

**Ю. В. СЕМЕНЮК
Ю. М. ЛИСЕЦЬКИЙ**

ГІБРИДНА ВІЙНА. СУТНІСТЬ, СКЛАДОВІ, МОДЕЛЬ

Проаналізовано погляди зарубіжних і вітчизняних дослідників на сутність та зміст сучасних воєн, які дедалі частіше набувають гібридного характеру. Показано, що в основі гібридних війн – широкий спектр конфронтаційних дій, до яких вдаються у рамках гнучкої стратегії із довгостроковими цілями, заснованої на комплексному застосуванні різних компонентів для дестабілізації противника. Серед них економічний тиск і санкції, інформаційна підготовка, політичне оформлення протиборчих сторін, методи таємної війни та робота спецслужб тощо. Визначені сутність гібридної війни, як багатовимірного міждержавного протистояння, та її основні складові. Запропоновано модель гібридної війни, яка дозволить досліджувати та аналізувати ідеї, концепції, принципи, методи, засоби, які мають застосовуватися при протидії гібридній агресії.

Ключові слова: гібридні війни, складові, виміри, міждержавні протистояння, модель.

Semenyuk Yurii, Lysetskyi Yurii. Hybrid war. Entity, components, model

The article analyzes the views of foreign and domestic researchers on the nature and content of modern wars, which increasingly take on a hybrid character. It is shown that hybrid wars are based on a wide range of confrontational actions employed within the framework of a flexible strategy with long-term goals. This strategy relies on the comprehensive use of various components to destabilize the opponent. Among these components are economic pressure and sanctions, information preparation, the political structuring of opposing sides, covert warfare methods, and the activities of intelligence services, among others. The essence of hybrid warfare as a multidimensional interstate confrontation and its main components are identified. A model of hybrid warfare is proposed, which will allow the study and analysis of ideas, concepts, principles, methods, and means to be applied in countering hybrid aggression.

Key words: hybrid wars, components, measurements, interstate confrontations, model.

© СЕМЕНЮК Юрій Володимирович – кандидат політичних наук, Національний університет оборони України; ORCID: 0000-0002-9415-4427; e-mail: snik71083@gmail.com

© ЛИСЕЦЬКИЙ Юрій Михайлович – доктор технічних наук, доцент, Воєнна академія імені Євгенія Березняка; ORCID: 0000-0002-5080-1856; e-mail: Yurii.Lysetskyi@snt.ua

Вступ. Нині людство постало перед викликами гібридних війн, а це потребує адекватного і гнучкого реагування та завчасного виявлення нових імовірних загроз безпеці держави. У контексті цієї проблеми необхідно якомога детальніше дослідити таке явище, як гібридна війна, що стала одним з ефективних інструментів впливу на міжнародні відносини та міждержавного протиборства [1]. Тому завдання визначення сутності, складових сучасної гібридної війни та побудови її моделі є дуже актуальним.

Метою статті є аналіз змін сутності та змісту війн у сучасних умовах, наявних визначень гібридних воєн, сутності, основних складових гібридної війни та побудова її моделі.

Стан розробки проблеми та методи дослідження. Гібридні війни досліджувалися як зарубіжними, так і вітчизняними вченими та експертами. Це праці Ф. Хоффмана [2], В. Михаеля [3], П. Мансора [4], Д. Уізера [5], Є. Магди [6], В. Горбулина [7] та ін. Водночас деякі аспекти їх сутності, сучасних складових досліджені недостатньо. Що стосується моделі гібридної війни, то окремі автори писали про необхідність та ефективність використання моделі гібридної війни, формулювали вимоги до неї, визначали послідовність розробки, деякі компоненти, але самої моделі гібридної війни так і не наводили [8].

Методологічною основою дослідження є системний підхід та системний аналіз. Враховуючи особливості предметної галузі, також використовуються методи факторного аналізу, порівняння, сценарного аналізу, прогнозування, моделювання та методи прийняття рішень.

Виклад основного матеріалу. В сучасних умовах значно змінюється сутність та зміст війн, дедалі частіше вони мають гібридний характер, хоча даний феномен не можна вважати абсолютно новим. Так, ще видатний китайський стратег і мислитель Сунь-дзи, що жив у VI ст. до н. е., у своєму відомому трактаті про військову стратегію «Мистецтво війни» писав: «Здобути сто перемог у ста битвах – це не вершина військового мистецтва. Повалити ворога без бою – ось вершина» [9]. Тобто можна вважати, що перші риси «гібридних» дій були описані ще в VI столітті до нашої ери.

Окремі дослідники вважають, що автором концепції «гібридних війн» є Френк Хоффман, колишній офіцер морської піхоти, а нині – науковий співробітник міністерства оборони США, яку

він виклав у монографії «Конфлікт у ХХІ столітті. Поява гібридної війни» (2007 р.). Він вважається відомим теоретиком у сфері збройних конфліктів та воєнно-політичної стратегії, думку якого беруть до уваги в керівних колах країн НАТО [2]. Хоффман дефінував гібридну війну як «загрози, які включають повний спектр різних способів ведення військових дій, в тому числі використання конвенціональних можливостей, тактики нерегулярних сил, терористичні дії із застосуванням недискримінаційного насилля і примусу, заворушення, ініційовані злочинними елементами, які застосовуються обома сторонами і різними недержавними гравцями» [2].

В. Горбулін у монографії «Світова гібридна війна: український фронт» також стверджує, що вперше термін гібридна війна виник у військовому середовищі США – у Корпусі морської піхоти [7]. З відкритих джерел цей термін можна зустріти ще до 1998 року, коли Р. Волкер визначив його як поєднання звичайної війни зі спеціальними операціями і дослідив ознаки гібридної війни на прикладі війни США за незалежність. Він вважав, що структурна організація морської піхоти є гібридною за природою і порушував питання про те, що інші роди військ у нових умовах мають застосовувати цей досвід. В. Немет спробував довести, що поширення «гібридних спільнот» (hybrid societies) актуалізує «гібридне ведення війни» (hybrid warfare) і потребує створення «гібридних сил» (hybrid forces) [10].

