МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут «Інститут державного управління»

До захисту
Завідувач кафедри публічної політики
д.держ.упр., проф.
_____ Дзюндзюк В.Б.

ПРАВОВІ АСПЕКТИ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

Кваліфікаційна робота на здобуття освітнього ступеня «магістр»
281 Публічне управління та адміністрування
28 Публічне управління та адміністрування

Виконавець
здобувач 2 курсу, групи ППГЗ-1-23 К.О Андрієнко

Науковий керівник
к.держ.упр., доц. К.І. Козлов

Харків – 2024

ЗМІСТ

ВСТУП

Актуальність роботи. В умовах сучасного життя проблеми неконвенційних загроз і гібридної конфліктності стали пріоритетними темами у воєнно-політичних та безпекових документах як НАТО, Європейського Союзу так і України. Це обумовлено посиленням гібридних загроз, які виходять за межі традиційних воєнних дій і включають використання політичного, економічного, інформаційного, кібернетичного та інших інструментів для дестабілізації держав та регіонів. В Україні гібридні загрози стали особливо актуальними через конфлікт із Росією, що створило нові виклики для державного управління, бізнесу, громадськості та окремих регіонів. У даному значенні взаємодія державної влади з громадськістю стає критично важливою та необхідною. Процедура цієї взаємодії є потрібною для раціональної протидії гібридним загрозам враховуючи наступні причини. По-перше, запровадження воєнного стану та тісно поєднані з ним умови до національного керівництва потребують від парламенту більшої праці, раціональності та оперативності. Воєнний стан викликає перед країною новітні виклики відносно керівництва кризовими ситуаціями, дотриманням національної безпеки та покращення стійкості цивілізованого суспільства до гібридних атак та маніпуляційних дій. По-друге, активне взаємовідношення установ публічної влади з сучасною громадськістю є дуже важливим, адже збільшується відношення громадської позиції на прийняття управлінських рішень. Сьогодні, громадянське суспільство займає керівну роль у покращенні суспільної довіри до національних інститутів, а також у протидії гібридним атакам. Залучення всіх громадян до обговорення та вирішення безпекових питань дає можливість посилювати громадянську згуртованість та мобілізацію на взаємопідтримку національних інтересів.

Дану тематику на сьогодні досліджували такі вітчизняні вчені як: Дзюндзюк Б., Кудь О., Крутій О., Лопадченко І., Радченко О., Бакуменко А. Також питанням публічної політики в сучасних умовах гібридних загроз вивчали Андрієвський Т., Василевич Ю., Колесник В., Коломієць О. Особливу увагу в Україні приділено визначенню основних характеристик конфліктів нового типу,

зокрема неконвенційних та «гібридних», що є ключовими елементами конфліктності сучасного концептуального порядку. Дані аспекти отримали відображення у доктринальних документах вищих органів державної влади та управління. Країна зосередилася на підборі нових методів та засобів для забезпечення національної безпеки, що є актуальним у зв'язку з потребою адаптації до перемінних умов сучасної безпеки та збільшення гібридних загроз на світовій арені.

В умовах гібридної війни та незвичайних зовнішніх загроз в Україні дуже важливо вдосконалювати процедури спільної роботи між державними галузями та громадськими організаціями для покращення ефективності керівних рішень та здійснення рівноваги національної стійкості до міжнародних на внутрішньо-національних загроз. Останнім часом воєнна агресія, налаштована на Україну, зумовила нас підійти з новим підходом до цього питання та покращити політику у галузі взаємовідношення влади та сучасної громадськості в умовах гібридних загроз. Гібридна агресія має різницю саме комплексним підходом та застосуванням високотехнологічних інструментів для досягнення стратегічних цілей. Це не тільки традиційні військові дії, але й системний вплив у міжнародній, політичній, економічній, інформаційній, соціальній та культурній галузі життя.

Такий підхід робить особливо важливим вдосконалення інструментів публічного управління, котрі надають можливість забезпечити раціональну взаємодію між владою та громадськістю. Серйозне поширення сучасних технологій взаємодії між громадянами та державними установами висуває нові передумови до покращення процедур публічного управління. Це, наприклад, відноситься, до формування гнучких та адаптивних комунікаційних структур, котрі дозволяють швидко реагувати на інформаційні виклики та надавати громадянам своєчасну та правомірну інформацію. Спільні стратегії, котрі розробляються для раціональної комунікації між владою та громадськістю, також мають враховувати, що в умовах гібридної війни противник намагається не тільки зменшити вплив та довіру державних інституції, але і також поширити

розкол у цивілізованому суспільстві. Тому, дані події, вимагають правильного тлумачення властивостей гібридних загроз та розвитку цих механізмів, котрі дозволяють не тільки інформувати громадян, але і також залучати їх до процедури прийняття відповідних актів та створення загально-національної стратегії протидії. Таким чином, формування новітніх методів у галузі національної безпеки має на завданні не тільки покращити обороноздатність, а й замінити міцні засади для структури національної безпеки, яка зможе раціонально протистояти різним формам сучасних загроз.

Мета роботи є вивчення теоретичних засада та підготовка рекомендацій правових основ протидії гібридним загрозам у сучасному світі, а

Для досягнення визначеної мети поступово були вирішені такі *завдання*:

- дослідити поняття та характеристика гібридних загроз

- вивчити нормативно-правову базу щодо протидії гібридним загрозам на національному та міжнародному рівні;

- проаналізувати практики застосування правових норм у протидії гібридним загрозам у світовій практиці;

- вивчити Український досвід правового регулювання боротьби з гібридними загрозами;

- запропонувати шляхи удосконалення національного законодавства у сфері протидії гібридним загрозам;

- запровадити міжнародний досвід у боротьбі з гібридними загрозами.

Об'єктом дослідження є протидія гібридним загрозам.

Предметом дослідження є протидія гібридним загрозам шляхом удосконалення нормативно-правового забезпечення.

Методи дослідження. При написанні кваліфікаційної (магістерської) роботи теоретико-методологічною базою вивчення став системний підхід до аналізу правових аспектів протидії гібридним загрозам. Було узагальнено наявну інформацію за темою цього вивчення та використано такі методи дослідження: аналогії та порівняння (дослідження гібридних загроз у світі, та боротьби з нею); метод комплексності (вивчення предмета роботи з точки зору як негативного

явища); аналізу та синтезу (надання певних пропозицій щодо покращення правової основи боротьби гібридним загрозам).

Практичне значення отриманих результатів полягає в тому, що органи державної влади в своїй діяльності можуть керуватись теоретичними та практичними положеннями, що були запропоновані в кваліфікаційній роботі.

Основні положення кваліфікаційної роботи були заслухані та обговорені на засіданні кафедри публічної політики Навчально-наукового інституту «Інститут державного управління».

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ПРАВОВОГО РЕГУЛЮВАННЯ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

1.1 Поняття та характеристика гібридних загроз

Гібридні загрози стали одним із ключових викликів сучасного світу, адже вони використовують як військові, так і невоєнні методи впливу, серед яких маніпуляція свідомістю займає центральне місце. Застосування політичних і нейролінгвістичних технологій створює широкі можливості для маніпулятивного впливу, що робить дослідження цього явища надзвичайно актуальним на сьогодні. Гібридна війна - це форма конфлікту, де традиційні військові методи інтегровані з невоєнними засобами, такими як економічний тиск, кібератаки, дезінформація та політичні маніпуляції у суспільстві. Її основна мета досягнення стратегічних цілей без прямого військового вторгнення або його мінімізація. Сучасні політичні та нейролінгвістичні технології стали потужним інструментом у гібридній війні, націленим на маніпуляцію свідомістю та формування вигідних наративів у суспільстві. Аналіз іноземного та вітчизняного досвіду дозволяє визначити ключові загрози та розробити ефективні механізми протидії. Вивчення цих аспектів є не лише науковою необхідністю, а й практичним кроком у забезпеченні безпеки держави та її громадян. Як зазначено в Конституції України захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [1].

