ДАНИЛЮК О. В.
здобувач
(Науково-дослідний інститут публічного права)

УДК 342.9
DOI https://doi.org/10.32842/2078-3736/2023.3.76

ПОНЯТТЯ, СУТНІСТЬ ТА ОСОБЛИВОСТІ ГІБРИДНИХ ЗАГРОЗ ЯК ОБ'ЄКТ АДМІНІСТРАТИВНОГО ПРАВОГО ДОСЛІДЖЕННЯ

В науковій статті, на підставі аналізу наукових позицій та норм чинного законодавства, визначено, що «гібридні загрози» – це цілеспрямована, системна, нормативно визначена діяльність спеціально створених суб'єктів сектору безпеки і оборони певної держави по відношенню до іншої шляхом одночасного використання різноманітних інструментів (правових, економічних, соціальних, інформаційних, культурних, кадрових) впливу на всі сфери суспільного розвитку з метою підриву незалежності, територіальної цілісності та унеможливлення реалізації національних інтересів та забезпечення національної безпеки в цілому.

Акцентовано увагу, що основними особливостями гібридних загроз національній безпеці з позиції адміністративно-правової науки є: 1) це завжди цілеспрямована та системна діяльність; 2) для цього створюються спеціальні державні суб'єкти, які наділяються відповідним функціоналом; 3) є складовою зовнішньої політики держави; 4) має нормативне врегулювання; 5) запобігання та протидія гібридним загрозам є складовою державної політики щодо забезпечення національної безпеки будь якої держави; 6) зміст такої діяльності передбачає в своєчасному прогнозуванні, виявленні та унеможливленні досягненні результату, який був закладений в останні; 7) одночасно використання інструментів впливу на всі сфери суспільного розвитку держави; 8) метою є підрив національної безпеки, незалежності та територіальної цілісності без застосування активних бойових дій.

Запропоновано, під адміністративно-правовими відносинами запобігання та протидії гібридним загрозам розуміти публічно-правові відносини, які урегульовані нормами адміністративного права, мають цілеспрямований, системний та публічно-владний характер, які спрямовані на збір, обробку, облік, моніторинг інформації щодо потенційних та реальних загроз всім сферам суспільного розвитку шляхом їх своєчасного виявлення та унеможливлення настання наслідків, які були заплановані стороною їх застосування.

Ключові слова: *адміністративно-правові відносини, гібридні загрози, запобігання, протидія, гібридні загрози, національна безпека, національні інтереси, загрози національній безпеці, реальні та потенційні загрози, суб'єкти сектору безпеки і оборони.*

Danyliuk O. V. The concept, essence and features of hybrid threats as an object of administrative legal research

In the scientific article, based on the analysis of scientific positions and norms of current legislation, it is determined that "hybrid threats" are purposeful, systematic, normatively determined activities of specially created subjects of the security and defense sector of a certain state in relation to another through the simultaneous use of various tools (legal, economic, social, informational, cultural, personnel)

influence on all spheres of social development with the aim of undermining independence, territorial integrity and making it impossible to realize national interests and ensure national security as a whole. It is emphasized that the main features of hybrid threats to national security from the point of view of administrative and legal science are: 1) it is always a purposeful and systematic activity; 2) for this, special state entities are created, which are assigned the appropriate functionality; 3) is a component of the state's foreign policy; 4) has regulatory regulation; 5) prevention and counteraction of hybrid threats is a component of the state policy to ensure the national security of any state; 6) the content of such activity involves timely forecasting, detection and impossibility of achieving the result that was laid down in the latter; 7) simultaneous use of tools of influence on all spheres of social development of the state; 8) the aim is to undermine national security, independence and territorial integrity without the use of active hostilities. It is proposed that the administrative-legal relations of prevention and counteraction of hybrid threats should be understood as public-legal relations, which are regulated by the norms of administrative law, have a purposeful, systematic and public-authority nature, which are aimed at the collection, processing, accounting, monitoring of information about potential and real threats all spheres of social development through their timely detection and prevention of the consequences that were planned by the party applying them.

