УДК 35.088.6(477)

І. В. Аблазов,
к. політ. н., професор, начальник кафедри міжнародних відносин та стратегічних комунікацій, Воєнна академія імені Євгенія Березняка
ORCID ID: https://orcid.org/0000-0001-6293-8043
В. І. Абрамов,
д. філос. н., професор кафедри міжнародних відносин та стратегічних комунікацій, Воєнна академія імені Євгенія Березняка
ORCID ID: https://orcid.org/0000-0002-4228-4799

DOI: 10.32702/2306-6814.2023.2.74

ТЕАТР ГІБРИДНОЇ ВІЙНИ: ПОСТНЕКЛАСИЧНА МЕТОДОЛОГІЯ АНАЛІЗУ НЕВИЗНАЧЕНОСТЕЙ, РИЗИКІВ І ЗАГРОЗ У КОНФЛІКТАХ СУЧАСНОСТІ

I. Ablazov,
PhD in Political Sciences, Professor, Head of the Department of International Relations and Strategic Communications, Yevgeny Bereznyak Military Academy
V. Abramov,
Doctor of Sciences in Philosophy, Professor of the of the Department of International Relations and Strategic Communications, Yevgeny Bereznyak Military Academy

HYBRID WAR THEATER: POST-CLASSIC METHODOLOGY OF UNCERTAINTY ANALYSIS, RISKSAND THREATS IN MODERN CONFLICTS

У статті здійснено аналіз сучасних підходів до інтерпретації категорії "театр гібридної війни" та її використання щодо забезпечення національної безпеки, які можуть застосовуватись у практичній діяльності фахівцями розвідки в умовах посилення тенденцій щодо використання м'якої сили в сучасній війні з російським агресором. Наведено схему онтології проблематики національної безпеки в умовах прямого військового конфлікту як засобу досягнення геополітичними гравцями своїх національних інтересів. Наголошено, що висока динамічність розвитку світових подій й глибокі зрушення в безпековій сфері викликали розробку та впровадження різноманітних неконвенційних (асиметричних) способів і методів протиборства на театрі гібридної війни. Відзначено, що у вітчизняних дослідженнях проглядається позитивна тенденція додання категорії "національна безпека" все більшого системного значення. Розглядаються особливості та проблеми інформаційно-аналітичної роботи в розвідувальних органах України щодо виявлення гібридних загроз в умовах розвитку асиметричних способів і методів протиборства. Показано, що постнекласична пізнавальна стратегія виступає в якості методологічної основи з питань деталізації компонентів театру гібридної війни. Розкрито постнекласичні уявлення феномену складності театру гібридної війни як наукової категорії та запропоновано можливу типологію концепцій щодо його складності. Визначено, що оцінка стану театру гібридної війни стає неоднозначною, допускаючи безліч варіантів. На цій підставі сформульовано та обгрунтовано принципові відмінності постнекласичної раціональності від класичної щодо вивчення та розробки й реалізації публічної політики забезпечення національної безпеки в умовах гібридних загроз. Обгрунтовується доцільність використання адаптивного підходу й методу нечіткої логіки щодо розкриття задумів вирішення проблемних ситуацій, відображення особливостей використання механізмів адаптивного управління в умовах рухливості й невизначеності зовнішнього та внутрішнього середовища театру гібридної війни. Запропоновано нові підходи щодо прогнозування дій противника ще до прийняття ним рішення на розв'язання агресії, а також способи адаптації інформаційно-аналітичної роботи до складного середовища театру гібридної війни.

The article analyzes modern approaches to the interpretation of the category "hybrid war theater" and its use for public administration in the field of national security. The scheme of ontology of problems of national security in the conditions of departure from a format of direct military conflict as means of achievement by geopolitical players of the national interests is resulted. It is emphasized that the high dynamics of world events and deep changes in the security sphere have caused the development and implementation of various unconventional

(asymmetric) methods and techniques of confrontation in the theater of hybrid warfare. It is noted that domestic research shows a positive trend of giving the category of "national security" increasing systemic importance. Peculiarities and problems of information-analytical work in public administration bodies on detection of hybrid threats in the conditions of development of asymmetric methods and methods of confrontation are considered. It is shown that the post-classical cognitive strategy serves as a methodological basis for detailing the components of the hybrid war theater. Post-classical ideas of the phenomenon of complexity of hybrid war theater as a category of science of public administration are revealed and a possible typology of concepts concerning its complexity is offered. It is determined that the assessment of the state of the hybrid war theater becomes ambiguous, allowing many options. On this basis, the fundamental differences between post-classical rationality and classical rationality in the study and development and implementation of public policy to ensure national security in the context of hybrid threats are formulated and substantiated. The expediency of using the adaptive approach and method of construction of rhizome models and the method of fuzzy logic to reveal the ideas of solving problem situations, reflecting the peculiarities of the use of adaptive control mechanisms in conditions of mobility and uncertainty of external and internal environment of hybrid war theater is substantiated. New approaches to predicting the actions of a potential adversary before he decides to resolve aggression, as well as ways to adapt information and analytical work to the complex environment of the theater of hybrid warfare are proposed.

Ключові слова: національна безпека, театр гібридної війни, міждисциплінарна методологія, постнеокласична наука, метод нечіткої логіки.

Key words: national security, hybrid war theater, hybrid war theater, interdisciplinary methodology, post-neoclassical science, rhyme of security space, fuzzy logic method.