Визначення терміну «гібридної загрози», в сучасному розумінні має три головних тлумачення. По-перше, це гібридна загроза це гібридність у певній військовій ситуації, котра має відношення до особливостей здійснення бойових дій, де переплітаються різноманітні форми та методи військового протистояння. Ця гібридність зумовлює адаптацію військового ворога до ситуації, застосування

як традиційного озброєння, так і особливих нетрадиційних засобів ведення війни. По-друге, гібридна загроза це гібридність у методології та тактиці ворона, в цій ситуації гібридні загрози тлумачиться як відповідна стратегія та тактика дій ворона, спрямована на отримання певних політичних завдань. Це охоплює в себе кількість певних методів жорсткого насилля та активних дій, як приклад, це може бути пропаганда, кібероперації, інформаційні атаки та сильний економічний вплив. По-третє, гібридна загроза це певна гібридність у відношенні сил, котрі формує та забезпечує певна країна, гібридність означає вид сили та продуктів, потрібних для дотримання безпеки. Як визначено в Законі України «Про основи національного спротиву» складовими національного спротиву є територіальна оборона, рух опору та підготовка громадян України до національного спротиву це може передбачати формування як традиційних збройних сил, так і спеціальних підрозділів, здатних до гнучкої та адаптивної протидії різним формам загроз - від кібербезпеки до протидії дезінформації [2].

Загалом, під «гібридною загрозою» вважають дії противника, котрий адаптовано поєднує звичайне озброєння, нерегулярні тактики, терористичні методи та злочинні дії у зоні конфлікту для досягнення своїх політичних завдань. Гібридні загрози є комплексним явищем, що об’єднує різні форми ведення війни - від звичайного бойового озброєння та військових формувань до терористичних актів, насилля та злочинної поведінки.

Визначення «гібридні загрози» охоплює дії, котрі здійснюються як державними, так і недержавними структурами, та мають на меті підірвати або завдати шкоди цільовій групі через вплив на процедуру прийняття рішень на різних рівнях починаючи від місцевого і до міжнародного. Дані загрози спеціально спрямовані на вразливі місця демократичних країн та інститутів, функціонуючи в різних галузях, таких як політична, економічна, військова, громадянська та інформаційна [3].

Гібридні загрози зазвичай координуються та поєднуються використовуючи широкий аспект методів та засобів. Вони мають на завданні уникнути безпосереднього виявлення та залишатися «нижче порога», що ускладнює їх

ідентифікацію. Такий підхід надає можливість агресору досягати своїх завдань через спільні, непрямі дії, котрі дуже важко безпосередньо пов’язати із певним учасником або країною.

Таким чином, поняття «гібридні загрози» та «гібридні війни» є близькими за змістом і поділяють низку спільних характеристик. До основних рис обох явищ відноситься участь як державних, так і недержавних суб'єктів на різних рівнях, що діють як ворожі актори. Відношення формується відповідним методом, тобто нелінійними, багаторівневими та прихованими атаками на певні сфери життєдіяльності суспільства. Такі дії часто поєднують традиційні (військові) та нетрадиційні (економічні, інформаційні, кібернетичні) засоби, з акцентом на невійськових методах для покращення стратегічних та тактичних завдань. Це робить гібридні загрози та гібридні війни суттєво складними для протидії, бо вони спрямовані на реалізацію викликів сучасного суспільства, уникаючи безпосереднього воєнного конфлікту. Для приклад науковець Ф. Гофман вказує наступне поняття гібридної війни - як повного арсеналу усіх різновидів війни, включаючи звичайні здатності, нерегулярні тактики та утворення, терористичні дії, пов’язані з насильством та кримінальними заворушеннями [4, с. 97].

Більшість дослідників визнають інформаційну війну центральним елементом гібридної війни, що визначає її характер та інтенсивність. Цей феномен відображає практичну реальність сучасних конфліктів, де інформаційна складова нерідко стає вирішальною у досягненні стратегічних цілей. Розвиток засобів масової інформації, інтернет-технологій і соціальних мереж значно розширив можливості маніпулятивного впливу на свідомість громадян конкурентних країн. Інформаційна війна — це комплекс дій, спрямованих на формування або зміну світогляду мас, їхніх політичних уподобань, емоційного стану чи соціальної поведінки. У рамках гібридної війни інформаційні атаки використовуються для:

- дискредитації державних інституцій;
- підриву довіри до уряду;
- стимулювання соціального розколу;

- створення альтернативних наративів для виправдання агресивних дій.

В умовах глобалізації та розвитку цифрових технологій інформаційна війна втрачає чіткі кордони, перетворюючись на постійний процес, де держави змагаються за вплив на свідомість не лише громадян конкурентів, а й міжнародної спільноти. Інформаційна війна є невід'ємною складовою гібридних конфліктів, що визначає їхню ефективність та тривалість. У випадку українсько-російського протистояння вона стала ключовим полем битви за свідомість населення. Постійний розвиток технологій і засобів комунікації підкреслює необхідність удосконалення механізмів захисту від маніпулятивного впливу, а також просування правдивої інформації у глобальному просторі.

Слід відмітити, що у «Концепції забезпечення національної системи стійкості» від 20 серпня 2021 року, котра відноситься формування національної стабільності, визначається важливість формування процедур для виявлення та аналізу загроз та можливостей. Тому, значну зосередженість, приділено потребі формування на національному та місцевому рівнях відповідної мережі аналітично-експертних, наукових та навчально-методичних заходів, котрі б займалися проблематикою національної безпеки та розвитку стійкості. Дані центри мали б зосереджуватися на дослідженні загроз новітнього концептуального типу, що суттєво для здійснення на сучасні виклики та ситуації [5].

Спеціалісти у галузі безпеки вказують, що першим методом до здійснення даної стратегії має бути фіксування подій та випадків на міжнародній арені. Завданням даного моніторингу є зумовлення певних викликів та загроз як зовнішнього, так і внутрішнього характеру. Також суттєвим є осмислення певних ризиків через інтеграції міжнародних інноваційних підходів у освітню та наукову галузь враховуючи та розвитком національних засобів та практик.

На мій погляд, вказані чинники визначають актуальність дослідження досвіду організаційно-функціональних та керівних аспектів функціонування певних органів держав НАТО та ЄС. Для прикладу, дуже важливим може бути

практика даних держав у галузі дослідженні гібридних викликів, котрий є невід'ємною частиною структури військово-політичного керівництва зазначених міжнародних організацій [6].

В Україні на сьогодні відсутні спеціалізовані органи чи організації, котрі б спрямовували власні зусилля на вивченні новітніх методів гібридної конфліктності, наприклад, таких як військові гібридні загрози. Однак, відповідну інтегративну та операційну роль у дослідженні даної проблематики здійснює «Платформа Україна – НАТО з аналізу практики протидії гібридній війні в Україні». Дана структурна платформа була сформована у 2016 році під час засідання Комісії Україна – НАТО у рамках Варшавського саміту [7]. Головними цілями цієї Платформи є покращення засобів встановлення гібридних загроз, вивчення уразливих місць у структурі державної безпеки, охорона суттєво важливих об'єктів, вдосконалення стратегічних організацій, а також охорона цивільного населення та протидія тероризму у світі.

У свою чергу, українська структура даної Платформи є складовою частиною більш широкої Платформи Україна – НАТО з вивчення досвіду протидії гібридній війні, формування котрої визначено нормами. Комплексного пакету допомоги НАТО для України. Даний пакет був затверджений на засіданні Комісії Україна – НАТО на рівні керівників держав та їх урядів 9 липня 2016 року у Польщі, а саме у Варшаві [7].

Проблематика міжнародної співпраці в формуванні шляхів протидії гібридним загрозам більш детальніше вивчається у працях вченого-конфліктолога О. Данилюка. Вчений вивчає певні підходи та практичні сфери, котрі реалізовуються у євроатлантичному просторі для аналізу та викорінення цих гібридних загроз. Вивчення тематики та системних сфер тлумачення цієї концепції гібридної війни також закріплені в спільних робота українських вчених, котрі структурують вчення про підходи до дослідження гібридних загроз та дотримання безпеки [8, с.160].

Окрім цього, у працях конфліктологів країн НАТО та їхніх колег аналізується досвід створення дослідницької інфраструктури, орієнтованої на

виявлення та вивчення гібридних загроз, і шляхи впровадження цих досліджень у військово-політичну практику НАТО. Ці дослідження дають можливість узагальнити системні та практичні методи протидії гібридним викликам та надають можливість сприяють розвитку одного підходу до безпекової політики в умовах сучасної конфліктності.

У пункті 13 Підсумкової декларації саміту НАТО, котрий проходив у Шотландії у вересні 2014 року, найперше, на високому рівні було досліджено проблематику про потребу підготовки Альянсу до гібридних військових конфліктів («hybrid warfare»). Тому, під гібридною війною переважно розуміти взаємо поєднану широкого аспекту прямих бойових дій та секретних операцій, котрі відбуваються за єдиним методом, із залученням військових сил, добровольчих та нерегулярних утворень, а також різних цивільних систем [9].

