DOI 10.34132/pard2024.24.14

Dmytro Karamyshev
Valentyn Suvorov
Roman Sobol

OVERCOMING SYSTEMIC VULNERABILITIES OF THE SPHERES OF INFLUENCE OF HYBRID THREATS IN ENSURING STABILITY AND COMPREHENSIVE SECURITY IN THE CONDITIONS OF EUROPEAN INTEGRATION

The article summarizes international experience and methodical approaches regarding the complex solution of tasks to overcome systemic vulnerabilities in the spheres of influence of hybrid threats and the formation of a national resilience ecosystem. Defines that the characteristic features of hybrid aggression are the use of a wide range of military, paramilitary and non-military means, which include tools of political, economic, and humanitarian influence of the enemy on the defining spheres of society's life. The asymmetry of hybrid aggression involves non-linearity and rhizomorphism, as well as the use of various means of influence and borders between war and peace, but does not affect the conceptual foundations and vector of its promotion of war. It is a prerequisite and accompanies the escalation of the conflict, which under certain conditions, often unforeseen, develops into full-scale military operations. Hybrid aggression uses mainly hidden means of informational and psychological confrontation and pressure, which includes: destabilization, provocation, incitement, propaganda, disinformation, discrediting, terrorist actions and cyber attacks, blackmail, etc. in relation to objects of hybrid influence.

It is justified that one of the most important aspects of the processes of institutionalization of the environment in the field of the formation of comprehensive security of society should be considered the formation of a national ecosystem of sustainability with the appropriate structuring, which is a certain set of subsystems, components and elements that

provide the dynamics of development and the main characteristics of the processes of institutionalization of the corresponding ecosystem of sustainability in various spheres of society's life on the basis of clear principles of its functioning, as well as the possibilities of using appropriate methods and means of response in conditions of hybrid threats. Emphasis is placed on the expediency of using the integrated ecosystem of resilience (CORE) model to analyze and find effective ways and means of countering hybrid threats that are potentially vulnerable to democratic societies and capable of influencing decision-making processes and creating cascading effects, as well as for forecasting (foresight) of various scenarios of the development of events in conditions of hybrid threats, as it demonstrates, among other things, dependencies between society, the state and clusters, as well as multilateral communities and global levels.

An approach to defining integrated domains (macrodomains), whose spheres and tools of impression have a certain consistency, is proposed. An integrated approach to the systematization of domains of hybrid threats made it possible to conditionally differentiate their totality into 5 meaningful components (integrated macrodomains): 1) strategic (economic-infrastructural): economic domains, domains of critical infrastructure; domain of spatial (space) activity; 2) political (political-legal): political domains; legal domains; domains of public administration; diplomatic domains; defense (military-paramilitary): military domains; intelligence activity domains; societal (socio-humanitarian): cultural domains; social domains; information (information-technological): information domains; cyber domains. An integrated approach to the definition of meaningful components (integrated macrodomains) will contribute to prompt recognition and countermeasures against the use of standardized tools of hybrid influence on adjacent spheres (domains).

It is noted that, based on the scope and spectrum of application of hybrid threat tools, the insufficient capacity of the professional security sector to effectively counter hybrid aggression, relying solely on its own resources, is determined. It is emphasized that under the conditions of the permanent spread of hybrid threats, the professional

security sector cannot be isolated from society as a sphere of influence of tools of hybrid influence and feels an urgent need to focus more on public awareness of hybrid threats and the search for new and even non-paramilitary ways of countering hybrid aggression with on the part of the proactive public.

Key words: *national security, national resilience, integrated security, integrated model of the ecosystem of resilience, hybrid war, hybrid aggression, hybrid threats, spheres (domains) of hybrid threats, tools of hybrid influence.*

«У гібридної війни немає краю.
Наслідком гібридної війни може
бути лише гібридний мир»
Д. Карамишев

Постановка проблеми у загальному вигляді. Ефективне протистояння окремих демократичних країн викликам глобалізації передбачає об'єднання їх потенціалів для вирішення проблем виживання за умов збереження певного розмаїття. Тому, серед основних потреб забезпечення стійкості національних держав до зовнішніх впливів та кризових явищ, що обумовлені зовнішньо-політичними чинниками є пошук більш гнучких форм їх інтеграції у т.ч. у сфері міжнародної безпеки, що впливає на прийняття важливих стратегічних рішень стосовно забезпечення як глобальної конкурентоспроможності демократичних країн, так і їх стійкості до зовнішніх впливів на арені міждержавних відносин в умовах гібридних загроз [14].

Перебування України в стані перманентної гібридної війни, зумовлює визначення пріоритетів державної політики щодо забезпечення всеохоплюючої безпеки та оборони, де безпека людини і суспільства, як категорія, яка є чутливою до демократичних впливів, що пов'язані із забезпеченням як особистого, так і колективного захисту потребує інституціалізації та реальних механізмів реагування на зовнішні впливи, кризові явища та надзвичайні ситуації, що

 DOI 10.34132/pard2024.24.14

обумовлені повномасштабними воєнними діями, шляхом реалізації відповідних заходів [15].