ПОСТАНОВКА ПРОБЛЕМИ В ЗАГАЛЬНОМУ ВИГЛЯДІ

В академічному середовищі з'явилася потреба обґрунтувати нові тенденції змін у світі на підставі трансформації сучасної методології науки, яка виникла в зв'язку з переходом від монодисциплінарних дискурсів до міждисциплінарних та необхідністю діалогу класичних, некласичних і постнекласичних пізнавальних стратегій. Такими феноменами сучасного розгляду національної безпеки (далі НБ) є: складність, нелінійність, ризомність, трансгресія, ламінарність, асиметрія, мережевість народження, функціонування та розвитку систем безпеки. На нашу думку, феномен НБ не може бути ефективно досліджений за допомогою існуючих дисциплінарних методологій в рамках класичної і некласичної науки, оскільки він володіє властивостями саморозвитку, які вимагають осмислення з використанням постнекласичного типу раціональності.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Питання забезпечення НБ є надзвичайно актуальним та широко досліджується українськими науковцями, серед яких: В. Богданович, О. Власюк, А. Семенченко, Г. Ситник, В. Смолянюк та інші. У свою чергу, актуальній проблематиці стабільності системи як фактору забезпеченням безпеки приділяють увагу такі дослідники: О. Давіденко, С. Мокляк, О. Руденко, М. Шевченко та інші. В основу трактування НБ як можливості реалізації інтенцій суб'єкта дедалі частіше покладається парадигма його самореалізації як втілення (реалізації) властивих йому цінностей, цілей, інтересів. Зазначені аспекти процесу розробки та впровадження політики забезпечення НБ активно досліджуються сучасними вітчизняними вченими: М. Кармазіною, Н. Ніжником, Л. Чупрієм, С. Хамулою та іншими. Можна констатувати наявність спектра теоретичних підходів, окремих принципів та ідей щодо визначення сутності НБ, які неможливо класифікувати за однією підставою.

Таким чином, для більшості феноменів сучасного світу, в тому числі НБ, характерною є швидкоплинність змін, їх непередбачуваність, нелінійність, відкритість і складність організації, що детермінує інший напрямок перебігу процесів і розвитку структур на кордоні порядку й хаосу що знайшло своє відображення у трактуванні визначення "театр гібридної війни". Таке бачення проблеми вимагає доповнення існуючого логіко-понятійного та методологічного інструментарію підходів, заснованих на ідеалах і нормах класичної, некласичної науки та постнекласичної науки. Необхідно зазначити, що авторами було здійснено спроби попередньої розробки постнекласичної теорії складності НБ, що знайшло відображення в публікаціях [1; 2; 9].

В даній роботі під час з'ясування сутності та змісту поняття "театр гібридної війни" в якості окремої наукової категорії, на нашу думку, особливої уваги заслуговують наступні спеціальні методи аналізу театру гібридної війни: застосування адаптивного підходу; побудова ризомальних моделей; морфологічна будова мережевої архітектури театру гібридної війни; використання методу нечіткої логіки.

МЕТА І ЗАВДАННЯ СТАТТІ

З урахуванням зазначеного вище метою статті є наукове обґрунтування причин і чинників, що зумовлюють відмінності й нерівномірності в розробці концепту "те-

Таблиця 1. Класифікація видів війни за невоєнним типом насильства

Вид війни	Головна мета	Джерело
Кібервійни	спрямовані на руйнування критичної інфраструктури противника	Cyberdeterrence and Cyberwar // Th e RAND Corporation. 2009.
Інформаційно-алгоритмічні війни	з використанням штучного інтелекту	Weaponised AI is coming. Are algorithmic forever wars our future? // The Guardian. 2018.
Проксі-війни	війни на територіях третіх країн та регіонів	Peering into the Crystal Ball. Holistically Assessing the Future of Warfare // Th e RAND Corporation. 2020.
Когнітивні війни	Спрямовані на поразку свідомості	Countering cognitive warfare: awareness and resilience // Johns Hopkins University & Imperial College London. 2021.
Мережевоцентричні віни	Їх головний принцип - усунення акценту з платформи на мережу	Cebrowski A.K., Garstka J.J. Networkcentric Warfare: Its Origin and Future // Proceedings. January 1998.
Соціальни війни (societal warfare).	Війни, що спрямовані на руйнування соціальної інфраструктури противника	Th e Emerging Risk of Virtual Societal Warfare // Th e RAND Corporation. 2019.
Ментальні війни	Спрямовані на руйнування світогляду і цивілізаційних основ противника.	U.S. wages psychological war on Moscow — Russian defense adviser // Reuters. 2021. URL: https://www.reuters.com/article/us-russia-usa-minds-idUSKBN2BH1TD (дата звернення: 21.02.2022).

атр гібридної війни" та вимагають упровадження адекватних методів інформаційно-аналітичної діяльності з виявлення гібридних загроз в Україні.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Війна це суспільно-політичне явище, продовження політики насильницькими засобами. На відміну від сутності війни, її характер і зміст постійно розвиваються. Гіперзвук, цифровизація і роботизація стають домінуючими тенденціями створення нових зразків зброї, військової і спеціальної техніки. Космос, інформаційний і кіберпростір все активніше використовуються в ході збройної боротьби. При цьому протиборства в економічній, інформаційній, консцієнтальній (ментальній, когнітивній) сферах є самостійними, взаємопов'язаними формами дій (протиборства), що розширюють зміст категорії "війна" загалом. Дискурс характеру війни ведеться дуже інтенсивно (див. табл. 1).

