ДЕРЖАВНЕ УПРАВЛІННЯ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ

DOI: https://doi.org/10.26565/1992-2337-2023-2-05
УДК 351

Карамишев Дмитро Васильович,
доктор наук з державного управління, професор,
професор кафедри публічної політики
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: dvk1vip@gmail.com https://orcid.org/0000-0003-1617-3240

Соболь Роман Георгійович,
кандидат наук з державного управління, доцент,
доцент кафедри публічної політики
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: sobol_roma@ukr.net https://orcid.org/0000-0002-3176-3807

Мирна Надія Володимирівна,
кандидат наук з державного управління, доцент,
доцент кафедри права, національної безпеки та європейської інтеграції
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: mail4myrna@gmail.com https://orcid.org/0000-0003-3351-5572

Євдокимов Вадім Олександрович,
кандидат економічних наук, доцент,
доцент кафедри публічного управління та державної служби
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: v.ievdokymov@karazin.ua https://orcid.org/0000-0003-0620-4939

ВПЛИВ ГІБРИДНИХ ЗАГРОЗ НА СУЧАСНУ НАЦІОНАЛЬНУ БЕЗПЕКУ УКРАЇНИ

Як цитувати: Карамишев Д. В., Соболь Р. Г., Мирна Н. В., Євдокимов В. О. Вплив гібридних загроз на сучасну національну безпеку України. *Державне будівництво.* 2023. № 2 (34). С. 54–66. DOI: https://doi.org/10.26565/1992-2337-2023-2-05
In cites: Karamyshev, D.V., Sobol, R.G., Myrna, N.V., Yevdokymov, V.O. (2023). The influence of hybrid threats on the modern national security of Ukraine. *State Formation, no. 2 (34), 54–66.* DOI: https://doi.org/10.26565/1992-2337-2023-2-05 [in Ukrainian].

Анотація. У статті зроблено огляд сучасного стану впливу гібридних загроз на сучасну національну безпеку в Україні. Чітко ідентифіковано поняття «гібридні загрози» та визначні заходи протидії. Виділені слабкі місця (небезпеки) і гібридні загрози безпеці Україні та суспільства на сучасному етапі.

Ключові слова: гібридні загрози, національна безпека, організація процесу управління, регуляторна політика, економічна безпека, енергетична безпека.

Постановка проблеми. Гібридна напад Росії проти України змінився в активну фазу на початку 2022 р., хоч шкідницьку практику проти України вона почала вести одразу після оприлюднення Україною самостійності у 1991 р.

Переконання українських вчених-аналітиків також вказують про те, що Росія всякчас орудувала над послабленням України, і ця практика особливо збільшилась з приходом В. Путіна до керівництва.

Отже, гібридний вплив Росії несе небезпеку українському товариству через свою невизначеність та використання її в якості об'єкта й, одночасно, механізму агресії. Тому проблема впливу гібридних загроз на сучасну безпеку України вельми актуальна та потребує негайного вирішення.

Аналіз останніх досліджень і публікацій. Питання дослідження гібридних загроз є відносно молоді, але вже багато науковців присвятили свої праці теоретичним дослідженням, практичним розробкам та аналізу впливу гібридних загроз на сучасну безпеку України. До таких вчених необхідно віднести наступних: Гончар М., Жук С., Зварич О., Максак Г., Мартинюк В., Тищенко Ю., Чижова О., Чубик А. та інших.

Постановка завдання. Метою статті є аналіз процесу впливу гібридних загроз на сучасну безпеку України та з'ясування основних підходів щодо їх зменшення.

Виклад основного матеріалу. В Європейському Союзі чітко визначено «гібридні загрози» та визначено контрзаходи, розроблено низку документів, зокрема Глобальну Концепцію Європейського Союзу, Колективний документ щодо противенства гібридним загрозам (6 квітня 2016 р.) [4] та Спільний звіт до Європейського парламенту та Європейської ради щодо його виконання (19 липня 2017 р.) [5], Операційного протоколу Європейського союзу щодо протиборства з гібридними загрозами «EU Playbook» (5 липня 2016 р.), Спільного робочого документа «Східне партнерство – 20 передбачуваних звершень 2020 р.»: Фокус – на ключових пріоритетах і реальних результатах» (15 грудня 2016 р.), звіт Європейського парламенту «Боротьба з гібридними загрозами: співробітництво Європейського Союзу – NATO» (березень 2017 р.) [6].