Варто відмітити, що декларація визначала на важливості щільної співпраці між країнами-учасниками НАТО для знешкодження нетрадиційних загроз, серед котрих важливу увагу зосереджували пропагандистським осередками, кібератакам та сепаратистським рухам. Для покращення готовності до цих гібридних загроз та відпрацювання взаємних дій у гібридній війні в Латвії був сформованих спеціальний осередок під назвою «Strategic Communications Centre of Excellence». Даний центр фокусується на підготовці певних стратегій та розробкою методів для раціональної протидії в передумовах гібридної війни, котрий включає також кібербезпеку, і інформаційні методи, спецоперації.

Співпраця НАТО та ЄС у галузі по боротьбі з гібридним загрозам формується спільними організаційними системами. Однією з даних систем стала Міжвідомча комісія з боротьби з гібридними загрозами, сформована Європейською комісією та Європейською зовнішньополітичною службою. Завданням даної комісіє є формувати загальнонаціональне інформування про функціонування європейським інституцій, котрі здійснюють боротьбу з гібридними загрозами [9].

Окрім того, при Розвідувальному та ситуаційному центрі ЄС було засновано особливі підгрупи для формування інформаційної політики про

гібридні загрози. Також у Польщі та Румунії були створені контррозвідувальні Центри НАТО з протидії гібридним загрозам, взаємопов'язаним з розвідувальною діяльністю. Військова організація НАТО також сформувала підгрупи підтримки з ціллю боротьби з гібридними загрозами, котрі можуть бути відправлені в держави, котрі постраждали або страждають від даних гібридних загроз.

Хочу відмітити, що Європейський Союз у рамках власної стратегії хочу визначити незалежні шляхи та системи в сфері захисту та безпеки, в тому числі, для протидії гібридним загрозам сучасності. Дана обставина показує бажання до більшої незалежності, особливо в передумовах збільшення конкуренції в рамках євроатлантичної спільноти, де керівні позиції посідають Німеччина та Франція. Згідно до «Стратегічного порядку денного ЄС на 2024–2029 роки», Рада міністрів ЄС із загальних справ визначила резолюцію, котра закріпили керівні сфери для протидії гібридним загрозам та покращення стійкості держав-учасників. Однією з головних завдань цього документу є вдосконалення співпраці з світовими організаціями, наприклад як НАТО, а також з державами-учасниками ЄС для посилення спільної та колективної стабільності [10].

Європейський Союз впевнений, що система протидії гібридним загрозам має бути масштабною і чітко структурованою, беручи до спільної праці, як державних, так і недержавних учасників, інших організацій. Вона включає такі сфери, як формування та запровадження планів із захисту кібербезпеки, протидія дезінформаційним нападам та покращення захисту мирного населення від зброї масового знищення. У даному розумінні у структурі Європейської зовнішньополітичної служби сформовано Об’єднаний гібридний осередок (Hybrid Fusion Cell), котрий займається збором та аналізом інформації про новітні гібридні загрози. Підрозділи спільноти спеціалізуються на вивченні різних типів загроз, охоплюючи хімічну, бактеріологічну, радіологічну, ядерну, кібернетичну, а також проблематику контррозвідувального захисту та логістичної безпеки.

Таким чином, система Центрів сучасного досвіду для підбору та вивчення

даних про гібридні загрози та тактики гібридної війни, сформована в вітчизняних державах Балтії та Фінляндії, займає суттєву роль у здійсненні порядку денного НАТО та ЄС. На міжнародному рівні проблематика формування та протидії гібридним загрозам займають одне з центральних місць у стратегіях та заходах, котрі формуються на форумах Альянсу. Дані сучасні центри накопичують та формують теоретичні розробки, котрі активно застосовують для підтримки форумів НАТО і ЄС.

Інституції, котрі займаються дослідженням гібридної конфліктності, налаштовані у воєнно-політичну структуру НАТО та ЄС, надаючи її когнітивне підґрунтя. Вони дуже щільно працюють з іншими аналітичними та керівними системами, що дає здатність реалізовувати системних підхід до протидії гібридним загрозам. Дана факт забезпечує загальну взаємодію та погодженість роботи Альянсу у галузі виявлення, аналізу та формуванні певних стратегій боротьби.

Тому, наша держава та міжнародні країни, зокрема Європейський Союз за останні роки суттєво посилив свою нормативну базу та інституційні можливості для боротьби з гібридними загрозами, враховуючи їх багатогранність та динамічність. Цей процес охоплює розвиток термінології, визначення ключових сфер ризику та створення спеціалізованих органів, здатних ефективно координувати дії на наднаціональному рівні.ЄС досяг значного прогресу в адаптації своєї нормативної та інституційної бази до нових типів гібридних загроз. Зусилля спрямовані на підвищення стійкості держав-членів, зміцнення стратегічної автономії та створення умов для ефективної співпраці з міжнародними партнерами. Проте, залишається важливим постійне вдосконалення механізмів координації, обміну інформацією та реагування для забезпечення безпеки в умовах швидкоплинних викликів.

1.2 Нормативно-правова база щодо протидії гібридним загрозам на національному та міжнародному рівні

У цьому підрозділі, хочу зазначити, що нинішнє законодавство нашої держави, котре включає різноманітні аспекти захисту національної безпеки, є досить розвинутим та багаторівневим, реалізовуючи засади для протидії різним загрозам, в тому числі і гібридним. У сучасному українському законодавстві слід визначити декілька ключових структурних складових. По-перше, це важливе стратегічні нормативні акти для протидії загрозам національної безпеки. Засади та принципи державної політики відносно національної безпеки були визначені Концепцією національної безпеки України, схваленою Верховною Радою України [5].

Модернізація механізмів публічного управління в умовах гібридних загроз стає критично важливим фактором для забезпечення державної безпеки, стабільності суспільства та його здатності протистояти багатошаровим і асиметричним загрозам, які не обмежуються лише фізичним протистоянням, але й проникають у всі сфери життя держави. Сучасне життя, для прикладу загострення нестабільності у світовій безпековій структурі, потребують перегляду когнітивних та доктринальних загал інституції національної безпеки та оборонної потужності країн. Вчені у галузі безпеки переважно зазначають про потребу формування інноваційних вирішень, можливих уявляти та протидіяти великим загрозам гібридного характеру, котрі стали властивими для сучасного світу та України, зокрема.

У даній Концепції національна безпека розуміється як відповідний стан захищеності людини, цивілізованого суспільства та країни від внутрішніх та міжнародних загроз. До об’єктів охорони Концепція визначила, окрім національного суверенітету та територіальної цілісності, також демократичний стан суспільства, права та свободи особи, котра говорить про комплексний підхід до безпеки від гібридних загроз. Документ включав головні зовнішні та внутрішні небезпеки, охоплюючи політичні, економічні, соціальні, воєнні, екологічні та науково-технологічні галузі сучасного життя. Тому, проблематика інформаційної безпеки тоді не було у такому розмірі розвинутою через властивості тодішнього розвитку. По-друге, документація довгострокового

планування та стратегічні документи спеціального характеру. На даному етапі проблематика національної безпеки України визначена через певні стратегічні документи, котрі формують довгострокове планування в сферах оборони держави, економіки, енергетики, кібербезпеки, тощо. Дані документи визначають керівні сфери розвитку національної безпеки та формують політику країни у певних галуззях. По-третє, підзаконні нормативні акти, котрі формують положення законів у галузі протидії гібридним та іншим загрозам. Тому, окрім загальних принципів та концепцій, наявні також підзаконні акти, налаштовані на виконання законодавчих норм у певних галуззях протидії загрозам. Вони охоплюють акти уряду, накази та інструкції органів державної влади, котрі регулюють функціонування у певних галузях національної безп5еки, наприклад, у кібербезпеці, протидії дезінформації, охорони критичної інфраструктури тощо [5, с.74].

Дана концепція закріпила базу для майбутніх нормативно-правових документів, котрі формують взаємодію установ державної влади, громадських організацій та громадян у галузі національної безпеки. Відповідно до Головного закону України, координаційні функції у даній галузі, визначені за Радою національної безпеки і оборони України (РНБО), котра несе відповідальність за саме стратегічне планування та взаємодію діяльності у галузі національної безпеки [1].

Однак, Концепція мала переважно декларативний характер та не формувала чітких процедур реалізації норм. За останні два-три роки українське законодавство доповнилось нормативно-правовими актами, котрі регулюють чіткі сфери та механізми, налаштовані на забезпечення охорони від гібридних загроз та інших небезпек, котрі постали перед нашою державою.

