УДК 32.019.51(477)
https://doi.org/10.34142/24130060.2022.25.2.03

# ІНФОРМАЦІЙНА СКЛАДОВА ГІБРИДНОЇ ВІЙНИ: УКРАЇНСЬКІ РЕАЛІЇ

**Ю.С. Дібікова**
Харківський національний педагогічний університет імені Г.С. Сковороди

*У статті висвітлюються питання інформаційного аспекту гібридної війни проти України. З'ясовуються поняття гібридної війни, її сутність, зміст та інформаційна складова. Відбувається дослідження гібридної війни як комбінації конвенційних, нелінійних, асиметричних засобів для досягнення політичних та військових цілей.*

*Відзначено, що гібридна війна – це відносно нове явище, але воно постійно трансформується разом зі змінами, що відбуваються у світі. Одним із суттєвих аспектів гібридної війни є використання медіа та інформаційного простору для поширення пропаганди, фейкових новин, дезінформації, провокацій та маніпулювання громадською думкою.*

*Окреслені основні способи використання сучасних інформаційних технологій в гібридній війні.*

*Акцентовано увагу на тому, що під час повномасштабного російського вторгнення збереження інформаційного суверенітету, забезпечення ефективного функціонування системи безпеки в інформаційній сфері потребують розробки та розвитку дієвих стратегій і тактик протидії сучасним інформаційним загрозам.*

***Ключові слова:*** *гібридна війна, кібератака, мас-медіа, соціальні мережі, громадська думка, кібербезпека*

# INFORMATION COMPONENT OF HYBRID WARFARE: UKRAINIAN REALITIES

**Yu. Dibikova**

*The relevance of the scientific issues of the article is determined by the fact that the modern Ukrainian state is in a complex geopolitical context, in which hybrid warfare has become one of the key challenges for national security.*

*The article highlights the information aspect of the hybrid warfare against Ukraine. The concept of hybrid warfare, its essence, content and informational component are clarified. Hybrid warfare is being researched as a combination of conventional, non-linear, asymmetric means to achieve political and military goals.*

*It was noted that hybrid warfare is a relatively new phenomenon, but it is constantly transforming along with the changes taking place in the world. One of the essential aspects of hybrid warfare is the use of media and information to spread propaganda, fake news, disinformation, provocations, manipulation of public opinion, formation of certain ideas and beliefs among the population, creation of chaos and disinformation, attraction of support from internal and external actors.*

*The main ways of using modern information technologies in hybrid warfare are outlined: cyber-attacks, disinformation and propaganda, information intelligence, impact on cyber-physical systems, cyber espionage, etc.*

*Attention is focused on the fact that during a full-scale Russian invasion, modern Ukraine faces special challenges in the field of information security: preservation of information sovereignty, ensuring the effective functioning of the security system in the information system require the development and development of effective strategies and tactics for countering modern information threats.*

*Ukraine is taking a wide range of measures to counter hybrid warfare, protecting its sovereignty, independence and territorial integrity. The development of a strong and democratic media system, support of independent journalists and initiatives to increase education of cyber security and media literacy, strengthening international cooperation, implementation of technical, institutional, and legislative measures to protect information systems are key factors for overcoming information aggression from the Russian Federation.*

***Key words:*** *hybrid warfare, cyber-attack, mass media, social networks, public opinion, cyber security*

**Постановка проблеми.** Актуальність наукової проблематики статті зумовлена тим, що сучасна українська держава знаходиться у складному геополітичному контексті, в якому гібридна війна стала одним із ключових викликів для національної безпеки. Гібридна війна – це сучасний вид конфлікту, що поєднує в собі військові, політичні, економічні, соціальні та інформаційні засоби впливу з метою досягнення стратегічних цілей. Відповідно, гібридна війна – це форма конфлікту, яка синтезує елементи традиційної військової агресії з нестандартними методами, такими як кібератаки, поширення дезінформації, вплив на громадську думку та ін. Тобто вона має на меті досягнення політичних та військових цілей шляхом використання традиційних військових дій з неофіційними, неконвенційними та нелінійними методами.

Отже, існує потреба у науковому, всебічному дослідженню гібридної війни як соціополітичного феномену сучасного світу, що суттєво трансформує розгортання політичних процесів, функціональне призначення політичних інститутів, стратегії державотворення та практики організації політичного життя. При цьому, інтенсифікації принципів медіатизації політичної дійсності, посилення впливу засобів масової комунікації на розгортання всіх політичних і соціальних процесів (Dibikova, 2021, s. 16) актуалізують дослідження інформаційної складової гібридної війни.