У Загальному рамковому документі зауважено, що головні виклики миру та стабільності лежать у східному та південному сусідстві Європейського союзу, хоча на відміну від вищезгаданого документу Європейського парламенту, який чітко ідентифікує Російську Федерацію та ІД, причини цих викликів не уточняються [1].

У глобальній стратегії Європейського союзу навіть зазначено, що "європейський порядок безпеки було порушено на Сході", а причиною названо "недодержання Росією інтернаціонального права та дестабілізацію України".

У Спільній доповіді Європейському парламенту та Раді зазначається, що «загрози все частіше приймають нетрадиційні форми».

У Суцільному рамковому папірці гібридні загрози концепційно визначаються як «інтегрування насильницької та підривної практики, традиційних і нетрадиційних засобів (тобто військових, дипломатичних, технологічних, економічних), які тямлять скоординовано використовуватися державами або недержавні актори для звершення визначених цілей, зостаючись за порогом офіційно оголошеної війни" [2].

У вищезазначеній доповіді Європейського парламенту гібридна війна визначається як "ситуація, в якій країна, на додачу до поєднання інших прийомів (тобто економічних, політичних і дипломатичний) вдається до відкритого застосування озброєних сил насупроти іншій країні і гібридна загроза як «подія, яка появляється зв'язку відмінних часток, які водночас закладають більш важку та багатовимірну небезпеку» [3].

У Європейському Союзі галузі противенстві таким загрозам класифікуються таким чином: інформаційний сектор, енергетичний сектор, логістика та інфраструктура, військовий сектор, охорона здоров'я та харчова безпека, кіберпростір, фінансовий сектор, промисловий, громадський чи соціальний вимір.

Потрібно сказати, що Європейський Союз дуже серйозно ставиться до визначення гібридних загроз, і минулого року вже було запропоновано створити гібридний термоядерний осередок Європейського союзу у рамках Розвідувально-ситуаційного центру Європейського Союзу. На цю нову побудову, яка досягла повної оперативної спроможності в травні 2017 року, покладено завдання збору, аналізу та обґрунтування гласної та негласної інформації щодо індикаторів гібридних загроз та сповіщень. Цей центр наводить гібридні загрози до європейського знаменника та інформує про них інституції Європейського союзу та країни-члени Європейського союзу, у тому номері у проформі «гібридного бюлетеня».

Водночас було запропоновано створення Центру компетенції з противенству гібридним загрозам, котрий було запущено у Фінляндії у квітні 2017 р. [7] і буде зосереджено на дослідженні таких загроз та інструментів противенству їм. Країни походження гібридних загроз у розумінні Європейського Союзу можуть експлуатувати вразливих членів суспільства та нав'язувати їм дійові та екстремістські думки за допомогою сучасних каналів зв'язку (пропаганди).

Тому Європейський Союз бачить підвищення обізнаності громадськості та боротьбу з пропагандою як центральне завдання в

інформаційному секторі. Створено спеціальну групу «Stratcom East», запущено спецпроект EU-STRAT, який також працює в країнах Східного партнерства, а видалення нелегального інформаційного контенту спирається, зокрема, на Антитерористичну мережу, Центр Європейського Союзу є частиною Європолу.

У кіберсфері Європейський Союз прийняв Стратегію Європейського Союзу з кібербезпеки, Європейський порядок денний безпеки та Директиву про мережеву та інформаційну безпеку. Окремо Європейська комісія заснувала Агентство Європейського Союзу з мережевої та інформаційної безпеки для боротьби з кіберзагрозами на рівні Європейського Союзу і Платформу мережевої та інформаційної безпеки для взаємодії інституцій Європейського Союзу з державними та приватними суб'єктами. Отже кіберпростір було створено.

Важливо зазначити, що в енергетичному секторі як протидію гібридним загрозам Загальний рамковий документ визначає необхідність диверсифікації напрямів та шляхів постачання енергоресурсів до Європейського Союзу, зокрема розріст Південного газового коридору, постачання Каспійський газ і створення хабів зрідженого газу.

