

УДК 327.5: 316.77 “19/20”

DOI: <https://doi.org/10.21564/2663-5704.62.310919>

Кундеус Оксана Миколаївна, кандидатка політичних наук, доцентка, доцентка кафедри міжнародних відносин, Рівненський державний гуманітарний університет, Україна
e-mail: oksana.kundeus@rshu.edu.ua
ORCID ID: 0000-0002-1162-3858

Вівчар Інна Володимирівна, кандидатка політичних наук, доцентка кафедри міжнародних відносин, Рівненський державний гуманітарний університет, Україна
e-mail: Innavivchar79@gmail.com
ORCID ID: 0000-0002-9952-5696

Крет Ольга Віталіївна, кандидатка політичних наук, доцентка, доцентка кафедри міжнародних відносин, доцентка кафедри документальних комунікацій та бібліотечної справи, Рівненський державний гуманітарний університет, Україна
e-mail: Olga.kret@rshu.edu.ua
ORCID ID: 0000-0003-1736-3863

ІНФОРМАЦІЙНА ВІЙНА: СУТНІСТЬ ТА ОСОБЛИВОСТІ (КІНЕЦЬ ХХ – ПОЧАТОК ХХІ СТ.)

У науковій розвідці висвітлено проблему наростання та становлення поняття «інформаційна війна» на межі ХХ та ХХІ ст., що було зумовлене завершенням холодної війни та розпадом біполярної системи міжнародних відносин. Проаналізовано основні підходи до визначення змісту поняття «інформаційна війна», її принципи та завдання. Інформаційна війна визначається як складова частина ідеологічної боротьби.

Ключові слова: *інформаційна війна, психологічна війна, інформаційне протиборство, мережеві війни, стратегічна розвідка.*

Постановка проблеми. Інформаційна війна проти нашої держави з боку Російської Федерації розпочалася задовго до повномасштабного вторгнення Росії в Україну. Дослідження поняття інформаційна війна надзвичайно актуальне в реаліях повномасштабного вторгнення РФ, позаяк інформаційна війна стала повноцінним елементом російсько-української війни, що слугує різним

політичним цілям: ведеться в освітній, соціальній, воєнній, духовній сферах. Реалізується ця концепція широким колом сучасних можливостей інформаційно-психологічної війни та масштабними кібератаками. Відповідно постає потреба в детальному дослідженні цього поняття, його витоків та становлення в зазначений період.

Аналіз останніх досліджень та публікацій. Тема інформаційної війни, форми та технології її ведення неодноразово ставали предметом аналізу в численних наукових працях вітчизняних та зарубіжних експертів.

Теоретичним аспектам інформаційних воєн присвячено праці таких науковців, як О. Дубас [5], Б. Юськів [3], В. Жадько [2], Г. Почепцов [1], Є. Скулиш [6]. Особливості ведення інформаційної війни з'ясовують В. Горбулін [12], В. Петрик [13]. А. Худолій [7] досліджує теорію мережевих війн та розкриває їх вплив на суспільство. При написанні статті було використано такі першоджерела, як директива Міністерства оборони США DODD (Department of Defense Directive) 3600 під назвою «Information war» [4], де вказується роль та мета інформаційної війни в сучасних реаліях. Особливо слід відзначити праці американських авторів корпорації RAND (Research and Development), яка проводить дослідження на замовлення Міністерства оборони США: монографію Р. Моландера, Е. Рідділа та П. Вільсона «Strategic information warfare: a new face of war» [10], у якій наведено основні сучасні характеристики інформаційної війни та обґрунтовано їх поділ на тактичні та стратегічні.

Разом із тим вказана тема залишається недостатньо дослідженою, особливо враховуючи активне упровадження та розроблення нових форм та методів інформаційних війн, що робить цю тему ще більш актуальною для подальшого аналізу.

Формулювання цілей: аналіз та окреслення особливостей інформаційної війни наприкінці ХХ та початку ХХІ ст.

Виклад основного матеріалу. На сьогодні однозначну відповідь на питання щодо виникнення та поширення поняття «інформаційна війна» знайти складно. Тому наведемо декілька визначень різних науковців.

