Грановський Микола Володимирович,
аспірант кафедри політології та філософії,
Харківський регіональний інститут державного управління
Національної академії державного управління при Президентові України,
м. Харків
ORCID 0000-0002-8554-7456

УДК 35-355.01 **doi: 10.34213/ap.20.02.24**

АНАЛІЗ ГІБРИДНИХ ОПЕРАЦІЙ ТА УПРАВЛІНСЬКІ РІШЕННЯ ЩОДО ПРОТИДІЇ ТАКИМ З'ЯВИЩАМ – ІНОЗЕМНИЙ ДОСВІД

У сучасному світі спостерігається тенденція до значного зростання кількості гібридних конфліктів, які стають все більш витонченими й непередбачуваними. Стаття присвячена теоретичним і практичним аспектам таких з'явищ, як гібридна війна, гібридний конфлікт або агресія, що впливають на безпеку міжнародного середовища, а також діям органів державної влади щодо протидії таким загрозам, зокрема, у країнах ЄС. Під час аналізу зазначеного питання було здійснено спробу надати відповідь на такі запитання: "У чому виражається суть гібридних дій? Як відбувається їх еволюція? Який є характер сьогоднішньої гібридної агресії?" Аргументи, викладені у статті, підтверджують необхідність подальшого проведення досліджень гібридних дій, які порушили цілісність державних кордонів багатьох країн, у тому числі й України, та продовжують становити реальну загрозу безпеці в Європі та світі. Сучасна практика гібридних операцій з боку агресора демонструє кардинальну зміну тактики та засобів, які використовує держава-гравець світового рівня проти супротивника, який є слабким і нездатним захищати цілісність власної території.

Ключові слова: безпека; гібридна війна; гібридний конфлікт; гібридні дії; гібридні операції; тероризм.

Постановка проблеми. Початок XXI ст. характеризується новими викликами у сфері міжнародної безпеки. Вважається, що припинення "холодної війни" не ліквідувало внутрішніх або регіональних джерел конфліктів і не забезпечило стабільного мирного співіснування країн у світі. На думку експертів, міжнародне співтовариство стикається не стільки з прямим збройним конфліктом, скільки з одним із різновидів військових операцій, які можна також назвати гібридними. На жаль, такі з'явища, як збройні повстання, партизанські та внутрішні війни, а також інші дрібні конфлікти незабаром стануть звичними типами конфліктів у новому світовому порядку. Тому, можна припустити, що найближчим часом різні держави будуть залучені, прямо чи опосередковано, до нових збройних конфліктів [18].

Аналіз останніх досліджень і публікацій. Дослідженню трансформацій форм та характеру війн і воєнно-політичних конфліктів нового покоління ("гібридних війн") присвячено доробки зарубіжних учених Я. Берзніса, Р. Глена, Ф. Гоффмана, Дж. Калха, Ф. Ван Каппена, М. Кревельда, Т. Мак Куєна, У. Лінда, Дж. Метіса, У. Немета, Е. Тоффлера, Т. Хубера та ін. Широке застосування способів та методів воєнно-політичних конфліктів гібридного типу для вирішення міждержавних проблем на сучасному етапі спонукали також вітчизняних науковців до поглибленого їхнього аналізу. Так, останнім часом дослідженню питань "гібридної війни" присвячені роботи В. Горбуліна, Ю. Климчука, Г. Луцишини, Є. Магди, Б. Парахонського, Г. Перепелиці, Г. Ситника, А. Слюсаренка, Л. Смоли, М. Требіна, Г. Яворської та ін.

В арміях багатьох країн світу аналіз та дослідження досвіду, накопиченого як в невеликих локальних конфліктах у минулому, так і в рамках багатонаціональних операцій на початку XXI ст., проводяться вже на стратегічному рівні [17].

Основною проблемою є нездатність подолати стагнацію, в якій опинилося сучасне військове мистецтво через зростаючу складність конфліктів та методів їх вирішення [13]. Точне прогнозування майбутнього, особливо збройних конфліктів, надзвичайно важке через динаміку дій, що розвиваються, та непередбачуваність реакцій з боку сторін конфлікту. Це відповідає давній сентенції, згідно з якою "...війна сповнена пристрастей, недостовірної інформації та помилок в оцінці, і нарешті, багато чого в ній трапляється випадково" [12]. Однак, виходячи з існуючих тенденцій, можна сформулювати тезу про те, що в сучасному світі зросте кількість місць, де можуть відбуватися збройні конфлікти, зросте загроза безпеці та інтересам, у тому числі, країн Північноатлантичного альянсу та держав, які прагнуть до нього вступити. Вказані аргументи додатково підтверджують необхідність проведення ще більш поглиблених досліджень гібридної діяльності, яка, використовуючись державними чи недержавними структурами, становить реальну загрозу безпеці в Європі та світі.