Для захисту критичної інфраструктури існує Європейська програма захисту критичного підґрунтя, а Європейське оборонне агентство робить над дефініцією необхідного потенціалу захисту. Щоб протистояти гібридним загрозам у військовому секторі, Європейський Союз обмежився посиленням розвідувальних служб, розвитком відповідних можливостей для захисту критичної інфраструктури та боротьбою з використанням міні-дронів [4].

Задля протиборства з гібридними загрозами Євросоюз співпрацює з іншими країнами та міжнародними будовами – ОБСЄ, ООН та NATO. У Спільній декларації Президента Європейської Ради, Президента Європейської Комісії та Генерального секретаря NATO від липня 2016 року першим завданням було визначено «підвищення спроможності протистояти гібридним загрозам» [8]. Європейський Союз і NATO також розробили серію з 42 пропозицій, десять з яких безпосередньо стосуються противенстві гібридним загрозам.

У межах співробітництва з третіми країнами Європейська Комісія вживає заходів для зміцнення стабільності країн-партнерів, зокрема України, через Інструмент сприяння безпеці та миру. Забезпечення стратегічної комунікаційної підтримки та додаткової підтримки управління кордоном. Окремо, більшість експертів з України (78,4 %) допускають, що тісніша співпраця між Україною та Європейський Союз може підвищити стійкість України до гібридних загроз [9].

У Європейському Союзі протидію гібридним загрозам досі розглядають як комплекс тактичних заходів і не ідентифікують

інтегральний живець таких гібридних загроз, яке вже дійсно грозить безпеці Європи – Російську Федерацію. Проте в Україні, яка вже останні роки намагається протистояти гібридній агресії РФ, не прийнято жодного документа щодо протидії гібридним загрозам. Тому Україна має взяти за зразок подібні документи Європейського Союзу та поглибити співпрацю з Європейським Союзом у цьому плані [10].

Незважаючи на повномасштабну війну Росії проти України, гряда гібридних загроз залишаються актуальними з 2014 року до сьогодні та становлять загрозу дестабілізації та безсилість нашої країни, недодержання фундаментальних прав і свобод, пониження рівня життя та, в факт миролюбного буття громадян України. Для визначення гібридних загроз, чого в Україні ще не робили, використовуються фундаментальні для теорії «безпеки» поняття «ризик», «виклик», «загроза», «небезпека», та «надзвичайна ситуація» – слід диференціювати. Часто деякі з них ототожнюють і вживають як тотожні, що не завжди відписує дійсності. Незважаючи на численні дослідження проблем безпеки в Україні та за кордоном, єдиних, загальноприйнятих визначень наведеного ланцюжка понять не існує.

Тим не менш, можна зробити деякі узагальнення і систематизації і дати визначення системи координат. Ключові концепції ми сформулюємо на основі методології як українських спеціалістів, окремо Горбуліна - Качинського, так і закордонних. Безпека – обставина захисту та збереження стабільного буття та піднесення об'єкта (системи), при якому ймовірність зміни внаслідок зовнішніх або внутрішніх впливів будь-яких параметрів (властивостей) функції мінімальна - близька до нуля.

Англійські співавтори І. Функ і А. Вег-Ноллс атестують безпеку як «обставину свободи від ризиків і загроз». Небезпека й Безпека, які часто сприймаються як протилежності через мовну специфіку української та деяких інших слов’янських мов, насправді протилежностями не є. Адекватно до сприймання Горбуліна - Качинського, рівень безпеки визначається в сегменті від 0 до 1.

Тому можна припустити, що «небезпека» займає проміжне положення в ланцюжку «безпека» – «поклик» – «небезпека» – «погроза» – «катастрофа». Аналізуючи та узагальнюючи визначення ключових категорій безпеки, що існують у вітчизняних та закордонних джерелах, є можливість раціоналізувати ключові визначення.

Так, катастрофа – обставина, протилежна безпеці, що пояснюється докорінною зміною параметрів функціонування об'єкта, що призводить до руйнування і ряду пов'язаних з цим негативних наслідків для навколишнього середовища і людей.