Для концептуалізації поняття гібридної війни важливе значення мало формування у США уявлень про багатокомпонентну війну. У 1996 році Т. Гюбер сформулював компактне і зрозуміле визначення основного методу цієї війни: «Багатокомпонентна війна – це одночасне використання проти противника регулярних, або основних, військ та іррегулярних, або повстанських, сил» [11].

У своєму звіті за 2017 рік Генеральний секретар НАТО Єнс Столтенберг навів таке визначення: гібридні війни – це «комбінація військових і невійськових, таємних і відкритих дій, що включають дезінформацію, пропаганду, розгортання іррегулярних збройних формувань аж до використання регулярних сил» [12].

Аналіз наявних визначень гібридних воєн і поглядів фахівців на їх структуру показує, що одна з основних рис такої війни – це приховане залучення найманих збройних формувань і сторонніх орга-

нізацій для вирішення завдань міждержавного протиборства при супроводі збройних дій, всебічними відволікаючими маневрами [1]. З точки зору сучасних поглядів, такі наймані формування вже можна вважати підрозділами для ведення гібридних війн та прихованих дій. Проте в гібридній війні використовуються не тільки найманці, а й повстанці, партизани тощо. Про це докладно пише в своїй статті Джеймс К. Уізер [5]. Військовий історик Петер Р. Мансур, наприклад, визначає гібридну війну як «конфлікт, що має на увазі поєднання конвенціональних військових сил і нерегулярних сил (партизан, повстанців і терористів), які можуть бути державними або недержавними акторами, що діють задля досягнення спільної політичної мети» [4]. Існує безліч прикладів гібридної техніки і гібридного підходу на тактичному, оперативному і стратегічному рівнях, де нерегулярні бійці довели, що можуть стати прокляттям для численних конвенціональних збройних сил [13]. Такі величезні армії, як Велика армія Наполеона та Вермахт Гітлера, з великими зусиллями боролися з нерегулярними бійцями, які розуміли і використовували місцевий людський і географічний ландшафт та нападали на вразливі бази постачання та лінії комунікацій. Згодом партизанські операції почали істотно і стійко впливати на більш широкі конвенційні військові кампанії, частиною яких вони були. Антиповстанські кампанії в Іраку та Афганістані ще раз показали, наскільки важко перемогти переконаних нерегулярних бійців, без порушення людських прав місцевого населення, тим самим підтримуючи внутрішню і міжнародну суспільну підтримку кампанії.

Під час війни з Грузією в 2008 році російська федерація (рф) використовувала поєднання регулярних збройних сил, південноосетинських і абхазьких поліцій і російських сил особливого призначення, що діяли під прикриттям образу сил «місцевої оборони». Вважається, що такі гібридні війни відрізняються від їх форм у минулому, є комбінуванням конвенціональних і нерегулярних методів війни. У минулому конвенційні та нерегулярні операції проводилися паралельно, окремо один від одного, а не інтегрованим чином, як нині. Крім того, операції, що проводилися нерегулярними бійцями, зазвичай були допоміжними для кампаній конвенціональних збройних сил.

У сучасній історії найбільш раннім із класичних прикладів гібридних дій, який реалізує декілька компонентів з їх складу,

може бути громадянська війна в Іспанії 1936–1939 роки. Аналіз цього конфлікту, з точки зору сучасної термінології, показує, що в ньому велось типове гібридне протиборство між фашизмом в особі Італії та Німеччини, за підтримки Португалії, та комунізмом в особі СРСР. Боротьба не просто чужими руками, а й на території чужої країни, при дотриманні угоди про «невтручання», підписаної іншими європейськими державами [14]. Надалі прикладів гібридних війн ставало більше: як у жорсткому варіанті, наприклад, силова та інформаційна підтримка дій збройних формувань опозиції і приватних військових компаній у Сирії та Лівії, палестинського ісламістського бойового угруповання ХАМАС, яке керує сектором Газа і фактично воює з Ізраїлем, так і більш м'які варіанти, у формі таємної підтримки лідерів різних «революцій» і «національно-визвольних» рухів.

До 2014 року типовим прикладом військових дій, що відповідають сучасним дефініціям гібридної війни, був конфлікт між Ізраїлем і «Хезболлою». Остання, що отримувала підготовку і обладнання від Ірану, стала несподіванкою для Ізраїлю у витонченому поєднанні партизанської і конвенційної військових тактик та використанням озброєння і комунікаційних систем, що асоціювалися з озброєними силами розвинених країн. На стратегічному рівні «Хезболла» ефективно використовує Інтернет та інші медіа для інформації і пропаганди. Її інформаційний менеджмент із початку конфлікту виявився більш успішним та впливовим на світову думку, ніж менеджмент Ізраїлю.

Як показують наведені вище приклади, гібридне поєднання конвенціональних і нерегулярних методів війни застосовувалося протягом всієї людської історії. Дії росії проти України у 2014 році підвищили інтерес до концепції гібридної війни, адже слово «гібридна» виявилось найбільш вдалим для опису різноманітності та поєднання інструментів і методів, застосованих РФ під час анексії Криму, підтримки сепаратистських груп у Східній Україні та ведення бойових дій у Донецькій і Луганській областях України.