В ході досліджень найбільш характерних рис сучасного протиборства щодо забезпечення НБ досить часто вживаються такі поняття, як "гібрідни загрози", "гібридна війна" і "гібридна агресія". Загальноприйнятого трактування даних термінів поки немає. На наш погляд, сенс "гібридності" може полягати в створенні невизначеного (багатозначного) середовища та його націленості на слабкі або незахищені держави з використанням в основному невійськових способів досягнення політичних і стратегічних цілей. На думку військових фахівців США, за рахунок гібридних загроз противник прагне запровадити в оперативну обстановку такі зміни, які змусять опонентів реагувати в усіх напрямах діяльності. Подібні загрози можуть одночасно створювати економічну нестабільність, сприяти формуванню серед населення атмосфери недовіри до чинної влади, ставити під удар інформаційні мережі та системи, висувати привабливі гасла, що відповідають цілям агресора, ініціювати штучну гуманітарну кризу, а також породжувати передумови для фізичного усунення опонентів.

Д. Меттіс і Ф. Хоффман відзначають, що гібридна загроза визначається одночасним застосуванням противником звичайних озброєнь, використанням нерегулярної тактики, тероризму та злочинної діяльності в зоні бойових дій для досягнення своїх політичних цілей. Тому в гібридній війні будуть вирішуватися наступні питання: наскільки правильно військово-політичне керівництво оцінює характер військових дій за участю недержавних суб'єктів й іноземних бойовиків; чи наявні в складі збройних сил різні типи збройних формувань (регулярні та нерегулярні), призначені для ведення військових дій; чи існує множинність сценаріїв розгортання військового конфлікту, щоб зробити його гібридним; чи можуть рішення військово-політичного керівництва в ході війни оцінюватися як злочинні, спрямовані на отримання доходів або підтримку бандформувань [11].

Ми приходимо до висновку, пише Ф.Хоффман, що в майбутньому ми зіткнемося не з противником, який обирає будь-який один, нетрадиційний чи інший, спосіб протистояння, а з противниками, які одночасно поєднують всі способи протистояння, що проявляються у вигляді мультимодальних (змішаних) або гібридних воєн. У такому разі "гібридна війна" — це поєднання смертоносності міждержавного конфлікту з фанатичністю постійно тліючої партизанської війни (irregular warfare). При цьому поняття "гібридність" відноситься як до організаційних аспектів війн, так і до застосовуваних засобів. Організаційно гібридні війни можуть мати ієрархічну політичну структуру в поєднанні з децентралізованими елементами або мережевими тактичними підрозділами. Засоби протистояння, які вони обирають, також можуть бути гібридними за формою і застосуванням [10, p. 28].

Генерал-лейтенант Б. Ходжес на закритій конференції в 2015 році в Німеччині заявив, що Росія розробила теорію "гібридної війни", яку успішно реалізувала в Криму, а через кілька років буде здатна одночасно вести три операції. Під операцією він мав на увазі поточний конфлікт в Україні: саме Москва веде війну з Києвом. На черзі тепер країни Балтії і Грузія.

Необхідно назвати найбільш ефективні заходи, які рекомендовані до застосування в гібридної війні: використання сучасних технологій пропаганди та інформаційної обробки населення країни-супротивника; створення негативного образу існуючого режиму; дискредитація державних лідерів та управлінців; висування агентів впливу з місцевого населення, надання їм фінансової й організаційної підтримки; організація мітингів протесту і провокацій. При можливості — організація громадянської непокори у великому масштабі, а також вплив на політичних лідерів країни-супротивника фінансовими інструментами, що перебувають під контролем європейської та американської банківської систем, в тому числі фінансовими й економічними санкціями, заборо-

ною на видачу кредитів та іншого фінансового забезпечення.

Синхронізовані та взаємно посилювані операції по впровадженню гібридних загроз можуть проводитися в інформаційній, соціальній, інфраструктурній, економічній та військовій сферах [6]. В якості складової гібридних загроз можуть виступати неконвенційні бойові дії, спрямовані на надання підтримки рухам опору або повстанським силам. При цьому створюється інфраструктура, яку переорієнтовано з державного сектора в приватний. Подібна переорієнтація нерідко стає опорою для проведення гібридних операцій. Такий підхід зазвичай застосовується для дій в "сірій зоні" або "театрі гібридної війни". Відхід від формату прямого військового конфлікту як засобу досягнення геополітичними гравцями своїх національних інтересів викликав розробку та впровадження різноманітних неконвенційних (асиметричних) способів і методів протиборства. Деякі з яких наведено у табл. 2.

Таблиця 2. Неконвенційні (асиметричні) способи і методи геополітичного протиборства на театрі гібридної війни

№ з/п	Загальноприйняте найменування	Сутність і зміст діяльності
	Війни з руйнування суб'єктності держави та втраті її суверенітету на основі управління сенсами	Створенні невизначеного (багатозначного) середовища та приділенню особливої уваги несиловим технологіям зміни політичних режимів, інструментам руйнування суб'єктності держави з використанням соціальних технології управління на основі сенсу (смислу) як нового та найбільш ефективного методу м'якої сили
	Ментальна війна	Спрямовані на руйнування світогляду і цивілізаційних основ противника.
1	Техносферна війна	Операції із застосуванням засобів кіберзахисту і кіберзброї проти систем державної влади та військового управління, економічних систем і критично важливих систем технологічного управління, що використовують кіберресурси
2	Психологічна боротьба	Поширення дезінформації з метою дискредитації органів публічного і військового управління країни-противника, придушення волі особового складу ЗС і населення до опору
3	Боротьба в медіапросторі	Протистояння засобів мовлення і медіахолдингів в інтересах формування вигідного для себе інформаційного простору та купівлі лояльних місцевих ЗМІ
4	Нові терористичні війни (new terror war)	Проведення класичних терактів і диверсій в сукупності з використанням можливостей сучасних технологій: злому серверів банківських і державних організацій, використання кіберпростору, телефонний тероризм та вербування через соціальні мережі та комп'ютерні ігри в терористичну діяльність
5	Боротьба в сфері міжнародного законодавства (international law warfare)	Проголошення права першими встановлювати правила регулювання міжнародної діяльності в новій сфері, використання легальних підходів для створення спірних моментів та ситуацій незгоди в міжнародних організаціях
6	Наркотична боротьба (drug warfare)	Розповсюдження наркотичних речовин в заданому регіоні для дестабілізації спільноти
7	Боротьба за використання недержавих організацій	Незаконне використання доходів від нелегальної діяльності для фінансування протестів опозиційних рухів
8	Контрабандна боротьба (smuggling warfare)	Створення невизначеності на фондових ринках через цілеспрямоване порушення балансу попиту і пропозиції, перехоплення управління над найбільшими корпораціями, руйнування усталеного економічного порядку