Так, катастрофа – своєрідний верхній термін у ланцюжку «критичне явище» – «надзвичайна обставина» – «катастрофа». Їх можна розглядати як

синоніми машинних систем, але для систем людина-машина соціальні системи можуть утворювати причинно-наслідковий зв'язок. Нижче ланцюжок «критичне явище» – «надзвичайна ситуація» – «лихо» розглядатиметься як синонім до використання узагальненого терміна «надзвичайна ситуація».

Виклик – виражений або висловлена думка суб'єкта вчинити певні дії, які можуть вплинути на стан безпеки об'єкта. Особливістю виклику є його подвійність. Він включає як потенційний ризик у невизначеній формі, так і потенційну можливість набуття об'єктом нової якості через реалізацію наміру суб'єкта. Усвідомлення проблеми є важливим для виготовлення домовленостей для мінімізації вкритих тіньових наслідків і максимізації вкритої доданої оцінки. Ризик постає як виклик і має потенційний (віртуальний) характер до початку практичної діяльності. Як норма, під ризиком розуміють стан настання певної незручної події, яка може завдати збитків і спричинити низку збитків.

Термін risk в давніх видозмінах нинішніх мов означає схожі поняття: італійською risicare – маневрувати між скелями, французькою riscer – порогом, що обходить скелю. Взаємини зі словом «скеля» невипадкова, адже воно сягає корінням в епоху первинного мореплавства у берегових водах, коли спотичка зі скелею означало аварію судна.

Так, ризик – це параметр невизначеності, випадку розвитку об'єкта, який з різним ступенем ймовірності може призводити до постійного виникнення небезпек і небезпек, які, у свою раз, можуть викликати надзвичайну ситуацію з негативними наслідками. Небезпека – стан рівноваги, в якому виявлятимуться події, факти та процеси, які за певних обставин можуть призвести до кількісного зростання ризику, що призведе до його трансформації в загрозу, а за інших обставин – до уникнення такої трансформації.

Так, загроза – це стан, при якому ймовірність неминучості надзвичайної ситуації перевищує ймовірність її ненастання, отже прогресування небезпеки проявляються шкідливі фактори, спосібні викликати шкоду людині, суспільству тощо, впливають на стан і навколишнє середовище та мають інші небажані наслідки [5].

Основними характеристиками ланцюга «Небезпека» – «Ризик» – «Загроза» є: ймовірність настання події, що виражається в тим, що вона вміє відбутися або не відбутися; невизначеність наслідків, невизначеність результатів ризикованої діяльності, мінливість ступеня ризику в порі та під дією інших об'єктивних і суб'єктивних чинників, що знаходяться в динаміці.

Висновки з даного дослідження і перспективи подальших досліджень. Отже, з огляду методології слабкі місця та недоробки в ладі національної безпеки потрібно досліджувати як загрози, які противник рано чи пізно використає для створення загрози чи проектування загрози.

Слабкі сторони (загрози) та гібридні небезпеки безпеці України та братії на нинішньому етапі:

по всій країні:

управлінські:

– політична війна «всі проти всіх» у колі українського істеблішменту, спровокована всевладдям з ціллю узяття виборчої незалежності правлячої політичної групи, стимульована ззовні нападником через внутрішню агентуру;

– низька ефективність ради через її роздробленість на корпоративні сегменти, що підриває парламентсько-президентську модель, яка визначена Основним законом України;

– недостатній рівень професіоналізму державної служби України;

– піар-діяльність влади в Україні замість наочної;

гібридні загрози:

– консервовані й модернізовані з довоєнного періоду контури зовнішнього управління маскуються під громадсько-політичну будову «Український вибір» (Євразійський вибір), комунікаційну протоку для перемовин з агресором у рамках Мінської угоди;

– ловитва на громадян України та вираз фальшивих груп тощо з метою формування репутації України як військової та злочинної країни та виготовлення новітніх засобів тиску на Київ;

– медійна кампанія дискредитації іноземними ЗМІ щодо незаконного надання Україною технологій та ІКТ до країн-ізгоїв і зон конфлікту (ракетних двигунів до КНДР, надання зброї до Південного Судану), щоб представити Україну як агресора міжнародного права і як країна, яка порушує міжнародне право, підтримує сумнівні режими;

– інтегровані дії загального характеру (саботаж критичної інфраструктури + кібератаки + резонансні вбивства + дифамація вищого керівництва держави), спрямовані на підвищення протестного потенціалу громади проти недійової влади;