Так, Г. Почепцов вважає, що прямими попередниками терміна «інформаційна війна» можна вважати: «психологічна війна», «політична війна», «психологічна операція», «інформаційна операція»; початки їх вживання в офіційних документах і наукових працях сягають перших десятиліть ХХ ст. [1, с. 557–558]. «Вперше термін психологічна війна в 1920 р. застосував британський історик Дж. Фуллер, котрий аналізував Першу світову війну. І цей термін взяли на озброєння американці. Вони датують власне використання цього терміна 1940 роком. Відповідний англійський ва-

ріант цього терміна – політична війна. Саме цей термін почали з 1957 р. використовувати в американських офіційних документах. Цікаво, що сучасний термін, який використовує НАТО, а саме інформаційні операції, може використовуватися взагалі при відсутності натяку на бойові дії» [2, с. 29].

Вважається, що термін «інформаційна війна» вперше використав Томас Рон у звіті «Системи зброї й інформаційна війна» 1976 р., складеному для компанії «Boeing». Автор відмітив, що значення інформаційної інфраструктури для американської економіки прогресивно зростає, тому саме вона є вразливою як у воєнний, так і в мирний час [3, с. 18]. Ця проблематика зацікавила американських військових і, як наслідок, цей предмет активно обговорювався в американських військових колах вже у 1980-х рр. Саме тоді вже викристалізувалось розуміння інформації як цілі, так і зброї. Офіційно терміни «інформаційна боротьба» та «інформаційна війна» вперше були запроваджені 21 грудня 1992 р. в директиві Міністра оборони США DODD 3600 під назвою «Інформаційна війна» [4]. У директиві зазначається «необхідність всебічного врахування інформаційних ресурсів при управлінні Збройними Силами в умовах протидії противника» [3, с.18].

О. Дубас у статті «Інформаційна війна: нові можливості політичного протистояння» наголошує на тому, що початок активної зацікавленості наукової спільноти, здебільшого за кордоном, питаннями інформаційних протистоянь датується 80-ми – 90-ми рр. ХХ ст. Термін «інформаційна війна» має сучасну історію. Він з'явився в середині 80-х рр. ХХ ст. у зв'язку з новими завданнями Збройних сил США після закінчення «холодної війни». Його виникнення стало результатом роботи групи американських теоретиків, які займаються військовими проблемами, таких як Г. К. Екклз, Г. Г. Самерз та ін. Згодом це поняття з'явилося в документах Міністерства оборони США в 1990 р. Саме з цього моменту було розпочато дослідження цього феномену. Більш популярним термін став після проведення операції «Буря в пустелі» у 1991 р. в Іраку, де нові інформаційні технології вперше було застосовано з військовою метою [5, с. 71].

У 1993 р. в директиві № 30 Комітету начальників штабів Міністерства оборони (МО) США вже було викладено основні принципи ведення інформаційної війни. Починаючи з 1994 р., США, за участю представників військово-політичного керівництва країни, проводять офіційні наукові конференції, присвячені інформаційним війнам. Проведенням конференцій займався новостворений Центр інформаційної стратегії і політики, завданням якого стало вивчення можливостей використання інформаційних технологій у військових конфліктах ХХІ ст. [3, с.18].

Одним із перших теоретиків інформаційної війни визнано Мартіна Лібікі. У його праці «Що таке інформаційна війна?», вперше опублікованій Національним інститутом оборони США в 1995 р., саме поняття не визначено. Замість цього М. Лібікі описує форми інформаційної війни, серед яких сім основних і двадцять додаткових. Уся система «Information Warfare» описується схемою, з якої й випливає поняття «інформаційна війна» [5, с. 69].

У лютому 1996 р. МО США ввело в дію «Доктрину боротьби із системами контролю й управління». Цей документ містив виклад принципів боротьби з системами контролю і управління і застосування інформаційної війни у воєнних діях.

У жовтні 1998 р. МО США вводить у дію «Об'єднану доктрину інформаційних операцій» («Joint Doctrin Of Information Operation»), у якій уперше офіційно підтверджується факт підготовки американців до проведення наступальних інформаційних операцій. Раніше представники Пентагона завжди підкреслювали оборонну спрямованість заходів США в інформаційній сфері. Новим документом передбачається можливість проведення наступальних інформаційних операцій не тільки у військовий, але і в мирний час. При цьому представники США, коментуючи ці положення, стверджують, що наступальна інформаційна зброя застосовуватиметься при повному дотриманні міжнародних норм і договорів [3, с.19].