Особливість сучасної війни полягає у комбінування традиційних воєнних і асиметричних невоєнних дій, військових і невійськових способів і засобів ведення війни, тобто фактично втрати чітких меж між війною і миром. При цьому, активні воєнні дії зазвичай є запорукою перемоги над ворогом, який здебільшого використовує звичайні військові способи і засоби. У той час, як віртуалізація суспільних відносин та використання сучасних технологій відкриває надзвичайні можливості у веденні гібридної війни нового типу, завдяки формуванню мереж та глобальному впливу на них, а також використанню смарт технологій.

Сучасні загрози та виклики міжнародній безпеці і національній безпеці в Україні стають все більш непередбачуваними і динамічними та набувають ознак гібридізації, що зачипає різні сфери суспільства та стосується різних рівнів прийняття рішень щодо формування і реалізації державної політики у відповідних сферах. Однією з умов успішної нової зовнішньої політики є адекватна оцінка безпекового потенціалу держави, чітке розуміння викликів, загроз та відповідних ресурсів для досягнення визначеної мети [3]

Аналіз останніх досліджень і публікацій. Аналіз літературних джерел, що відображають проблемні організаційно-управлінські питання забезпечення стійкості та комплексної безпеки в умовах гібридних загроз свідчить про значну кількість документів стратегічного характеру, що прийняті упродовж останніх років у т.ч., спираючись на європейські стратегії та матеріали міжнародних аналітичних досліджень у сфері забезпечення стійкості до гібридних загроз. Щодо українського досвіду актуалізації та комплексного розв'язання проблем впливу гібридних загроз на формування національної стійкості та комплексної безпеки, то відповідні питання в різний спосіб знайшли своє відображення у публікаціях В. Абрамова, С. Андрущенка, Е. Балашова, О. Бєлова, М. Білоконя, В. Богдановича, О. Бортнікової, О. Бусол, М. Головянко, В. Горбатенка, В. Горбуліна, В. Гордійчука, М. Грановського, С. Гришко, Д. Дубова, В. Злакомана, Д. Карамишева, Б. Качинського, А. Колодка, О. Корнієв-

ського, В. Косевцова, В. Мандрагелі, Н. Нижник, О. Литвиненка, М. Орел, О. Резнікової, А. Семенченка, Г. Ситника, В. Смолянюка, Д. Тихомирова, О. Хилька, А. Хряпинського та ін.

Систематизація та узагальнення матеріалів зазначених дослідників надає змогу формування методичних і практичних підходів щодо подолання системних вразливостей сфер впливу гібридних загроз у забезпеченні стійкості та комплексної безпеки в умовах європейської і євроатлантичної інтеграції України. Усе це робить зазначену проблематику надзвичайно актуальною та потребує чіткого визначення сутності та складових відповідних сфер (доменів) гібридних загроз та відповідних інструментів гібридного впливу.

Формулювання цілей статті (постановка завдання). Мета статті полягає в узагальненні міжнародного досвіду, організаційних засад та методичних підходів стосовно комплексного розв'язання завдань щодо подолання системних вразливостей сфер впливу гібридних загроз і формування національної екосистеми стійкості та забезпечення комплексної безпеки в Україні в умовах євроінтеграції.

Виклад основного матеріалу дослідження. Термін «гібридна війна» увібрав складний характер війни XXI ст., до якої залучено багато суб'єктів, де розмиті відмінності між традиційними видами збройних конфліктів і навіть між поняттями війни і миру. Під цим терміном слід розуміти різновид ескалації конфліктів, властивий для XXI ст., що поєднує застосування державних та недержавних, традиційних і нетрадиційних стратегій, ресурсів, засобів, методів підривної діяльності, механізмів кібервійни з метою досягнення певних політичних цілей [10]. Глосарій з гібридних загроз тлумачить термін «гібридна війна», як синхронізоване використання багатьох інструментів влади, підібраних з урахуванням конкретних вразливостей у всьому спектрі соціальних функцій для досягнення синергетичних ефектів [8].

Гібридна війна відрізняється від ведення традиційної війни головним чином своїм характером, формою та способами ведення, а також низкою характеристик, які мають суттєвий вплив на її перебіг, серед яких особливої уваги заслуговують такі моменти:: стратегічне і оперативно-тактичне неядерне стримування ворога шляхом

 DOI 10.34132/pard2024.24.14

масового оснащення військ новітніми засобами збройної боротьби для ведення операцій без'ядерного та неконтактного (дистанційного) бою; розширення простору та масштабів збройного протистояння, застосування різних способів ураження військових і невійськових об'єктів і комунікацій; протистояння в інформаційній площині та використання новітніх інформаційних технологій тощо [3].