Key words: *administrative-legal relations, hybrid threats, prevention, counteraction, hybrid threats, national security, national interests, threats to national security, real and potential threats, subjects of the security and defense sector.*

Постановка проблеми. Поняття «гібридна війна» є найбільш прийнятним терміном для характеристики сучасної агресивної політики рф як з теоретичної, так і з практичної точок зору. В даному випадку мова йде про поєднання мілітарних, квазімілітарних, дипломатичних, інформаційних, економічних засобів задля досягнення державою власних політичних цілей на міжнародній арені, у відносинах з іншими акторами [1, с. 15].

Кінцевим завданням гібридної агресії є встановлення таємного контролю за урядом або частини уряду іншої держави з метою зміни її геополітичного курсу, зовнішньої та внутрішньої політики. Це збігається з розумінням завдань сучасної війни, що підтримуються й академічними дослідниками. Томас Ніссен з Королівського коледжу оборони Данії прямо зазначає, що сучасні війни стосуються більшою мірою не контроля над територією, а контроля над населенням та процесом прийняття політичних рішень [2, с. 8]. Для здобуття такого контролю можуть активно використовуватись місцеві політичні партії та ЗМІ, що керуються агентами впливу, через яких або через інших агентів з числа місцевих підприємців агресор здійснює таємне фінансування такої діяльності.

Таким чином, визначення поняття, сутності та особливостей гібридних загроз з позиції адміністративно-правової науки набуває не аби якого значення та потребують уваги з боку вчених адміністративістів.

Тому *метою* цієї статті є визначення категорії «гібридні загрози» та особливостей останньої з позиції адміністративно-правової науки.

Аналіз останніх досліджень та публікацій. Зазначені питання стали предметом дослідження багатьох вчених, які цікавились проблемами забезпечення національної безпеки та національних інтересів держави. Так, до останніх можна віднести: А. А. Головко, В. А. Ліпкан, А. Г. Мосейко, Г. О. Пономаренко, С. П. Пономарьов, А. В. Рубан, В. В. Сокуренко, С. В. Чумаченко, А. П. Хряпинський, та багато інших. Наголосимо, що зазначені вчені лише опосередковано торкались питань щодо визначення категорії гібридні загрози, тому означене питання є актуальним і своєчасним враховуючи події, які відбуваються на сьогодні в світі.

Виклад основного матеріалу. Звернення до Закону України «Про національну безпеку України» дає нам законодавче визначення цієї категорії. Так, під загрозами національній безпеці слід розуміти явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [3]. Якщо звернутись до тлумачних словника то під категорією «гібрид» як правило розуміють – перемішування, результат природного чи штучного схрещування між двома організмами різних елементів. Виходячи з цього можна запропонувати «робоче визначення» «гібридних загроз», як цілеспрямованої, системної, нормативно визначеної діяльності спеціально створених суб'єктів сектору безпеки і оборони певної держави по відношенню до іншої шляхом *одночасного* використання різноманітних інструментів (правових, економічних, соціальних, інформаційних, культурних, кадрових) впливу на всі сфери суспільного розвитку з метою підриву незалежності, територіальної цілісності та унеможливлення реалізації національних інтересів та забезпечення національної безпеки в цілому.

Головною метою гібридної війни є підрив здатності держави (суспільства) здійснювати опір агресії, досягнення неконвенційними методами власних політичних цілей. У цьому контексті об'єктами гібридної агресії стають стратегічні економічні підприємства, елементи критичної військової, енергетичної та соціальної інфраструктури. Відтак, можна виділити безпековий, економічний, соціальний та інфраструктурний напрямки серед основних, на які здійснюється атака в рамках гібридної операції.