Сучасні гібридні війни не є чимось абсолютно новим, а є продовженням використовуваних раніше різноманітних форм міждержавного протистояння, відрізняються комплексним застосуванням різних форм військового і невійськового протиборства, істотним зростанням технологічних можливостей щодо реалізації різно-

манітних дій, а також масштабами, обумовленими глобалізацією сучасного світу. Гібридна війна містить певний набір складових, за допомогою яких одночасно здійснюється вплив на противника за різними напрямками. Далі визначимо ці складові та проаналізуємо їх зміст [14].

Протягом тривалого історичного періоду можна простежити використання інформаційної складової гібридних дій. Так, вправним майстром розробки і реалізації технологій гібридної війни був засновник найбільшої у світовій історії континентальної імперії – Чингісхан (1162–1227). Його баскаки (збирачі податків) виконували роботу сучасних засобів масової інформації, поширюючи провокаційні та дезінформаційні чутки серед населення, перед походом татар на чужі землі. Згодом подібні дії ставали дедалі масштабнішими та різноманітнішими. Так, агітаційні листівки часів Першої світової війни послужили прототипом такої складової сучасної гібридної війни, як її медійний супровід. У формі, наближеній до сучасної, цей процес вперше запустила Великобританія, порушивши в 1915 році негласну заборону на публікацію фотографій вбитих солдатів противника. У роки війни у В'єтнамі, з появою телебачення, війна буквально «зробила крок з екранів у кожен будинок». Зараз, в еру загальної інформатизації, війна ведеться практично у прямому ефірі. І для гібридних дій дуже важливо, хто буде формувати картинку цього ефіру. З урахуванням цього в даний час обсяг і завдання інформаційного протиборства істотно розширюються, створюються спеціалізовані формування інформаційно-психологічної боротьби та навіть кіберсили, здатні координувати проводити інформаційні операції та кампанії. В якості прикладу можна навести російські ЗМІ, які виступають виключно за «методичками» кремля, відому петербурзьку «фабрику тролів» Пригожина, організовані групи російських хакерів під безпосереднім управлінням гру гш рф і фсб, що представляють серйозну загрозу світовому кіберпростору.

З настанням постіндустріальної епохи інформаційне протиборство доповнилося діями в кіберпросторі та застосуванням деструктивних соціально-політичних технологій [15]. Останні нині використовуються настільки інтенсивно, що їх можна виділити як ще одну складову гібридної війни. Більше того, їх різноманітність навіть дозволяє проводити внутрішню класифікацію таких дій: від

простої фінансової та інформаційної підтримки опозиційних течій і створення всередині держави-противника «п'ятої колонії», до впровадження агентів впливу, які забезпечують так звану «м'яку окупацію» (soft occupation).

Практика показує, що такі дії не лише ефективніші, а й істотно дешевші прямого військового втручання. Наприклад, на підтримку керованого військового режиму у Венесуелі в 60–70-і роки минулого століття США витрачали близько 200 мільйонів доларів щорічно. У ХХІ столітті спроба встановити в цій країні свій уряд коштувала США близько 10–15 мільйонів щороку, що витрачаються на фінансування «опозиції» [14]. Різниця в ціні питання – в рази. Але справа навіть не в економії коштів: для протидії багатьом країнам пряме військове протиборство просто небезпечне, а розхитування їх державної системи зсередини відносно безпечніше.

Одним із аспектів практичного застосування інформаційного протиборства можна вважати використання, в якості обґрунтування гібридних дій, національного питання. З давніх часів фактор національного складу територій міг бути підставою для їх анексії сусідніми державами, як це сталося в 1938 році зі Судетською та Тешинською областями Чехословаччини, зайнятими під приводом «захисту» співвітчизників Німеччини та Польщі відповідно. Інший варіант гібридних дій – відокремлення етнічно відмінних регіонів і створення на їх основі окремих «держав» під зовнішнім протекторатом, як це відбулося за «допомогою» рф з Придністров'ям в 1992 році, Абхазією в 1992–1993 роках, Південною Осетією, де протистояння з Грузією тричі переростало в збройні конфлікти у 1991–1992, 2004 і 2008 роках. У новітній історії, із зростанням мобільності населення, подібні «передгібридні» дії можуть реалізовуватися шляхом надання громадянства на території чужої держави, легітимізації громадян, придбання землі або нерухомості, міграції.

Найважливіший аспект гібридних війн – їх економічна складова. В історичній ретроспективі її використання розпочалося після переходу від натурального господарювання і відокремлених національних економік до світової системи господарювання, пов'язаної з міждержавним розподілом праці та міжнародною торгівлею. Історія демонструє безліч методів, що використовувалися в рамках цієї складової протиборства. Франція в період наполеонів-

ських війн підробляла англійські, австрійські та російські грошові знаки [14]. У наш час, з настанням епохи глобалізації, фінансова складова гібридних війн істотно посилилася, як за масштабами застосування, так і за різноманітністю використовуваних методів. Останні змінюються, від прямого блокування фінансових рахунків окремих осіб і навіть урядів держав-супротивників, до непрямих методів на основі заборон. Прикладом першого типу дій може бути блокування закордонних рахунків Іраку в 2012 році і Венесуели в 2019, рф у 2022 році. Непрямі методи чітко простежуються в забороні на проходження коштів через «треті країни» і компанії або блокуванні доступу іранських банків до системи SWIFT в 2018 році і російських у 2022.

