

ПРО ТРАКТУВАННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ: ВІД ТЕХНІЧНО-КІБЕРНЕТИЧНОЇ ДО ІСТОРИКО-ПСИХОЛОГІЧНОЇ ПАРАДИГМИ

Мелекєсцев Кирило Ігорович,
*кандидат історичних наук,
старший викладач кафедри історії України
та спеціальних галузей історичної науки
Донецького національного університету
імені Василя Стуса
k.melekestsev@donnu.edu.ua
orcid.org/0000-0003-4931-9576*

У дослідженні аналізуються питання зміни дефініції поняття «інформаційна війна» в роботах українських і зарубіжних дослідників та генезу цього поняття. А саме чому західних авторів цікавили здебільшого технічно-кібернетичні аспекти поняття (що розглядають інформацію в математичному полі), а українських авторів, особливо істориків і політологів, історико-психологічні (інформація в призмі пропаганди). **Мета дослідження** – проаналізувати відмінності між «історико-психологічним» та «технологічно-кібернетичним» розумінням поняття «інформаційна війна» (та варіацій) в українській і зарубіжній літературі, дослідивши хронологію, причини і наслідки цих відмінностей. **Методи дослідження** ґрунтуються на компаративному аналізі, порівнюючи явища вертикально (хронологічні зміни у трактуванні інформаційної війни) та горизонтально (регіональні відмінності). Визначивши хронологію читання поняття в Україні, ми ідентифікуємо генезу поняття та час виникнення відмінностей у його прочитанні між регіонами Земної кулі. **Результати дослідження:** 1) трактування «інформаційної війни» у Європі та в Північній Америці має за генезу роботи канадського культуролога М. Маклуена 1960-х рр., проте з його праць про медіум були зроблені різні висновки у різних регіонах; 2) історико-психологічне трактування було присутнє в американській дослідницькій думці навіть до 2010-х рр., проте прогало у «боротьбі за увагу» (і фінансування) технологічно-кібернетичній парадигмі у 1990-х рр.; 3) історичний розвиток перших десятиліть ХХІ ст. показав США необхідність знов звернути увагу на психологічні операції серед усіх аспектів інформаційних операцій; 4) поняття «інформаційна війна» не є ідеальним перекладом англійського “information warfare”, натомість слід говорити про інформаційні методи ведення війни чи про інформаційне протистояння.

Ключові слова: інформаційна війна, інформаційне протистояння, інформаційні операції, історіографія, кібервійна, психологічні операції.

ON THE DEFINITIONS OF INFORMATION WARFARE: FROM A TECHNICAL-CYBERWAR TO A HISTORICAL-PSYOP PARADIGM

Mieliekiestsev Kyrylo Ihorovych,
*Candidate of Historical Sciences,
Senior Lecturer at the History of Ukraine
and Auxiliary Sciences of History Department
Vasyl' Stus Donetsk National University
k.melekestsev@donnu.edu.ua
orcid.org/0000-0003-4931-9576*

The study analyzes changes in the definition of “information war” in the works of Ukrainian and foreign researchers and the genesis of this concept. Namely, why Western authors were mostly interested in technical and cybernetic aspects of the concept (considering information in the mathematical field), while Ukrainian authors, especially historians and political scientists, have shown interest in historical and psychological (information in the context of propaganda). **The purpose of the study** is to analyze differences between the “historical-psychological” and “technological-cybernetic” understanding of the concept of “information warfare” (and its variations) in Ukrainian and foreign literature, examining the chronology, causes and consequences of these differences. **Research methods** are based on comparative analysis, comparing phenomena vertically (chronological changes in the interpretation of information warfare) and horizontally (regional differences). Having determined the chronology of how the concept is read in Ukraine, we identify the genesis of the concept and the time of differences in defining it between the regions of the world. **The results of the study:** 1) the interpretations of “information warfare” in both Europe and North America have their origins in the works of Canadian culturologist M. McLuhan in the 1960s, however, various conclusions were made in different regions from his works on

the medium; 2) historical and psychological aspects were present in American thought even before the 2010s, but lost in the “struggle for recognition” (and funding) to the technological-cybernetic paradigm in the 1990s; 3) the historical development of the first decades of the 21st century has shown the United States the need to pay attention to psychological operations among all aspects of information operations again; 4) the concept of “information war” present in Ukrainian works is not an ideal translation of the English “information warfare”, as the term is about information methods of waging war, not of an “information war” in itself.