Слід згадати і про перший галузевий Закон України «Про національну безпеку України», адже він став дуже суттєвим кроком у побудові нормативних засад для захисту національних інтересів та забезпечення безпеки особи, громадянського суспільства та держави від різних типів гібридних загроз. Цей Закон вперше закріпив національні інтереси України, котрі включають як

необхідності та цінності сучасного народу, так і цінності країни в цілому. Для прикладу, до національних інтересів відносять реалізацію охорони особи, захист громадянського суспільства та країни, котра включає великий аспект життєвоважливих галузей діяльності [11].

Сучасним законодавством сформовано системне розуміння національної оборони, котра охоплює взаємо доповнення безпеки громадського суспільства та країни, а також розгляд зовнішніх та внутрішніх аспектів національної безпеки. Він включає такі ключові галузі, як:

- зовнішньополітична сфера;
- військова діяльність;
- внутрішньополітична діяльність;
- економічна сфера;
- соціальна і гуманітарна діяльність;
- науково-технологічна діяльність;
- екологічна діяльність;
- інформаційна діяльність [12].

Також слід згадати, що у цьому Законі також формуються нормативна та техногенна галузь, хоча вони не були досліджені до цього, але законодавство чітко відображає критичні та потенційні загрози для кожної з цих галузей. До учасників забезпечення національної безпеки у документі включено громадян та їхні утворень, що говорить про прагнення залучити громадянське суспільство до захисту країни.

В свою чергу, закон цей не визначив конкретного інституційного виконання для подальшої реалізації його положень. Певні процедури та система органів, відповідальних за реалізацію завдань у галузі національної безпеки, лишились неповною та недослідженою. Це стало передумовою потреби подальшого розвитку законодавства та інституційних процедур, які б забезпечували раціональне виконання умов даного базового закону в умовах сучасних викликів і загроз.

У Законі України «Про національну безпеку України» значну увагу

приділено взаємодії державних інститутів та суспільства в забезпеченні національної безпеки. Однією з важливих новацій стало введення категорії громадської безпеки та порядку, поряд з державною безпекою, що підкреслює необхідність захисту не тільки державних інтересів, а й прав та свобод людини і громадянина. Це створює чітке бачення, що безпека громадян є важливою складовою загальної системи національної безпеки. Закон визначає, що забезпечення громадської безпеки та порядку є пріоритетним завданням діяльності сил безпеки, інших державних органів, органів місцевого самоврядування, посадових осіб та громадськості. Це свідчить про важливість спільних і узгоджених дій усіх цих суб'єктів у реалізації та захисті національних інтересів, а також у протидії загрозам [11].Також цей Закон визначає інституційну систему забезпечення національної безпеки, котра охоплює включає детальне формування галузей відповідальності та процедур взаємодії центральних органів виконавчої влади. Тому, на глобальному рівні формується узгоджена структура, в котрій кожен орган має своє певну ціль та відповідальність у процедурі захисту національних питань.

Загалом, даний Закон ще більше визначає на системному підході до дотримання безпеки в нашій державі, де керівну роль відіграють не лише національні установи, а й громадськість, наприклад, через активну участь у захисті прав і свобод, а також фіксуванні та знешкоджені гібридних загроз [11].

Вдосконалення українського законодавства України у галузі цивільного захисту від гібридних загроз та кібербезпеки є керівним моментом у дотриманні національної оборони держави, особливо в умовах сучасних загроз, які можуть мати різноманітний характер - від техногенних і природних катастроф до кібернетичних атак.

Закон України «Про основні засади забезпечення кібербезпеки України» є важливим етапом у сфері оборони інформаційних та цифрових структур, котрі є критично важливими для діяльності українського суспільства та економіки. Цей закон визначає перелік нових визначень та понять, котрі стосуються кібернетичних гібридних загроз:

- це формування наступних визначень «кібернетичний інцидент», «кібератака», «кібербезпека», що дає можливість чітко окреслити предмет і коло діяльності, що стосується кібербезпеки;
- визначення процедур виявлення, запобігання та нейтралізації загроз національній безпеці в кіберпросторі;
- підтримка сталого розвитку інформаційного суспільства і цифрової інфраструктури, а також формування передумов для безпечного комунікаційного середовища;
- створення державного реєстру об'єктів критичної інформаційної інфраструктури, для яких визначено вимоги кіберзахисту, індикатори кіберзагроз, а також вимоги до здійснення незалежного аудиту інформаційної безпеки [13];

Даний Закон також звертає увагу на важливості взаємовідношення між державними установами та приватним галузь у розділі кібербезпеки, котра є важливим для формування раціональної структури захисту критичної інфраструктури держави від кіберзагроз. В цілому, дані закони і їх виконання надають можливість посилити готовності України до реагування на сучасні виклики в різних галуззях, починаючи від техногенних катастроф до сучасних кібернетичних гібридних атак.

Закон України «Про основи національного спротиву» є важливим етапом у розвитку системи національної безпеки держави, котра порівнюється до сучасних загроз війни, наприклад, в умовах повномасштабної збройної агресії. Цей Закон визначає концепцію загального спротиву, котрий визначає активну участь людей у дотриманні національної безпеки та територіальної цілісності країни. Закон передбачає залучення усіх своїх громадян, незалежно від їх соціального статусу, до спротиву, котрий може включати не лише військову службу, але й інші форми активної участі в дотримання національної оборони [2].

Варто згадати, шо керівним моментом цього Закону є формування руху опору, налаштованого на відсіч збройній агресії, обороні державного суверенітету та територіальної цілісності держави, а також на меті ворогу завдати

великих втрат. Дані принципи відповідають теорії партизанської боротьби, де збирається весь народ для протистояння з ворогом. Також у ньому існують положення відносно підготовки громадян до діянь у випадку гібридній агресії, наприклад, через структуру військових зборів та покращення рівня цивільної оборони. Даний закон визначає на виклики сучасної безпеки, котрі потребують від країни не лише сильної армії та високого рівня громадянської активності [2].

Сучасна методика національної оборони України, визначена указом Президента України, є головним довгостроковим актом, котрий формує керівні методи у забезпеченні національної оборони та є важливим структурним елементом законодавчого та інституційного забезпечення національної боротьби.

Варто і зазначити Про Стратегію національної безпеки від 2015 року У даній Стратегії, визначалась потреба системного до охорони безпеки, в котрому збільшувалось значення не військових організацій. Тому, це давало розуміння, що звичні методи та засоби військової безпеки мають поєднуватися з новітніми процедурами політичної, економічної та соціальної стабільності, що надає можливість сформувати стабільність країни перед зовнішніми та внутрішніми гібридними загрозами [14].

Головні напрями безпеки:

- дотримання територіальної цілісності та суверенітету країни у міжнародних впливах;
- формування незалежної економічної ситуації та національних запасів для захисту від дійсних енергетичних викликів чи економічних агресій;
- боротьба з інформаційними гібридними загрозами та конфліктами, наприклад, в умовах гібридних війн, котрі включають інформаційні операції, дезінформацію;
- дотримання прав та свобод громадян, соціальної незалежності, забезпечення якості життя населення.

У нинішніх реалія даний документ вимагає правильної адаптації до викликів сьогодення, таких як гібридні загрози, кіберзагрози, інформаційні спеціальні операції та інші незвичні форми протидії, котрі активно

застосовуються державами-ворогами в сучасних операціях.

Отже, тактика та стратегія національної оборони України та сучасне законодавство, зокрема Закон України «Про основи національного спротиву», формують засади для виконання системного підходу до дотримання національної безпеки, в котрому важливу роль займає мобілізація не тільки збройних сил, а й всього народу держави для протидії сучасним гібридним загрозам [2].

Окрім цього, стратегія воєнної безпеки України 2021 року є також керівним актом, котрий формує керівні сфери вдосконалення воєнної оборони та силового потенціалу держави. Вона виходить із концепції стійкого та всеохоплюючої відсічі та опору, котрий зумовлює застосування усіх дієвих ресурсів та форм боротьби для протидії агресії, котра виходить за рамки звичайної воєнної сили. Застосування усього потенціалу країни, у випадку агресії визначено мобілізацію не тільки військових сил, а й політичних, економічних, міжнародно-правових (дипломатичних), духовних та культурних ресурсів, що забезпечить комплексний підхід до відсічі загрози. Стратегія наголошує на здатності застосування не тільки традиційних методів збройної боротьби, а й асиметричних дій – наприклад, застосування невоєнних засобів для одержання військових та політичних завдань. Даний підхід має охоплювати сучасні методи гібридної війни, включаючи інформаційні операції, кіберзагрози та інші нетрадиційні гібридні методи.