Окрім цих напрямків слід окремо розглядати цивілізаційно-ідеологічний та культурно-інформаційний напрямки, де об'єктом національного інтересу виступає дещо ефемерна категорія ідентичності. Саме суспільна ідентичність є основою держави-нації і формує запит на визначення національних інтересів держави, реалізації заходів щодо їх досягнення. Прагнення агресора нанести удар саме по ідентичності оппонента цілком логічне, оскільки ставить питання щодо доцільності опору, спричиняє так звану «кризу ідентичності» та дезорганізацію внутрішніх інституцій. Атаки на такі об'єкти національного інтересу мають на меті ерозію волі держави до спротиву, що значно полегшує для агресора не тільки завдання організації та реалізації агресії, але й заходи щодо легітимізації цих процесів.

В цілому, можна говорити про те, що гібридні операції спрямовані проти *об'єктів національних інтересів* держави, сконцентрованих навколо чітко визначеного кола стратегічних напрямків, що формують її потенціал та здатність до спротиву. Ми пропонуємо застосовувати в даному випадку наступну класифікацію об'єктів національних інтересів, розглядаючи їх на прикладі України та російсько-української війни:

- Сектор оборони: мобілізаційні ресурси; стратегічні резерви; сфера військово-технічного обслуговування; контррозвідувальна спроможність тощо.
- Сектор безпеки: цивільний захист; сфера медичної безпеки; екологічна безпека тощо.
- Сектор економіки: середній та малий бізнес; стратегічні галузі промисловості; фінансові (у тому числі – банківські) послуги; агросектор тощо.
- Сектор критичної інфраструктури: енергетика; водопостачання; транспортна інфраструктура (залізнична, авіаційна, дорожня, морська) тощо.
- Соціальний сектор: якість та вартість комунальних послуг; доступність та якість освіти, медичного обслуговування; якість транспортної інфраструктури.
- Сектор національних маркерів: українська мова та культура; історична пам'ять; європейська та євроатлантична інтеграція; ідентичність у широкому сенсі.

На руку агресору грає наявність *гібридних вразливостей об'єктів національного інтересу* – слабких місць у національній структурі, які можуть бути ефективно використані проти країни іншими державами з метою підриву національної безпеки та ослаблення країни з метою подальшого її контролю. Доцільним буде запропонувати наступну класифікацію таких вразливостей: економічні (бідність населення, безробіття, високий рівень цін та низькі заробітні плати, поганий рівень розвитку інфраструктури тощо); соціальні (низький рівень освіченості населення, злочинність тощо); соціо-політичні (духовне гноблення, політичний

тероризм, ідеологічні, міжпартійні, міжконфесійні та внутрішні збройні конфлікти, війни тощо); соціо-культурні (конфліктні ситуації на міжнаціональному, етнічному, расовому чи релігійному ґрунті); екологічні.

Гібридній війні притаманні багатовимірні операції, в яких відбувається синхронізоване застосування комплексних атак на вразливості в різних сферах суспільного життя держави. Такі атаки підпорядковані єдиному плану та замислу, але для сторонніх спостерігачів на перший погляд він не є очевидним. Отже, слід глибше аналізувати подібні події, шукаючи реальний інтерес агресора в проведенні тих чи інших дій – зазвичай він має іншу сутність, аніж той, що лежить на поверхні. Наприклад, застосування торгових дискримінацій щодо окремих українських підприємств в поєднанні з інформаційними операціями та заходами індивідуального впливу може бути ознакою здійснення тиску на певні політичні групи або спробою регіональної дестабілізації, а не прикладом економічної війни. Активні заходи по підриву українo-угорських стосунків насправді можуть бути інструментом стримування євроатлантичної інтеграції України, а не роботою на розпалювання етнічного сепаратизму [4].

У контексті протистояння гібридним загрозам важливості набуває поняття *«стійкості»* – здатності протистояти змінам і загрозам, зберігаючи при цьому статус-кво. Державна та суспільна стійкість є здатністю держав і суспільств реформуватися на вимогу часу, трансформуватися у відповідності до актуальних викликів і таким чином відновлюватись після зовнішніх і внутрішніх криз. Державна стійкість також означає забезпечення державного суверенітету – суспільного верховенства держави та повнити її прав у межах міжнародно визнаних кордонів; здатність самостійно приймати рішення у внутрішній та зовнішній політиці, протидіяти будь-яким неконституційним впливам.