Метою статті є проведення аналізу гібридних з'явищ та досвіду протидії іноземних держав гібридним агресіям, у тому числі через прийняття відповідних рішень органами державного управління, з невизначеним ворогом, який вказує, що об'єкти гібридних операційне мали можливості використовувати стандартні тактики, а парадигму безпеки, яка була заснована на традиційних військових технологіях державних систем оборони та методах ведення військових операцій, було повністю підірвано [13].

Виклад основного матеріалу. Етимологія терміна "гібридизація" походить від латинського слова "hybrida" – перемішування – помісь, комбінація двох або більше різних об'єктів або характеристик, властивостей в одному об'єкті [2].

На даний момент сучасне міжнародне середовище стикається з новим викликом, який полягає у протидії загрозі, що може виникнути внаслідок можливого гібридного конфлікту.

Під гібридизацією можна розуміти співіснування елементів "старих" і "нових" воєн, класичних збройних конфліктів та "постмодерних" воєн, зіткнень національних армій та асиметричних конфліктів, військових супертехнологій та примітивних озброєнь, боротьби за території та ресурси, а також суперечки про ідентичність та цінності, протистояння східної цивілізації цивілізацією Заходу [13].

На думку Т. Хубера – автора концепції війни як складного продукту, використання підрозділів збройних сил та розпорошених нерегулярних сил у бойових операціях не буде ефективним без централізованого, орієнтованого на мережу управління військовими операціями та належного визнання простору військової конфронтації [8]. Всебічне визначення гібридної діяльності повинно максимально врахувати весь досвід цього типу операцій за останні десятиліття. Спрощена заява про те, що гібридна війна – це "партизанська війна + сучасні технології", є лише частиною правди і може стосуватися лише недержавних суб'єктів. Подібна діяльність з боку такого суб'єкта, як держава, набагато ширша. Спектр методів, що використовуються агресором, може варіюватися від традиційного ведення збройної війни, із застосуванням нетрадиційної зброї, кібернетичної зброї та інформаційної війни, до діяльності спеціальних служб, в яких зберігається розпад суспільств, через активацію агентства впливу [11], а також тероризму або підтримки та використання кримінальних дій. Вся діяльність підпорядковується вищій політичній меті даної держави-агресора.

Латвійський аналітик Я. Берзніс називає гібридну війну війною четвертого покоління. Однак, на думку деяких військових експертів, зокрема російських, гібридну агресію можна називати "війною нового покоління", правила ведення якої принципово змінилися. Зросла роль невійськових засобів (економічних, культурних) для досягнення політичних і стратегічних цілей. Такі заходи значно ефективніші за класичні військові методи Під час гібридних операцій "…широко застосовуються асиметричні дії, що дозволяють усунути навіть перевагу противника під час збройних зіткнень. Так, для створення постійного фронту на всій території ворожої держави використовуються формування спеціального призначення, потенціал внутрішньої опозиції, інформаційний вплив, а також постійно мінливі форми та методи впливу". У підході до гібридних конфліктів немає різниці між війною та миром у класичному розумінні цих термінів, а також між військовослужбовцями та таємною діяльністю, що у значній мірі відрізняється від того, на чому традиційно зосереджувались теоретики війни. Важливим елементом у "війні нового покоління", є стирання різниць між рівнями дій: стратегічним, оперативним та тактичним і між наступальними та захисними діями. Безконтактність, дистанційність, вплив на противника стає основним засобом досягнення цілей бою та операцій. Гібридна війна може перетворити повністю стабільну країну на арену найбільш інтенсивного збройного конфлікту за кілька місяців або навіть днів!" [14; 13].