За визначенням європейського центру передового досвіду з протидії гібридним загрозам (Hybrid CoE), «гібридні загрози – це скоординовані та синхронізовані дії, які навмисно спрямовані на системні вразливості демократичних держав та інститутів за допомогою широкого спектру засобів» [11]. Тобто, це – загрози нового типу, які акцентують увагу на таких ознаках, як: асиметрія; мультидоменність, як інструментів, так і вразливостей; перебування нижче порогу атрибуції, тобто неможливість ідентифікувати діяльність як злочинну і однозначно визначити її суб'єктність [19].

Як зазначає А. Колодка, поряд із поєднанням старих і нових методів ведення війни, що передбачає свідому агресію, спостерігається поєднання військових дій з інформаційною війною на всіх рівнях комунікацій, від стратегічних до лоакальних [17].

Важливою ознакою та наслідком реалізації гібридних загроз є агресія без офіційного оголошення війни і створення на території опонента, а також в його когнітивному просторі атмосфери керованого хаосу. Слід зазначити, що гібридні впливи досягають своєї мети, як на індивідуальному рівні (особи, яка приймає рішення), так і на колективному рівні через когнітивний злам (cognitive hack), прояви якого мають такі ознаки, як: дезорієнтація, зневіра і втрата впевненості у своїх цінностях і переконаннях; деморалізація, пасивність і байдужість до власних цінностей і переконань; дестабілізація, що супроводжується різного роду деструктивними вчинками, що може присвести навіть до несвідомої руйнації власного середовища на користь зловмисника через необізнаність щодо стійкості та необгрунтовані рішення і негативні наслідки стосовно власного безпекового простору [19].

Щодо терміну «когнітивна війна», то слушним видається його тлумачення колективом авторів Johns Hopkins University & Imperial

College London у статті, під назвою «Countering cognitive warfare: awareness and resilience» («Протидія когнітивній війні: усвідомлення та стійкість»), яка опублікована у NATO Review20 травня 2021 року, де зокрема зазначено, що «сьогодні когнітивна війна прагне посіяти сумніви, запровадити суперечливі наративи, поляризувати громадську думку, радикалізувати групи і спонукати їх до дій, які можуть зруйнувати або розділити згуртоване суспільство» [5].

Формування національної екосистеми стійкості України в умовах гібридних загроз на основі європейських безпекових стратегій передбачає застосування інституціонального підходу до формування відповідної екосистеми. Українські дослідники, В. Абрамов, О. Бортнікова, розглядали сферу національної безпеки на засадах інституціоналізму, що дозволило уявити її у вигляді складної сфери, яка формується шляхом інтеграції її змістовних складових та міжінституціональної взаємодії, що стосується здійснення зовнішньої і внутрішньої політики держави, розвитку економіки, політично-правових відносин, соціальної життєдіяльності, збереження культурної й духовної самобутності, екологічної та інформаційної захищеності тощо [1, 2].

Екосистеми являють собою складні системи, які виходять за межі системи у звичайному розумінні та включають комплекс компонентів, які складають не лише структуру системи та відображають внутрішньосистемні зв'язки, а й характеристики зовнішнього середовища системи, його вплив на систему та умови функціонування системи в зазначеному середовищі. На думку О. Кунах, О. Жукова та О. Пахомова принципова відмінність звичайної системи і, як на наш погляд, еволюціонуючої екосистеми полягає в тому, що система – це впорядковано взаємодіючі і взаємопов'язані компоненти, які утворюють єдине ціле, а екологічна система – це складна ієрархічна структура організованої матерії, в якій при об'єднанні відповідних компонентів у більші функціональні одиниці з'являються нові якості, яких не було на попередньому рівні, що висвітлює одну з основних парадигм системного підходу [18].

Комплексна модель екосистеми стійкості (CORE) розроблена за спільної ініціативи Об'єднаного дослідницького

 DOI 10.34132/pard2024.24.14

центру Європейської комісії (JRC) і Європейського центру з протидії гібридним загрозам (Hybrid CoE) (англ. European Centre of Excellence for Countering Hybrid Threats), який є міждержавним Центром боротьби з гібридними загрозами — кібератаками, пропагандою та дезінформацією для формування узагальненої картини, щодо основних шарів, рівнів, а також сфер, які можуть бути вразливими для гібридних загроз, полегшення розпізнавання гібридних загроз, визначення інструментів впливу на відповідні сфери та прийняття рішень на різних рівнях реалізації державної політики та управління, сприяння забезпеченню стійкості проти гібридних загроз і превентивним заходам що стосуються виявлення шкідливої діяльності зовнішніх акторів [12].

В основу запропонованої моделі екосистеми стійкості CORE покладена наступна структуризація її підсистем і компонентів: основа, або ядро екосистеми з позиції забезпечення демократичних принципів її функціонування включає в себе 7 концептуальних основ, які суб'єкти гібридної загрози прагнуть підірвати: почуття справедливості та рівного ставлення; громадянські права та свободи; політична відповідальність і підзвітність; верховенство права; стабільність; надійність/доступність; можливості передбачення; простори екосистеми поділяється на три окремі складові: громадський простір, простір управління та простір обслуговування, – які уособлюють три сектори суспільства; шари екосистеми представляють різні «рівні», які існують в організації суспільства: локальний (місцевий); національний; міжнародний. Така диференціація є цілком доречною, оскільки впливи, а також способи дії гібридних загроз та відповідні засоби можуть бути різними на відповідних рівнях [12].