Своєчасне *розкриття планів та замислів гібридних операцій* та протидія їм вимагає спільного усвідомлення гібридних загроз всіма стейкхолдерами (урядом, громадянським суспільством та міжнародним співтовариством), а також їхнього тісного співробітництва при виявленні та відбитті гібридних атак. Спільний моніторинг тенденцій та відслідковування кейсів, що мають ознаки активних заходів противника, обмін інформацією про аномалії дозволять визначати «велику картину» подій, зрозуміти наявні вразливості, якими користується супротивник, та шляхи усунення таких вразливостей.

Таке співробітництво має здійснюватися на базі спеціальних постійних міжвідомчих та міжнародних виконавчих інституцій, в яких провідну роль мають обіймати органи національної безпеки та оборони. Ці структури здійснюють особливу експертизу в сфері підривної діяльності; здатні застосовувати спеціальні засоби збору інформації про таку діяльність та здійснювати специфічні заходи оперативної протидії, не притаманні цивільним відомствам. Органи національної оборони, на які покладена відповідальність за загальну координацію урядових зусиль у випадку військової ескалації, мають бути тісно залучені і до планування гібридної оборони на етапах, де військові засоби не застосовуються. Така залученість необхідна в тому числі для того, щоб вчасно виявити розгортання мереж нетрадиційної війни, які до початку ескалації будуть маскуватись під легітимну активність. Ці ж органи мають бути ключовими в формуванні системи національної стійкості – як загальноурядової, так і загальносуспільної.

Такий підхід відповідає позиції західних теоретиків та практиків, які відповідальні за формування сучасної моделі комплексної гібридної оборони НАТО. До її складу входять наступні компоненти: інтегрована національна система протидії, що базується на загальноурядовому та загальносуспільному підході, та інтегрована міжнародна система протидії, що базується на співробітництві НАТО та ЄС. Обидві системи доповнюють одна одну в процесі виявлення, аналізу та стримування гібридних загроз та в процесі виявлення вразливостей, посилення готовності та розбудови стійкості. Таким чином вони забезпечують не лише ситуаційну обізнаність, але й всебічну безпеку.

Основу гібридної війни становить підривна діяльність, що здійснюється ворожими спецслужбами відповідно до своїх таємних планів та замислів. Протидія такій діяльності вимагає детального розуміння природи підривної діяльності, форм, методів та способів,

якими вона здійснюється. У зв'язку з цим провідну роль в організації міжвідомчої протидії гібридній агресії необхідно відводити представникам органів національної безпеки та оборони, і особливо представникам спеціалізованих підрозділів органів розвідки та контррозвідки [5, с. 14]. Така провідна роль також обумовлена тим, що саме ці органи уповноважені відповідно до своїх функцій застосовувати спеціальні методи здобуття інформації, протидії діяльності ворожих спеціальних служб та реалізації заходів щодо запобігання, усунення та нейтралізації загроз національним інтересам, що не притаманні іншим державним органам.

За своєю природою протидія підривній діяльності ворожих спецслужб суттєво відрізняється від правоохоронної функції держави і вимагає інших підходів та іншого правового регулювання. Розкриття та припинення такої діяльності від початку не має орієнтуватися на кримінально-процесуальну перспективу, в тому числі тому, що значна частина підривних дій противника, особливо на ранніх стадіях гібридної агресії, не носить протиправного характеру. Боротьба з гібридними загрозами вимагає унеможливлення не лише наслідків, але й самої підривної діяльності, і не може орієнтуватися на кримінально-правову репресію. Операції по впливу на прийняття політичних рішень органами влади, формуванню бажаної противнику суспільно-політичної обстановки та її дестабілізації вимагають застосування інших, аніж кримінально-процесуальні, форм протидії. Стратегічною метою організації гібридної оборони є здатність протидіяти не окремим проявам діяльності ворожих спецслужб, а самим ворожим спецслужбам. Ефективність гібридної оборони визначається не кількістю зірваних акцій противника, а проникненням в його плани та замисли, розкриттям механізмів та агентурних мереж, що використовуються для підривної діяльності. Мова йде про унеможливлення діяльності ворожих спецслужб, а не просте притягнення до кримінальної відповідальності її кадрових співробітників та посібників – конкретних виконавців.