У свою чергу в документі НАТО від 25 серпня 2010 р. "Bi-Sc Input To New Nato Capstone Concept for the Military Contribution to Counter Hybrid Threats" можна знайти оцінку гібридних загроз глобальній безпеці у XXI ст. Дослідження НАТО вказує, що майбутній потенційний супротивник буде поєднувати різні моделі війни і одночасно використовувати комбінацію звичайної, нерегулярної, терористичної та злочинної діяльності, що називається гібридною війною або гібридною загрозою. Було визначено, що змістом цієї діяльності буде поєднання звичайних можливостей з тактикою нерегулярних збройних сил, а також терористичної та злочинної діяльності [7]. Суть злочинної діяльності у цьому випадку полягатиме у дестабілізації функціонування місцевої влади та підтримці повстанців та всіх опозиціонерів шляхом постачання технологічно вдосконаленої зброї, боєприпасів та фінансових ресурсів. Злочинні угруповання, які функціонують як ієрархічна структура в урбанізованому середовищі, становитимуть як основу, так і підтримку широко зрозумілої гібридної діяльності, включаючи наркотерроризм. Передбачається, що противник, щоб отримати перевагу, буде використовувати всі вищезазначені бойові моделі одночасно, а також високотехнологічні системи та використовувати їх конкретними способами для досягнення власних цілей.

Результати аналізу досвіду проведених гібридних операцій вказують на те, що в майбутньому оперативному середовищі домінуватиме гібридна форма дій, спрямованих на найбільш вразливі пункти збройних сил держав, що беруть участь у конфлікті, або на критичну інфраструктуру держави-учасниці конфлікту. Слід очікувати, що потенційний супротивник використовуватиме всі можливі форми та методи військових операцій, а також різні тактики. Можна припустити, що у разі конфлікту та втручання, ворог змішається з місцевою громадою і віддасть перевагу довготривалим, повстанським та партизанським діям, включаючи можливе використання саморобних вибухових речовин та ракетного вогню. Крім того, ця діяльність може включати використання високотехнологічних систем озброєння з одночасним проведенням

класичної терористичної діяльності та діяльності в кібернетичному просторі, спрямованої на протидію як системам озброєнь, так і системам цивільної критичної інфраструктури. Це призведе до руйнівного впливу на функціонування держави.

На підставі результатів проведеного дослідження можна зробити висновок, що традиційні доктринальні зразки військових операцій втратили свою актуальність та не можуть продемонструвати свою ефективність у конфронтації з гібридним опонентом.

Прикладом, що ілюструє повний спектр методів та форм гібридної війни, коли слабший противник використовує їх проти сильнішого, може бути тривалий конфлікт між Ізраїлем та "Хізболлою". На підставі досвіду Ізраїлю за останнє десятиліття можна стверджувати, що нерегулярні засоби, якими користуються недержавні суб'єкти, трансформуються в гібридні дії, якими користуються держави. Майбутні виклики будуть пов'язані з тим, що потенційний опонент матиме набагато більш широкий спектр організаційних структур і використовуватиме більш складну стратегію і тактику, ніж та, з якою зіткнулася ізраїльська армія в 2006 р. "Хізболла" чітко продемонструвала, що недержавні суб'єкти здатні зробити достовірну оцінку стратегічних можливостей армій, відомих як Західна, та успішно протистояти їх найсучаснішим можливостям. Підсумовуючи, можна констатувати, що безперервний конфлікт Ізраїлю зі своїм недержавним ворогом свідчить про масштаби розвідувальних, військових та інформаційних зусиль ізраїльської армії та спецслужб для створення умов для нейтралізації та ліквідації терористичної організації.

Завдяки підтримці з боку Ірану та вкоріненню його в Лівані, "Хезболла" стала небезпечною загрозою не тільки для Ізраїлю, але і для регіону Близького Сходу. Перемога "Хезболли" над ізраїльською армією у 2006 р. продемонструвала ефективність цієї організації та рівень її загрози сусіднім державам у 2006 р. Питання подальшого розвитку цієї організації, безумовно, є відкритим і не може залишатися без уваги [3].

Досвід, отриманий у результаті операцій в Ірані та Афганістані, а також і внаслідок української кризи, показує, що держави можуть перетворювати регулярні підрозділи збройних сил у нерегулярні формування, які матимуть можливість адаптувати нову тактику, а потім підтримувати регулярні підрозділи.