Одним з керівних методів є також відшукування надійних способів комунікації з громадянами та дотримання їхніх прав та свобод життєдіяльності в умовах масштабної агресії. Дані положення мають охоплювати в себе як роз'яснювальну діяльність, так і формування структури цивільного захисту.

Указ Президента України від 17 вересня 2021 р. «Про Стратегічний оборонний бюлетень України» формує головні сфери реалізації воєнної політики держави в сутності всеохоплюючої оборони.

Головні норми Стратегічного оборонного бюлетеня:

- у цьому нормативному акті визначено перспективний стан Збройних Сил України, наприклад, головні здатності сил оборони, котрих варто отримати

для забезпечення національної оборони. Це відноситься як прямо військових структур, так і їх взаємодії з іншими державними силами, в тому числі, органами безпеки та цивільного захисту;

- закріплено певні напрямки вдосконалення сил оборони, де керівними є покращення підготовки особового складу, покращення технічного обладнання особового складу та взаємодія з союзниками та партнерами для покращення оборони країни;

- стратегічний військовий документ визначає структурні елементи теорії стабільності, наприклад ідею боротьби з викликами на гібридні загрози. Тому, потенційні загрози мають бути досліджені на початкових етапах, та структура оборони має бути здатна адаптуватися до перемінних умов, охоплюючи новітні технології та гібридні методи здійснення військових дій;

- документ визначає керівні положення, котрі мають бути отримані, і визначення для аналізу раціональності оборонної системи. Включає тільки формування раціональної оборони, а й дотримання взаємодопомоги між структурними елементами національної безпеки [14].

Отже, цей Стратегічний оборонний бюлетень України та Стратегія воєнної безпеки є нормативними актами, які взаємодоповнюють один одного та реалізовують національну оборону та надають можливість розвивати оборонну політику враховуючи сучасні гібридні загроз. Вони формують головні сфери розвитку оборонних здатності України та допомагають інтегрувати усі національні та громадських системи у забезпечення стійкості перед зовнішніми агресорами.

Документи Європейського Союзу, що розглядають гібридні загрози, стали основою для формулювання загальної стратегії боротьби з ними.

Варто виділити головні нормативні акти Європейського Союзу для протидії гібридним небезпекам:

- «Спільна структура протидії гібридним загрозам – відповідь Європейського Союзу» (2016), даний документ став нормативною базою для одного підходу до фіксування та боротьби гібридним загрозам на рівні

Європейського Союзу. Він формує керівні процедури боротьби та взаємодії між країнами-учасниками;

- «Підвищення стійкості та посилення можливостей для подолання гібридних загроз» (2018), даний документ охоплює тлумачення стійкості та визначає на потребі вдосконалення особливих інструментів для подолання гібридних небезпек, наприклад у кіберпросторі та в розумінні дезінформаційних конфліктів;

- «Звіт про впровадження Спільної програми протидії гібридним загрозам 2016 року та Спільного повідомлення 2018 року» (2020). Даний звіт став результатом попередньої діяльності Європейського Союзу, показуючи певні результати в реалізації програми боротьби з гібридними загрозами;

- Стратегія безпеки ЄС 2020, дана стратегія закріплює головні сфери ЄС у дотриманні безпеки, охоплюючи боротьбу з гібридними загрозами, наприклад, в розумінні нових викликів, таких як пандемії, зміни клімату та кіберзагрози [15];

У цьому нормативному акті визначено галузі де можуть бути застосовані дані гібридні загрози. Сформовано декілька головних аспектів, в котрих можуть фіксуватись внутрішні та внутрішні гібридні загрози:

- гібридні атаки на критичну інформаційну інфраструктуру, хакерські атаки;

- атаки на критичну інфраструктуру, атаки на енергетичні, транспортні, фінансові системи;

- охорона фінансової структури, протидія фінансовим маніпуляціям та неправомірне використанню грошових ресурсів;

- боротьба з насильницьким екстремізмом та радикалізації, боротьба з тероризмом та екстремізмом;

- у сфері охорони здоров’я, дотримання оборони в передумовах пандемії та біологічних загроз;

- космічні та морські загрози, зі сторони ворожих дії в цих сферах [15].

Країни-учасники Європейського Союзу несуть головну відповідальність за протидію з гібридними конфліктами, адже це покладається на певні країни,

наприклад, в аспекті їхніх національних меж. У випадку, коли гібридна загроза виходить за рамки національних меж або вимагає спільних завдань, юридична відповідальність спирається на організації Європейського Союзу, а саме: Європейська Комісія, Верховний представник ЄС з питань зовнішньої політики та безпеки, а також наступні нові структури:

- HFC (Hybrid Fusion Cell), спеціалізований центр для моніторингу та вивченням гібридних загроз;
- East Stratcom Task Force, група, котра займається протидією дезінформаційним кампаніям, в тому числі зі сторони Росії;
- Центр передового досвіду для протидії гібридним загрозам, здійснює вивчення та формування нових методів до протидії з гібридними загрозами.

Нормативно-правові акти Європейського Союзу, а саме документ 2018 року та Стратегія 2020 року, були налаштовані на протидії з певними зовнішніми гібридними загрозами:

- хімічні, біологічні, радіологічні та ядерні загрози: ці загрози є частиною гібридних атак, тому для їх протидії розроблені спеціалізовані заходи.
- кіберзагрози, документ 2018 року акцентує увагу на захисті критичної інформаційної інфраструктури та боротьбі з кібератаками.
- дезінформація, зокрема під час пандемії COVID-19, Стратегія 2020 року підкреслює важливість боротьби з дезінформацією та фейковими новинами, особливо в умовах кризових ситуацій [15].

Вищезазначені нормативні документи визначають важливий характер співпраці з офіційними міжнародними організаціями. Активна взаємодія між ЄС і НАТО для визначення методів та заходів відносно боротьби гібридним загрозам. Європейський Союз також вдосконалює взаємодію з міжнародними союзниками, в тому числі в рамках проекту G7 та інших багатонаціональних проектів, для дотримання колективної оборони та стабільності. Дані документи визначили основу для структурної боротьби з сучасними гібридними конфліктами, охоплюючи різні методи до кібербезпеки, боротьби з дезінформацією та захисту критичної інфраструктури. Європейський Союз продовжує працювати над

покращення даної правової основи, з урахуванням нових викликів та загроз в умовах глобалізації та постійного технологічного розвитку [10].

Тому, варто підсумувати, що Стратегія безпеки Європейського Союзу 2020 року, справді, є керівним актом, у значені адаптації Європейського Союзу до новітніх гібридних загроз. Вона є більш чіткою та налаштованою у своєму значенні до даних гібридних загроз, на відміну від інших стратегій, і визначає на важливість сучасного тлумачення даних викликів.

У Стратегії безпеки 2020 року гібридні загрози займають важливе положення, і це показується у другому розділі під назвою «Боротьба з загрозами, що розвиваються». Даний підрозділ включає не тільки звичні загрози, такі як збройні конфлікти чи тероризм, але й новітні форми боротьби, включаючи кіберзагрози, дезінформацію, маніпуляції через медіа та інші асиметричні методики та відношення. У даному значенні контексті Європейський Союз визнає потребу структурної та комплексної стратегії для протидії таким загрозам.

Тому, на сьогодні дана Стратегія ЄС визначає на важливості покращенні міждисциплінарних методів до боротьби з гібридними загрозами, де важливу роль займає взаємодія між країнами-учасниками ЄС, НАТО та іншими міжнародними союзниками. Охоплення таких сфер, як кібербезпека, боротьба з фінансовими злочинами та зловживаннями, контрзаходи в інформаційних операціях, є керівними для успішної протидії гібридним загрозам [15].

Також варто і зазначити, що як визначено в стратегії, звичайні закони війни, і ті, котрі закріплені в Женевських конвенціях 1949 року та додаткових протоколах 1977 року, не можуть належним чином визначати новітні гібридні операції, адже ці нормативні акти в основному відносяться до звичайних війн. Гібридні загрози часто мають нелінійний характер та включають не тільки військові, але і нетрадиційні економічні, соціальні та інформаційні методи впливу, що робить саме і застосування традиційних принципів jus in bello (права війни) [16].

У сучасних реаліях, коли військова конфлікти та сутички стають все більш складними та масштабними, а методи здійснення протидії змінюють межі між

мирними та воєнними діями, Женевські конвенції та традиційне міжнародне гуманітарне право стали не ефективними. Вони не можуть дотримати ефективну нормативну основу базу для деескалації військових конфліктів, котрі формуються в умовах гібридних війн, де часто відсутні чіткі лінії бойового зіткнення та зупинення ворога.