у військовій сфері:

управлінський:

– корупційна діяльність в оборонному секторі, зокрема в системах економічного, а також матеріально-технічного забезпечення військ;

– недозакінчення виготовлення справжнього порядку територіальної оборони України;

– території, забруднені мінно-вибуховими речовинами та залишками боєприпасів, що не розірвалися, мінно-вибуховими пристроями;

– незадоволених потреб (передбачених нормативами) учасників війни та звільнених військових;

– повільні темпи реформування та розвитку військової будови країни;

гібридні загрози:

– поведінка беззаконних збройних формувань на просторі України, спрямована на дестабілізацію внутрішньої суспільно-політичної ситуації в Україні, зрив роботи органів державної влади та місцевого самоврядування та утримання важливих промислових та інфраструктурних об’єктів;

– виробництво російськими організаціями та розвідкою в Україні легалізованих та законсервованих НЗФ у формі громадських організацій патріотичного спрямування, які чекають створення хаосу в державі та умов для переміни системи управління;

– діяльність воєнізованих груп зловмисника під прикриттям українських військових з метою його дискредитації;

– незаконне поширення (торгівля) зброї, що призводить до безконтрольного помістя зброєю народонаселенням країни та можливості придбання;

– поведінка найманців - громадян України та Росії та інших держав щодо вчинення терористичних і злочинних дій із використанням зброї, розривних речовин;

– загроза окупації військово-контрольованої частки територій України військовими організаціями країни-агресора під виглядом псевдомиротворчої дії;

– планові події щодо пониження ефективності ЗСУ та інакших військових організацій і силових будов;

в інформаційному полі:

управлінський:

– прогалини в законодавстві у галузі інформаційної безпеки, брак пригідних інструментів запобігання практики українських ЗМІ та протилежних речників інформації, які поширюють проросійські наративи чи іншу інформацію протиукраїнського кшталту;

– невисокий рівень злагодженості дій ДБР в інформаційному полі, що дозволяє зловмиснику використовувати інформаційну продукцію української волі в цілях власної популяризації;

– нерозвиненість політики інформаційного забезпечення консолідації національної ідентичності в Україні з метою поведінки з населенням України, насамперед на окупованих територіях;

– недостатнє фінансове та технічне забезпечення органів державної влади України для швидкого та вчасної реакції на підхожі вчинки інформаційного впливу на полі фінансової та технічної прерогативи Росії в інформаційній частині гібридної війни назустріч України;

гібридні загрози:

– незмінне вживання Росією професійних наративів та інформаційних етикеток в офіційній та дипломатичній сферах з метою делегітимізації української влади;

– створення Росією інформаційно-пропагандистських каналів для пониження української влади нормованими групами:

1) обиватели Росії та України на окупованих тернах;

2) обиватели України;

3) держави Заходу, компаньйони України у стримуванні агресії;

4) компанії країн сфери впливу Росії;

– відкритого та прихованого використання демократичних норм і порядків держав Європейського Союзу, а також США та інших країн-партнерів для неформальної дискредитації України та її замахів отримати міжнародну підпору задля протидії російській напади;

– дипломатичні та лобістські механізми на Заході, які використовує Росія задля викликання сумнівів у вірності дії держав Європейського Союзу щодо продовження санкцій проти Росії та легітимізації анексії Криму;

– розширене вживання Росією інформаційних протік зі створенням нових дезінформаційних рівчаків в Україну з ціллю деморалізації жителів та зниження його потенціалу опору агресору;

– використання українських телеканалів та інших ЗМІ для поширення проросійських наративів у розміреній формі або з опозиційними лозунгами;

– більше вживання громадянами України (навіть незважаючи на заборону в Україні) соціальних мереж задля комунікації;

– поширення інформаційної продукції з використанням місцевої, етнонаціональної та інших особливих ідентичностей серед громадян України з метою створення ліній розколу в суспільстві, формування відчування незахищеності, створення соціального підґрунтя для протестів і провокацій;

– формування ізольованої соціокультурної й інформаційної дійсності на окупованих просторах України, ненадання жителям цих територій доступу до української інформаційної сфери;

– вживання українських аналітиків задля формування негативної інформаційної картини українського експертного середовища, делегітимізації вирішальних доказів російської напади;