Одним із перших прикладів економічної війни можна назвати «континентальну блокаду»: комплекс заходів із блокування торгівлі Великобританії, що проводилися Францією в 1806–1814 роках. У період XIX–XX століть найбільш поширеним видом економічної війни була саме морська блокада. До початку Першої світової війни блокаді піддавалися: Туреччина, Португалія, Нідерланди, Колумбія, Панама, Мексика, Аргентина і Сальвадор. Ініціаторами блокад були: Великобританія (12 разів), Франція (11 разів), Італія, Німеччина (3 рази), Австрія і Росія (2 рази) та Чилі [14]. Після Другої світової війни економічні санкції залишалися активним інструментом міжнародної політики. У період з 1971 року до кінця XX століття можна зазначити близько 120 випадків санкцій, насамперед у рамках економічної війни Заходу проти СРСР. Вказаний інструмент використовується і в XXI столітті: від загороджувального мита до американських законів «Про контроль над експортом», яким у 1949 році був створений Координаційний комітет з експортного контролю, та «Про протидію противникам Америки за допомогою санкцій» (Countering America's Adversaries Through Sanctions Act, CAATSA) 2017 року. Цей тип санкцій фахівці іноді виділяють в окрему форму дій – технологічне протиборство.

Ще одна складова гібридного протиборства, що знаходиться на межі гуманітарно допустимого, – ресурсне. Його різновиди застосовувалися з давніх часів, у формі блокування фортець при облозі, перекриття доступу провіанту і води. Нині із зростанням технічних можливостей і різноманітністю економічних зв'язків у сучасному світі з'являються нові форми ресурсного протиборства у формі

транспортної, енергетичної та навіть водної блокади, що своїми масштабами призводять до екоциду цілих територій. Типові приклади таких дій – спроба відвести води річки Йордан від Ізраїлю, яка стала однією з причин «шестиденної війни» 1967 року, блокада росією судноплавства у Чорному морі впродовж 2022-2023 років та системне руйнування портової інфраструктури України, що фактично унеможливило постачання зерна морським шляхом до інших країн, знищення греблі Каховської гідроелектростанції 6 червня 2023 року здійснене окупаційними силами рф, що призвело до масштабної екологічної катастрофи і є актом екоциду. Кібердиверсії, здійснювані для руйнування електроенергетики Венесуели в 2019 році [14]. Знищення росією об'єктів електроенергетики України в 2022–2024 роках, їх захоплення, підриг та ракетні обстріли. Так, у березні 2022 року були захоплені російськими військами Запорізька АЕС, яка є найбільшою атомною електростанцією в Європі, та Запорізька ТЕС. А влітку цього ж року була окупована Вуглегірська ТЕС на Донеччині. Наймасивніших ударів по українських енергооб'єктах було завдано 22 і 29 березня та 11 квітня 2024 року. Так, 22 березня 2024 року ворог знищив Зміївську ТЕС на Харківщині, яка постачала електроенергією три області України: Харківську, Полтавську та Сумську, повністю зруйнував Харківську ТЕЦ-5, одну з найбільших в Україні, внаслідок руйнування цієї теплоелектроцентральної Харків втратив основні потужності генерування теплової та електричної енергії. Серйозно пошкоджено Ладизинську ТЕС у Вінницькій області. Також рф вдарила по найбільшій в Україні Дніпровській ГЕС у Запорізькій області – було щонайменше вісім влучань. Після цього зупинили роботу обидві електростанції ДніпроГЕСу, ГЕС-1 і ГЕС-2, пошкодження останньої є критичними. Бурштинська ТЕС у Львівській області за два роки російського вторгнення стала однією з енергетичних цілей, по якій росіяни найчастіше завдавали ракетних та дронівих ударів. Найгірша за наслідками атака сталася під час масованого обстрілу 22 березня 2024 року. Тоді як і на Ладизинській станції того ж дня, і на Бурштинській ТЕС постраждали всі енергоблоки. Канівська ГЕС (Черкаська область) і Дністровська ГЕС (Чернівецька область) були серед цілей масованої російської атаки по енергооб'єктах 29 березня 2024 року. Вночі та вранці 11 квітня 2024 року рф знов атакувала енергетичну інфраструк-

туру України – ракети типу «Х-69» влучили у Трипільську ТЕС, яка була найбільшим постачальником електроенергії до Київської, Черкаської та Житомирської областей, унаслідок чого вона повністю знищена.

Ще однією і досить потужною складовою гібридних війн стала кіберзброя. Яскравим прикладом цього є кібератаки російських хакерів, спрямовані на державні відомства та об'єкти критичної інфраструктури США, Канади, Великобританії, Німеччини, Франції, Італії, України. Наймасштабніші кібератаки на об'єкти критичної інфраструктури та державні інформаційні ресурси України: на окремі офіційні веб-сайти та системи ІТ-сектора (13.01.2022 р.); на близько 70 державних веб-сайтів, зокрема Міністерства оборони України, Міністерства закордонних справ, Державної служби з надзвичайних ситуацій, додатку «Дія» та ін. (14.01.2022 р.); DDoS-атака на державні та банківські сайти України, що тривала понад 5 годин, а цілями були близько 15 банків, зокрема Приватбанк та Ощадбанк, а також сайти домену gov.ua (15–16 лютого 2022 р.); кібератака вірусом FoxBlade на державні ресурси, ІТ-сферу, енергетику і фінансовий сектор з метою знищення баз даних (23.02.2022 р.); на мережу «Київстар», що на дві доби повністю зупинила роботу оператора та призвела до непрацездатності частини банкоматів, POS-терміналів та інформативно-платіжних терміналів Приватбанку, Ощадбанку, Райффайзен банку, Правекс банку, сервісів Монобанку (12.12.2023 р.).

Широкое використання інформаційних технологій у сучасних конфліктах прискорює трансформацію війни та надає їй нової якості за рахунок появи військових операцій принципово нового типу, метою яких є інформаційне руйнування соціально важливих сфер держави та інформаційно-психологічний тиск на противника, щоб зламати його волю, без застосування зброї. В умовах глобалізації та інформаційно-технологічної революції арсенал впливу противника доповнюється технологіями його символічного знищення, спрямованими на духовні і ціннісно-мотиваційні сфери діяльності людей [14]. Для розуміння і осмислення характеру сучасної війни важливого значення набуває чинник, що обумовлює вторинність завдань окупації території противника і захоплення ресурсів, на противагу завданням встановлення стратегічного, всеосяжного контролю над свідомістю населення

країни-мішені та отримання повної влади над завойованою державою.