Key words: information war, information warfare, information operations, historiography, cyberwar, psychological operations.

Вступ. Поняття «інформаційна війна» нерідко трапляється у сучасних обговореннях історії України, що стає об’єктом пропаганди. Проте, спробувавши пошукати конкретну дефініцію та генезу поняття, можна знайти досить відмінні характеристики, які здебільшого можна поділити на дві групи: технічно-кібернетичні (що розглядають інформацію в математичному полі) та історико-психологічні (інформація в призмі пропаганди). Як і чому з’явилися такі кардинально різні читання одного поняття, допоможуть відповісти історія та історіографія.

Мета дослідження – проаналізувати відмінності між «історико-психологічним» та «технологічно-кібернетичним» розумінням поняття «інформаційна війна» (та варіацій) в українській і зарубіжній літературі, дослідивши хронологію, причини і наслідки цих відмінностей.

За **методологією** дослідження являє собою компаративний аналіз літератури, порівнюючи явища вертикально (хронологічні зміни у трактуванні інформаційної війни) та горизонтально (регіональні відмінності). Визначивши хронологію читання поняття в Україні, ми ідентифікуємо генезу поняття та час виникнення відмінностей у його прочитанні між різними регіонами Земної кулі.

Поява широкого поняття та знайомство з ним в Україні. «Інформаційній війні» в Україні станом на 2022 р. приділили чимало уваги. У 2015 р. ужгородський дослідник Г. Сасин розкрив хронологію дослідження (та пошуку дефініції) явища в локальному для українських дослідників інформаційно-науковому просторі таким чином: перші відкриті публіци дослідження канадського культуролога Герберта Маршала Маклуена у 1960-х рр., монографія 2003 р. московського автора С. Расторгуєва, услід – численні роботи українських авторів, які особливо активізувалися з початком московського збройного вторгнення в Україну у 2014 р. (Сасин, 2015). Це яскраво характеризує українське зацікавлення темою як певний “problem-solving”, набуття нею актуальності разом з руйнацією статус-кво, коли явище інформаційних впливів з метою досягнення військової мети стали частіше «помічати». З цієї хронології зрозумілою також стає специфіка визначення поняття українськими авторами, здебільшого істориками та політологами: Р. Чирва,

Є. Магда, І. Костюк, Д. Богуш та О. Юдін так чи інакше відштовхуються від психологічного, пропагандистського виміру інформаційної війни. Дослідження саме такого аспекту інформаційного протистояння є досить логічним для українських гуманітаріїв, навіть якщо «першопроходець» М. Маклауен оперував у ширшій парадигмі інформації, залучаючи до поняття навіть електричне світло, що зробило економічну діяльність сучасного суспільства цілодобовою (McLuhan, 1975).

Звичайно, що є винятки з тенденції українських дослідників фокусуватися саме на «пропагандистському» аспекті інформаційної війни. П. Шпиґа та Р. Рудник зазначають 4 різні підходи до визначення поняття, два з яких ближче до північноамериканського дискурсу щодо проблеми: використання новітніх електронних засобів та кібернетичних атак, тобто погляд на інформацію крізь призму комп’ютерних даних (Шпиґа, 2014: 328). Про «віртуально-кібернетичний» підхід розкриття інформаційної війни в математичному вимірі також пише Б. Шемчук (Шемчук, 2019). Саме цей аспект того, що в англійській літературі відомо під назвою “information warfare”, до останнього часу був основним у дослідженні цього явища у США та Канаді. Можна сказати, що слова культуролога М. Маклауена “the medium is the message” по-різному сприйняли продовжувачі у Старому та Новому світі: перші сконцентрувалися на видах і сутності впливу медій на людей, а останні – на значенні медіума як засобу комунікації. Лише у другій декаді ХХІ століття спостерігається зближення північноамериканських та європейських дослідників питання з відокремленням “information warfare” та “cyberwarfare”.