Наведені в таблиці способи і методи можуть доповнюватися і комбінуватися один з одним, в результаті цього в кожному конкретному випадку застосовується абсолютно новий вид протиборства. У зв'язку з цим можна стверджувати, що центральною віссю захисту національних інтересів як і раніше залишається збройна боротьба, а все інше групується навколо неї та утворює складну гібридну систему, в межах якої розвивається протистояння в різних сферах людської діяльності: соціально-економічній, адміністративно-політичній та культурно-світоглядній.

Одним з найефективніших видів зброї невійськового характеру по суті стали інформаційні ресурси. Невизначеність і ризики процесів розвитку протистояння обумовлюють хиткість контурів конфліктів сучасності, що носять гібридний характер, та вимагають нових підходів до розробки і реалізації відповідних стратегій і контрстратегій, до всебічної підготовки театру, на якому ведуться операції гібридної війни.

Найважливішим фактором, що визначає стратегію конфліктів нового покоління, слід вважати появу і використання терміну "сіра зона" як театр гібридної війни. Властивості нелінійності і невизначеності іманентно присутні в так званій "сірій зоні", яка в загальному вигляді являє собою стратегічний, регіональний та національний простір безпеки, в межах якого міжнародна система переформовується під правила нового світопорядку. Зміні в ній підлягають нормативно-правові положення, інститути, національні інтереси та пріоритети держав. Головна увага полягає в організації стратегій для мережевих підривних структур на території держави-об'єкта агресії, налагодженні відносин з місцевими опозиційними організаціями, застосуванні методів мотивації їх діяльності в несприятливих умовах, підтримці руху опору, проведенні психологічних операцій тощо [5]. Зростають масштаби психосоціальних факторів нетрадиційних методів ведення війни, особливої уваги заслуговують операції з розповсюдження та вироблення психологічного впливу.

Ключовою особливістю сучасного аналізу театру гібридної війни слід вважати пошук джерел гібридних загроз, а також впровадження адекватних методів інформаційно-аналітичної діяльності з їх виявлення.

В якості вихідних даних для аналізу театру гібридної війни в довгостроковій перспективі за основу можна брати базовий прогноз розвитку економічної, політичної, соціальної та духовної (морально-психологічної) обстановки, яка в загальних рисах характеризує спрямованість загроз. Доцільним є застосування адаптивного підходу та подальша деталізація прогнозу відповідно з поточним станом складних систем НБ, насамперед обстановки в зоні регіональних і локальних конфліктів та чинників, що впливають на їх розвиток.

З метою виявлення джерел гібридної агресії необхідно сформувати "дерево проблем" на підставі: оцінки

геополітичних ризиків; встановлення моменту, коли противник здатний прийняти рішення на проведення операції з використанням способів і методів гібридної агресії, вивчення складу, масштабу і характеру ризиків. Склад ризиків розкривається на основі можливостей і цілей того, хто їх формує, а також уразливих місць об'єкта впливу. Оцінка масштабу ризиків дозволяє виявити межі зони впливу, що залежать від кількості та доступності об'єктів загроз, а також можливостей їх попереднього вивчення. Характер ризиків найчастіше має приховану спрямованість, що максимально ускладнює завдання пошуку і визначення їх джерела, який, як правило, є анонімним.

Необхідно підкреслити, що висока ефективність аналізу театру гібридної війни складається з багатьох етапів, що можна використовувати для побудови моделей розвитку стану систем забезпечення національної безпеки України. На нашу думку, використання постнекласичної і комунікативної методології дає змогу розширити перспективи подальших досліджень щодо порушеної проблеми та здійснення політичних практик забезпечення НБ як напряму, що забезпечує можливість розробки і впровадження керування складними нелінійними соціальними процесами. Слід зауважити, що зміна початкових умов дає змогу вибрати один із можливих управлінських впливів, що детермінований середовищем розвитку НБ. Але водночас ми аж ніяк не створюємо його, а лише змінюємо управління НБ на парадигму "суб'єкт — полісуб'єктне середовище НБ", що відповідає постнекласичним практикам публічної політики.

Проте на основі викладеного вище вироблення оптимальних рекомендацій щодо участі суб'єкта в гібридній війні (насамперед прийняття рішень та планування дій у відповідь) все ще будуть утрудненими. У зв'язку з цим доцільно при роботі в складному середовищі переходити до адаптивного реагування і постійного коригування моделей театру гібридної війни. Такий підхід одним з перших виклав у своїй книзі "Жорсткий лідер" генерал-полковник ЗС США С. МакКрістал [7], який раніше керував проведенням спеціальних операцій в Іраку й Афганістані. Необхідність подібних перетворень викликана характерними саме для гібридної війни умовами ведення бойових дій проти іррегулярних збройних формувань. Саме ці обставини викликають потребу морфологічної будови мережевої архітектури публічного управління НБ.