Модель також містить узагальнену картину, що стосується доменів гібридних загроз і комплексу гібридного інструментарію, про що більш детально зазначено в документі під назвою «Стратегічний компас безпеки та оборони» (A Strategic Compass for a stronger EU security and defence in the next decade. Council of the European Union, 2022) [21].

Дослідження Європейського центру передового досвіду з протидії гібридним загрозам (European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) під назвою «Ландшафт гібридних загроз: концептуальна модель» (The Landscape of Hybrid Threats: A conceptual model) визначає як окремі сфери (домени), так і специфічні інструменти гібридного впливу в різних сферах (доменах), за допомогою яких ворожі суб єкти можуть досягати ефекту. При цьому кожна сфера може складатися з низки піддоменів, що включені до основних змістовних доменів, які містяться в моделі екосистеми стійкості CORE. Загалом було визначено 13 таких основних доменів концептуальної моделі, які разом із відповідними піддоменами можуть являти собою точки вразливостей для інструментів, що застосовуються ворожими суб'єктами впливу [7].

Як зазначає А. Хряпинський, сфери, тобто домени не слід досліджувати ізольовано, оскільки вплив на одну сферу може викликати каскадні ефекти в інши [16]. Тому, нами був запропонований підхід щодо визначення інтегрованих доменів (макродоменів), сфери та інструменти враження яких мають певну узгодженість.

Отже, інтегрований підхід до систематизації доменів гібридних загроз дозволив нам умовно поділити їх сукупність на 5 змістовних складових (інтегрованих макродоменів), які не є вичерпними, а лише сприяють їх структуризації:

1) Стратегічні (економіко-інфраструктурні): економічні домени, домени критичної інфраструктури; домен просторової (космічної) діяльності.

2) Політичні (політико-правові): політичні домени; правові домени; домени публічного управління; дипломатичні домени.

3) Оборонні (військово-парамілітарні): військові домени; домени розвідувальної діяльності.

4) Соцієтальні (соціо-гуманітарні): культурні домени; соціальні домени.

5) Інформаційні (інформаційно-технологічні): інформаційні домени; кібердомени.

 DOI 10.34132/pard2024.24.14

Інтегрований підхід до визначення змістовних складових (інтегрованих макродоменів) – це лише приклад того, що за усією різноманітністю сфер (доменів) гібридних загроз та відповідних інструментів гібридного впливу доцільно використовувати систематизацію, що дозволить оперативно робити уявлення про їх приналежність та узагальнено визначати засоби реагування, які можуть фокусуватися на ресурсності, технологічності, комунікаціях, інформованості, ціннісних установках, а також передбачати можливість використання стандартизованих інструментів гібридного впливу до суміжних сфер (доменів).

Серед специфічних інструментів гібридного впливу в різних сферах (доменах), за допомогою яких ворожі суб'єкти можуть досягати ефекту у зазначеному дослідженні (The Landscape of Hybrid Threats: A conceptual model) визначені такі, як: фізичні операції проти інфраструктури; створення та використання інфраструктурних залежностей (включаючи цивільно-військові залежності); використання лазівок у державному управлінні (включаючи управління надзвичайними ситуаціями); заохочення та здійснення корупційних дій; використання порогових значень, неатрибуція, прогалини та невизначеності в законі; використання правових норм, процесів, інститутів та юридичні міркування; підтримка політичних акторів; примус урядів та окремих політичних діячів; дипломатичні представництва та їх неофіційна діяльність; дипломатичні санкції; прямі закордонні інвестиції; фінансування культурних груп та аналітичних центрів; експлуатація соціокультурних розколів за ознаками етнічності, релігії, культури; залучення спільнот етнічної діаспори до здійснення свого впливу; операції спеціальних служб, розвідувальна підготовка, таємні операції, таємна розвідка; промислове шпигунство та контроль спеціалізованих технологій; використання сил спеціальних операцій; діяльність воєнізованих організацій і формувань (уповноважених); військові навчання, випробування стратегічної і тактичної зброї; дискредитаційні кампанії; контроль і втручання в ЗМІ; дезінформаційні та пропагандистські кампанії; кіберактивність, електронна діяльність (заглушення GNSS та крадіжка особистих даних); вплив на

академічні кола, запровадження та оновлення змісту освітніх програм тощо [7]

Як зазначає О. Резнікова, побудова складної багаторівневої національної системи оцінки загроз і ризиків має бути зосереджена на підвищенні готовності держави та суспільства до реагування на численні загрози, загалом – на зміцненні національної стійкості та відбуватися на основі єдиної методології оцінки ризиків і загроз національній безпеці, що допомагає порівнювати та класифікувати загрози та їх наслідки в різних сферах на основі єдиних критеріїв, а також ідентифікувати як ризики, так і наслідки для ключових цільових груп, а також спроможності, що необхідні для ефективного реагування на загрози на основі аналізу яких мають бути розроблені універсальні протоколи узгоджених дій щодо реагування на загрози та кризові ситуації на різних етапах їх розгортання [20].