Таким чином, держави не можуть сприйматися через призму наявності лише класичних збройних сил, а недержавні суб'єкти можуть асоціюватися лише з нерегулярною діяльністю, оскільки в майбутньому гібридні збройні сили можуть використовуватися непередбачувано.

Типовим прикладом того, як потужна держава веде гібридну війну зі слабшим противником, є конфлікт на Сході Україні, який можна розділити чотири етапи: політична диверсія, формування соціальної та політичної позиції сепаратистів, військове втручання та стримування, демонструючи потенціал нетрадиційних сил. Характерним для цього конфлікту є те, що вищезазначене етапи часто перекриваються і мають різну інтенсивність. Незважаючи на чіткі ознаки участі регулярних збройних сил, російська сторона офіційно заперечує участь у конфлікті. Експерти НАТО стверджують, що кризова ситуація виходить далеко за межі України. Росія вважає, що захист етнічних росіян не є відповідальністю країн, в яких вони проживають, і не підпорядковується їхнім законам, уряду чи конституції, але підпадає під РФ [15].

На думку К. Волкера – колишнього Спеціального представника Державного департаменту США з питань України (2017–2019), такий підхід російської влади до етнічних росіян, який, вже застосовувався раніше, наприклад, в Естонії у 2007 р., в Грузії у 2008 р. через проведення повільних, але систематичних дій,спрямованих на порушення суверенітету. Це було частиною стратегічного ландшафту, який був добре відомий Росії. Іноді це передбачає більш відкриті та очевидні кроки, іноді ці кроки є більш тонкими, це боротьба за допомогою економіки, іноді це кібератаки, що проводяться під виглядом незалежних активістів". "…Такий набір тактик гібридної війни застосовується Росією щонайменше 5–6 років".

Є багато передумов для висновку, що російсько-український конфлікт, нажаль, все ще перебуває на стадії розвитку. Час, що минув з початку російської агресії проти України, дозволив як європейським аналітикам та аналітикам НАТО опрацювати сценарії та методи гібридної війни, яку веде Росія. Елементом, який її ініціював, стала діяльність у сфері інформаційної війни. Аналізуючи сценарій російської агресії в Україні, можна поставити під сумнів тезу про те, що російська агресія розпочалася з протестів на Майдані. Багато вказує на те, що насправді російська атака почалася задовго до того, як президент В. Янукович залишив країну [4]. Військовій участі в конфлікті, де російські десантники з'явилися в Криму та на Донбасі фактично без ідентифікації, передував інформаційний наступ. За роки до конфлікту російська сторона розпочала експансію ЗМІ в Україні. Зброєю, яка була використана для дестабілізації інформаційної структури українських ЗМІ, виявилися російські медіа-компанії, за допомогою яких здійснювалось узгоджене інформаційне проникнення в Україну. Розширення було здійснено шляхом придбання акцій у ЗМІ у українських олігархів. Таким чином, українське суспільство почало отримувати інформацію, яка висвітлює ситуацію з точки зору інтересів Росії, а не України. Відбувалася маніпуляція ЗМІ суспільством. Створене таким чином підґрунтя перекривалося інтеграцією проросійських кіл та активізацією російських агентів впливу.

Можна виділити кілька ключових методів нападу та основні цілі втручання. По-перше, дезінформація. Участь солдатів супротивника маскується формуванням добровільних сепаратистських сил. Концентрація військ країни-агресора, перекинутих в Україну, відбувалася під приводом навчань у прикордонних регіонах. Хоча цей метод можна класифікувати як традиційний, його застосовували у війні з Грузією, він був новинкою у підготовці до війни в кіберпросторі. На початку агресії в мережі Інтернет з'явилися сотні сторінок та сайти соціальних мереж. Здавалося б, "незалежне та об'єктивне інформування" про події, але насправді взаємопов'язане та координуюче активні дії з дезінформації. Метою інформаційних атак є популяризація негативних явищ у суспільстві та урядовій еліті країни, виступаючої об'єктом агресії. Такі явища, як широко розповсюджена корупція, потужний націоналізм, і розриви між таборами влади президента та прем'єр-міністра виступили основними об'єктами нападів інформаційної війни. Інформаційна війна проти України супроводжується подібними діями з боку агресора в Європі та світі. Проводиться інтенсивна інформаційна кампанія, спрямована на посилення розколів у Європейському Союзі та НАТО щодо необхідності та обсягу допомоги Україні та законності санкцій проти неї. Для цього використовуються як міжособистісні контакти із західними політиками, економічні стимули та вплив ЗМІ. Інформаційний простір представляє та наголошує на російській версії подій, і загальною метою, схоже, є поділ громадської думки.