Мережеве управління — сучасний підхід до розуміння публічного управління як системи, побудованої на переході від ієрархічного управління до управління за допомогою мережевих структур. Поняття "мережева архітектура публічного управління в контексті забезпечення національної безпеки" пропонуємо розуміти як комплекс нормативно-правових та організаційно-управлінських вимог, що забезпечують узгоджений і взаємопов'язаний розвиток систем публічного управління й забезпечення національної безпеки в умовах динамічно змінюваного зовнішнього та внутрішнього безпекового середовища, з метою формування мережевої форми організації діяльності інститутів національної безпеки і оборони за рахунок партисипаторної взаємодії з інститутами громадянського суспільства, що, своєю чергою, передбачає реалізацію концепцій інформатизації суспільства, відкритого суспільства та суспільства відкритого доступу, а також публічної адміністрації, архітектури системи управління, цивільної та суспільної безпеки. Мережева морфологія передбачає значне послаблення ролі ієрархічних та вертикальних зв'язків, а також односторонніх та командних практик взаємодії учасників процесу розроблення та реалізації державно-управлінських рішень. При цьому сутність формування мережевої архітектури публічного управління зводиться до такого. По-перше, мережеві альянси можуть набирати різних форм: міжособистісні контакти, інформаційні обміни, стратегічні коаліції інституційно незалежних акторів, об'єднання міжнародних організацій. По-друге, мережа є хистким утворенням, тобто на різних часових відтинках активізуються лише окремі її елементи. По-третє, мережа — це сучасна постмодерністська організація, що локалізується не за місцем, а за часом.

Таким чином, використання мережевої парадигми для вивчення (морфологічної будови мережевої архітектури театру гібридної війни є завданням сучасної теорії публічного управління НБ. Актуальними завданнями щодо соціального проєктування мережевої архітектури публічного управління НБ передбачається розроблення концептуальної моделі формування мережевої архітектури публічного управління НБ, а також інтегрованої моделі формування інституціональної матриці публічного управління в контексті забезпечення НБ.

Ретельне опрацювання та врахування ризиків гібридної війни стали невід'ємною частиною і важливою складовою оцінки театру гібридної війни. Однак все частіше суб'єктам забезпечення НБ доводиться приймати рішення в умовах невизначеності, які можуть призвести до непередбачуваних наслідків. На жаль, існуючі на сьогоднішній день методи обліку та оцінки ризиків не позбавлені суб'єктивізму і сутнісних передумов, що призводять до неправильних оцінок ризиків гібридної війни. Теорія нечіткої логіки — це новий гносеологічний підхід, який динамічно розвивається у контексті оцінки ризиків. Останнім часом нечітке моделювання є однією з найбільш активних і перспективних напрямків прикладних досліджень в галузі управління та прийняття рішень.

Використання методу нечіткої логіки у даній роботі представлені: описом цього методу; визначенням ризику і невизначеності, обгрунтуванням необхідності застосування нових підходів до аналізу ризиків.

Необхідно розділяти поняття "ризик" і "невизначеність". Під невизначеністю ми розуміємо ситуацію, за якою можлива велика кількість результатів, але при яких результати дій не є детермінованими, тобто їх ймовірність невідома. Ризик — це: ситуація, в якій існує кінцева кількість випадків з відомою ймовірністю для кожного з них; можливість появи обставин, що обумовлюють невпевненість або неможливість отримання очікуваних результатів від реалізації поставленої мети; ймовірність втрат або ймовірність отримати результат, відмінний від очікуваного. Отже, ризик — це суб'єктивна оцінка об'єктивної невизначеності. Якщо невизначеність — непереборна якість середовища театру гібридної війни, то ризик — це чисельна характеристика можливості втрат.

При оцінюванні театру гібридної війни виникає необхідність оцінити певні якісні показники. Для оцінювання таких показників може бути застосований апарат теорії нечіткої множини, зокрема метод нечіткої логіки. У процесі оцінювання ефективності забезпечення НБ постає завдання кількісної формалізації якісних показників. Таким чином, завдання моделювання полягає в тому, щоб адекватно перевести якісні висловлювання експерта в кількісні уявлення [5, с. 123]. Нечітко-множинні описи, з одного боку, є набором адекватних формалізмів для моделювання систем в умовах суттєвої невизначеності, а з іншого — полем для нової інтерпретації класичних імовірнісних та експертних оцінок. Далі — перехід від класичного імовірнісного розподілу до імовірнісного розподілу з нечіткими параметрами з одночасним управлінням рівнем правдоподібності оцінок розподілу. Також можливий перехід від сукупності експертних оцінок до набору функцій належності, що створює нечіткий класифікатор [8].

Отже, стан театру гібридної війни є складною багатокритеріальною характеристикою, тому для її оцінювання пропонуємо використовувати методи, які враховували б усі складові елементи, видавали комплексний результат і надавали можливість аналізувати зміни, що відбуваються у процесі забезпечення НБ.

Тенденція збільшення складності реального театру гібридної війни і процесів управління, особливо у кризові періоди, при введенні особливих правових режимів, необхідність забезпечення ефективності та адекватності управління, а також урахування великої кількості різних факторів обгрунтовують застосування для оцінювання стану театру гібридної війни сучасної технології, побудованій на основі методу нечіткої логіки. Такий метод доцільно використовувати для побудови моделі театру гібридної війни, що враховує неповноту та неточність вхідних даних, коли, з одного боку, початковий опис обстановки заздалегідь виявляється неточним або неповним, а з іншого — намагання отримати вичерпну інформацію призводить до втрати часу і засобів.