Оцінюючи сучасні загрози національній безпеці та безпеці країн членів НАТО, США, разом з деякими іншими країнами альянсу вважають одним із найбільш перспективних напрямів протидії таким впливам впровадження концепції ведення «мультидоменних операцій» (Multi-Domain Operations) [6, 22], що включає в себе одночасне проведення скоординованих операцій, узгоджених за місцем і часом у декількох сферах (доменах) і просторах (земля, море, повітря, космос, кіберпростір) для ураження активів супротивника, наражаючи його на низку оперативних та/або тактичних дилем через комбіноване (змішане) застосування окремих військ (сил), залучених до побудови мультидоменного угруповання, в тісній взаємодії сил і засобів між різними сферами, для досягнення конкретних оперативно-тактичних завдань [13]. Щодо інших, провідних країн альянсу, то подібну концепцію запроваджує Великобританія, яка сконцентрувала увагу на можливостях багатодоменної інтеграції (Multi-Domain Integration) між трьома рівнями: органами державної влади, багатодоменним середовищем ведення операцій та союзниками [9].

За визначенням вже згаданих вище українських дослідників, В. Злакоман, В. Гордійчук, під мультидоменними (багатосферними) операціями слід мати на увазі комплексне застосування

 DOI 10.34132/pard2024.24.14

спроможностей наявних об'єднаних мультифункціональних сил в усіх сферах та вимірах з метою створення відносної переваги над супротивником, що передбачає, в першу чергу, протистояння в області останніх технологічних досягнень на основі передових технологій, які забезпечать ефективну систему ситуаційної обізнаності та управління [22].

Спільна декларація ЕС і НАТО (2016) наголошує на комплексному підході з протидії гібридним загрозам, у тому числі щодо підвищення обізнаності громадськості стосовно гібридних загроз, що є одним основних чинників формування, розвитку та підтримання обізнаності та стійкості суспільства [4].

Висновок. Визначено, що характерними рисами гібридної агресії є використання широкого спектру воєнних, парамілітарних і невоєнних засобів, що включають інструменти політичного, економічного, гуманітарного впливу супротивника на визначальні сфери життедіяльності суспільства. Асиметрія гібридної агресії передбачає нелінійність і ризоморфність, а також використання різного роду засобів впливу та межує між війною і миром, але не впливає на концептуальні засади та вектор її просування війни. Вона є передумовою і супроводжує ескалацію конфлікту, який за певних умов, частіше непередбачуваних – переростає у повномасштабні воєнні дії. Гібридна агресія використовує переважно приховані засоби інформаційно-психологічного протистояння та тиску, що передбачає: дестабілізацію, провокування, розпалення, пропаганду, дезінформацію, дискредитацію, терористичні акції і кібератаки, шантаж тощо по відношенню до обєктів гібридного впливу. Обгрунтовано, що одним з найбільш важливих аспектів процесів інституціоналізації середовища у сфері формування комплексної безпеки суспільства слід вважати формування національної екосистеми стійкості з відповідною структуризацією, що являє собою певну сукупність підсистем, компонентів та елементів, що забезпечують динаміку розвитку й основні характеристики процесів інституціоналізації відповідної екосистеми стійкості у різних сферах життедіяльності суспільства на основі чітких принципів її функціонування, а також можливостей використання відповідних

способів і засобів реагування в умовах гібридних загроз. Модель комплексної екосистеми стійкості (CORE) доцільно використовувати для аналізу та пошуку дієвих способів і засобів протидії гібридним загрозам, що є потенційно вразливими для демократичних суспільств і здатними впливати на процеси прийняття рішень та створювати каскадні ефекти, а також для прогнозування (форсайту) різних сценаріїв розвитку подій в умовах гібридних загроз. Вона демонструє залежності між суспільством, державою та кластерами, а також багатосторонніми спільнотами та глобальними рівнями. Запропоновано підхід щодо визначення інтегрованих доменів (макродоменів), сфери та інструменти враження яких мають певну узгодженість. Інтегрований підхід до систематизації доменів гібридних загроз дозволив провести умовну диференціацію їх сукупності на 5 змістовних складових (інтегрованих макродоменів): 1) стратегічних (економіко-інфраструктурні): економічні домени, домени критичної інфраструктури; домен просторової (космічної) діяльності; 2) політичних (політико-правові): політичні домени; правові домени; домени публічного управління; дипломатичні домени; оборонних (військово-парамілітарні): військові домени; домени розвідувальної діяльності; соцієтальних (соціо-гуманітарні): культурні домени; соціальні домени; інформаційних (інформаційно-технологічні): інформаційні домени; кібердомени. Інтегрований підхід до визначення змістовних складових (інтегрованих макродоменів) сприятиме оперативному розпізнаванню та протидії використанню стандартизованих інструментів гібридного впливу до суміжних сфер (доменів). Виходячи з масштабів та спектру застосування інструментів гібридних загроз, слід наголосити на недостатньої спроможності сектору професійної безпеки ефективно протидіяти гібридній агресії, розраховуючи виключно на власні ресурси. За умов перманентного поширення гібридних загроз, професійний безпековий сектор не може бути ізольований від суспільства, як сфери впливу інструментів гібридного впливу та відчуває гостру необхідність більшою мірою орієнтуватись на обізнаність суспільства щодо гібридних загроз та пошук нових і навіть непарамілітарних способів протидії гібридній агресії з боку