Україна програє інформаційну війну. Українські інституції протидії ще перебувають у початковій фазі свого створення. Ситуація додатково ускладнюється тим, що система безпеки та міжнародне право не передбачає такої сфери військової діяльності. Ні Статут ООН, ні установчі документи ОБСЄ не визначають ні поняття інформаційної війни, ні методи моніторингу, а також забороняють її ведення. Міжнародне право безпорадне перед російською агресією, про що свідчить відсутність реакції місії ОБСЄ на українські докази щодо російської дезінформаційної діяльності або навіть участь регулярних підрозділів російської армії у конфлікті. Міжнародні спостерігачі також обмежені у своїх діях [1].

Крім зазначеного, агресором використовують гуманітарні конвої в якості одного з елементів камуфльованого переозброєння сепаратистських сил. Спостерігається кореляція між гуманітарними конвоями та збільшенням інтенсивності військових операцій сепаратистів [6].

Через проведений аналіз можна зробити висновок, що Російська Федерація може використовувати "український успіх" як шаблон для подальшого використання. Зрозуміло, що ризикує не тільки Україна, але й кожна країна, населена російською меншиною. Методи, використані під час гібридної війни в Україні, можуть бути перенесені в інші регіони, включаючи країни Балтії. Можна припустити, що основною та ефективною дією для припинення агресивних тенденцій Росії є єдність західних держав та підтримка України критично важливими військовими можливостями. Досвід нещодавніх конфліктів, де елементи гібридних операцій широко використовуються, показує, що потенціал недержавних суб'єктів, особливо впливати у військовій сфері, постійно зростає.

Потужність держави-агресора в поєднанні з елементами гібридної війни доводить слабкість, в якій опинилися міжнародні інститути безпеки, і доведені до цього часу міжнародні угоди були поставлені під сумнів. Хоча в теоретичному плані більшість експертів дотримуються думки, що неспроможність зупинити агресивні дії проти України на сучасному етапі призведе до зростаючої загрози дестабілізації всього регіону Центральної та Східної Європи.

Що стосується міжнародного досвіду, то в ЄС майже п'ять років тому розпочала роботу оперативна робоча група зі стратегічних комунікацій Європейського Союзу – East StratCom Task Force, діяльність якої спрямовано на:

– роз'яснення ключових аспектів політики Європейського Союзу, створення його позитивного іміджу та протидія дезінформації;

– ефективну комунікацію та просування політики ЄС щодо Східного партнерства;

– загальний розвиток медійного простору в країнах Східного партнерства та країнах-членах ЄС, що передбачає сприяння свободі ЗМІ;

– вдосконалення механізмів, що уможливлюють передбачення, оцінку та реагування ЄС на дезінформацію, яка поширюється зовнішніми акторами [9];

– надання інформаційної підтримки делегаціям ЄС в Азербайджані, Вірменії, Білорусі, Грузії, Молдові, Україні;

– оперативна група випускає щотижневий Огляд дезінформації на сайті https://euvsdisinfo.eu.

А з вересня 2017 р. у м. Гельсінкі (Фінляндія) функціонує Європейський центр протидії гібридним загрозам (The European Centre of Excellence for Countering Hybrid Threats) (далі – Центр).

Рішення щодо створення Центру було прийнято представниками країн НАТО та ЄС, а його засновниками виступили 12 країн: Фінляндія, Швеція, Норвегія, США, Франція, ФРН, Великобританія, Іспанія, Польща, Естонія, Латвія і Литва. Початковий річний бюджет Центру склав близько 1,5 млн євро.

Метою зазначеної структури є протидія "новим загрозам, спрямованим на дестабілізацію", проведення досліджень, аналіз гібридних загроз та методів боротьби з ними, організація спільного навчання для країн-учасниць, а також організація і проведення консультацій на стратегічному рівні між учасниками ЄС та НАТО, із залученням до діалогу урядових та неурядових експертів.