Однією з найважливіших сфер гібридних операцій є культура, культурно-цивілізаційні цінності та свідомість населення країни впливу. При цьому робиться ставка не на зміст, а на мінливість форм, а зміст як такий відходить на другий план та втрачає цінність, і тоді з населенням можна виконувати будь-які маніпуляції. Водночас сучасна масова культура передбачає зниження культурної, інтелектуальної планки подачі матеріалу для аудиторії. Для доступності інформація для широкої аудиторії не повинна вимагати великих інтелектуальних зусиль глядача і слухача, впливаючи виключно на емоції споживача контенту. В результаті не з'явилося жодної принципово нової ідеології або системи цілісних поглядів, які могли б претендувати на цивілізаційну значущість. Замість ідеології пропонується яскравий «піар» з розмитими, нечіткими та доволі широкими інтерпретаціями ідей та сенсів, які хибно трактують як історичну картину, так і сучасне розуміння сучасного світу. За відсутності ідеології, покликаної спонукати народ до дії, «майстри» гібридних технологій провокують людей і підбурюють протестні рухи для організації заворушень і різних протистоянь. Тут масова культура, її інформаційно-семантичне поле найчастіше використовується як гібридна зброя війни нового типу. З одного боку, це консцієнтальна зброя, спрямована на злам історичного коду пам'яті народу та знищення об'єктивного трактування світової історії. З іншого – взаємопов'язана з першою морально-правова зброя, коли відверта брехня стає правовою підставою для збройної агресії, арешту іноземних громадян і економічного тиску на державу. Мабуть, саме тому «російсько-українська смислова війна реалізувалася в постійній реінтерпретації подій, коли з двох альтернативних джерел для опису обирається те, яке найбільше відповідає запланованим цілям війни». На підтвердження цього Євген Магда наводить низку прикладів даного феномена [6]:

знищення прикладу військової належності: «зелені чоловічки», «ввічливі люди»;

знищення прикладу незаконності: «народний мер», «народний губернатор», «народна самооборона», «возз'єднання Криму»;

посилення негативних характеристик противника: «бойовики», «карателі», «каральна операція», «хунта», «самопроголошена київська влада», «самопроголошений прем'єр»;

завищення свого позитиву аж до сакралізації: «Крим наш», «місто російських моряків», «місто російської слави»;

опис дій і підбір відповідної мотивації з метою їх легітимації: захоплення адміністративних будівель пояснюється словами: «Це ж наше, народне, а ми народ».

Мета інформаційної та психологічної війни зрештою одна – зламати моральний дух противника, ввести його в оману і в кінцевому підсумку перемогти малими жертвами з мінімальними витратами матеріальних ресурсів. Важливий нюанс – інформаційна та психологічна війна значно дешевше класичної війни в плані використання матеріальних ресурсів. Водночас, у контексті додатку інтелектуальних ресурсів, такий вид протистояння є набагато витратніший, оскільки вимагає більш ретельної роботи над проектуванням стратегії і тактики, обчисленням слабких сторін противника і комплексу заходів впливу, які здатні дати максимальний ефект [6].

Ще в якості окремого компонента гібридної війни українські дослідники В. Горбулін і Є. Магда виділяють енергетичну складову, хоча зазвичай аналітики енергетичне вимірювання гібридної війни обходили стороною [6,7]. Але рф досить ефективно використовувала енергетичну зброю проти України і європейських країн. Використання енергетичної зброї для досягнення політичних, стратегічних цілей не є ноу-хау рф. Достатньо згадати нафтову кризу 1973 року, викликану введенням ембарго ОПЕК на поставку нафти країнам Заходу, які підтримали Ізраїль у війні Йом-Кіпур. Вуглеводні ніколи не були звичайним товаром, їх ринок традиційно був чутливим до політичних коливань. За часів існування біполярного світу політична складова енергетичних взаємовідносин була радше винятком, ніж правилом, а в умовах багатополярного світу енергетичний базис практично не обходиться без політичної надбудови. Спокуса використовувати енергетичні важелі в політичних цілях виглядає прямо пропорційно реальному впливу держави на події у світі.

Ф. Хоффман, аналізуючи війни ХХІ століття, слушно зауважує, що війна – це не лише воєнні дії, ведення боїв, необхідно брати до уваги соціально-культурні, техно-економічні й геополітичні вимі-

ри війни [2]. Війна є динамічною реальністю, і наше розуміння та лексикон також мають змінюватися, щоб бути на вістрі часу. Нові умови потребують нових типів зброї для максимально ефективного реагування і нових творчих методів і концепцій.

У цілому дії гібридні війни багато в чому є традиційними (стандартними), елементами збройного конфлікту або протистояння держав. Серед них – економічний тиск і санкції, інформаційна підготовка, політичне оформлення протиборчих сторін, методи таємної війни та робота спецслужб тощо. Отже, в основі гібридних війн – широкий спектр конфронтаційних дій, до яких вдаються у рамках гнучкої стратегії із довгостроковими цілями, заснованої на комплексному застосуванні різних компонентів для дестабілізації противника.

З проведеного аналізу можна зробити висновок, що, незважаючи на деякі відмінності поглядів вітчизняних і зарубіжних дослідників та експертів на сутність гібридної війни, в них є багато спільного. На нашу думку, основною відмінністю гібридної війни, є те, що протистояння між державами відбувається одночасно в декількох різних вимірах: військовому; політичному; дипломатичному; економічному; ресурсному; енергетичному; кібертехнологічному; інформаційно-комунікаційному; соціально-психологічному, культурному; ідеологічному (рис.1).