в кіберзоні:

управлінський:

– низька культура та низький рівень знань державних функціонерів щодо безпеки їх роботи та їх приватного листування та спілкування засобами електронного зв’язку;

– установка інформаційного забезпечення, розробленого заграничними, в тому числі російськими, фірмами і неліцензійного;

гібридні загрози:

– великі кібератаки на центри оборони, предмети стратегічної та напруженої інфраструктури України;

– технічні резерві приховати справжніх злочинців у кіберпросторі;

– вживання програмних наслідків для негласного збору інформації про осіб та спілок на території України;

– несанкційний шлях до власних та службових електронних ящиків українських службовців та чиновників;

в економічному секторі:

управлінський:

– приховане переформатування ключових компаній з метою відновлення старих механізмів економічної залежності України або створення нових;

– обговорення часткою громадян України Російської Федерації як місця заслуг;

гібридні загрози:

– збереження наявності російських фінансових установ в Україні, які подовжують ревізувати велику частку фінансів компаній і громадян;

– контроль ключових економічних активів в Україні, особливо в енергетичному секторі, російськими або проросійськими власниками, що допускає тихий саботаж (диверсії, умовні аварії та простої), а також введення шкодливого програмного забезпечення для подальші кібератаки, знищення стратегічних компаній;

– зовнішньоекономічний вплив на діяльність великих компаній, що створює умови для впливу на великі трудові громади та управління ними;

в енергетиці:

управлінський:

– внутрішній ринок газу, який продовжує на третину залежати від транзиту газу через України;

– незбалансованість ринку вугілля в Україні;

гібридні загрози:

– призупинення Росією поставок газу територією України;

– ухилення від активізації Росії під видом російсько-турецької ділової співпраці щодо реалізації проектів інфраструктурного вирівнювання газотранспортної функції української газотранспортної системи;

у сфері прав людини:

управлінський:

– ігнорування владою проблем кримськотатарського народу, який може бути використаний агресором;

– сприйняття громадянами України Росії - як соціально та релігійно неоднорядного товариства;

гібридні загрози:

– вживання зовнішнім органом питань «заборони привілеїв національних меншостей», «недодержання прав у галузі мовного питання;

– використовування недержавних організацій, активістів та політичних груп для дестабілізації стану під виглядом псевдоаргументів про порушення прав людини та національних меншин;

– підбурювання представників певної релігійної громади до захисту своїх нібито порушених прав та розпалювання міжконфесійної ворожнечі;

у сфері історичної політики:

управлінський:

– низький рівень поінформованості суспільства про справжню історію України;

– збереження пострадянських наративів у книжках історії;

гібридні загрози:

– вживання Росією стратегії об'єднання, що базується на культурній, етнічній та державній єдності України та Росії, як вона нібито існує або до якої прагне в майбутньому, супроводжується політикою реанімації концепції Російської імперії «єдиного трьох руських народів»;

– намагання Росії етнізувати українське суспільство як частину історичного минулого та спротив формуванню сучасної української нації;

– представлення української виключно як «етнічно-української» з одночасним протиставленням її російській, кримськотатарській, грецькій, болгарській тощо.

Виявлені вразливі місця та гібридні загрози дають змогу оцінити спроможність держави забезпечити громадську безпеку та є індикаторами для такої оцінки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Світова гібридна війна: Український фронт. Національний інститут стратегічних досліджень. Київ : НІСД, 2017. 145 с. URL: http://www.niss.gov.ua/articles/2431/

2. Сприяння розбудові можливостей України гарантувати безпеку суспільства в умовах гібридних загроз. результати експертного опитування. URL: https://geostrategy. org.ua/images/%D0%94%D0%BE%D1%81%D0%BB%D1%96%D0%B4%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F_%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%81%D1%8C%D0%BA%D0%BE%D1%8E.pdf

3. The Role of the Black Sea in Russia's Strategic Calculus. Byron Chong. CIMSEC. URL: http://cimsec.org/role-black-sea-russias-strategic-calculus/31805

4. Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats – a European Union response. European Commission. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

5. Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats – a European Union response. EU Council URL: http://data.consilium.europa.eu/doc/document/ST-11539-2017-INIT/en/pdf