Однією з важливих ознак підривної діяльності є конспіративність її здійснення. Така конспіративність може передбачати як таємність безпосереднього здійснення підривної діяльності (конспіративна по характеру діяльність), так і наявність таємної підривної мети у дій, що здійснюються відкрито (конспіративна по меті діяльність). Конспіративність здійснення підривної діяльності обумовлена не лише необхідністю приховувати її від державних органів країни, проти якої вона здійснюється, але й здатністю забезпечити правдоподібне заперечення участі в такій діяльності країни-агресора у випадку провалу операції. Таке правдоподібне заперечення дозволяє агресору уникати суспільного та міжнародного засудження та суттєво ускладнює застосування в гібридній обороні відкритих форм протидії. Як і в роки Холодної війни, гібридне протиборство в своїй основі є протистоянням спеціальних служб і має широко застосовувати принципи таємної боротьби як в нападі, так і в обороні.

На ренесансі спецслужб у зв'язку з загостренням гібридного протистояння наголошує в своїй статті «Нова ера для розвідки НАТО» перший заступник Генерального секретаря НАТО з питань розвідки та безпеки Арндт Фрейтаг фон Лорінгховен [6]. Створення в 2017 році Об'єднаного управління розвідки та безпеки НАТО було першим в історії Штаб-квартири Альянсу об'єднанням представників окремих політичних та воєнних розвідок, що є також зразком успішної міжвідомчої взаємодії. Попри занепокоєння через можливий конфлікт професійних культур та підходів, об'єднання розвідок дозволило забезпечити підготовку чітких розвідувальних оцінок; підвищити ефективність зусиль та уникнути дублювання; використовувати природні переваги політичних та воєнних розвідок; створити нову культуру співробітництва, необхідну для протидії гібридним, терористичним та кібернетичним загрозам.

До Об'єднаного управління також був включений Офіс безпеки НАТО (NATO Office of Security – NOS). Це мало не лише убезпечити від витоків інформації, що вкрай важливо для взаємної довіри при обміні розвідувальною інформацією, але й унеможливити використання вразливостей противником. Об'єднання в одній інституції функцій розвідки та безпеки також створило передумови для щоденного співробітництва між ними.

На рівні Європейського Союзу також здійснюються дії, спрямовані на посилення міжвідомчої та міжурядової взаємодії спецслужб по виявленню, протидії та реагуванню на гібридні загрози, розвиток розвідувальної та контррозвідувальної експертизи в цій сфері [7].

Попри те, що гібридна війна планується та організовується спеціальними службами, притаманна їй багатовимірність вимагає широкого залучення всіх державних та недержавних інститутів не лише для оборони, але й для атаки. Така практика спостерігається навіть в авторитарних країнах, які розглядають гібридні війни як головну лінію майбутніх протистоянь, а не тимчасовий феномен. В РФ, наприклад, продовжується централізація цивільних, військових, медійних та економічних спроможностей. Оптимізація та підлаштування таких урядових інструментів під потреби гібридних воєн відбувається не лише тому, що, відповідно до російських військових теоретиків, такі форми війни все частіше зустрічаються, але й тому, що вони є ефективнішими, аніж традиційні війни.

Таким чином, не лише країни НАТО і ЄС, але й їхні авторитарні антагоністи сьогодні схиляються до комплексного підходу до ведення гібридної війни та особливої ролі в ній розвідувальних та контррозвідувальних органів.