Практичним проявом діяльності НАТО у сфері стратегічних комунікацій стало відкриття Центру передового досвіду з питань стратегічних комунікацій НАТО (The NATO Strategic Communications Centre of Excellence), що отримав статус міжнародної організації (Латвія, 2014). Зокрема, центр був створений сімома країнами-партнерами, серед яких Латвія, Литва, Естонія, ФРН, Польща, Сполучене Королівство та Італія.

Головна місія центру полягає в підтримці процесу розвитку потенціалу НАТО, посиленні ефективності місій та їх функціональної складової через забезпечення повної і своєчасної експертизи стратегічних комунікацій. З огляду на те, що метою центру стало поліпшення стратегічних комунікаційних можливостей НАТО за допомогою проведення досліджень і аналізу, розробки концепцій, досліджень, а також освітньої і професійної підготовки. Центр працює як дослідницька установа, яка здійснює науково-аналітичну, навчально-методичну та інформаційно-комунікативну діяльність, а також проводить тестування науково-практичних підходів.

До діяльності центру залучено міжнародних експертів з різних сфер стратегічних комунікацій, в тому числі публічної дипломатії, зв'язків з громадськістю, військових зв'язків з громадськістю, інформаційних операцій і психологічних операцій, а також фахівців із суміжних сфер для проведення семінарів і конференцій,організованих під управлінням центру. Розвиток спроможності НАТО у сфері стратегічних комунікацій є метою діяльності Центру передового досвіду з питань стратегічних комунікацій.

На базі вказаного центру розроблено низку спеціальних навчальних курсів зі стратегічних комунікацій, видається журнал "Стратегічні комунікації у сфері оборони" (Defence Strategic Communications); здійснюються дослідження; проводяться конференції та семінари на теми: роль пропаганди в сучасному світі, російська інформаційна війна проти України, маніпулятивні техніки, перетворення соціальних медіа на зброю, практика НАТО щодо стратегічних комунікацій тощо [10].

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. На підставі проведеного дослідження можна зробити висновок, що еволюція гібридної діяльності, особливо за останнє десятиліття, була дуже динамічною і підтвердила ефективність досягнення стійкої переваги над суперником. Сучасні гібридні операції проводяться з поєднанням в застосуванні конвенційної зброї, партизанської війни, тероризму та злочинної поведінки з метою досягнення певних політичних цілей, основним інструментом якої є створення державою-агресором в державі, обраній для агресії, внутрішніх протиріч та конфліктів з подальшим їх використанням для досягнення політичних цілей агресії, які досягаються звичайною війною.

Досвід, отриманий в результаті операцій в Іраку та Афганістані, і перш за все, збройного конфлікту в Україні, показує, що саме держави можуть транс-

формувати регулярні підрозділи збройних сил у нерегулярні формування, які матимуть класичні можливості, та адаптувати нетрадиційні методи операцій, а потім підтримуватимуть регулярні підрозділи. Збройний конфлікт також продемонстрував не лише слабкість української сторони, а й неефективність організацій, відповідальних за забезпечення міжнародної безпеки: НАТО, ОБСЄ та ООН.

Подальша ескалація гібридної діяльності в Україні, безсумнівно, загрожує державам Північноатлантичного альянсу. Методи, що використовуються агресором у гібридній війні в Україні, можуть бути перенесені не лише на території країн-колишніх республік Радянського Союзу, але і в країни Балтії, Польщу та Румунію. Кризисна ситуація в Україні повністю змінила ситуацію з безпекою в регіоні Центральної та Східної Європи. Затяжний конфлікт матиме наслідки, виражені у зниженні рівня міжнародної безпеки, а врахування уроків "гібридних війн" однозначно сприятиме розбудові та посиленню секторів безпеки і оборони як окремих країн, так і коаліцій країн в умовах проведення "війн нового покоління".

А подальше тривання гібридного конфлікту на Сході нашої країни вимагає від України активних дій та ефективних управлінських у сфері запобігання та протидії гібридним загрозам. Треба чітко розуміти, що затягування у часі вирішення конфлікту безумовно призведе його до стану "замороженого", що майже автоматично, кажучи літературною мовою, "ставить хрест" на європейських та євроатлантичних перспективах України на невизначений термін.

Список використаних джерел

1. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства : Аналітичний документ. Київ, 2018. URL: https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok_XXI-end_0202.pdf (дата звернення: 03.02.2020).

2. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Гібрид_(значення) (дата звернення: 03.02.2020).