Ураховуючи сучасні наукові напрацювання щодо визначення поняття інформаційної війни, було сформульовано її дефініцію.

Інформаційна війна – це різновид інформаційного протиборства, в основі якого лежить чітко сформульована стратегія з ясною картиною успіху як кінцевої мети та який складається з дій, спрямованих на досягнення інформаційної переваги над противником і забезпечення власної інформаційної безпеки, що є невід'ємним складником національної безпеки.

Головним завданням інформаційної війни між державами є знищення сукупної політичної могутності іншої держави такими шляхами: підрив її міжнародної репутації і, як наслідок, створення перешкод для підтримання міжнародних зв'язків (міжнародна ізоляція); завдання шкоди всім складникам національної безпеки держави; послаблення панівної еліти, що імовірно призведе до повалення встановленого нею соціально-політичного режиму.

Заходи інформаційної війни мають на меті деструктивний вплив на головний об'єкт – це свідомість окремої людини та громадська думка .

Окрім цього, виокремлюють такі об'єкти посягань інформаційної війни: загальні, спеціальні, та об'єкти розвідувальних спрямувань.

Свою чергою, до загальних об'єктів зараховують: правопорядок, мобілізаційну готовність та боєздатність збройних сил, зовнішньополітичні зв'язки та міжнародний авторитет держави.

До спеціальних об'єктів інформаційної війни належать: суспільство загалом та певні його прошарки зокрема, наприклад маргіналізовані групи, такі як засуджені, представники певних релігійних, радикальних політичних та соціальних течій тощо.

До об'єктів розвідувальних спрямувань інформаційної війни зараховують: засоби масової інформації та комунікації, аналітичні центри, міністерства, відомства та органи державного управління, політичні партії, громадські організації, профспілки зокрема [6, с. 28–29].

Одна з базових характеристик інформаційної війни – розмивання концепту правди. Мета полягає не в тому, щоб запустити інші версії правди, а в тому, щоб розмити саме поняття правди [7, с. 112].

Наприкінці ХХ ст. американська корпорація RAND («Research and Development») провела низку досліджень із метою вивчення інформаційного простору в контексті новітніх інформаційних війн і вперше ввела поняття стратегічної інформаційної війни. Згідно зі звітом 1999 р., головним місцем битви є інформаційна інфраструктура, мережа електропостачання, а також інші комп'ютерні системи. Тісний взаємозв'язок цих систем робить їх вразливими до систематичних збоїв, а можливість доступу до них із-за кордону робить ці системи чутливими до атак, походження яких важко ідентифікувати. Більш того, майстерно вчинену інформаційно-технічну атаку навіть важко розпізнати як таку. Дослідники корпорації RAND також наголошують на такому парадоксі: що складнішою і розвиненішою є система, то вразливішою вона є. Відтак сприйнятливішими до атак є системи високорозвинених країн, таких як США [8, с. 131].

Звіт корпорації RAND «Глобальний курс інформаційної революції: постійні теми та регіональні особливості» 2003 р. містить ґрунтовні висновки на основі досліджень сучасного інформаційного простору й технологій. Зокрема, дослідники Р. Хандлі, Р. Андерсон, Т. Біксон, Р. Неу виділяють: загрози та виклики так званому операційному суверенітету держави, тобто здатності здійснювати ефективний контроль всередині держави, при цьому конституційний суверенітет (верховенство легальної влади в країні) не підлягає викликам інформаційної революції; розваги як провідну форму новітніх інформаційних послуг, що включають не лише дозвілля, але й навчальні тренінги; створення нових бізнес-моделей та головну роль електронної комерції, яка значно ускладнює державний контроль над рухом коштів та податків [9, с. 16, 38].

Окрему роль аналітики Р. Моландер, Е. Рідлі та П. Вільсон відводять стратегічній розвідці, вказуючи на такі її особливості в інформаційному суспільстві: складність визначення джерел збору інформації та застарілість геостра-

тегічного підходу виключно фокусуванням на національних державах, що зумовлює необхідність включення в поле зору недержавних акторів; труднощі у створенні сталого списку потенційних загроз, що пов'язано зі складною мультиполярністю (чи новою біполярністю) світу, де складно визначити, хто є ворог і на що він здатен [10, с. 24].