Ефективна реалізація Женевських конвенцій у конфліктах «сірої зони», які характеризуються розмитими межами між станом війни та миру, може бути обмеженою через низку чинників. Ці конфлікти зазвичай поєднують невоєнні засоби впливу, такі як економічний тиск, пропаганда, кібероперації, із застосуванням військових методів. У таких умовах традиційні механізми міжнародного гуманітарного права (МГП), включаючи Женевські конвенції, можуть бути недостатньо ефективними. Учасники таких конфліктів часто уникають оголошення війни або офіційного визнання свого залучення, що ускладнює застосування міжнародного гуманітарного права. Часто конфлікти ведуться за участю недержавних учасників, наприклад, приватних військових компаній, сепаратистських угруповань чи терористичних організацій, які не підпадають під чітке регулювання Женевських конвенцій. Женевські конвенції застосовуються до міжнародних та внутрішніх збройних конфліктів. У випадках «сірої зони» складно визначити, чи йдеться про збройний конфлікт, особливо коли немає відкритого використання військової сили. Женевські конвенції є фундаментом міжнародного гуманітарного права, але їх ефективність у конфліктах «сірої зони» обмежена через специфіку сучасних гібридних загроз. Для забезпечення їхньої дієвості необхідно розширити правове регулювання, модернізувати механізми моніторингу й притягнення до відповідальності, а також адаптувати їх до нових реалій [16].

Враховуючи, що гібридні загрози включать різноманітні галузі, охоплюючи кіберзагрози, включаючи інформаційну боротьбу, тероризм, зловживання технологіями, традиційні нормативні процедури, включаючи Женевські конвенції, проявляються неналежними для конкретної регламентації дій в умовах гібридних сутичок. В умовах гібридних загроз стає дуже важливо адаптувати

міжнародне гуманітарне право та сформувати нові процедури для їх реалізації в таких нових умовах, де активна агресія може бути виражена не тільки через військові дії, а й через нетрадиційні методи, які є менше помітні.

Тому, на сьогодні Стратегія безпеки ЄС 2020 року є важливим етапом у сфері адаптації Європейського Союзу до нових протидій у галузі безпеки. Вона формує потребу структурного підходу до боротьби з гібридними загрозами, охоплюючи формування нових нормативних та стратегічних інструментів для реалізації стабільності перед такими загрозами. У зв'язку з тим, що традиційні процедури правового визначення, як, наприклад, Женевські конвенції, не є досить раціональними для визначення сучасних гібридних дій, важливо брати до уваги на адаптацію міжнародного законодавства до нових умов сучасних конфліктів.

Суттєва зосередженість до кіберзагроз у сучасних реаліях, зокрема в розумінні України, є результатом потреби адаптації положень національної безпеки до нових викликів, котрі створюються через розвиток інформаційних технологій та глобалізацію.

Варто загадати таке визначення, як «сіра зона» та значення недержавних агресорів, адже нинішні військові конфлікти часто включають нелінійні та нетрадиційні засоби здійснення боротьби, стає важко визначити чіткі лінії між миром і війною. «Сіра зона» характеризується відсутністю прозорості у діях як державних, так і недержавних акторів. Недержавні структури, такі як приватні військові компанії, хакерські групи чи інформаційні кампанії, можуть впливати на ситуацію в державі без явних військових дій, що робить контроль і реагування на такі загрози значно складнішими [17, с.127].

Зміну акценту в міжнародному гуманітарному праві з національного суверенітету на гуманітарні основи прав та свобод людини формує правову невизначеність, яку активно використовують як державні, так і недержавні учасники. Тому, даний факт дозволяє зловживати правовими процедурами для виправдання або знецінення їх дій у таких «сірих зонах».

Дотримання сучасного міжнародного права та його ключові моменти в час

активних соціальних мереж також мать велике значення. Нинішні реалії, наприклад, розповсюдження фейкових та не правдивих новин та зловживань через соціальні мережі, ускладнюють реалізацію дотримання міжнародного гуманітарного права, наприклад, в галузі прав людини. Створення неправильних тлумачень нормативних законів та їх застосування для виправдання дій або для оскарження дій ворогів стає дедалі більшою проблемою, з котрою зустрілись багато країн та міжнародних організацій.

В час активних соціальних мереж будь яка інформація може розповсюджуватись миттєво, що дає можливість маніпулювати суспільною думкою, збільшувати недовіру до діяльності влади та підривати авторитет нормативно-правових положень. Даний факт підвищує значущість вдосконаленню нормативних положень, котрі будуть мати можливість зможуть правильно реагувати на нові форми гібридних загроз.

Тому, хочу згадати, що в нашій державі за останні часи наявний значний прогрес в формуванні інституцій та технічних методів для боротьбі з кіберзагрозами. Важливим етапом стало формування Національного координаційного центру кібербезпеки, котрий став важливим органом для кооперування дій з питань кіберзахисту на рівні Ради національної безпеки і оборони України (РНБО). Даний факт говорить про прагнення країни реалізувати цілісність та стійкість національної кіберінфраструктури. Стратегія кібербезпеки України, сформована враховуючи найкращі результати практики НАТО та інших міжнародних учасників, охоплює не тільки державні органи, але й учасників господарювання, громадські утворення та окремих осіб. Це дає можливість сформувати більш раціональну структуру національної безпеки, котра розрахована на широке співробітництво та інтеграцію різних секторів [17].

Враховуючи те, що кіберзагрози постійно мають міжнародний характер та не обмежені певними кордонами, важливим елементом є міжнародна робота у даній сфері, в тому числі з учасниками з НАТО. Діяльність міжнародних союзників забезпечує можливість надати потрібну підтримку у боротьбі з кіберзагрозами, здійснити обмін інформацією та розвивати спільні стратегії [18].

Враховуючи те, що з огляду на швидкісний розвиток сучасних технологій, досить вагомим фактом, є те, щоб українська кіберстратегія була гнучкою та постійно адаптувалася до нових гібридних загроз.

Тому, важливу увагу слід приділяти підготовці особового складу, формування новітніх технологій захисту та покращенню кіберстійкості державних та приватних інституцій. Також варто збільшувати значущість громадянського суспільства в проблематиці кібербезпеки, наприклад, через навчання людей, здійснювати роз'яснювальну роботу та формування інструментів для швидкого доступу до ресурсів для захисту від кіберзагроз.

Таким чином, сьогодні Україна посилює потужну інституційну систему для протидії кіберзагрозам, спираючись на світові стандарти.Проте, для раціональної протидії сучасним гібридним загрозам варто активно залучати всі сектори сучасного суспільства, в тому числі бізнес, громадські організації та окремих громадян. Зважаючи на те, що складність сучасних загроз, національна оборона України вимагає постійного розвитку нормативних та технічних методів, а також щільної взаємодії на міжнародній арені.

РОЗДІЛ 2
АНАЛІЗ ПРАВОВИХ МЕХАНІЗМІВ ПРОТИДІЇ ГІБРІДНИМ ЗАГРОЗАМ

2.1 Аналіз практики застосування правових норм у протидії гібридним загрозам у світовій практиці

Аналіз практики застосування правових норм у протидії гібридним загрозам у світовій практиці є важливим аспектом дослідження сучасної безпеки. Гібридні загрози включають поєднання військових, економічних, інформаційних, кібернетичних та політичних інструментів для досягнення стратегічних цілей.

Сучасне міжнародне право передбачає відповідальність держави за агресивні дії, включаючи кібернетичні атаки, підтримку тероризму або використання інформаційної пропаганди. Однак визначення конкретної відповідальності в умовах гібридних загроз ускладнене через труднощі в ідентифікації джерела загрози. Порушення інформаційного або кібернетичного простору іншої держави може розглядатися як порушення суверенітету, що є забороненим згідно зі Статутом ООН. Європейський Союз прийняв низку стратегій, включаючи Стратегію кібербезпеки (EU Cybersecurity Strategy), яка поєднує правові та організаційні механізми для протидії гібридним загрозам. США, використання закону про протидію дезінформації (Countering Foreign Propaganda and Disinformation Act) для боротьби з іноземним втручанням у внутрішні справи, зокрема в кіберпросторі [15].