 DOI 10.34132/pard2024.24.14

проактивної громадськості. Формування національної екосистеми стійкості спрямовано на подолання системних вразливостей сфер впливу гібридних загроз у забезпеченні комплексної безпеки суспільства.

Стаття надійшла до редакції: 07.02.24

ПОДОЛАННЯ СИСТЕМНИХ ВРАЗЛИВОСТЕЙ СФЕР ВПЛИВУ ГІБРИДНИХ ЗАГРОЗ У ЗАБЕЗПЕЧЕННІ СТІЙКОСТІ ТА КОМПЛЕКСНОЇ БЕЗПЕКИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

У статті узагальнено міжнародний досвід та методичні підходи стосовно комплексного розв'язання завдань щодо подолання системних вразливостей сфер впливу гібридних загроз і формування національної екосистеми стійкості. Визначено, що характерними рисами гібридної агресії є використання широкого спектру воєнних, парамілітарних і невоєнних засобів, що включають інструменти політичного, економічного, гуманітарного впливу супротивника на визначальні сфери життєдіяльності суспільства. Асиметрія гібридної агресії передбачає нелінійність і ризоморфність, а також використання різного роду засобів впливу та межує між війною і миром, але не впливає на концептуальні засади та вектор її просування війни. Вона є передумовою і супроводжує ескалацію конфлікту, який за певних умов, частіше непередбачуваних – переростає у повномасштабні воєнні дії. Гібридна агресія використовує переважно приховані засоби інформаційно-психологічного протистояння та тиску, що передбачає: дестабілізацію, провокування, розпалення, пропаганду, дезінформацію, дискредитацію, терористичні акції і кібератаки, шантаж тощо по відношенню до обєктів гібридного впливу.

Обгрунтовано, що одним з найбільш важливих аспектів процесів інституціоналізації середовища у сфері формування комплексної безпеки суспільства слід вважати формування національної екосистеми стійкості з відповідною структуризацією, що являє

собою певну сукупність підсистем, компонентів та елементів, що забезпечують динаміку розвитку й основні характеристики процесів інституціоналізації відповідної екосистеми стійкості у різних сферах життєдіяльності суспільства на основі чітких принципів її функціонування, а також можливостей використання відповідних способів і засобів реагування в умовах гібридних загроз. Наголошується на доцільності використання моделі комплексної екосистеми стійкості (CORE) для аналізу та пошуку дієвих способів і засобів протидії гібридним загрозам, що є потенційно вразливими для демократичних суспільств і здатними впливати на процеси прийняття рішень та створювати каскадні ефекти, а також для прогнозування (форсайту) різних сценаріїв розвитку подій в умовах гібридних загроз, оскільки вона демонструє у тому числі залежності між суспільством, державою та кластерами, а також багатосторонніми спільнотами та глобальними рівнями.

Запропоновано підхід щодо визначення інтегрованих доменів (макродоменів), сфери та інструменти враження яких мають певну узгодженість. Інтегрований підхід до систематизації доменів гібридних загроз дозволив провести умовну диференціацію їх сукупності на 5 змістовних складових (інтегрованих макродоменів): 1) стратегічних (економіко-інфраструктурні): економічні домени, домени критичної інфраструктури; домен просторової (космічної) діяльності; 2) політичних (політико-правові): політичні домени; правові домени; домени публічного управління; дипломатичні домени; оборонних (військово-парамілітарні): військові домени; домени розвідувальної діяльності; соцієтальних (соціо-гуманітарні): культурні домени; соціальні домени; інформаційних (інформаційно-технологічні): інформаційні домени; кібердомени. Інтегрований підхід до визначення змістовних складових (інтегрованих макродоменів) сприятиме оперативному розпізнаванню та протидії використанню стандартизованих інструментів гібридного впливу до суміжних сфер (доменів).

Зазначено, що виходячи з масштабів та спектру застосування інструментів гібридних загроз визначається недостатня спроможность сектору професійної безпеки ефективно проти-

 DOI 10.34132/pard2024.24.14

діяти гібридній агресії, розраховуючи виключно на власні ресурси. Наголошується, що за умов перманентного поширення гібридних загроз, професійний безпековий сектор не може бути ізольований від суспільства, як сфери впливу інструментів гібридного впливу та відчуває гостру необхідність більшою мірою орієнтуватись на обізнаність суспільства щодо гібридних загроз та пошук нових і навіть непарамілітарних способів протидії гібридній агресії з боку проактивної громадськості.