3. Оборонно-промисловий кур'єр : Інформаційне агентство. URL: http://opk.com.ua/як-заповідав-сун-цзи/ (дата звернення: 03.02.2020).

4. Артюх В. Туман гібридної війни: чому шкідливо мислити гібридно. URL: https://commons.com.ua/uk/tuman-gibridnoyi-vijni-chomu-shkidlivo-misliti-gibridno/ (дата звернення: 03.02.2020).

5. Війна нового покоління. *Українська літературна газета*. 15.10.2018. URL: https://litgazeta.com.ua/articles/vijna-novogo-pokolinnya/ (дата звернення: 03.02.2020).

6. Укрінформ. URL: https://www.ukrinform.ua/rubric-ato/2818620-es-pro-rosijski-gumkonvoi-l udi-strazdaut-vid-rozpocatogo-rosieu-konfliktu.html (дата звернення: 03.02.2020).

7. Bi-sc input to a new nato capstone concept for the Military contribution to countering hybrid threats. URL: https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf (дата звернення: 03.02.2020).

8. Huber T. M. Compound Warfare: That Fatal Knot. URL: https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/compound_warfare.pdf (дата звернення: 03.02.2020).

9. EEAS homepage: Questions and Answers about the East Strat Com Task Force. URL: https://goo.gl/aJS2xk (дата звернення: 03.02.2020).

10. European Centre of Excellence for Countering Hybrid Threats. URL: https://www.hybridcoe.fi (дата звернення: 03.02.2020).

11. Kuk A. I. Kanwa wywiadu agenturalnego. Warszawa, 1994. C. 19. URL: https://szpiegul.pl/blog/o-kanwie-wywiadu-agenturalnego/ (дата звернення: 03.02.2020).

12. Jaskólski Michał. Kilka uwag o wojnie. URL: https://core.ac.uk/download/pdf/229244246.pdf (дата звернення: 03.02.2020).

13. Strona internetowa Biura Bezpieczenstwa Narodowego RP. URL: https://www.bbn.gov.pl/pl/prace-biura/publikacje/inne-wydawnictwa/3545,Biblioteka-BN-Asymetria-i-hybrydowosc-stare-armie-wobec-nowych-konfliktow.html (дата звернення: 03.02.2020).

14. Berzinš J. The New Generation of Russian Warfare. URL: https://www.aspen.review/article/2017/the-new-generation-of-russian-warfare/ (дата звернення: 03.02.2020).

15. The Russian Military Forum: Russia's Hybrid War Campaign: Implications for Ukraine and Beyond. URL: https://www.csis.org/events/russian-military-forum-russias-hybrid-war-campaign-implications-ukraine-and-beyond (дата звернення: 03.02.2020).

16. Wrzosek M. Zagrożenia militarne a bezpieczeństwo Europy.

URL: https://zbrojni.blob.core.windows.net/pzdata/TinyMceFiles/kwartalnik_bellona4_2012.pdf (дата звернення: 03.02.2020).

17. Zeszyty Naukowe Akademii Obrony Narodowej nr 2 (99). 2015. ISSN 2299-6753. URL: https://depot.ceon.pl/bitstream/handle/123456789/9904/Banasik,%20Parafianowicz.pdf?sequence=1&isAllowed=y (дата звернення: 03.02.2020).

Hranovskyi M. V.,
Postgraduate Student of Political Science and Philosophy Department,
KRI NAPA, Kharkiv
ORCID 0000-0002-8554-7456

ANALYSIS OF HYBRID OPERATIONS AND MANAGEMENT DECISIONS TO COUNTER SUCH PHENOMENA IS FOREIGN EXPERIENCE

The beginning of the XXI century is characterized by new challenges in the field of international security. It is believed that the end of the Cold War did not eliminate domestic or regional sources of conflict and did not ensure the stable peaceful coexistence of countries in the world. According to experts, the international community is facing not so much a direct armed conflict, but one of the types of military operations, which can also be called hybrid. In today's world there is a tendency to significantly in crease the number of hybrid conflicts, which are becoming more sophisticated and unpredictable.

The article is devoted to theoretical and practical aspects of such phenomena as hybrid war, hybrid conflict or aggression, which affect the security of the international environment, as well as the actions of public authorities to counter such threats, in particular in the EU.