Одним з важливих завдань будь-якої оборони є забезпечення *стримування* противника від здійснення небажаних (ворожих) дій. Існуюча теорія військового стримування була розвинена в роки Холодної війни насамперед для стримування сторін (НАТО та Варшавського блоку) від застосування ядерної зброї. Значною мірою сучасна гібридна війна, її переважно таємні та невійськові методи ведення, є продуктом системи ядерного стримування, що фактично унеможливила прямий військовий конфлікт між головними суперниками. Тим не менш, це не призвело до відмови від протистояння, а лише примусило СРСР шукати інші шляхи для вирішення власних геополітичних задач – що власне і стало поштовхом до формування концепції сучасної гібридної війни [1, с. 59].

Сьогодні, у зв'язку з тим, що деякі країни застосовують інструменти гібридної війни з метою зміни існуючого міжнародного порядку, актуалізується необхідність розробки нових методів стримування. Наприклад, заступник командувача об'єднаними силами НАТО в Європі британський генерал Адріан Бредшоу наголошував на тому, що відповіддю на «гібридні методи ведення війни» має стати «гібридне стримування» [8]. В останні роки НАТО доклала значних зусиль для того, щоб бути готовою до нових викликів, проте так і не охопила всього діапазону задач, пов'язаних з гібридною війною. Сучасна політика НАТО по стримуванню гібридної агресії все ще здебільшого заснована на швидкому військовому реагуванні [9], що по своїй суті є реагуванням на фінальну стадію лише одного з можливих варіантів гібридної агресії (який передбачає збройну ескалацію). Вона не означає стримування противника від підривної діяльності як такої. Враховуючи той факт, що гібридна агресія може здійснюватись нижче рівня збройного конфлікту з використанням переважно або навіть виняткова невійськових методів, ми вважаємо, що концепція ефективного гібридного стримування вимагає перегляду стратегій, розроблених в роки Холодної війни, з врахуванням цих змін [5, с. 60].

Основні вимоги до стримування та ключові умови його досягнення, розроблені в роки Холодної війни, все ще залишаються в силі – проте набувають нового значення в контексті застосування невійськових методів. Зберігають свою актуальність також вимоги до стримування, описані Томасом Шеллінгом в його роботі «Зброя та вплив» [10]: визначення джерела агресії, повідомлення агресора про свої наміри відповісти на небажану поведінку, реальна наявність засобів, необхідних для такої відповіді.

Такий підхід в рівній мірі може застосовуватись як для гібридного стримування, так і для примусової дипломатії. Водночас традиційне розуміння стримування та примусу здебільшого розглядає в якості інструменту впливу на противника загрозу застосування військової сили [11]. Це було виправдано для лінійних конфліктів, де військова сила займала центральну роль. Проте природа гібридного протистояння вимагає нового набору інструментів з високою питомою вагою невійськових заходів та нових вимог до ключових умов досягнення стримування та примусу, поетапного підходу до застосування заходів та нового розуміння рамок ескалації-деескалації. Також надзвичайно важливо правильно визначати об'єкт, на який має здійснюватися такий примус, оскільки в авторитарних країнах, яким притаманно застосування гібридної агресії, таким об'єктом будуть не лише самі державні

інститути, а насамперед фізичні особи, що їх контролюють. На нашу думку, правильне розуміння мотивації таких осіб та їхніх інтересів (що часто можуть не збігатися або навіть суперечити інтересам їхньої держави) є основою для планування заходів впливу, що відтак вимагають обов'язкового залучення фахівців з політичної психології до аналізу ситуації [5, с. 62-63]. Стримування в гібридному протистоянні – це складна соціальна взаємодія, яка має враховувати природу людини, її психологію та емоції – страх, сміливість, довіру, бажання влади та помсти.

В основі стримування в гібридному протистоянні зберігається здатність держави завдати противнику шкоду, достатню для того, щоб вплинути на його поведінку та примусити утриматись від здійснення певних дій. Загроза заподіяти таку шкоду є основною переговорною силою та має служити стримуючим фактором через неминучі видатки та втрати, які понесе противник у випадку здійснення агресивних дій. В основі ефективного стримування та примусу має лежати максимальне посилення негативних наслідків для противника у випадку його небажаної поведінки, переважання негативних наслідків над позитивними.