6. Countering hybrid threats: EU-NATO cooperation. Briefing. European Parliamentary Research Service. URL: http://www.europarl.europa.eu/RegData/etudes/ BRIE/2017/599315/ EPRS_BRI(2017)599315_EN.pdf

7. European Centre of Excellence for Countering Hybrid Threats established in Helsinki. Finish Government. URL: http://valtioneuvosto.fi/en/article/-/ asset_publisher/10616/ eurooppalainen-hybridiuhkien-osaamiskeskus-perustettiin-helsinkiin

8. Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. NATO. URL: http://www.nato.int/cps/en/natohq/official_texts_133163.htm

9. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)). URL: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2016-0441+0+DOC+PDF+V0//EN

Стаття надійшла до редакції 13.10.2023 р.
Стаття рекомендована до друку 23.11.2023 р.

Karamyshev D. V.,
Doctor of Public Administration,
Full Professor of the Public Policy Department,
Educational and Scientific Institute «Institute of Public Administration»,
V. N. Karazin Kharkiv National University,
4, Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: dvk1vip@gmail.com https://orcid.org/0000-0003-1617-3240

Sobol R. G.,
PhD in Public Administration,
Associate Professor of the Public Policy Department,
Educational and Scientific Institute «Institute of Public Administration»,
V. N. Karazin Kharkiv National University,
4, Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: sobol_roma@ukr.net https://orcid.org/0000-0002-3176-3807

Myrna N. V.,
PhD in Public Administration,
Associate Professor of Law, National Security and European Integration chair Department,
Educational and Scientific Institute «Institute of Public Administration»,
V. N. Karazin Kharkiv National University,
4, Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: mail4myrna@gmail.com https://orcid.org/0000-0003-3351-5572

Yevdokymov V. O.,
PhD in Economics,
Associate Professor of Public Administration and Civil Service Department,
Educational and Scientific Institute «Institute of Public Administration»,
V. N. Karazin Kharkiv National University,
4, Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: v.ievdokymov@karazin.ua https://orcid.org/0000-0003-0620-4939

THE INFLUENCE OF HYBRID THREATS ON THE MODERN NATIONAL SECURITY OF UKRAINE

Annotation. The article reviews the current state of the impact of hybrid threats on modern national security in Ukraine. The concept of "hybrid threats" and important countermeasures are clearly identified. Weak points (dangers) and hybrid threats to the security of Ukraine and society at the current stage are highlighted.

Key words: hybrid threats, national security, management process organization, regulatory policy, economic security, energy security.

REFERANCES

1. Svitova hibrydna viina: Ukrainskyi front. (2017). Natsionalnyi instytut stratehichnykh doslidzhen. Kyiv: NISD. URL: http://www.niss.gov.ua/articles/2431/ [in Ukrainian].
2. Spryiannia rozbudovi mozhlyvostei Ukrainy harantuvaty bezpeku suspilstva v umovakh hibrydnykh zahroz. rezultaty ekspertnoho opytuvannia. URL: https://geostrategy. org.ua/ images/%D0%94%D0%BE%D1%81%D0%BB%D1%96%D0%B4%D0%B6%D0%B5%D0%BD %D0%BD%D1%8F_%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%81%D1% 8C%D0%BA%D0%BE%D1%8E.pdf [in Ukrainian].

3. The Role of the Black Sea in Russia's Strategic Calculus. Byron Chong. CIMSEC. URL: http://cimsec.org/role-black-sea-russias-strategic-calculus/31805

4. Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats – a European Union response. European Commission. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

5. Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats – a European Union response. EU Council URL: http://data.consilium.europa.eu/doc/document/ST-11539-2017-INIT/en/pdf

6. Countering hybrid threats: EU-NATO cooperation. Briefing. European Parliamentary Research Service. URL: http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf

7. European Centre of Excellence for Countering Hybrid Threats established in Helsinki. Finish Government. URL: http://valtioneuvosto.fi/en/article/-/asset_publisher/10616/eurooppalainen-hybridiuhkien-osaamiskeskus-perustettiin-helsinkiin

8. Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. NATO. URL: http://www.nato.int/cps/en/natohq/official_texts_133163.htm

9. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)). URL: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2016-0441+0+DOC+PDF+V0//EN

The article was received by the editors 13.10.2023.
The article is recommended for printing 23.11.2023.