**Аналіз актуальних досліджень.** У сучасному теоретико-методологічному дискурсі існує висока ступінь зацікавленості щодо

дослідження різних аспектів гібридної війни. Значна кількість науковців зробила свій внесок у розуміння сутності гібридного війни, її витоків, чинників і наслідків та запропонували рекомендації щодо протидії та підвищення стійкості країн до таких загроз. Серед дослідників цього явища треба визначити як українських, так і зарубіжних фахівців: М. Айшервуд, С. Асланов, М. Бонд, К. Вітман, А. Вітцель, В. Власюк, В. Горбулін, Г. Динис, Д. Кілкьюллен, М. Лівоніус, Є. Магда, Р. Ньювсон, В. Петрик, Т. Рід, І. Рущенко, І. Тодоров, М. Требін, Френк Г. Хоффман та інші.

**Метою статті** є дослідження інформаційного аспекту гібридної війни проти України.

**Виклад основного матеріалу.** Гібридна війна – це відносно нове явище, але воно постійно трансформується разом зі змінами, що відбуваються у світі. У західній суспільно-політичній думці науковий інтерес щодо гібридних загроз і гібридного способу ведення воєнних дій виник на хвилі розуміння ефективної діяльності Хезболли під час другої Ліванської війни у 2006 р. Уперше згадування цього терміну можна знайти у промові генерал-лейтенанта Джеймса Меттіса 8 вересня 2005 р. (McCulloh & Johnson, 2013, s. 55). Разом з Френком Хоффманом, аналізуючи сучасні виклики глобалізації, новітні технології та практики воєнної науки, вони дійшли висновку, що майбутні війни будуть визначатися саме гібридними способами і стратегіями (Mattis & Hoffman, 2005).

У сучасній науці існують різні визначення гібридної війни. Так, Андреас Вітцель (Andreas Wittel) визначає гібридну війну як конфлікт, в якому здійснюється поєднання різних форм атак і використовується широкий спектр інструментів, що включає як військову силу, так і неофіційні засоби, наприклад, кібератаки, інформаційну війну, дестабілізацію, дезінформацію тощо (Andreas Wittel, 2016).

Відомий сучасний теоретик у галузі збройних конфліктів та воєнно-політичної стратегії Френк Г. Хоффман (Frank Hoffman) вважає гібридну війну системою стратегічних дій, в якій поєднуються різні засоби ведення

бойових дій, включаючи військові, політичні, економічні, інформаційні, культурні та технологічні аспекти. Головна мета гібридної війни – досягти політичної мети шляхом використання різних засобів. Він наголошує, що «поряд із асиметричними конфліктами та неконвенційними війнами (ситуації, коли явні бойові дії не ведуться) існує також поняття «гібридні війни», які зараз усе частіше використовуються» (Hoffman, 2006, s. 38-42). Ф. Хоффман зазначає, що гібридні конфлікти є мультимодальними (тобто такими, що ведуться в різні способи) та багатоваріантними, які не вписуються у рамки простої конструкції ведення збройного конфлікту чи війни. Тобто майбутні загрози можуть більшою мірою бути охарактеризованими як гібридне співвідношення традиційних та нерегулярних стратегій і тактик, де використовуються децентралізоване планування та виконання, участь недержавних акторів із застосуванням одночасно простих і складних технологій (Hoffman, 2007, s. 20-22).

Схожої думки дотримується М. Бонд, яка зазначила, що майбутні війни будуть виглядати як вид гібридної війни, проектуючи усі елементи національної влади уздовж континууму діяльності, пов'язаних зі стабільністю, безпекою, організацією та здійсненням операцій, а також безпосередніми бойовими діями. Водночас вона визначає гібридну війну як парадигму операцій зі стабілізації в несформованих державах (Bond, 2007).

Група стратегічного прогнозування Корпусу морської піхоти США розглядає гібридні війни як об'єднання низки різних режимів ведення війни, в тому числі звичайних можливостей, тактики нерегулярних утворень, терористичних актів, включаючи невибіркове насильство і примус, а також активізацію криміналу в країні (U.S. Marine Corps, 2008, s. 1).