Згідно з думкою дослідників К. Манстед і Е. Розенбах, на сьогодні інформація є найбільш значущим та конкурентним геополітичним ресурсом та «новою нафтою», який не лише здатний завдавати економічних втрат, але і впливати на міжнародні відносини, що зумовлює гонитву держав та недержавних акторів за інформаційною владою. Дослідники наголошують, що авторитарні уряди вже давно усвідомили колосальну роль інформації і, як наслідок, обмежують своє внутрішнє інформаційне середовище й відмежовують своїх громадян від глобальних інформаційних потоків, водночас перетворюючи інформацію на зброю і використовуючи її проти демократичних держав. Зокрема, Китай та Росія вважають, що стратегічна конкуренція за володіння інформацією у XXI ст. є так званим «змаганням із нульовою сумою», себто є переможець і є переможений; також ці держави надають великого значення технологіям та талантам для перетворення набору даних на корисну інформацію. Однак демократії залишаються принципово не готовими до стратегічної конкуренції в інформаційну еру. Зокрема, із закінченням холодної війни перевага США в інформаційних технологіях була беззаперечною, проте у XXI ст. важливість інформації як геополітичного ресурсу для США зросла, а інформаційна перевага зменшилась. Демократії також вважали втручання у внутрішній інформаційний простір чимось на кшталт дистопії Дж. Оруелла, а інформаційні стратегії непотрібними з огляду на дружню зовнішню політику. Отже, щоб мати змогу конкурувати з авторитарними режимами в боротьбі за інформаційну перевагу, демократіям слід приділити належну увагу розвитку національної безпекової та економічної стратегії щодо геополітики інформації [11].

Відзначимо, що складниками сучасного глобального інформаційного простору є організаційні структури, інформаційні ресурси (регіональні, національні та світові), інформаційна інфраструктура та медіасистеми і засоби масової комунікації [12, с. 118]. Серед засобів масової комунікації чільне місце посідають ЗМІ, що відіграють ключову роль у формуванні громадської думки та політичному житті більшості держав. Це робить ЗМІ одним із найефективніших інструментів маніпуляції громадською думкою та впливу на інформаційну безпеку. Тому варто розглянути такі фактори впливу на самі ЗМІ: нормативно-правове регулювання, яке повинно включати баланс між надмірним контролем та цілковитою безкарністю для суб'єктів, які вислов-

люють людиноненависницькі та антидержавні ідеї тощо під соусом «демократичної свободи слова»; комерціалізація ЗМІ, тобто основна мета – отримання прибутку, а найкраще продається скандальна інформація з мінімумом змістового навантаження (неймовірні фейкові факти, насильство тощо), тобто спрацьовує так звана ринкова цензура; залежність від власника, що, відповідно, зумовлює представлення інтересів групи, яка лобіюється самим власником [13, с. 190–195].

З точки зору ІІсО важливою є емоційний складник подачі інформації, який повною мірою здатне забезпечити телебачення. Рухомий відеоряд створює ефект присутності та зумовлює ідентифікацію глядача з подіями, що є дуже переконливим та зводиться до логіки на підсвідомому рівні, що якщо «я бачу на власні очі – отже, це правда».

Ми вважаємо, що в контексті сучасних ІВ та ролі в них ЗМІ заслуговує на увагу таке медійне явище, як інфотеймент. Інфотеймент – це парасольковий термін, що охоплює поєднання інформації та розваги в межах різних медіажанрів. Сам лінгвістичний термін являє собою злиття двох слів – інформація (information) та розвага (entertainment) – і означає два взаємопов’язані напрямки: новини, що стають більш розважальними, та розваги, які порушують політичні питання. Прикметно, що поява цього явища сягає кінця 1980-х рр., що, на нашу думку, дозволяє провести паралель із завершенням блокового протистояння та демократизацією суспільства в цілому. За рахунок легкої подачі інформації інфотеймент здатний залучити значно ширшу аудиторію, ніж суха подача новин, оскільки, згідно з медійною теорією «користі і задоволення», споживання медіа відбувається не лише з метою отримання інформації, але й розваги, формування думки та підготовки до майбутніх політичних та соціальних подій. Серед жанрів інфотейменту доцільно виділити ті, які ми вважаємо найбільш вдалим для використання з метою здійснення пропагандистської діяльності, а саме: політична сатира, політичні ток-шоу та політична фантастика (наприклад політичні фантастичні серіали). Різноманітність жанрів та відсутність монополії на таку медійну продукцію вочевидь роблять інфотеймент надійним інструментом для пропаганди та просування потрібних наративів у ненав’язливій, розважальній формі [14].