Реформи розвідки та збройних сил і зміни парадигми у США. Звичайно, у США так само визначали різні царини інформаційного протистояння, серед них і психологічну, але фокусувалися саме на значенні для військової справи сучасних носіїв інформації: електронних комунікацій та засобів глобального зв’язку. Каліфорнійський дослідник М. Лібіцкі (свого часу представник впливового аналітичного центру RAND Corporation) у 1995 р. був критиком самого поняття “information warfare”, зазначаючи його абстрактність, широкість тлумачення, а також низьку актуальність для власне військової справи. Ба більше, на думку дослідника, не можна було

взагалі говорити про окрему «інформаційну» техніку ведення війни, натомість, існує кілька різних форм інформаційного протистояння, «кожна з яких претендує на визначальну роль у концепції». Таких форм М. Лібіцкі виокремив сім, фактично здебільшого повторивши варіативність інформаційних операцій за класифікацією Збройних сил США, але з додатком визначеного ще М. Маклауеном економічного фактора. А саме: 1) командно-диспетчерське протистояння завдає ударів по центрах прийняття рішень ворога та їх комунікації з рештою сил; 2) протистояння розвідки з урахуванням розробки та захисту систем пошуку знань щодо поля бою; 3) радіоелектронне та криптографічне протистояння; 4) психологічні операції, в яких інформація використовується, щоб вплинути на свідомість союзників, нейтральної сторони та супротивників; 5) хакерська війна, під час якої атакуються комп'ютерні системи; 6) економічна інформаційна війна з блокуванням інформації або її контролю задля досягнення економічного панування; 7) кібервійна, «здебільшого футуристична» (прим авт.: станом на 1995 рік) (Libicki, 1995).

Всі ці форми, на думку дослідника, були мінімально пов'язані між собою, мало придатні для аналізу за фактами і, зрештою, стосуються або історичного досвіду про те, що інформаційні технології впливають, але не контролюють ведення бойових дій, до «фантастичного, на кшталт припущення про суспільства та організації, які необов'язково є істинними» (описуючи ідею «глобального села» та фразу про «істинно тотальну війну за допомогою інформації» М. Маклауена). Проте чи не найбільш яскравим елементом «розгромної» роботи М. Лібіцкі буде той факт, що, надавши цілих сім варіантів трактування поняття, він все одно фокусується не на психологічній чи економічній, а саме на технічній стороні питання. Саме технічного аспекту ведення бойових дій стосуються контраргументи американського автора: що атаки на інформаційні системи не стануть доцільнішими просто через більшу поширеність тих систем; що якщо «монолітні комп'ютерні, комунікаційні архітектури» поступаються місцем розподіленим системам, то віддача від багатьох форм інформаційної війни зменшується; що інформація взагалі не актуальний медіум для ведення бойових дій, «за винятком деяких вузьких аспектів, таких як електронні перешкоди зв'язку» (Libicki, 1995). Тобто, знаючи в теорії про психологічну компоненту інформаційного протистояння, опонент розвитку цього напрямку знань (а йдеться про аналітичне дослідження, складене на замовлення Департаменту оборони США) взагалі проігнорував таке явище у висновках, а сконцентрував свої аргументи на технічних питаннях, які, з іншого боку, майже не враховувалися

європейськими дослідниками. Між тим за визначенням, що міститься у Спільній публікації 3-13 для Збройних сил США, «до інформаційних операцій відносять комплексне застосування засобів електронної боротьби (EW), операції комп'ютерної мережі (CNO), психологічні операції (PSYOP), військову хитрість (MILDEC) та забезпечення безпеки оперативників (OPSEC) у поєднанні з визначеними допоміжними та пов'язаними з ними можливостями впливати, порушувати, змінювати чи брати під контроль ворожі людські чи автоматизовані засоби прийняття рішень, захищаючи власні» (Joint Publication 3-13, 2014). Тобто, незважаючи на критику об'єднання таких різних напрямів під однією «парасолькою» (різниця з переліком сфер інформаційного протистояння за М. Лібіцкі лише у відсутності економічної боротьби, з винесенням командно-диспетчерської частини у «допоміжні та пов'язані впливи»), «широка» парадигма інформаційного ведення війни залишилася актуальною у сучасній американській військовій науці з 2014 р. Однак цьому передував період схвалення критики М. Лібіцкі, який запропонував обмежити інформаційні операції до «дешевого» штабу хакерів.