Цікавим є трактування гібридної війни Р. Ньювсона, який під цим терміном розуміє комбінацію конвенційних, іррегулярних та асиметричних засобів, що включають постійну маніпуляцію політичним та ідеологічним конфліктом, а також залучення сил спеціальних операцій та конвенційних збройних сил, агентів розвідки, політичних провокаторів, представників

медіа, економічний шантаж, кібератаки; проксі-сервери і сурогати, паравійськові, терористичні і кримінальні елементи (Newson, 2014.)

Відповідно, у сучасній науці з'являється концепція гібридних війн, що описує новітню війну як сегрегацію конвенційних, нелінійних, асиметричних засобів для досягнення мультимодальних цілей. Важливо відзначити, що поняття гібридної війни є досить широким і може включати різні аспекти залежно від контексту та наукової спрямованості.

Одним із суттєвих аспектів гібридної війни є використання медіа та інформаційного простору для маніпулювання громадською думкою, формування певних уявлень та переконань серед населення, створення хаосу та дезінформації, залучення підтримки з боку внутрішніх і зовнішніх гравців.

Існують різні способи використання сучасних інформаційних технологій в гібридній війні. Серед найпоширеніших є кібератаки, поширення дезінформації та пропаганди, інформаційна розвідка, вплив на кіберфізичні системи, кібершпигунство та ін.

Так, протягом останніх кількох років Україна зазнала численних кібератак з боку РФ. Ці кібератаки були спрямовані на різні сектори інфраструктури та урядові установи з метою завдання шкоди, перешкоджання функціонуванню та збору розвідувальної інформації, для здійснення шкідливих дій, таких як злам систем, крадіжка чи пошкодження інформації, перешкоджання роботі критичних інфраструктурних об'єктів.

Узагалі, можна умовно класифікувати кібератаки на три основні групи: перша – це операції інформаційного впливу, які реалізуються через кібератаки (наприклад, через злам медіа або веб-ресурсів офіційних органів); друга – це кібершпигунство для отримання інформації; третя – це операції ефекту, тобто деструктивні кібероперації, внаслідок яких знищують дані, інфраструктуру тощо (наприклад, атаки на телеком-провайдерів, онлайн-сервіси, зокрема й державні).

Росія почала війну проти України 24 лютого 2022 року, але російські кібератаки проти України тривають із моменту незаконної анексії Росією

Криму у 2014 році, посилившись безпосередньо перед повномасштабним вторгненням у 2022 році. За цей період найбільше постраждали державний, енергетичний, медійний, фінансовий, бізнесовий та некомерційний сектори України.

Одна з найбільш відомих кібератак на Україну була пов'язана з енергетичним сектором. У грудні 2015 року було здійснено кібератаку Blackenergy, яка спричинила масштабне відключення електроенергії в певних регіонах Західної України. Це стало першою документованою кібератакою, яка призвела до реальних наслідків для енергетичної інфраструктури.

Взагалі, з початку війни було здійснено понад 200 тисяч кібератак на об'єкти енергетичної інфраструктури, а водночас за весь 2021 рік їх було зафіксовано 900 тисяч (Enerhoreforma, 2022). Як повідомив заступник міністра енергетики з питань цифрового розвитку, цифрових трансформацій і цифровізації Фарід Сафаров, то «за 47 днів війни кількість кібератак на сферу енергетики перевищила 200 тисяч, тоді як за весь минулий рік їх кількість складала 900 тисяч. За останній період зафіксовано 50 спроб DdoS-атак. Щодо самого міністерства, то тільки за останній тиждень було приблизно 20 тисяч інцидентів з питань кібербезпеки, які мали б уразити його інфраструктуру» (Enerhoreforma, 2022).

Що стосується кібератак на держоргани України, то упродовж 2021 року працівники Служби безпеки України локалізували понад 2 тис. кібератак на електронні ресурси органів влади (DIM, 2022).

Окрім цього, РФ постійно здійснює кібератаки й на медичну інфраструктуру. Так були зареєстровані кібератаки на медичні установи, які намагалися паралізувати роботу систем збереження медичної інформації та надання медичних послуг.

Отже, під час російської військової агресії перед сучасною Україною постають особливі виклики у сфері інформаційної безпеки. Російська держава використовує різні засоби масової комунікації, включаючи телебачення, радіо, Інтернет та соціальні мережі для поширення пропаганди

та маніпулювання громадською думкою. Фейкові новини, дезінформація, провокації та спеціальні інформаційно-психологічні операції (ІПСО) стали невід'ємною частиною гібридної війни, спрямованої на породження хаосу та розколу в українському суспільстві, ліквідацію незалежності України, підрив державного суверенітету, повалення конституційного ладу, посягання на територіальну цілісність держави, замахи на знищення української ідентичності, пропаганду насильства, жорстокості, ідей сепаратизму, розпалювання національної, міжетнічної, релігійної, расової ворожнечі та ненависті, посягання на конституційні права та свободи.