Важливо відмітити, що у 2001 р. американські спеціалісти Дж. Аркіла та Д. Ронфельд з Науково-дослідного інституту національної оборони (National Defense Research Institute) розробили концепцію мережевих воєн. У звіті «Поява мережевих воєн» («The advent of the netwar») наголошується на різниці між кібервійнами та мережевими війнами, а саме: кібервійни мають місце в конфліктах високої та середньої інтенсивності, спрямовані проти урядових та військових мереж, тобто пов’язані з воєнними діями; мережеві війни ха-

рактерні для конфліктів низької інтенсивності, тобто з цивільного боку із залученням недержавних, невійськових та інших нерегулярних сил. Ці два терміни спираються на два твердження: конфлікти все більше і більше залежатимуть та відбуватимуться навколо інформації та комунікації; інформаційна революція зміцнює не ієрархічні, а мережеві форми організації. Отже, мережева війна – це конфлікт на соціальному (цивільному) рівні, що включає невоенні дії та учасників, що спираються на мережеві форми організації (злочинці, терористи, радикали та революціонери нової ери тощо), себто складаються з невеличких груп які комунікують за допомогою інтернету, часто без штаб-квартири чи централізованого управління (наприклад «Хамас»). Необхідність нового терміна зумовлена низкою відмінностей від кібервійни: мережа розпорошених, взаємопов'язаних вузлів, мінімум ієрархії, відсутність центрального командування, локальна ініціатива – панархія, централізована доктрина та децентралізована тактика, тісна комунікація та функціональна інформація. Можливості наступальних дій є такими: функціональна диференціація з інтероперабельністю (взаємозамінністю), значні можливості мобілізації, проникнення та збереження секретності. Можливості оборони: гнучкість, складність зламати та перемогти як цілісну організацію. Також характерним є стирання меж між нападом та захистом. Таку мережеву структуру мають, зокрема, транснаціональні кримінальні організації, терористичні та сепаратистські угруповання. Ці мережеві структури становлять різний рівень загрози: глобальний з метою зміни світопорядку (наприклад радикальні ісламісти, недержавні активісти та ідеологічні рухи інформаційної ери); інші протагоністи, які можуть бути регіональними або локальними (більшість етнонаціоналістичних рухів, повстанці тощо); вертикальні та горизонтальні комунікації та зв'язки, що означає можливість використання локальних груп глобальними акторами та можливість зв'язків між локальними та транснаціональними групами. Отже, мережеві війни – це логічний наслідок інформаційної революції, яка уможливила тісний зв'язок між елементами [15].

Згідно з теорією мережевих війн, як зазначає дослідник А. Худолій, сучасні конфлікти відбуваються в чотирьох сферах – фізичній, інформаційній, когнітивній і соціальній. Вирішальний ефект досягається за рахунок системного використання всіх цих елементів. Фізична сфера є традиційною для війни, саме в ній відбувається зіткнення фізичних сил у часі та просторі. Інформаційна сфера складається з самої інформації; осіб, організацій та систем, які отримують, обробляють та передають інформацію; а також когнітивного, віртуального та фізичного простору, у якому це все відбувається. Когнітивна – це ментальна сфера особи, яка приймає рішення, та цільова аудиторія, у межах якої люди думають, сприймають, уявляють та вирішують. Соціальна

сфера охоплює низку факторів, серед яких – соціальні, культурні та поведінкові фактори, що характеризують ставлення та діяльність населення конкретного регіону або оперативного середовища [7, с. 108].