Цілком можливо, що головною частиною дискусії було саме питання алокації коштів на розвиток тієї чи іншої парадигми розвитку Збройних сил США. У службовій записці щодо питань інформаційного протистояння до звіту «Снайдерівської комісії» про результати реформування діяльності розвідки від 1997 р. Б. Люїс назвав М. Лібіцкі експертом з питання інфоборотьби, але при цьому дав таку характеристику: «Лібіцкі хоче, щоб уряд спочатку визначив, наскільки вразливою взагалі є національна інформаційна інфраструктура. Він хоче фінансування досліджень і розробок щодо посилення методів безпеки та їх своєчасного поширення. Він вважає, що уряд США має працювати над досягненням міжнародного консенсусу щодо того, що таке погана поведінка з боку держави та які відповідні міри щодо цього можуть бути. Він підкреслює, що уряд не повинен витратити більше зусиль на традиційну розвідку для інформаційної війни. Щоб бути хакером, потрібно зовсім небагато, здебільшого розум і мотивація – дві речі, які на око не виміряти. Кваліфікований хакер може використовувати домашню комп'ютерну систему для проникнення в безліч систем» (Lewis, 1997). Тобто як спеціаліст у своїй сфері (хакерство) М. Лібіцкі був взагалі противником розширення сутності інформаційного протистояння та інфооперацій та бажав зосередження коштів держави саме на питаннях хакерства і захисту від нього. Саме це пояснює «забутий» ним гуманітарний аспект поняття.

«Забутий» гуманітарний аспект та «війни п'ятого покоління». Щодо пропонентів теорії

інформаційного протистояння, причому з урахуванням саме гуманітарного складника, то в тому ж 1995 р. вийшла стаття Р. Шапранскі “Theory of Information Warfare: Preparing for 2020”, яка, споглядаючи з 2022 р., справді вийшла значно більш «візіонерською» щодо інформаційної компоненти у війнах майбутнього. Продовжуючи слова М. Маклуена про те, що Третя світова війна стане «партизанською інформаційною війною без поділу на військових та цивільних», Р. Шапранскі проаналізував децентралізацію центрів впливу на конфлікти та центрів прийняття рішень у контексті глобалізації та підвищення рівня доступності інформації для широких народних мас. Звичайно, стаття не обходить і технічних аспектів, електронної та «кібервійни», зазначаючи, що залежність супротивника від інформаційних систем для прийняття рішень робить його уразливішим для ворожих маніпуляцій цими системами (маючи на увазі комп’ютерні та інші електронні системи комунікацій). Проте військовий аналітик вийшов за межі технічних методів ведення бойових дій, оглянув значення інформації для стратегічного рівня протистояння: успішними будуть атаки як на знання, так і на системи переконань їхніх людських цілей. Найгострішою цю проблему він вважав саме для демократій, яка, на думку Р. Шапранскі, потребує трьох компонентів для успішної військової справи: народної волі, «правди на своїй стороні» та технологічної переваги. «Якщо ж втрачається впевненість у моральності дій своєї сторони, то як в ефекті доміно за нею зникне народна підтримка, технологічне верховенство, і, врешті, зникнуть збройні сили» – фраза автора втілює у собі дух старої американської ідеалполітики, при цьому є катастрофічно правдивою в історичних контекстах американського суспільства після В’єтнамської війни та після Іракської війни: втрата впевненості у справедливості війни вдаряла по американських збройних силах більше, ніж будь-які конкретні воєнні негаразди. Проаналізувавши різні компоненти ідеї, автор зробив рекомендацію: «інструменти» є під рукою, і оскільки інформаційна зброя є потужною, ба більше, універсальною, то завданням держави має бути надання захисту від неї як для комбатантів, так і для цивільних. При цьому з поширенням доступу до інформаційних систем у світі інформаційне протистояння буде відбуватися незалежно від держави та поза її контролем, тому в інтересах держави є отримання хоча б часткового контролю над ситуацією через створення зброї інформаційного протистояння та проведення інформаційних атак (Szapranski, 1995).

Ідеї Р. Шапранскі заклали основу для сучасного розширення парадигми інформаційного протистояння від такої, що зосереджена навколо протистояння комп’ютерних та інших електронних

систем, до поєднання вивчення новітніх інформаційних систем з прийомами їх використання для психологічного впливу. З урахуванням зміни парадигми у військово-аналітичному дискурсі США з’явився термін «Війна п’ятого покоління» (*Fifth Generation Warfare, 5GW*). У 2009 році у статті Д. Екса про війни п’ятого покоління зазначено: «наступне покоління війни – так зване «п’яте покоління» – не матиме армій або чітких ідей. Це буде «вир насильства», багатостороннє та неочікуване руйнування, мотивоване більше масовим розчаруванням, ніж якимись послідовними планами на майбутнє. 5GW – це те, що відбувається, коли незадоволені люди світу спрямовують свій відчай на найочевидніший символ усього, чого їм не вистачає» (Ахе, 2009). США «у світі після 11 вересня 2001 року» не могли вже ігнорувати психологічний, ідеологічний аспекти війни, а результати Іракської війни (зокрема, викриття неправдивості заяв уряду про боротьбу саме зі зброєю масового знищення) актуалізували «копирсання в історії» на фоні деморалізації американців, їхньої зневіри у зовнішній політиці.