Рис. 1. Виміри гібридної війни

Отже, гібридна війна є за своєю сутністю багатовимірним між-державним протистоянням.

Нині дуже швидко змінюються традиційні та розвиваються нові способи ведення гібридної війни, що, у свою чергу, потребує перегляду класичних воєнних методів прогнозування і планування, як наступальних, так і оборонних стратегій. Як і будь-яка інша війна, гібридна війна містить елементи недостовірності та невизначеності. Так, недостовірність розвідувальної інформації та постійне втручання випадковостей призводять до того, що сторони конфлікту в дійсності стикаються із цілковито протилежним станом речей, ніж очікували, і це не може не позначатися на плануванні або принаймні на тих уявленнях про положення, які лягли в основу планів.

Одним із способів зменшення невизначеності при прогнозуванні, оцінці ресурсів, розробленні стратегії та плану оперативних дій є застосування моделювання. Моделювання дозволяє відображати вплив просторових і часових параметрів конфлікту, сприяти проведенню якісного аналізу воєнно-політичних ситуацій, запобігати впливу чинника спонтанності та забезпечувати обґрунтованість вжитих заходів із протидії противнику. Для побудови моделі гібридної війни необхідно насамперед сформулювати її призначення та вимоги до неї. Модель гібридної війни повинна відображати багатовимірний характер такої війни, операції якої охоплюють всі сфери держави-жертви і проводяться в інформаційному та кіберпросторах. Процеси та етапи створення моделі гібридної війни як складної системи повинні базуватися на таких методологічних елементах, як: системний підхід, системний аналіз, моделі супроводу її на етапах життєвого циклу (ЖЦ), математичне та імітаційне моделювання.

Системний підхід, як відомо, – універсальна методологія, яка має три складові: цілеорієнтація, систематизація і формалізація. Будь-яка складна система орієнтована на задоволення певних потреб, а метою процесу побудови є створення такої системи. Глобальна мета декомпонується на цілі нижчих рівнів, які досягаються шляхом вирішення сукупності завдань.

Загалом модель – це абстрактне уявлення реальності в будь-якій формі (математичній, фізичній, символічній, графічній або дескриптивній), що дозволяє отримати відповіді на досліджувані

питання. У цьому дослідженні модель гібридної війни являтиме собою графічно-математичний опис, який визначає її цілі, завдання, методи і засоби. Під час дослідження моделі гібридної війни її представляємо як об'єкт, що має просторові та часові обмеження. На першому етапі, дотримуючись системного аналізу як прикладної наукової методології, необхідно виділити модель гібридної війни за певними ознаками із зовнішнього середовища, встановивши водночас саме ті відносини, які її з нею пов'язують [8]. Далі, виходячи з мети створення моделі гібридної війни, формуємо її елементарний базис, структуру, функції. Враховуючи, що будь-який аналіз базується на декомпозиції, необхідно звертати увагу на явище емерджентності, вплив зовнішнього середовища. У результаті виконання системного аналізу отримуємо модель гібридної війни (рис. 2).

Сукупність цілей визнається у вигляді певної системи E_z . Тоді будь-який елемент $e \in E_z$ можна представити у вигляді:

$$e = \langle R_e, Q_e, P_e, V_e, T_e \rangle, \quad (1)$$

де R_e – результат, досягнення якого необхідне відповідно до заданої цілі;

Q_e – вектор параметрів, що характеризують необхідну кількість R_e ;

P_e – вектор параметрів вимог, що висуваються до процесу отримання результату R_e ;

V_e – вектор параметрів, що характеризують витрати ресурсів на отримання R_e ;

T_e – час отримання результату R_e .

Безліч задач, вирішення яких необхідне для досягнення цілі e , позначається E_s . Для множин E_z і E_s справедливе наступне співвідношення. Задача $e \in E_s$ стає ціллю $e \in E_z$, якщо задані величини Q, V, T , де Q – вектор якості результатів вирішення задачі s , V – вектор, що характеризує витрати ресурсів на розв'язання задачі, T – час завершення рішення.

Метод визначається як система (E_a, S_a) , де E_a – безліч операцій (кінцеве), S_a – структура на множині операцій.

Система E_c що реалізує рівень засобів, являє собою сімку елементів:

$$E_c = \langle M_e, M_a, L, O, I, P, T \rangle \quad (2)$$

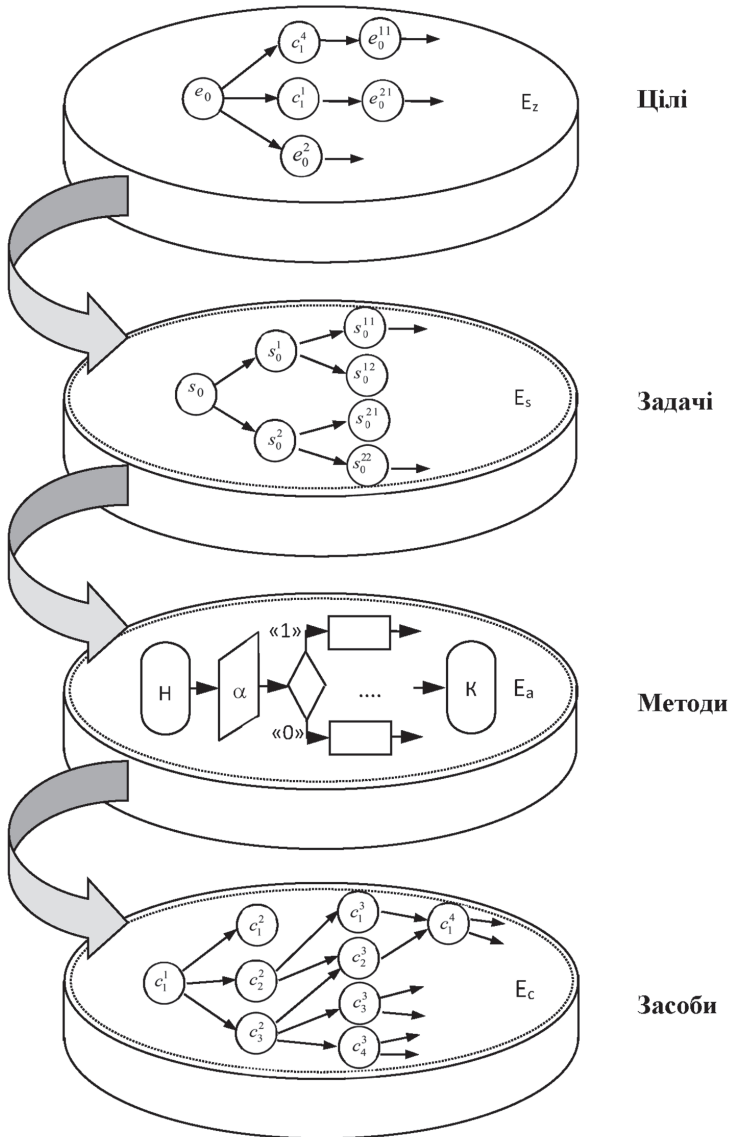


Рис. 2. Модель гібридної війни

із заданою структурою S_c , де складові елементи – види забезпечень: M_e – методичне, M_a – математичне, L – лінгвістичне, O – організаційне, I – інформаційне, P – програмне, T – технічне.

Особливість процесу системного дослідження – його ітераційний характер, що реалізується через ланцюг відображень:

$$E_z \rightarrow E_s \rightarrow E_a \rightarrow E_c, \quad (3)$$

де E_z – непорожня множина цілей, E_s – кінцева множина задач, E_a – кінцева множина методів, E_c – непорожня множина засобів.

Для трансформації $\langle \text{цілі} \rangle \rightarrow \langle \text{засоби} \rangle$ основним атрибутом є категорія ймовірного, для зворотної трансформації $\langle \text{засоби} \rangle \rightarrow \langle \text{цілі} \rangle$ – категорія бажаного (рис. 3).

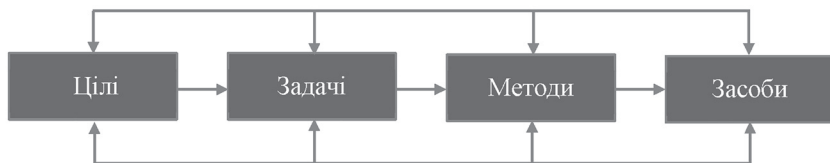


Рис. 3. Ітераційний процес формування моделі гібридної війни

Наступною складовою процесу створення моделі гібридної війни є її прогностичний супровід на всіх етапах ЖЦ. Модель гібридної війни у процесі ЖЦ динамічна на етапах функціонування та модернізації. Функціонування разом із модернізацією є певним логіко-динамічним процесом [8]. Моделюючи гібридну війну, здійснюємо тим самим прогнозування за рахунок вирішення завдань ідентифікації невідомих залежностей та їх оптимізації на основі статистичної та експертної інформації. Також побудова моделі гібридної війни супроводжується необхідністю вибору оптимальних варіантів з альтернативних. Для вирішення цього завдання необхідно використовувати сценарний аналіз, прогнозування, теорію і методи прийняття рішень.

Отже, у зв'язку з труднощами здобуття нових знань моделювання набуває дедалі більшої значущості в дослідженні проблеми гібридних війн. При цьому моделі виступають як ефективний інструмент вивчення конфліктів ХХІ століття і використовуються для вирішення завдань управління, створюючи основу для трансформації об'єкта дослідження в інтересах забезпечення націо-

нальної безпеки. Використання моделі гібридної війни дасть можливість досліджувати та аналізувати ідеї, концепції, принципи, методи та засоби, які мають застосовуватися для протидії гібридній агресії.

Висновки. На основі аналізу поглядів зарубіжних і вітчизняних дослідників та експертів на сутність та зміст сучасних воєн можна визначити сутність гібридної війни як багатовимірного міждержавного протистояння. Її основними складовими є: військова; політична; дипломатична; економічна; ресурсна; енергетична; кібертехнологічна; інформаційно-комунікаційна; соціально-психологічна, культурна; ідеологічна. Запропонована модель гібридної війни допоможе оцінювати характер і небезпеку ситуацій, що виникають, визначати ступінь політичного та військового ризику, напрям політичного і військового процесу, засоби розв'язання кризи, погоджувати застосовуваний комплекс гібридних загроз у рамках єдиного задуму, відображати процеси прогнозування, використання ресурсів і стратегічного планування. Ця модель являє собою ефективний інструмент для відображення і управління процесами підготовки та ведення (або організації відсічі) гібридної війни.

1. Лисецький Ю.М., Семенюк Ю.В., Павленко Д.Г. Міждержавні протистояння. Нові реалії. *Держава і право*. Сер. Політичні науки. 2021. № 89. С. 249–257.
2. Hoffman F.G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies, 2007. P. 14.
3. Michael W. Isherwood. Airpower for Hybrid Warfare. *Mitchell Institute for Airpower studies*, 2009. June. P. 33. URL: <https://www.airforcemag.com/article/1009hybrid>.
4. Mansoor P.R., Murray W. Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. Cambridge, New York: Cambridge University Press, 2012. 334 p.
5. Уїзер Д.К. Сенс гібридної війни. *Connections*. The Quarterly Journal. 2016. Vol. 15, № 2. P. 84–100.
6. Магда Є.В. Гібридна війна: выжить и победить. Харків: Віват, 2015. 320 с.
7. Світова гібридна війна: український фронт: монографія / за заг. ред. В.П. Горбуліна. Київ: НІСД, 2017. 496 с.
8. Лисецький Ю.М. Системна модель гібридної війни. *Вчені записки Таврійського національного університету імені В.І. Вернадського*. Сер. Державне управління. 2022. Т. 33 (72) № 1. С. 111–116.
9. Сунь-цзи. Мистецтво війни / за ред. Т. Клірі. Київ: Софія, 2018. 224 с.
10. Nemeth W.K. USMC, Future War and Chechnya: A Case for Hybrid Warfare. Monterey, California: Naval Postgraduate School, 2002. URL: <https://core.ac.uk/download/pdf/36699567.pdf>.
11. Huber T.M. Compound Warfare. That Fatal Knot / T.M. Huber (ed.); US Army Command