Висновки. Із закінченням холодної війни біполярна система міжнародних відносин відійшла в історію. Ці зміни в міжнародних відносинах відбуваються на тлі інформаційної революції, яка створила нові виклики для національної безпеки держав: складність ідентифікації ворога та передбачення інформаційних атак, виникнення мережевих структур (зокрема терористичних організацій), що протистоять державним і наділені потужністю та можливостями, сумірними з державними; потужні ЗМІ, у тому числі інтернет-джерела, які формують громадську думку і можуть бути інструментами в руках ворога як всередині держави, так і за її межами.

Таким чином, інформаційні війни – це особливий феномен, який у політичному аспекті є продовженням 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. Це новітня форма боротьби ХХІ ст., яка призводить до ураження всіх сфер функціонування держави. Інформаційні війни небезпечні тим, що з їхньою допомогою можуть вестися неоголошені, невидимі війни, які загрожують міжнародній безпеці. Тому розроблення заходів захисту повинно стати пріоритетним у політиці національної безпеки як окремої держави, так і світового співтовариства загалом.

Значимо, що запорукою перемоги в інформаційній війні передусім є ініціатива держави в інформаційному просторі противника, коли вдається поширювати власні наративи й порядок денний, змушувати противника реагувати та захищатися.

ЛІТЕРАТУРА

1. Почепцов Г. Г. Інформаційна політика : навч. посіб. Київ : Знання, 2008. 663 с.
2. Гібридна війна і журналістика. Проблеми інформаційної безпеки: навч. посіб. / за заг. ред. В. О. Жадька; ред.-упор.: О. І. Харитоненко, Ю. С. Полтавець. Київ : Вид-во НПУ імені М. П. Драгоманова, 2018. 356 с.
3. Юськів Б. М. Опорний конспект лекцій з дисципліни «Інформаційні війни» для студентів спеціальності 7.030404 «Міжнародна інформація». Рівне : РІС КСУ, 2003. 55 с.
4. Department of Defense. Information Warfare: Department of Defense. *Internet Archive 1992*: Desember 21, 1992, Number TS-3600.1. URL: <https://archive.org/det>

- ails/14F0492Doc01DirectiveTS3600.1/page/n3/mode/2up. (дата звернення 22. 06. 2024).
5. Дубас О. Інформаційна війна: нові можливості політичного протидорства. *Освіта регіону: політологія, психологія, комунікації*. 2010. № 1. С. 69–73.
 6. Скулиш Є. Історія інформаційно-психологічного протидорства. Київ : Наук.-вид. від. Нац. акад. СБ України, 2012. 211 с.
 7. Худолій А. О. Інформаційна війна 2014–2022 рр. : монографія. Острого : Вид-во Нац. ун-ту «Острозька академія», 2022. 208 с.
 8. Khalilzad Z. Strategic Appraisal The Changing Role of Information in Warfare. *RAND 1999*: 1999, Number MR-1016-AF. doi: <https://doi.org/10.7249/MR1016>.
 9. Hundley R. The Global Course of the Information Revolution Recurring Themes and Regional Variations. *RAND 2003*: 2003, Number MR-1680-NIC. doi: <https://doi.org/10.7249/MR1680>.
 10. Molander R., Riddile A., Wilson P. Strategic Information Warfare A New Face of War. *RAND 1996*: 1996, Number MR-661-OSD. doi: <https://doi.org/10.7249/MR661>.
 11. Mansted K., Rosenbach E. The Geopolitics of Information. *Australian national university 2019*: May 28, 2019. URL: <https://nsc.crawford.anu.edu.au/departments-news/14338/geopolitics-information> (дата звернення 20. 06. 2024).
 12. Горбулін В. Світова гібридна війна: український фронт. Київ : НІДС, 2017. 496 с.
 13. Петрик В. Інформаційно-психологічне протидорство. Київ : Київ. політехн. ін-т ім. І. Сікорського, 2018. 386 с.
 14. Букс. М. Інформаційно-розважальна система. *Міжнародна енциклопедія досліджень журналістики*. 2019. April 29. doi: <https://doi.org/10.1002/9781118841570.iej0132>.
 15. Arquilla J. The Advent Of Netwar. *RAND 1996*: Number MR-789-OSD. doi: <https://doi.org/10.7249/MR789>.