Процес оцінювання стану театру гібридної війни, на нашу думку, складається із взаємопов'язаних етапів, якими є: 1) аналіз поточної ситуації; 2) уточнення організаційно-правового механізму (структури системи управління та функцій її елементів); 3) моніторинг результатів управління; 4) визначення ефективності управління з використанням комплексної моделі. На кожному із зазначених етапів виконуються методи якісного і кількісного аналізу, здійснюється аналіз чутливості (визначення чутливості до критерію при "послідовно-одиничній" зміні кожної змінної), сценарний аналіз та імітаційне моделювання. Мета використання цих методів — об'єктивність оцінювання ефективності публічного управління системою забезпечення НБ. Особливістю процесу є його циклічний характер, що відповідає сучасним вимогам до аналізу та оцінювання складності НБ). Кожний цикл процесу оцінювання розпочинається з аналізу поточної ситуації, який передбачає її логічне осмислення, визначення всіх доступних ресурсів (матеріальних, фінансових, інформаційних та ін.), виявлення основних факторів, які визначають розвиток ситуації, а також встановлення цілей управління. На цьому етапі рекомендується застосовувати евристичний (неформальний) метод побудови логічних сценаріїв для аналізу можливих напрямів розвитку ситуації. При цьому загальна мета аналізу стану театру гібридної війни складається з робочих або проміжних цілей протидії гібридним загрозам. Рівень досягнення таких цілей, які мають бути об'єктивно досяжними та ретельно деталізованими, можна розглядати як важливий індикатор ефективності публічної політики забезпечення НБ.

Рамки статті не дозволяють широко розглянути проблему інформаційної складності театру гібридної війни. Сучасна війна, у тому числі гібридна, не змінює своєї сутності. Вона є продовження політики, але до застосовуваних нею засобів насильства у сьогоденні віднесена інформаційна зброя. Саме тому можна констатувати, що разом з сухопутною, морською і повітряною сферами війни додатковим простором гібридної війни повною мірою став інформаційний.

Основна відмінність методу нечіткої логіки полягає у введенні лінгвістичних змінних (суб'єктивних категорій). Лінгвістичні змінні — це змінні, які не можна описати за допомогою математичної мови, тобто їм складно надати точну (об'єктивну) кількісну оцінку. Наприклад, поняття "висока" або "низька" (щодо вірогідності реалізації гібридних загроз) не мають чіткої межі й не можуть бути представлені точним математичним описом. Лінгвістичною змінною називається така змінна, значеннями якої є слова або пропозиції природної мови. У літературі нечітких множин лінгвістичні змінні також називають термножини (від англ. term — називати) [12].

Так, наприклад, для отримання інтегральної оцінки театру гібридної війни та впливу на його стан інформаційної зброї недостатньо тільки значень змінних кількісних показників: система контролю оперативної обстановки (комплексний моніторинг ЗМІ, соціальних мереж, "сірий" Інтернет); контроль джерел загроз (розширений набір джерел, рубрик, тем, які збурюють протестний електорат, співчуваючих та тих, хто ще не визначився). Необхідно також враховувати і якісні змінні: фокус інтересів гібридної війни, технології протиборства. Так, для отримання кількісної оцінки лінгвістичної змінної "умови для впливу на групову й індивідуальну поведінку та формування інформаційного портрету населення" задаємо інтервал значень оцінки від 0 до 10, де 0 — найсуворіші умови, що заважають процесу використання інформаційної зброї. На основі експертних оцінок, можна стверджувати, якщо інформаційний вплив планується вести в зоні театру гібридної війни (де ризики є підвищеними) і в умовах відсутності підготовчих робіт, то її оцінка буде коливатися від 0 до 3 балів, що буде означати суворі умови протиборства. Якщо ж інформаційний вплив планується на вже підготовленому просторі, в умовах соціально-політичної нестабільності, то оцінки змінної будуть набувати значень від 7 до 10 балів, що означає сприятливі протиборства. Оцінка кількісних змінних прийме значення в інтервалі від 3 до 7 балів, якщо умови будуть визначені як такі, що одночасно сприяють та перешкоджають інформаційному протиборству. Дані бали присвоюються або оцінювачами, або групою експертів, безпосередньо залучених до процесу аналізу театру гібридної війни.

Ще одним прикладом оцінки лінгвістичної змінної театру гібридної війни може служити нечіткість межі

змінної "низький відсоток підтримки інтересів і реалізації загроз". Який відсоток вважається низьким? Так, грунтуючись на формальній логікі, від експертів можуть бути отримані відповіді, наприклад, що відсоток менше 7% — низький, від 8 до 15% — середній, а від 16 і вище — високий. Межі між цими уявленнями є нечіткими, розмитими. Відповідно, поняття "низький відсоток підтримки інтересів і реалізації загроз" є суб'єктивною оцінкою.

Отже, нечіткі когнітивні схеми — це новий інструмент для моделювання економічних, політичних, соціальних та духовних станів й ситуацій театру гібридної війни. У таких випадках основним інструментом методу є функція приналежності як засіб перекладу лінгвістичних змінних на математичну мову для подальшого застосування методу нечітких множин. Функцією приналежності є функція, що задає ступінь або впевненість, з якою елементи деякої множини належать заданій нечіткій множині загроз гібридної війни. Наприклад: чим більше аргумент x відповідає нечіткій множині A, тим більшим є його значення, яке наближається до 1. Підставою для побудови функції приналежності також можуть служити експертні оцінки.