and General Staff College Press. Fort Leavenworth, KS, 2002. P. 2. URL: <https://apps.dtic.mil/sti/pdfs/ADA481548.pdf>. **12.** Лисецький Ю.М., Семенюк Ю.В., Старовойтенко О.О. Гібридна війна як багатовимірне протистояння. *Вісник воєнної розвідки*. 2021. № 67. С. 7–10. **13.** Лисецький Ю.М., Старовойтенко О.О., Семенюк Ю.В., Павленко Д.Г. Виникнення і еволюція гібридних воєн. *Держава і право*. 2021. Вип. 90. С. 159–168. **14.** Лисецький Ю.М., Старовойтенко О.О., Семенюк Ю.В., Павленко Д.Г. Гібридні війни. Компоненти та особливості. *Вчені записки Таврійського національного університету імені В.І. Вернадського*. Сер. Державне управління. 2021. Т. 32 (71) № 5. С. 63–70. **15.** Кармазіна М.С. Виклики сьогодення: дезінформація в контексті розвитку штучного інтелекту та когнітивних воєн сучасності. *Вісник воєнної розвідки*. 2024. № 80. С. 77–82.

References

1. Lysetskyi Yu.M., Semeniuk Yu.V., Pavlenko D.H. Mizhderzhavni protystoiannia. Novi realii. *Derzhava i pravo*. Ser. Politychni nauky. 2021. Vyp. 89. S. 249–257.
2. Hoffman F. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies, 2007.
3. Isherwood M. (2009). Airpower for Hybrid Warfare. *Mitchell Institute for Airpower studies*. Retrieved from <https://www.airforcemag.com/article/1009hybrid>.
4. Mansoor P. and Murray W. Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. Cambridge, New York: Cambridge University Press, 2012.
5. Wither J.K. Making Sense of Hybrid Warfare. *Connections*. The Quarterly Journal. 2016. #15 (2). S. 84–100.
6. Magda E. Hybrydnaia voina: vyzhyt y pobedyt. Ukraine. Kharkiv: Vivat, 2015.
7. Horbulin V. Svitova hibrydna viyna: ukraiinskyi front: monohrafiia. Ukraine, Kyiv: NISD, 2017.
8. Lysetskyi Yu. M. Systemna model hibrydnoi viiny. *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V.I. Vernadskoho*. Ser. Derzhavne upravlinnia. 2022. # 33 (72). S. 111–116.
9. Sun-Tzu. Mystetstvo viiny/ Ed. by Kliri, T. Ukraine, Kyiv: Sophiya, 2018.
10. Nemeth W.K. USMC, Future War and Chechnya: A Case for Hybrid Warfare. Monterey, California: Naval Postgraduate School, 2022. Retrieved from <https://core.ac.uk/download/pdf/36699567.pdf>.
11. Huber T.M. (Ed.). Compound Warfare. That Fatal Knot. US Army Command and General Staff College Press. Fort Leavenworth, KS. 2002. Retrieved from <https://apps.dtic.mil/sti/pdfs/ADA481548.pdf>.
12. Lysetskyi Yu. M., Semeniuk Yu.V. Hibrydna viina yak bahatovymirne protystoiannia. *Visnyk voiennoi rozvidky*. 2021. # 67. S. 7–10.
13. Lysetskyi Yu. M., Semeniuk Yu.V., Pavlenko D.H. Vynyknennia i evoliutsiia hibrydnykh voien. *Derzhava i pravo*, 2021. Vyp. 90. S. 159–168.
14. Lysetskyi Yu. M., Semeniuk Yu. V., Pavlenko D.H. Hibrydni viiny. Komponenty ta osoblyvosti. *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V.I. Vernadskoho*. Ser. Derzhavne upravlinnia. 2021. # 32 (71). S. 63–70.
15. Karmazina M. S. Vykylyky sohodennia: dezinformatsiia v konteksti rozvytku shtuchnoho intelektu ta kohnityvnykh voien suchasnosti. *Visnyk voiennoi rozvidky*. 2024. # 80. S. 77–82.

Semenyuk Yuri, Lysetskyi Yuri. Hybrid war. Entity, components, model

There have been analyzed how the essence and content of wars change in modern conditions, and the existing concepts of hybrid wars. There have been defined the essence of modern hybrid warfare as a multidimensional inter-state confrontation and its main components: military; political; diplomatic; economic; resource; energy; cyber-technological; information-communication; socio-psychological, cultural; ideological. A model of hybrid warfare is proposed, which will allow researching and analyzing ideas, concepts, principles, methods, and means that should be applied in countering hybrid aggression. This model represents an effective tool for depicting and managing the processes of preparation and conducting (or organizing the counter) of hybrid warfare. With the increasing difficulties in acquiring new knowledge, modeling is becoming increasingly significant in the study of hybrid warfare problems. Here, models serve as an effective tool for studying 21st-century conflicts and are used for management tasks, creating the basis for transforming the research object in the interest of national security.

Key words: hybrid wars, components, measurements, interstate confrontations, model.