

9. Saprykin, O. (2013), "Information expansion, information war and information attack in mass media on the example of Euro-2012", Visnyk Knyzhkovoï palaty, vol. 1, pp. 40—43.

10. Smol'ts, S.P. (2011), "Information warfare as a factor in the formation of social existence", Visnyk NTUU "KPI". Filosofiia. Psykholohiia. Pedahohika: zbirnyk naukovykh prats', vol. 3 (33), pp. 70—74.

11. Fes'kov, I.V. (2016), "The main methods of conducting hybrid warfare in the modern information society", Aktual'ni problemy polityky, vol. 58, pp. 66—76.

12. Shpyha, P.S. and Rudnyk, R.M. (2014), "Basic technologies and patterns of information warfare", Problemy mizhnarodnykh vidnosyn, vol. 8, pp. 326—339.

13. Yafonkin, A. and Shevchuk, V. (2017), "Information war against the state and information security of Ukraine", Forum prava, vol. 5, pp. 466—472.

14. Bhan, R. (2017), Information War: (Dis)information will Decide Future Wars, Educreation Publishing, New York, USA, available at: https://books.google.de/books?id=8_xDDwAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false (Accessed 05 Aug 2024).

15. The information portal "All-Ukrainian News" (2024), available at: <https://vv.org.ua/poslednienovosti/nacrada-iz-tb-zaboronila-transljaciju-na-teritorii-ukraini-shhe-troh-rosijskih-telekanaliv/> (Accessed 05 Aug 2024).

Стаття надійшла до редакції 12.08.2024 р.

<https://nayka.com.ua>

Електронне фахове видання

ДЕРЖАВНЕ УПРАВЛІННЯ
удосконалення та розвиток

Виходить 12 разів на рік

включено до переліку наукових фахових видань України
з питань **ДЕРЖАВНОГО УПРАВЛІННЯ**
(Категорія «Б»)

Наказ Міністерства освіти і науки України
від 28.12.2019 №1643

Спеціальність 281

e-mail: economy_2008@ukr.net

viber: +38 050 3820663