Класична література розрізняє два фундаментальні підходи до стримування: стримування відмовою (deterrence by denial) та стримування покаранням (deterrence by punishment) [12].

Перше передбачає здійснення заходів, спрямованих на зменшення ймовірності успіху небажаних дій, а також суттєве збільшення ресурсів, що необхідні противнику для їхнього здійснення. Такі заходи значною мірою будуть збігатись з заходами проактивної мітигації. Головне завдання стримування відмовою – підняти вартість небажаних дій противника до неприйнятного для нього рівня.

Стримування покаранням, у свою чергу, передбачає не захист об'єкта можливого нападу, а загрозу неминучого покарання противника за такий напад. Основним принципом стримування покаранням є його утилітарність або перспективність. Воно покликане змінити поведінку в майбутньому, а не просто забезпечити відплату або покарання за поточну або минулу поведінку. Головне завдання стримування покаранням – завдання противнику шкоди, що має суттєво перевищувати переваги, які він очікує отримати за рахунок здійснення небажаних дій.

Для планування заходів гібридного стримування має застосовуватись адаптована до природи гібридного протистояння методика аналізу зисків та витрат (cost–benefit analysis – CBA). При цьому аналіз зисків та витрат має проводитись окремо для кожної з груп інтересів країни-противника (політиків, бізнесменів, військових, населення в цілому) з метою розробки заходів впливу, що були б чутливими саме для визначених стейкхолдерів. При такому аналізі особливо важливо достовірно визначити справжні зиски, яких намагаються досягти ініціатори небажаних дій, а також найбільш болісні для них втрати [5, с. 65]. Здобуття інформації про такі інтереси має бути одним із пріоритетних завдань розвідувальних органів. При цьому варто пам'ятати, що суспільна підтримка важлива не лише для демократичних, але й для авторитарних лідерів. Відтак зиском може виступати не реальне досягнення конкретного результату, а й суб'єктивне сприйняття в якості зиску того чи іншого факту населенням.

Стратегія ефективного стримування має відповідати так званому «правилу трьох Сі» («three C`s of deterrence»), що вимагає наявності трьох інтегральних компонентів: спроможностей (capability) завдати шкоди інтересам противника; переконливості (credibility) в намірі та готовності завдати такої шкоди; комунікації (communication) – двостороннього розуміння та усвідомлення, що сторони однаково поінформовані про всі можливі зиски та втрати у випадку здійснення противником небажаних дій [13].

В той час, як заходи стримування відмовою спрямовані на посилення національної стійкості та значною мірою збігаються з заходами пом'якшення гібридних загроз, заходи стримування покаранням вимагають розробки спроможностей, що можуть бути застосовані до противника безпосередньо. При плануванні гібридного стримування варто враховувати, що винятково заходи посилення національної стійкості навряд чи зможуть змінити поведінку гібридного агресора. Для забезпечення бажаної поведінки опонента необхідно

дотримуватись балансу між заходами стримування відмовою та стримування покаранням [5, с. 66-67].

Ефективність стримування залежить насамперед від сприйняття можливості настання негативних наслідків самим об'єктом впливу. Наявність найбільш досконалих засобів нанесення шкоди не вплине на зміну поведінки агресора, якщо намір сторони, що обороняється, застосувати ці засоби не буде переконливим для агресора. Переконлива погроза передбачає, що у випадку відмови виконати вимоги, вона може бути виконана та неодмінно буде виконана. Формування у противника відчуття впевненості не лише у наявності засобів нанесення йому шкоди, але й в готовності їх застосувати – ключове завдання ефективного стримування, виконання якого вимагає досконалого застосування інтегрального компоненту примусу, яким є комунікація. Правильний вибір стратегії комунікації є критично важливим для забезпечення необхідного стримування. Вона має засновуватись на комплексному підході, не обмежуючись формальним інформуванням виключно вищого політичного керівництва. Інформація про наявність засобів нанесення шкоди та готовність її нанести у випадку не виконання вимог має бути прокомунікована до різних цільових груп, через різні канали, з різною інтенсивністю, в різний час та в різний спосіб.