Варто відмітити, що спільна структурна система співпраці НАТО та ЄС у сфері боротьби з гібридними загрозами затверджена Міжвідомчою комісією з боротьби з гібридними загрозами, котру було засновано Європейською комісією та Європейською зовнішньополітичною службою. Дана комісія налаштована кооперувати сили відносно інформування про функціонування європейських інститутів, котрі займаються боротьбою з гібридним загрозам, а також

підтримувати взаємодію обміну інформацією та спільну діяльність у даній галузі. До керівних аспектів євроатлантичної структури підготовки до попередження та запобігання гібридних загроз відносять системні навчання, котрі відбуваються в межах співпраці НАТО та ЄС. Дані спільні навчання включають різні сфери гібридної війни та конфліктності, що дає здатність як військовим, так і цивільним спеціалістам покращувати власні навички та досвід для раціональної протидії цим загрозам. Навчання також відбувається із залученням сучасної продукції та експертних заключень профільних мозкових центрів, котрі спеціалізуються на вивченнях гібридних загроз. Дані аналітичні матеріали дають можливість більш глибоко бачити сутність та процедуру перемін гібридної конфліктності, а також створювати більш правильні та сучасні стратегії протидії.

Велика Британія запровадження законодавства, спрямованого на підвищення прозорості в політичній рекламі та захист критичної інфраструктури. Слід виділити наступні дієві механізми протидії гібридним загрозам, по-перше, це розробка та впровадження нових міжнародних правових норм, які адаптуються до гібридного характеру сучасних загроз.

По-друге, створення механізмів обміну інформацією між державами та міжнародними організаціями.

По-третє, підвищення ефективності санкційних режимів проти держав, що застосовують гібридні методи агресії.

Тому, Гібридні загрози потребують комплексного підходу, що поєднує правові, технологічні, економічні та дипломатичні інструменти. Хоча існуючі правові норми частково забезпечують протидію, їх удосконалення та адаптація до нових реалій залишаються важливим завданням міжнародної спільноти.

Альянс НАТО прийняв концепцію «протидії гібридним загрозам», яка включає адаптацію статті 5 Північноатлантичного договору для кіберзагроз та інформаційних атак. НАТО, справді, є першою міжнародною організацією, котра сформувала концепцію гібридних загроз та нормативно виокремила їхні властивості. Проте, на нині Європейський Союз має більш вдосконалено та системну нормативно-правову основу для протидії з цим різновидом загроз, що

була сформована через згуртуванню власної сили на рівні Європейського Союзу і країн-учасників [17].

Також слід зазначити, що у 2016 році Європейська Комісія разом з Верховним представником ЄС із закордонних справ і політики безпеки почили формування програми протидії гібридним небезпекам. Вони започаткували Спільну систему боротьби гібридним загрозам – відповідь Європейського Союзу. Даний акт також загально відомий як Спільна рамкова програма 2016 року, закріплює керівні методи для захисту ЄС від гібридних небезпек. У цій стратегії вказано багато заходів для боротьби з гібридними впливами, виконання котрих покладено на Європейську Комісію, Верховного представника та спеціалізовані структури, зокрема Hybrid Fusion Cell (HFC) - Центр для аналізу гібридних загроз [15].

HFC створений у рамках Центру розвідки та ситуації ЄС (EU INTCEN) та Європейської служби зовнішніх дій (EEAS). Головне завдання HFC полягає в одержанні, обробці та обміні конфіденційною та загальнодоступною інформацією відносно індикаторів та попереджень щодо гібридних загроз. Він має відношення з представництвами ЄС, агентствами Комісії, національними відповідними пунктами країн-учасників та іншими органами для забезпечення ефективного реагування. Європейська Комісія реалізовує співпраці між державними установами та певними установами Європейського Союзу для протидії з гібридними небезпеками. У межах співпраці було надано рекомендації державам-членам сформувати національні пункти реагування, котрі мають взаємодію з HFC для обміну важливою інформацією, аналізу загроз та дотриманням безпечного зв'язку з ЄС [19].

Таким чином, Європейський Союз створив системний підхід до протидії гібридним небезпекам, котрий охоплює взаємодію між різними установами ЄС та країнами-учасниками. Це дозволяє виконувати не тільки реагування на загрози, але й раціональне попередження та координацію дій для їхньої нейтралізації.

Документ, присвячений протидії гібридним загрозам, наголошує на

необхідності ідентифікації та усунення вразливостей у ключових секторах, таких як інфраструктура, ланцюги постачання та суспільство. Щодо енергетики, то цей сектор є критично важливим, оскільки забезпечення стабільного енергопостачання та безпеки ядерної інфраструктури є основою національної безпеки. В документі відзначається потреба диверсифікації джерел енергії та покращення стандартів безпеки для збільшення стійкості енергетичної інфраструктури, особливо у ядерній галузі [19].

Щодо безпеки транспорту та мережі постачання, то цей акт наголошує на міжгалузевій взаємодії між цивільними та військовими угрупуваннями для оборони суттєво важливих морських об’єктів, важливих шляхів поставки та природних морських ресурсів. Велике значення зосереджується захисту морської торгівлі та ресурсів, котрі можуть бути піддані гібридним атакам.

На сьогодні, сучасні гібридні атаки також стосуються космічної інфраструктури, котра охоплює структури супутникового зв’язку. Тому, це документ вимагає здійснити постійний супутниковий зв'язок як надважливий структурний елемент національної безпеки. Нинішні реалії воєнних дій показали, що в Україні відсутні нормативні процедури для оперативного втручання на кризові випадки, взаємопов’язані з гібридними атаками. Імплементація наявний положень міжнародного гуманітарного права в українське законодавство може сильно покращити готовність держави до похожих загроз. Це надасть Україні можливість бути краще зібраною та готовою для зупинення гібридних атак або зменшення їхніх результатів [29, с.160].

Таким чином, документ підкреслює важливість не тільки вдосконалення нормативно-правових актів, але й реалізації заходів, спрямованих на підвищення стійкості основних секторів інфраструктури, що в умовах сучасних гібридних загроз є необхідністю для забезпечення національної безпеки. Документ також акцентує увагу на забезпеченні безпеки у таких важливих сферах, як кіберпростір, економіка та будівництво. Особлива увага приділяється питанням кібербезпеки та захисту від гібридних загроз у цифровій сфері, яка є вразливою до атак з боку недружніх держав або організацій. Крім того, було визначено

стратегію взаємодії з НАТО як ключовий елемент для підвищення ефективності протидії гібридним загрозам.

Співробітництво у сфери співпраці між ЄС і НАТО включають обмін інформацією та спільне вивчення загроз для реалізації актуальних даних про становище безпеки у різних районах. Взаємна співпраці в даній сфері налаштована на взаємну протидію дезінформації та пропаганді, а також на покращенні стійкості інформаційного простору. Співпраця у галузі кібербезпеки надає можливість ЄС і НАТО спільними зусиллями формувати раціональні методи захисту від кібератак, що є досить актуальним у теперішніх умовах.

ЄС і НАТО взаємодіють також у спільному плануванні дій для оперативного реагування на потенційні кризи, котрі можуть бути завдані гібридними загрозами.

Також міжнародні організації повинні мати єдину інформаційну політику відносно загроз для більш раціональної роботи та швидкого реагування. Ця взаємна співпраця покращує обидві організації та надає можливість повторювання зусиль, в той час, покращуючи якість захисту критичної інфраструктури. Прикладами успішної співпраці є створення Центру передового досвіду НАТО з кіберзахисту (Таллінн, Естонія), це платформа для обміну досвідом між країнами-членами НАТО і партнерами. Європейська мережа та інформаційна безпека (ENISA), співпраця з ЄС та державами-членами для стандартизації підходів до кібербезпеки.

Міжнародна організація цивільної авіації (ICAO), а саме встановлення спільних стандартів безпеки в авіації для протидії терористичним загрозам. Єдина інформаційна політика міжнародних організацій є невід'ємним елементом у боротьбі з сучасними гібридними загрозами. Вона дозволяє швидко адаптуватися до нових викликів, зменшувати ризики, пов'язані з критичною інфраструктурою, та ефективно використовувати доступні ресурси. Успішна координація зусиль на глобальному рівні стає важливим фактором у забезпеченні міжнародної стабільності [20].

Для нашої держави, котра є офіційно не є членом НАТО, також є важливим

вказати тактику та стратегію взаємодопомоги з НАТО та іншими світовими установами у національному законодавстві. Це надасть можливість здійснити більш структурний підхід до протидії гібридним загрозам, зважаючи на досвід та практику діяльності НАТО.