Застосування методу нечіткої логіки визначення складності театру гібридної війни, найчастіше мають на увазі системи нечіткого виведення, які лежать в основі різних процесів. Основними етапами цієї системи є: 1. Формування бази правил системи нечіткого виведення. 2. Фазифікація вхідних параметрів. 3. Агрегація. 4. Активізація підумов в нечітких правилах продукцій. 5. Дефазифікація. Дана схема відноситься до алгоритму нечіткого висновку Мамдані, який один з перших знайшов застосування в системах нечітких множин [9]. Підсумовуючи висловлене, можемо констатувати існування потреби в розробці методики аналізу та оцінки стану театру гібридної війни. Вирішити це завдання можливо за допомогою програмного продукту Fuzzy Tech. Скористаємося алгоритмом нечіткого висновку Мамдані для специфікації умов даного завдання й сформулюємо правила системи нечіткого виведення. Дане завдання вирішується в кілька етапів: Етап 1. Ідентифікація ризиків. Етап 2. Визначення ступеня впливу факторів на загальний ризик проекту використання гібридної зброї. Етап 3. Оцінка вхідних змінних і формування правил. Етап 4. Застосування методу нечіткої логіки для оцінки ризиків.

Застосування методу нечіткої логіки дозволило включити такі лінгвістичні фактори впливу загроз на театр гібридної війни, як матриця інтересів та загроз (картина у якості світлофору — червоний, жовтий і зелений), контроль за джерелом загроз, "теплова" мапа в соціальних мережах, аналіз зав'язків об'єктів Інтернету, аналіз активності суб'єктів соціальних мереж, збоїв в роботі обладнання, аналіз джерел інформаційних вкидань, наявність дозвільної документації до необхідного моменту часу та ін. А головне: це допомогло представити наочні результати для прийняття необхідного рішення.

Таким чином, використання методу нечітких множин дає низку переваг, дозволяючи: включати в аналіз якісні змінні; оперувати нечіткими вхідними даними; оперувати лінгвістичними критеріями; швидко моделювати складні динамічні системи та порівнювати їх із заданим ступенем точності; попереджати недоліки та обмежувати існуючі методи оцінки проектних ризиків протиборства на театрі гібридної війни.

ВИСНОВКИ

Зазначені особливості мережевості і нечіткої множинності театру гібридної війни у сукупності із постнекласичним методологічним апаратом, на наш погляд, перетворюють їх на інструмент, важливий для осмислення складності процесу забезпечення НБ України. Адже як теоретичний, мисленнєвий конструкт мережа (ризома) дозволяє моделювати поведінку інформаційних мереж та їхніх систем як на рівні системності, так і на рівні окремих соціальних агентів (індивідів, груп, класів, націй, держав тощо). Ризома театру гібридної війни залишається індиферентною до природи об'єктів, що входять до неї. Якщо оцінка театру гібридної війни не відповідає наявній структурній конфігурації, ризома створює новий вимір, прокладає нову лінію взаємодії, яка врахує особливості приєднаних елементів та узгоджує їх з існуючими. З огляду на зазначене, основним здобутком дослідження є репрезентація в категоріях некласичної науки та філософії постмодернізму процесу віртуалізації сучасних соціальних практик з метою виявлення закономірностей, тенденцій і суперечностей розвитку суспільства і системи забезпечення НБ.

Театр гібридної війни як соціальна мережа може мати вплив на контроль безпекового простору (економічного, політичного, соціального, ідеологічного, ментального та ін.), підтримання стану хаосу і безперервного конфлікту в країні, соціумі. У "гібридної" війні немає меж — ні моральних, ні просторових. Це сутнісне судження впливає на НБ, підвищує ризики й загрози стабільності нашої держави, вимагає пошуку і розробки відповідних концепцій протидії, в основу яких має бути покладено правило бумеранга — діаметральна зміна вектору загроз від об'єкта впливу до джерела їх формування.

Війна XXI ст., внаслідок обов'язкових спроб застосування воюючими сторонами всіх наявних в їх розпорядженні сил, засобів і способів ведення бойових дій, в абсолютній більшості випадків є гібридною. Тому актуальним, на наш погляд, є пошук адекватних методів аналізу театру гібридної війни, наповнення їх змістом та визначення топології майбутнього протистояння.

Перспективи подальших досліджень полягають у подальшій розробці методичного апарату аналізу театру гібридної війни, нових методів оцінки його стану та створення методичних рекомендацій їх застосування в публічній політики у сфері національної безпеки.

Література:

1. Абрамов, В. І, Борисевич, С. О., Смолянюк, В. Ф., Шевченко, М. М. (2018) Теоретико-методологічні засади формування кадрової безпеки в системі публічного управління [кол. монографія] Київ. НАДУ.

2. Абрамов, В. І. (2020) Безпека як трансгресія: онтологічний статус феномена національної безпеки. Інвестиції: практика та досвід, 15—16, 116—120.

3. Абрамов, В. І. (2020) Методологія постнекласичної науки в дослідженні національної безпеки та особливості державного управління в її забезпеченні.

Збірник наукових праць Національної академії державного управління при Президентові України, 2, 18—24.

4. Дельоз, Ж., Гваттарі, Ф. (2015) Що таке філософія? Львів: Астролябія.

5. Інтеграція психосоціальних моделей і методів у підхід НАТО до операцій (2010). Огляд досліджень системного аналізу Організації досліджень і технологій НАТО (RTO) (SAS-074). Взято з URL: https://www.researchgate.net/publication/224123774_Integration_of_Psycho-Social_models_and_methods_in_NATO's_approach_to_operations_A_review_of_NATO_Research_and_Technology_Organization_RTO_Systems_Analysis_Studies_SAS-074

6. Кравець, П., Киркало, Р. (2009) Системи прийняття рішень з нечіткою логікою. Вісник Національного університету "Львівська політехніка": Комп'ютерні науки та інформаційні технології, 650, 115—123.