Висновки. Підсумовуючи зазначимо, що «гібридні загрози» – це цілеспрямована, системна, нормативно визначена діяльність спеціально створених суб'єктів сектору безпеки і оборони певної держави по відношенню до іншої шляхом одночасного використання різноманітних інструментів (правових, економічних, соціальних, інформаційних, культурних, кадрових) впливу на всі сфери суспільного розвитку з метою підриву незалежності, територіальної цілісності та унеможливлення реалізації національних інтересів та забезпечення національної безпеки в цілому.

Основними особливостями гібридних загроз національній безпеці з позиції адміністративно-правової науки є: 1) це завжди цілеспрямована та системна діяльність; 2) для цього створюються спеціальні державні суб'єкти, які наділяються відповідним функціоналом; 3) є складовою зовнішньої політики держави; 4) має нормативне врегулювання; 5) запобігання та протидія гібридним загрозам є складовою державної політики щодо забезпечення національної безпеки будь якої держави; 6) зміст такої діяльності передбачає в своєчасному прогнозуванні, виявленні та унеможливленні досягненні результату, який був закладений в останні; 7) одночасно використання інструментів впливу на всі сфери суспільного розвитку держави; 8) метою є підрив національної безпеки, незалежності та територіальної цілісності без застосування активних бойових дій.

Адміністративно-правові відносини запобігання та протидії гібридним загрозам – це публічно-правові відносини, які урегульовані нормами адміністративного права, мають цілеспрямований, системний та публічно-владний характер, які спрямовані на збір, обробку, облік, моніторинг інформації щодо потенційних та реальних загроз всім сферам суспільного розвитку шляхом їх своєчасного виявлення та унеможливлення настання наслідків, які були заплановані стороною їх застосування.

Список використаних джерел:

1. Світова гібридна війна: український фронт / за заг. ред. В.П. Горбуліна. Київ : НІСД, 2017. 496 с. С. 15

2. Nissen T. The Weaponization of Social Media. Denmark: Royal Danish Defense College, 2015. 148 p. – 8.

3. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/go/2469-19.

4. Губар О. Угорщина назвала умови розблокування роботи комісії «Україна – НАТО». URL: https://www.dw.com/uk/uhorshchyna-nazvala-umovy-rozblokuvannia-roboty-komisii-ukraina-nato/a-55029588.

5. Данилюк О.В. Міжвідомче та міжнародне співробітництво при виявленні та протидії гібридним загрозам. Київ : 7БЦ, 2021. 192 с.

6. Loringhoven A. F. von. A new era for NATO intelligence. URL: https://www.nato.int/docu/review/articles/2019/10/29/a-new-era-for-nato-intelligence/index.html.

7. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). URL: https://www.hybridcoe.fi/

8. Beale J. Nato needs a grand strategy for Russia, says UK general. BBC. URL: https://www.bbc.com/news/uk-39151192.

9. Pindják P. Deterring hybrid warfare: a chance for NATO and the EU to work together? URL: https://www.nato.int/docu/review/articles/2014/11/18/deterring-hybrid-warfare-a-chance-for-nato-and-the-eu-to-work-together/index.html

10. Schelling T. Arms and Influence. 1966. 303 p.

11. Byman D., Waxman M. The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might. 2002. 300 p.

12. Rühle M. Стримування: що воно може (і не може) зробити. URL: https://www.nato.int/docu/review/uk/articles/2015/04/20/strimuvannya-shcho-vono-moyoe-ne-moyoe-zrobiti/index.html

13. Cornish P. Integrated Deterrence: NATO's 'First Reset' Strategy, GLOBSEC NATO Adaptation Initiative, 2017. C. 100-112.