REFERENCES

1. Pocheptsov, H. H. (2008). *Informatsiina polityka*. Kyiv: Znannia [in Ukrainian].
2. Hibrydna viina i zhurnalistyka. Problemy informatsiinoi bezpeky. (2018). V. O. Zhadka (Ed.). Kyiv: Vyd-vo NPU imeni M. P. Drahomanova [in Ukrainian].
3. Iuskiv, B. M. (2003). *Opornyi konspekt lektsii z dystsypliny «Informatsiini viiny»*. Rivne: RIS KSU [in Ukrainian].
4. Department of Defense. TS-3600.1 Information Warfare: Department of Defense. *Internet Archive*. URL: <https://archive.org/details/14F0492Doc01DirectiveTS3600.1/page/n3/mode/2up>. (Last accessed: 22. 06. 2024).
5. Dubas, O. (2010). *Informatsiina viina: novi mozhlyvosti politychnoho protyborstva. Osvita rehionu: politolohiia, psykhologhiia, komunikatsii – Education of the region: political science, psychology, communications, 1, 69–73* [in Ukrainian].

6. Skulysh, Ye. (2012). *Istoriia informatsiino-psykholohichnoho protyborstva*. Kyiv: Naukovo-vyd. vid. Nats. akad. SB Ukrainy [in Ukrainian].
7. Khudolii, A. O. (2022). *Informatsiina viina 2014–2022 rr.* Ostroh: Vydavnytstvo Natsionalnoho universytetu «Ostrozka akademii» [in Ukrainian].
8. Khalilzad, Z. (1999). Strategic Appraisal The Changing Role of Information in Warfare. *RAND, MR-1016-AF*. doi: <https://doi.org/10.7249/MR1016>
9. Hundley, R. (2003). The Global Course of the Information Revolution Recurring Themes and Regional Variations. *RAND, MR-1680-NIC*. doi: <https://doi.org/10.7249/MR1680>
10. Molander, R., Riddile, A., Wilson, P. (1996). Strategic Information Warfare A New Face of War. *RAND, MR-661-OSD*. doi: <https://doi.org/10.7249/MR661>
11. Mansted, K., Rosenbach, E. (2019). The Geopolitics of Information. *Australian national university*. URL:<https://nsc.crawford.anu.edu.au/department-news/14338/geopolitics-information> (Last accessed: 20. 06. 2024).
12. Horbulin, V. (2017). *Svitova hibrydna viina: ukrainskyi front*. Kyiv: NIDS [in Ukrainian].
13. Petryk, V. (2018). *Informatsiino-psykholohichne protyborstvo*. Kyiv: Kyiv. politekhn. in-t im. I. Sikorskoho [in Ukrainian].
14. Buks, M. (2019). Informatsiino-rozvezhalna systema. *U Mizhnarodnii entsyklopedii doslidzhen zhurnalistyky*. doi: 10.1002/9781118841570.iej0132 [in Ukrainian].
15. Arquilla, J. (1996). The Advent Of Netwar. *RAND, MR-789-OSD*. doi: <https://doi.org/10.7249/MR789>

Oksana Mykolaivna Kundeus, Candidate of Political Sciences, Associate Professor, Associate Professor of the Department of International Relations, Rivne State University of Humanities, Ukraine, Rivne.

Olga Vitaliivna Kret, Candidate of Political Sciences, Associate Professor, Associate Professor of the Department of International Relations, Rivne State University of Humanities, Ukraine, Rivne.

Inna Volodymyrivna Vivchar, Candidate of Political Sciences, Associate Professor of the Department of International Relations, Rivne State University of Humanities, Ukraine, Rivne.

INFORMATION WARFARE: ESSENCE AND FEATURES (END OF THE 20TH BEGINNING OF THE 21ST CENTURY)

The scientific research highlights the problem of the growth and formation of the concept of information war at the border of the 20th and 21st centuries, which was caused

by the end of the «Cold War» and the collapse of the bipolar system of international relations. The main approaches to defining the content of the concept of «information war», its principles and tasks are analyzed. Information warfare is defined as an integral part of ideological struggle.

Keywords: *information warfare, psychological warfare, information confrontation, network warfare, strategic intelligence.*