«Війна» чи «протистояння»? У всьому вищеописаному обговоренні понять щодо використання інформації взагалі і кібернетичної її сторони у військовій справі західні автори завжди використовують поняття “information warfare”, “cyber warfare”, а не “infowar, cyberwar”, тим часом в українській літературі здебільшого трапляється саме «інформаційна війна». У чому ж відмінність? Дослідник Джеймс Грін вдало пояснив, що “cyber warfare” відрізняється від терміна “cyberwar” тим, що “warfare” не означає масштаби, затягування в часі чи рівень руйнування, які зазвичай асоціюються з терміном «війна». Тобто “cyber warfare” включає прийоми, тактику та процедури, які можуть бути використані в гіпотетичній “cyber war”. Адже поняття «війна» передбачає великомасштабні дії, як правило, протягом тривалого періоду часу із застосуванням насильства задля досягнення цілей. Тому «кібервійна» мала б являти собою тривалий період обміну прямими кібератаками між націями з масштабним руйнуванням. Станом натеper таких війн не спостерігалось. Натомість, використовуються військові кібероперації за принципом «око за око» (2019 р. – кібератака США проти іранських систем озброєння у відповідь на збиття американського безпілотнока) (Green, 2016; Barnes, 2019).

Екстраполюючи з «кібервійни» на загальний контекст інформаційного протистояння, «інформаційною війною» слід було б називати тривалий конфлікт з обміном інформаційними атаками між силами, в ході якої самі інформаційні операції могли б завдати шкоди, за кількістю та якісним характером на рівні конвенційної війни. Таких

війн в історії людства ще не було. Натомість, можемо говорити про інформаційне протистояння, яке являє собою сукупність інформаційних операцій (як з боку державних, так і недержавних акторів міжнародних відносин), які сприяють підготовці, обґрунтуванню та проведенню воєнних дій. Тож поширений термін “information warfare” слід перекладати саме як «інформаційне протистояння», або «інформаційні методи війни».

Альтернативні «інформаційній війні» версії читання поняття і раніше використовувалися українськими дослідниками. Серед них і різні трактування «інформаційного протистояння», зокрема, як аспекту, а не аналогу «інформаційної війни». Думки істориків, політологів, правників, літературознавців, культурологів щодо трактування «інформаційного протистояння» можуть бути темою окремої статті, але навіть це визначення не є єдиною альтернативою. Конкретно дослідник О. Саприкін зазначав, що інформаційна експансія є набагато місткішим поняттям, ніж «інформаційна війна» або «інформаційна атака», даючи такий опис технології: «система, що склалася в засобах інформації розвинених держав,

і методи, використані для пропагандистського забезпечення певних геополітичних цілей» (Саприкін, 2013: 40).

Висновки. Таким чином, розглянутий матеріал провокує такі висновки: 1) трактування «інформаційної війни» у Європі та в Північній Америці має за генезу роботи канадського культуролога М. Маклуена 1960-х рр., проте з його праць про медіум були зроблені різні висновки у різних регіонах; 2) історико-психологічне трактування було присутнє в американській дослідницькій думці навіть до 2010-х рр., проте прогало у «боротьбі за увагу» (і фінансування) технологічно-кібернетичній парадигмі у 1990-х рр.; 3) історичний розвиток перших десятиліть ХХІ ст. показав США необхідність знов звернути увагу на психологічні операції серед усіх аспектів інформаційних операцій; 4) поняття «інформаційна війна» не є ідеальним перекладом англійського “information warfare”, натомість слід говорити про інформаційні методи ведення війни, чи про інформаційне протистояння – теперішній статус останнього визначення в українській науці варто дослідити в окремій статті.