Ключові слова: *національна безпека, національна стійкість, комплексна безпека, комплексна модель екосистеми стійкості, гібридна війна, гібридна агресія, гібридні загрози, сфери (домени) гібридних загроз, інструменти гібридного впливу.*

Received: 07.02.24

References

1. Abramov, V.I. (2011). Katehoriia «bezpeka»: vid metodolohichnykh zasad instytutsionalizmu do derzhavno-upravlinskoho zmistu [The category «security»: from the methodological foundations of institutionalism to the state-management content]. Problemy zabezpechennia natsionalnoi bezpeky Ukrainy na suchasnomu etapi derzhavotvorennia – Problems of ensuring the national security of Ukraine at the current stage of state-building, (pp. 7-12). H.P. Sytnyk (Ed.). Kyiv: NADU [in Ukrainian].

2. Bortnikova, O.H. (2012). Instytutsiinyi pidkhid do doslidzhennia system bezpeky v teorii derzhavnoho upravlinnia [Institutional approach to the study of security systems in the theory of public administration]. *Derzhavne upravlinnia: vdoskonalennia ta rozvytok – Public administration: improvement and development,* 6. Retrieved from: http://www.dy.nayka.com.ua/? op=1&z= 429 [in Ukrainian].

3. Busol, O. (2020). Hibrydni zahrozy: chy vyzhyve Ukraina? [Hybrid threats: will Ukraine survive?]. *yvu.com.ua.* Retrieved from: https://yvu.com.ua/gibrydni-zagrozy-chy-vystoyit-ukrayina/ [in Ukrainian].

4. Council conclusions on the 2016 EU-NATO Joint Declaration. (2016). *www.nato.int.* Retrieved from: https://www.nato.int/cps/uk/natohq/official_texts_133163.htm?selectedLocale=en [in English].

5. Countering cognitive warfare: awareness and resilience. (2021). *www.nato.int.* Retrieved from: https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html [in English].

6. Palavenis, D. (2022). Options for Small NATO Countries to Prepare for Multi-Domain Operations. *smallwarsjournal.com*. Retrieved from: https://smallwarsjournal.com/jrnl/art/options-small-natocountries-prepare-multi-domain-operations [in English].

7. Giannopoulos, G., Smith, H., & Theocharidou, M. (2021). *The Landscape of Hybrid Threats*. Luxembourg: Publications Office of the European Union. Retrieved from: https://doi:10.2760/44985 [in English].

8. Hryshko, S., Holovianko, M., & Tytarenko, M. (2021). *Hlosarii hibrydnykh zahroz [Glossary of hybrid threats]*. Retrieved from: https://warn-erasmus.eu/ua/glossary/ [in Ukrainian].

9. Kerivnytstvo. Multi-Domain Integration [Management. Multi-Domain Integration]. (2022). *www.gov.uk*. Retrieved from: https://www.gov.uk/guidance/multi-domainintegration [in Ukrainian].

10. Horbatenko, V.P. Hibrydna viina [Hybrid war]. (2022). *vue.gov.ua*. Retrieved from: https://vue.gov.ua/%D0%93%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%B0_%D0%B2%D1%96%D0%B9%D0%BD%D0%B0 [in Ukrainian].

11. Hibrydni zahrozy [Hybrid threats]. (2021). *www.hybridcoe.fi*. Retrieved from: https://www.hybridcoe.fi/hybrid-threats/ [in English].

12. Hibrydni zahrozy. Kompleksna ekosystema stiikosti [Hybrid threats. A comprehensive ecosystem of sustainability]. (n.d.). *www.hybridcoe.fi*. Retrieved from: https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/ [in English].

13. Judson, J. (2022). US Army adopts new multidomain operations doctrine. *www.defensenews.com*. Retrieved from: https://www.defensenews.com/land/2022/10/10/us-army-adopts-new-multidomainoperations-doctrine/ [in English].

14. Karamyshev, D.V. (2018). Dominanty hlobalnoho upravlinnia u vymirakh hlobalnoho rozvytku [Dominants of global governance in dimensions of global development]. *Teoriia i praktyka derzhavnoho upravlinnia – Theory and practice of public administration*, 4, (pp. 8-20) [in Ukrainian].

15. Karamyshev, D.V., & Hordiienko, L.P. (2023). Taktychna bezpeka yak skladova natsionalnoi bezpeky ta kompleksnoi oborony v umovakh zvychainoi ta hibrydnoi viiny [Tactical security as a component of national security and comprehensive defense under conditions of conventional and hybrid

warfare]. *Teoriia i praktyka derzhavnoho upravlinnia – Theory and practice of public administration*, 2 (77), (pp. 188-205). Retrieved from: http://doi.org/10.26565/1727-6667-2023-2-11 [in Ukrainian].