Також сучасні інформаційні технології, що застосовуються у гібридній війні, можуть бути використані для створення сприятливого образу агресора, дискредитації опонента та мобілізації власного населення.

Особливу роль у гібридній війні сьогодні грають соціальні мережі та відеохостинги такі, як Facebook, Twitter, Instagram, TikTok, YouTube тощо, які перетворюються на платформи для широкомасштабного поширення пропаганди, фейкових новин і дезінформації. Адже через створення фальшивих акаунтів та груп можна розповсюджувати спотворену інформацію та маніпулювати громадською думкою. Тобто, соціальні мережі активно використовуються у гібридній війні, надаючи можливість впливати на настрої та думки громадськості шляхом направленого розповсюдження певної інформації, наративів і пропаганди, які спрямовані на створення конфліктів, розпалювання національної ворожнечі, підрив стабільності тощо.

Також соціальні мережі можуть використовуватися для координації гібридних операцій, таких як масові протести, дестабілізація ситуації або організація деструктивних дій. Вони надають можливість швидко об'єднати прихильників та спрямувати їх дії у певному напрямку. Окрім цього, соціальні мережі надають додаткові можливості для здійснення шпигунства та розвідки. Ворог може встановлювати контакт зі співробітниками урядових установ або військових осіб з метою збору інформації або впливу на них.

На особливу увагу заслуговують дослідження тієї ролі, яку відіграють, так звані, «фабрики тролей» (або ботоферми) у сучасній гібридній війні. Оператори цих фабрик, які можуть бути пов'язані з зовнішніми гравцями або діяти на замовлення режиму, використовують велику кількість псевдоакаунтів у соціальних мережах або на інших інтернет-платформах для поширення дезінформації, маніпуляційного впливу на громадську думку, створення конфліктів, провокацій, розхитування суспільства тощо. Операції фабрик тролей можуть ініціюватися та фінансуватися державними структурами, політичними організаціями, приватними компаніями або індивідуальними акторами.

Фабрики тролей зазвичай мають визначені цілі, стратегії та способи поширення дезінформації. Вони можуть використовувати певні шаблони та алгоритми для створення продукування та розповсюдження фейків і певних наративів. Фабрики тролей зазвичай мають значну кількість спеціально створених акаунтів, які працюють одночасно для спотворення фактів і поширення дезінформації. Вони діють організовано, часто під керівництвом адміністраторів або координаторів, які контролюють дії тролів та розподіляють їхні завдання. Фабрики тролей активно використовують психологічні методи, створюючи емоційно заряджені теми там повідомлення.

Зараз Росія активно використовує фабрики тролей у соціальних мережах, зокрема Telegram, Twitter, Facebook і TikTok для розповсюдження дезінформації про війну в Україні. Найбільш відомою є Ольгінська фабрика тролів або Тролі з Ольгіна, яку пов'язують з Євгенієм Пригожиним (FINANCE.UA, 2014).

Поняття «Тролі з Ольгіна» походить від спеціально обладнаного для тролінгу офісу, який російські журналісти викрили у 2013 році в Ольгіні, історичному районі Санкт-Петербурга (FINANCE.UA, 2014). Пізніше назви «тролі з Ольгіна» або «ольгінські тролі» стали загальними щодо тролів, які використовуються для поширення російської пропаганди, без прив'язки до офісу в Ольгіні.

За даними американського видання BuzzFeed, із квітня 2014 року розпочалась організована кампанія із формування необхідної російській владі думки у країнах Західного світу про російську збройну агресію проти України у 2014 році. Такі висновки журналісти роблять із документів, які опинилися у їхньому розпорядженні. Як повідомляє видання, в документах містяться інструкції для коментаторів сайтів Fox News, Huffington Post, The Blaze, Politico и WorldNetDaily (BuzzFeedNews, 2014).

Отже, фабрики тролей є серйозною загрозою для інформаційної безпеки, і тому Україна активно працює над виявленням, аналізом та протидією таким викликам, розвиваючи власні засоби інформаційної оборони.

Таким чином, війна в Україні показує, що інформаційна сфера стала важливим фронтом конфлікту. Вона вимагає постійної уваги, розробки та розвитку дієвих стратегій і тактик протидії сучасним інформаційним загрозам.