Література:

1. Axe D. How to Win a “Fifth-Generation” War. *Wired*. January 3, 2009. URL: <https://www.wired.com/2009/01/how-to-win-a-fi/> (дата звернення: 28.06.2022).
2. Barnes J. E., Gibbons-Neff T. U.S. Carried Out Cyberattacks on Iran. *The New York Times*. 22 June 2019. URL: <https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html> (дата звернення: 28.06.2022).
3. Green J. A. *Cyber warfare: a multidisciplinary analysis*. London : Routledge, 2016.
4. Joint Publication 3-13. *Information operations*. Washington, DC : Joint Staff, 2014. URL: http://www.fas.org/irp/doddir/dod/jp3_13.pdf (дата звернення: 28.06.2022).
5. Lewis B.C. *Information Warfare. The Final Report of the Snyder Commission* / Ed. by Edward Cheng and Diane C. Snyder. Princeton : Princeton University, 1997. URL: <https://irp.fas.org/eprint/snyder/infowarfare.htm> (дата звернення: 28.06.2022).
6. Libicki M. *What Is Information Warfare?* Washington, DC : National Defense University, 1995. URL: <https://apps.dtic.mil/sti/pdfs/ADA367662.pdf> (дата звернення: 28.06.2022).
7. McLuhan M. *Understanding media: the extension of man*. London : Routledge & Kegan Paul, 1975.
8. Szapranski R. *A Theory of Information Warfare; Preparing for 2020*. Montgomery, Maxwell Air Force Base: Air University, 1995. URL: <https://apps.dtic.mil/sti/citations/ADA328193> (дата звернення: 28.06.2022).
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. Сасин Г.В. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір). *ГРАНІ*. 2015. № 3 (119). С. 18–23.
11. Шемчук В.В. Концептуальні підходи до розуміння інформаційної війни у сучасному світі. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія «Юридичні науки»*. 2019. Т. 30(69), № 3. С. 29–35.

References:

1. Axe, D. (2009) How to Win a “Fifth-Generation” War. *Wired*. January 3, 2009. Retrieved from: <https://www.wired.com/2009/01/how-to-win-a-fi/> [in English].
2. Barnes, J.E., Gibbons-Neff, T. (2019). U.S. Carried Out Cyberattacks on Iran. *The New York Times*. 22 June 2019. Retrieved from: <https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html> [in English].
3. Green, J.A. (2016). *Cyber warfare: a multidisciplinary analysis*. London: Routledge [in English].
4. Joint Publication 3-13. (2014). *Information operations*. Washington, DC: Joint Staff, 2014. Retrieved from: http://www.fas.org/irp/doddir/dod/jp3_13.pdf [in English].

5. Lewis, B.C. (1997) Information Warfare. *The Final Report of the Snyder Commission* / Ed. by Edward Cheng and Diane C. Snyder. Princeton: Princeton University. Retrieved from: <https://irp.fas.org/eprint/snyder/infowarfare.htm> [in English].
6. Libicki, M. (1995). What Is Information Warfare? Washington, DC: National Defense University. Retrieved from: <https://apps.dtic.mil/sti/pdfs/ADA367662.pdf> [in English].
7. McLuhan, M. (1975). *Understanding media: the extension of man*. London: Routledge & Kegan Paul.
8. Szapranski, R. (1995). *A Theory of Information Warfare; Preparing for 2020*. Montgomery, Maxwell Air Force Base: Air University. Retrieved from: <https://apps.dtic.mil/sti/citations/ADA328193> [in English].
9. Saprykin, O. (2013). Informatsiina ekspansiia, informatsiina viina ta informatsiina ataka u zasobakh masovoi informatsii na prykladi Yevro-2012 [Information expansion, information war and information attack in the media on the example of Euro-2012]. *Visnyk Knyzhkovoï palaty*. No. 1. Pp. 40–43 [in Ukrainian].
10. Sasyn, H.V. (2015). Informatsiina viina: sutnist, zasoby realizatsii, rezultaty ta mozhlyvosti protydii (na prykladi rosiiskoi ekspansii v ukrainskyi prostir [Information war: essence, means of realization, results and possibilities of counteraction (on the example of Russian expansion into the Ukrainian space)]. *HRANI*. No. 3 (119). Pp. 18–23 [in Ukrainian].
11. Shemchuk, V.V. (2019). Kontseptualni pidkhody do rozuminnia informatsiinoi viiny v suchasnomu sviti [Conceptual approaches to understanding information war nowadays]. *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V.I. Vernadskoho. Serii „Yurydychni nauky”*. T. 30(69), No. 3. Pp. 29–35 [in Ukrainian].

Стаття надійшла до редакції 30.06.2022
The article was received 30 June 2022