16. Khriapinskyi, A.P. (2022). Sfery vplyvu ta instrumenty realizatsii hibrydnykh zahroz: modeli ta mekhanizmy [Spheres of influence and tools for implementing hybrid threats: models and mechanisms]. *Derzhavne budivnytstvo – State construction*, 2 (32), (pp. 60-67). Retrieved from: https://doi.org/10.26565/1992-2337-2022-2-06 [in Ukrainian].

17. Kolodka, A. (2022). Kryzovyi upravlinnia v umovakh povnomasshtabnoi viiny [Crisis management in conditions of full-scale war]. *Naukovyi visnyk: Publichne upravlinnia – Scientific Bulletin: Public Administration*, (2 (12), (pp. 75-86). Retrieved from: https://doi.org/10.33269/2618-0065-2022-2(12)-75-86 [in Ukrainian].

18. Kunakh, O.M., Zhukov, O.V., & Pakhomov, O.Ye. (2023). *K-56 Otsinka stanu ekosystem ta yikh komponentiv (vybrani temy) [K-56 Assessment of the state of ecosystems and their components (selected topics)]*. Dnipro: Typohrafiia ARBUZ [in Ukrainian].

19. Balashov, E., Bilokon, M., Borozentseva, T., Holovianko, M., Hryshko, S., & Zhovtenko, T. (et al.). (2023). *Metodyka navchannia v umovakh hibrydnykh zahroz [Methodology of training in conditions of hybrid threats]*. Kharkiv: TOV «Tekhnolohichnyi tsentr HRUP. Retrieved from: https://sciencebookgroup.org/catalog/view/338/533/2377 [in Ukrainian].

20. Reznikova, O.O. (2022). *Natsionalna stabilnist v umovakh minlyvoho seredovyshcha bezpeky [National stability in the conditions of a changing security environment]*. Kyiv: NISD. Retrieved from: https://niss.gov.ua/sites/default/files/2022-03/reznikova-ukraineresilience2022_02. pdf [in Ukrainian].

21. A Strategic Compass for a stronger EU security and defence in the next decade. Council of the European Union. (2022). *www.consilium.europa.eu.* Retrieved from: https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/ [in English].

22. Zlakoman, V.V., & Hordiichuk, V.V. (2022). Kontseptsiia bahatoprofilnoi diialnosti oborony Ukrainy: tekhnolohichnyi aspekt [The concept of multi-domain operations for the defense of Ukraine: technological aspect]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony – Modern information technologies in the field of security and defense*, 3 (45), (pp. 37-44). Retrieved from: https://doi.org/10.33099/2311-7249/2022-45-3-37-44 [in Ukrainian].

Відомості про авторів / Information about the Authors

Дмитро Карамишев, д.держ.упр., професор, професор кафедри публічної політики ННІ «Інституту державного управління» Харківського національного університету імені В.Н. Каразіна, м. Харків, Україна. E-mail: dvk1vip@gmail.com, orcid: https://orcid.org/0000-0001-8599-2923.

Dmytro Karamyshev, Doctor of Sciences in Public Administration, Full Professor of the Department of Public Policy, Educational and Scientific Institute «Institute of Public Administration» of V. N. Karazin Kharkiv National University, Kharkiv, Ukraine. E-mail: dvk1vip@gmail.com, orcid: https://orcid.org/0000-0001-8599-2923.

Валентин Суворов, к.держ.упр., доцент кафедри громадського здоров'я та управління охороною здоров'я Харківського національного медичного університету, м. Харків, Україна. E-mail: vip.suvorov@gmail.com, orcid: https://orcid.org/0009-0002-0196-4269.

Valentyn Suvorov, Candidate of Sciences in Public Administration, Assistant Professor of the Department of Public Health and Health Care Management of the Kharkiv National Medical University, Kharkiv, Ukraine. E-mail: vip.suvorov@gmail.com, orcid: https://orcid.org/0009-0002-0196-4269.

Роман Соболь, к.держ.упр., доцент кафедри публічної політики ННІ «Інституту державного управління» Харківського національного університету імені В.Н. Каразіна, м. Харків, Україна. E-mail: sobolroma3@gmail.com, orcid: https://orcid.org/0000-0002-3176-3807.

Roman Sobol, Candidate of Sciences in Public Administration, Assistant Professor of the Department of Public Policy, Educational and Scientific Institute «Institute of Public Administration» of V. N. Karazin Kharkiv National University, Kharkiv, Ukraine. E-mail: sobolroma3@gmail.com, orcid: https://orcid.org/0000-0002-3176-3807.

 DOI 10.34132/pard2024.24.14

Karamyshev, D., Suvorov, V., & Sobol, R. (2024). Overcoming systemic vulnerabilities of the spheres of influence of hybrid threats in ensuring stability and comprehensive security in the conditions of european integration. Public Administration and Regional Development, 24, 628-647. https://doi.org/10.34132/pard2024.24.14