During the analysis of this question, an attempt was made to answer the following questions: "What is the essence of hybrid actions? How is their evolution? What is the nature of today's hybrid aggression?".

The arguments presented in the material confirm the need for further research into hybrid actions that have violated the integrity of the state borders of many countries, including Ukraine, and continue to pose a real threat to security in Europe and the world.

The current practice of hybrid operations on the part of the aggressor demonstrates a radical change in the tactics and means used by the world-class player state against the enemy, who is weak and unable to defend the integrity of its own territory.

The power of the aggressor state, combined with the elements of a hybrid war, proves the weakness of international security institutions, and the international agreements that have been proven of have been called in to question. Although in the most experts believe that the failure to stop the conflict in eastern Ukraine at the present stage will lead to a growing threat of destabilization of the entire region of Central and Eastern Europe.

Keywords: security; hybrid war; hybrid conflict; hybrid actions; hybrid operations; terrorism.

References

1. Hibrydni zahrozy Ukraini i suspilna bezpeka. Dosvid EU i Skhidnoho partnerstva: Analitychnyi dokument. (2018). Kyiv URL: https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok_XXI-end_0202.pdf [in Ukrainian].

2. Vikipediia. URL: https://uk.wikipedia.org/wiki/Hibryd_(znachennia) [in Ukrainian].

3. Oboronno-promyslovyi kurier: Informatsiine ahentstvo. URL: http://opk.com.ua/iak-zapovidav-sun-tszy/ [in Ukrainian].

4. Artiukh, V. Tuman hibrydnoi viiny: chomu shkidlyvo myslyty hibrydno. URL: https://commons.com.ua/uk/tuman-gibridnoyi-vijni-chomu-shkidlivo-misliti-gibridno/ ([in Ukrainian].

5. Viina novoho pokolinnia. Ukrainska literaturna hazeta. (15.10.2018). URL: https://litgazeta.com.ua/articles/vijna-novogo-pokolinnya/ [in Ukrainian].

6. Ukrinform. URL: https://www.ukrinform.ua/rubric-ato/2818620-es-pro-rosijski-gumkonvoi-ludi-strazdaut-vid-rozpocatogo-rosieu-konfliktu.html [in Ukrainian].

7. Bi-sc input to a new nato capstone concept for the Military contribution to countering hybrid threats. URL: https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf.

8. Huber, T.M. Compound Warfare: That Fatal Knot. URL: https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/compound_warfare.pdf.

9. EEAS homepage: Questions and Answers about the East Strat Com Task Force. URL: https://goo.gl/aJS2xk.

10. European Centre of Excellence for Countering Hybrid Threats. URL: https://www.hybridcoe.fi.

11. Kuk, A.I. (1994). Kanwa wywiadu agenturalnego. Warszawa, *19*. URL: https://szpiegul.pl/blog/o-kanwie-wywiadu-agenturalnego/ [in Polish].

12. Jaskólski, Michał. Kilka uwag o wojnie. URL: https://core.ac.uk/download/pdf/229244246.pdf [in Polish].

13. Strona internetowa Biura Bezpieczenstwa Narodowego RP. URL: https://www.bbn.gov.pl/pl/prace-biura/publikacje/inne-wydawnictwa/3545,Biblioteka-BN-Asymetria-i-hybrydowosc-stare-armie-wobec-nowych-konfliktow.html [in Polish].

14. Berzinš, J. (2017). The New Generation of Russian Warfare. URL: https://www.aspen.review/article/2017/the-new-generation-of-russian-warfare/.

15. The Russian Military Forum: Russias Hybrid War Campaign: Implications for Ukraine and Beyond. URL: https://www.csis.org/events/russian-military-forum-russias-hybrid-war-campaign-implications-ukraine-and-beyond.

16. Wrzosek, M. (2012). Zagrożenia militarne a bezpieczeństwo Europy. URL: https://zbrojni.blob.core.windows.net/pzdata/TinyMceFiles/kwartalnik_bellona4_2012.pdf [in Polish].

17. Zeshyty Naukove Akademii Obrony Narodovey nr 2 (99). 2015. ISSN 2299-6753. URL:https://depot.ceon.pl/bitstream/handle/123456789/9904/Banasik,%20Parafianowicz.pdf?sequence=1&isAllowed=y [in Polish].

Надійшла до редколегії 20.06.2020 р.