Так, українська влада підтримує інформаційну свободу та незалежність мас-медіа, що є важливим чинником у протидії російській дезінформації та кіберпропаганді. Також використовуються інформаційні кампанії, спрямовані на формування позитивного образу України та залучення підтримки з боку міжнародної спільноти. Україна активно співпрацює з міжнародними партнерами, включаючи НАТО та Європейський Союз, для обміну інформацією та координації заходів з кібербезпеки.

Україна створила спеціальні кібербезпекові структури, наприклад, Державна служба спеціального зв’язку та захисту інформації, які відповідають за захист критично важливої інформації та інфраструктури країни, таких як енергетичні системи, транспорт, фінансові установи тощо.

Українські кібербезпекові фахівці активно працюють над виявленням і відбиттям кібератак. Вони займаються моніторингом кіберпростору, виявленням шкідливих програм та розробкою відповідних захисних технологій. Україна вдосконалює технічні заходи для виявлення, запобігання

та реагування на кібератаки, включаючи використання міжнародних стандартів безпеки, розробку власних кіберзахисних рішень, інформаційних систем та мереж.

Крім того, Україна сприяє підвищенню кібербезпеки у громадському секторі та бізнесі. Уряд надає підтримку організаціям, що займаються кібербезпековими дослідженнями та інноваціями.

Проте, боротьба з інформаційною агресією є складним завданням, яке потребує не лише зусиль держави, але й активної участі громадськості. Розвиток критичного мислення у населення, медіаграмотність та розробка спільних стратегій співпраці між державними структурами, недержавними інститутами та громадськістю можуть значною мірою посилити інформаційну оборону України.

**Висновки і перспективи подальших досліджень.** Таким чином, Україна вживає широкий спектр заходів для протидії гібридній війні, захищаючи свій суверенітет, незалежність та територіальну цілісність. Розвиток сильної та демократичної медіа-системи, підтримка незалежних журналістів та ініціатив з підвищення освіти у сфері кібербезпеки та медійної грамотності, посилення міжнародної співпраці, впровадження технічних, інституційних, законодавчих заходів для захисту інформаційних систем є ключовими факторами для подолання інформаційної агресії з боку РФ. Широкомасштабне військове російське вторгнення в Україну та гібридна війна є складними викликами, які вимагають комплексного підходу та усвідомлення всіх аспектів, наслідків та ризиків, і це становить перспективи подальших наукових досліджень у цьому напрямку.

**ЛІТЕРАТУРА**

1. Дібікова, Ю.С., 2021. Цифровізація політичного простору в Україні: проблеми та тенденції. *Сучасне суспільство: Збірник наукових праць*, 2 (23), с.15-25.
2. ДІМ, 2022. *Понад 2 тис. кібератак на урядові ресурси нейтралізувала за рік*

**REFERENCES**

1. Dibikova, Yu.S., 2021. Tsyfrovizatsiia politychnoho prostoru v Ukraini: problemy ta tendentsii. *Suchasne suspilstvo: Zbirnyk naukovykh prats*, 2 (23), s.15-25.
2. DIM, 2022. *Ponad 2 tys. kiberatak na uriadovi resursy neitralizuvala za rik*

*СБУ (ІНФОГРАФІКА)*. [online] (Останнє оновлення 18 Січень 2022) Доступно: https://kanaldim.tv/ponad-2-tys-kiberatak-na-uryadovi-resursy-nejtralizuvala-za-rik-sbu-infografika/ [Дата звернення 12 квітня 2022].