7. Навчальний циркуляр сухопутних військ США ТС 7-100. (2010) Взято з URL: https://commons.m.wikimedia.org/w/index.php?title=File:TC_7-100_-_Hybrid_Threat_pdf&page=10

8. Стэнли Мак-Кристал, Крис Фасселл, Коллинс Тантум, Дэвид Сильверман. Жесткий лидер Правила менеджмента от генерала Афганской войны (2020) Взято з URL: https://barracuda-book.com/p1393867620-stenli-makkristal-kris.html.

9. Штовба, С. Д. (2001) Введение в теорию нечетких множеств и нечеткую логику. Винница: Издательство Винницкого государственного технического университета.

10. Ablazov I., Abramov V., Mokliak S., Smolianiuk (2021). Theory-practice problems of public national security policy related to the concept of "complexity" (methodological aspect). Political Science and Security Studies Journal, Vol. 2, No. 4, 28—35.

11. Hoffman F. G. (2007) Conflict in the 21-st century. The rise of hybrid wars. Arlington: Potomac Institute for policy studies.

12. Mattis J. N., Hoffman F. G. (2005) Future Warfare: The Rise of Hybrid Wars. US Naval Institute Proceedings Magazine. November. Vol. 132/11/1, 233. Pp. 18—19. Взято з Url: http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf

13. Zadeh, L. A. (2002) Toward a Perception-Based Theory of Probabilistic Reasoning with Imprecise Probabilities. Journal of Statistical Planning and Inference, Vol. 105 (1). Pp. 233—264. Взято з https://www.researchgate.net/publication/228551318_Toward_a_PerceptionBased_Theory_of_Probabilistic_Reasoning_with_Imprecise_Probabilities

References:

1. Abramov, V.I. Borysevych, S.O. Smolianiuk, V.F. and Shevchenko, M.M. (2018), Teoretyko-metodolohichni zasady formuvannia kadrovoi bezpeky v systemi publichnoho upravlinnia [Theoretical and methodological principles of the formation of personnel security in the system of public administration], NADU, Kyiv, Ukraine.

2. Abramov, V. (2020), "Security as a transgress: ontological status of the national security phenomenon", Investytsiyi: praktyka ta dosvid, vol. 15—16, pp. 116—120.

3. Abramov, V.I. (2020), "Methodology of post-non-classical science in the study of national security and peculiarities of state administration in its provision", Zbirnyk naukovykh prats' Natsional'noi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy, vol. 2, pp. 18—24.

4. Del'oz, Zh. and Hvattari, F. (2015), Scho take filosofiia? [What is philosophy?], Astroliabiia, Lviv, Ukraine.

5. Bacon, T.J. Jones, P. Garrett, R.B. and Tolk, A. (2010), "Integration of Psycho-Social models and methods in NATO's approach to operations; A review of NATO Research and Technology Organization (RTO) Systems Analysis Studies (SAS-074)", available at: https://www.researchgate.net/publication/224123774_Integration_of_Psycho-Social_models_and_methods_in_NATO's_approach_to_operations_A_review_of_NATO_Research_and_Technology_Organization_RTO_Systems_Analysis_Studies_SAS-074 (Accessed 25 Dec 2022).

6. Kravets', P. and Kyrkalo, R. (2009), "Decision-making systems with fuzzy logic", Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika": Komp'iuterni nauky ta informatsijni tekhnolohii, vol. 650, pp. 115—123.

7. wikimedia.org (2010), "US Army Training Circular TS 7—100", available at: https://commons.m.wikimedia.org/w/index.php?title=File:TC_7-100_-_Hybrid_Threat_pdf&page=10 (Accessed 25 Dec 2022).

8. Mak-Krystal, S. Fassell, K. Tantum, K. Syl'verman, D. (2020), "Hard leader. Management rules from the general of the Afghan war", available at: https://barracuda-book.com/p1393867620-stenli-makkristal-kris.html (Accessed 25 Dec 2022).

9. Shtovba, S.D. (2001), Vvedenye v teoryiu nechetkykh mnozhestv y nechetkuiu lohyku [Introduction to fuzzy set theory and fuzzy logic], Yzdatel'stvo Vynnytskoho hosudarstvennoho tekhnycheskoho unyversyteta, Vynnytsa, Ukraine.

10. Ablazov, I. Abramov, V. Mokliak, S. and Smolianiuk (2021), "Theory-practice problems of public national security policy related to the concept of "complexity" (methodological aspect)", Political Science and Security Studies Journal, vol. 2, no. 4, pp. 28—35.

11. Hoffman, F.G. (2007), Conflict in the 21-st century. The rise of hybrid wars, Potomac Institute for policy studies, Arlington, USA.

12. Mattis, J.N. and Hoffman, F.G. (2005), "Future Warfare: The Rise of Hybrid Wars", US Naval Institute Proceedings Magazine, vol. 132/11/1, no. 233, pp. 18—19, available at: http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf (Accessed 25 Dec 2022).

13. Zadeh, L.A. (2002), "Toward a Perception-Based Theory of Probabilistic Reasoning with Imprecise Probabilities", Journal of Statistical Planning and Inference, vol. 105 (1), pp. 233—264, available at: https://www.researchgate.net/publication/228551318_Toward_a_PerceptionBased_Theory_of_Probabilistic_Reasoning_with_Imprecise_Probabilities (Accessed 25 Dec 2022).

Стаття надійшла до редакції 09.01.2023 р.