3. Енергореформа, 2022. *Кількість кібератак на об'єкти енергетичної інфраструктури з початку війни збільшилася майже вдвічі*. [online] (Останнє оновлення 12 Квітень 2022) Доступно: http://reform.energy/news/kilkist-kiberatak-na-obekti-energetichnoi-infrastrukturi-z-pochatku-viyni-zbilshilasya-mayzhe-vdvichi-20140 [Дата звернення 10 червня 2022].
4. Andreas Wittel, 2016. *Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right*. Prague: Mayak Intelligence, p. 76.
5. BuzzFeedNews, 2014. *Documents Show How Russia's Troll Army Hit America*. [online] (Last update 2 June 2014) Available at: https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america#.knOJA7YNgZ [Accessed 21 June 2022].
6. FINANCE.UA, 2014. *Де живуть тролі у РФ: як працюють інтернет-провокатори в Санкт-Петербурзі і хто ними заправляє*. [online] Доступно: http://news.finance.ua/ua/news/~/320589 [Дата звернення 21 червня 2022].
7. Hoffman, F., 2007. *Conflict in the 21st Century: The Rise of Hybrid War*. Arlington: Potomac Institute for Policy Studies.
8. Hoffman F., 2006. How Marines are preparing for hybrid wars. *Small Wars Journal,* p. 38-42.
9. Mattis, James N. and Frank Hoffman, 2005. *Future Warfare: The Rise of Hybrid Wars*. [online] Available at: http://milnewstbay.pbworks.com/f/MattisFourBlockWar USNINov2005 [Accessed 12 April 2022].
10. McCulloh, Timothy, and Richard Johnson, 2013. *Hybrid Warfare JSOU Report*. 13-14 August 2013. Joint Special Operations University.

*SBU (INFOHRAFIKA)*. [online] (Ostannie onovlennia 18 Sichen 2022) Dostupno: https://kanaldim.tv/ponad-2-tys-kiberatak-na-uryadovi-resursy-nejtralizuvala-za-rik-sbu-infografika/ [Data zvernennia 12 kvitnia 2022].

3. Enerhoreforma, 2022. *Kilkist kiberatak na obiekty enerhetychnoi infrastruktury z pochatku viiny zbilshylasia maizhe vdvichi*. [online] (Ostannie onovlennia 12 Kviten 2022) Dostupno: http://reform.energy/news/kilkist-kiberatak-na-obekti-energetichnoi-infrastrukturi-z-pochatku-viyni-zbilshilasya-mayzhe-vdvichi-20140 [Data zvernennia 10 chervnia 2022].
4. Andreas Wittel, 2016. *Hybrid War or Gibridnaya Voina? Getting Russias non-linear military challenge right*. Prague: Mayak Intelligence, p. 76.
5. BuzzFeedNews, 2014. *Documents Show How Russias Troll Army Hit America*. [online] (Last update 2 June 2014) Available at: https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america#.knOJA7YNgZ [Accessed 21 June 2022].
6. FINANCE.UA, 2014. *De zhyvut troli u RF: yak pratsiuiut internet-provokatory v Sankt-Peterburzi i khto nymy zapravliaie*. [online] Dostupno: http://news.finance.ua/ua/news/~/320589 [Data zvernennia 21 chervnia 2022].
7. Hoffman, F., 2007. *Conflict in the 21st Century: The Rise of Hybrid War*. Arlington: Potomac Institute for Policy Studies.
8. Hoffman F., 2006. How Marines are preparing for hybrid wars. *Small Wars Journal*, p. 38-42.
9. Mattis, James N. and Frank Hoffman, 2005. *Future Warfare: The Rise of Hybrid Wars*. [online] Available at: http://milnewstbay.pbworks.com/f/MattisFourBlockWar USNINov2005 [Accessed 12 April 2022].
10. McCulloh, Timothy, and Richard Johnson, 2013. *Hybrid Warfare JSOU Report*. 13-14 August 2013. Joint Special Operations University.
11. Newson, Robert A., 2014. *Counter-*

11. Newson, Robert A., 2014. *Counter-Unconventional Warfare Is the Way of the Future. How Can We Get There?* [online] Available at: http://blogs.cfr.org/davidson/2014/10/23/counterunconventional-warfare-is-the-way-of-the-future-how-can-we-get-there/ [Accessed 12 April 2022].
12. U.S. Marine Corps, 2008. *Hybrid Warfare and Challengers*. Strategic Vision Group Information Paper.

*Unconventional Warfare Is the Way of the Future. How Can We Get There?* [online] Available at: http://blogs.cfr.org/davidson/2014/10/23/counterunconventional-warfare-is-the-way-of-the-future-how-can-we-get-there/ [Accessed 12 April 2022].
12. 12. U.S. Marine Corps, 2008. *Hybrid Warfare and Challengers*. Strategic Vision Group Information Paper.

**Інформація про автора**

**Дібікова Юлія Сергіївна** – кандидат політичних наук, доцент, доцент кафедри політології, соціології і культурології Харківського національного педагогічного університету імені Г.С. Сковороди; e-mail: krasnokua@gmail.com; ORCID: https://orcid.org/0000-0003-4135-9100.

Стаття надійшла до редакції: 09.09.2022 р. Прийнята до друку: 28.09.2022 р.