Тому, подальша адаптація української нормативної бази до стандартів НАТО надасть Україні збільшити стійкість у боротьбі з гібридними небезпеками та інтегруватися у європейські структури безпеки. Варто і зазначити, що Європейський Союз дуже активно працює над боротьбою з гібридним загрозам, котрі дуже часто є загрозою для стійкості та оборони європейських держав. Головною для даної діяльності стали Спільна рамкова програма 2016 року та Спільне повідомлення 2018 року, котрі визначили основу для формування стратегії протистояння гібридним викликам, в тому числі в інформаційній галузі. У межах даної стратегії ЄС кожного року показує звіти, котрі формують реалізацію методів, визначених цими документами [21].

Останній опублікований звіт ґрунтується на передумовах, зумовлених гібридною політикою росії, наприклад, на організаціях дезінформації, котра збільшилась в межах війни Росії проти України. У цьому значені важливу увагу вказано саме інформаційним атакам, налаштованим на європейське громадське суспільство, та заходам Європейського Союзу, налаштованих на протидію даним загрозам. Цей звіт визначає значущість захисту інформаційної безпеки, дотримання стабільності усередині Європейського Союзу та посилання стабільності європейських інститутів перед гібридними загрозами. Дані щорічні звіти реалізовують керівну роль у процедурі моніторингу дій, налаштованих на посиленні європейської політичної системи, адже вони не тільки визначають досягнення, але й слугують базою для подальшого покращення процедур захисту, забезпечуючи адаптивність та раціональність європейських стратегій у боротьбі з новітніми небезпеками. Звіти також зумовлюють співпрацю між країнами-членами Європейського Союзу, допомагаючи обміну практикою та погодженню заходів для покращення загальної інформаційної витривалості [22].

2.2 Український досвід правового регулювання боротьби з гібридними загрозами

Особлива актуальність питання гібридної війни для України зумовлена реаліями протистояння з росією, котра досить використовує даний новий типаж військових та інформаційних дій проти України. На основі мого вищезазначеного визначення тлумачити гібридну війну слід як новий різновид конфлікту, котрий формується між країнами або з участю недержавних учасників, терористичних організацій та діалектично взаємопов'язаний із обмеженням звичайної війни у міжнародному гуманітарному праві як засобу національної політичної ситуації. Україна є одним із ключових прикладів держави, котра зіткнулася з гібридними загрозами, зокрема з боку Російської Федерації. Цей досвід сформував унікальні підходи до правового регулювання боротьби з гібридними загрозами, що охоплюють як національне законодавство, так і міжнародні ініціативи.

У більш вужчому тлумаченні гібридна війна, за думкою більшості військових фахівців, є системою регулярних та нерегулярних засобів здійснення бойових дій. В той час, у широкому значенні котрий краще відображає реалії сучасного конфлікту, гібридна війна включає різні ворожі дії, котрі охоплюють неофіційні, неавторизовані або замасковані воєнні й невоєнні методи відношення. Дане протистояння налаштоване на підрив та послаблення усіх галузей суспільного життя, в тому числі, на функціонування державних сфер, економічну стабільність, соціальні комунікації та формування поведінки населення. Дане тлумачення визначає багатокомпонентність та комплексність загроз, котрі формує гібридна війна, вимагаючи від країн формуванні раціональної структури протидії як на рівні військової, так і невійськової безпеки. Тому, для України надзвичайно важливо адаптувати власні стратегії захисту, включаючи практику світової спільноти та інтегруючи процедури міжнародного гуманітарного права для протидії таким гібридним викликам [23, с.221].

Тому, сьогодні гібридна війна як певні інтелектуальні та протиправні дії є

актуальною через здатність досягти великих результатів при досить малих витратах та найменших репутаційних умовах. Це робить її привабливим інструментом у сучасних міжнародних відносинах, де подібні тактики можуть мати великий вплив без прямої збройної агресії. Такий підхід означає, що гібридна війна не є тимчасовим явищем, а стає дедалі частішим чинником у практиці та політиці в цілому. Тому, стратегія та процедура протидії на неї має бути не стандартним планом, а динамічним методом, котрий здатний адаптуватися до новітніх викликів та загроз. Це схоже на незавершену відкриту політичну філософію, де основними незмінними системними елементами залишаються цінності та принципи права.

У даному розумінні актуальною є теорія державної стабільності, котра налаштована на дотримання та покращення країни та громадського суспільства, дотримання їхньої безпеки, охорона національних інтересів, а також підтримку політичної та культурної самовпевненості. Даний підхід позволяє виділяти гібридну війну як постійний процес, котрий потребує постійної готовності та адаптивності до кожної гібридної атаки [23].

Концепція національної стійкості також допомагає відрізняти різні види загроз та викликів, що надає можливість раціональніше структурувати сили для їх нейтралізації та формувати правильні відповіді, налаштовані на збереження стабільності та розвитку в умовах нових ризиків. Виклики сучасності включають всі галузі нашого життя, а саме: соціальну, економічну, технологічну, екологічну та гуманітарну. Їхня сутність є різною: починаючи від неврегульованих соціальних питань та ресурсних обмежень до конфліктів певних груп населення та недоліків гуманітарного вдосконалення. Дані сучасні виклики є факторами уразливості громадського суспільства, проте, в той же час, вони можуть стати точками зіткнення за певної умови стратегічного методу до їх вирішення. Як зазначається в аналізі, державна політична ситуація та суспільні відносини, котрі ґрунтуються на чіткості, інклюзивності, оперативності, стратегічному плануванні та розумовому здійсненні, вправі перемінити ці виклики на здатності для покращення громадського суспільства, покращення якості життя населення

та покращення державної стабільності.

Однак, у випадку коли дані виклики лишаються без достатньої уваги, вони можуть перерости в небезпеку для особи, сучасного суспільства та країни в цілому. Здебільшого це відноситься умов гібридного зіткнення, коли уразливі точки громадського суспільства можуть бути місцем для зовнішнього перешкоджання та різних маніпуляцій. Даний взаємозв'язок між економічним, технологічним, екологічним та суспільним вдосконаленням тільки закріплює даний взаємовплив, роблячи виклики багатоплановими та дуже важкими для врегулювання.

Слід зазначити, що Україна передбачила дані фактори у стратегічному підході до дотримання національної охорони. Наприклад, Указ Президента України від 17 вересня 2021 року «Про Стратегічний оборонний бюлетень України» закріплює керівні сфери воєнної політики країни в умовах воєнного стану. Даний документ визначає всеохоплюючий захист, закріплює майбутню модель Збройних Сил України, їх головні можливості, стратегічні завдання та очікування. У цьому бюлетені також визначається структурні елементи теорії стабільності, котрі взаємопов'язують виклики із здатністю їх переростання у гібридні загрози [14].

Тому, властивістю даного методу є акцент на прогнозі на майбутнє, вивченням та підбору ефективних відповідей та результатів. Це дозволяє не тільки реагувати на дійсні загрози, однак і створювати безпечне середовище, стабільне до майбутніх викликів. Тому, наша держава інтегрує у свою тактику захисту новітні методи до дотримання національної незалежності, котрі ґрунтуються на дослідженні вразливостей та зміцненні адаптивних здатностей. Це дуже потужний крок до посилення країни в умовах як внутрішніх, так і зовнішніх умов, а також у відношенні інтеграції до європейської безпекової спільноти.

Хочу зазначити, що саме Стратегічний оборонний бюлетень України базується на нормах Закону України «Про основи національного спротиву» та теорії всеохоплюючого захисту, котрий спрямований на максимальне

застосування сили. країни та громадського суспільства в умовах, коли дотримання воєнної переваги з ворогом є дуже важким. База даної тактик є ідея незвичних та непрямих дій, визначена у Стратегії національної оборони України [14].

Незвичні дії досліджуються як метод дотримання переваги за рахунок застосування уразливих місць ворога та максимального дотримання своїх сильних сторін. Це охоплює по-перше, перехоплення ініціативи – дії, котрі заставляють ворога реагувати на неочікувані сценарії. По-друге, забезпечення руху сил, формування передумов для маневрування збройними силами та методами з ціллю уникнення сутичок. По-третє, моральна перевага, тобто застосування певних факторів національних цінностей та громадської підтримки, котра дотримує моральний підйом захисників та демотивує ворога. До інформаційної боротьби слід віднести заборону російських телеканалів, онлайн-ресурсів та соціальних мереж та використання фактчекінгових платформ для боротьби з дезінформацією.

Україна є одним із лідерів у розробці правових та інституційних механізмів для протидії гібридним загрозам. Її досвід є важливим не лише для внутрішньої безпеки, але й для міжнародної спільноти, яка може використовувати українські практики як модель для адаптації до власних викликів.

Пропаганда як інструмент інформаційної війни має широкий спектр методів, спрямованих на маніпулювання суспільною свідомістю. Вона використовується для формування вигідних для ініціатора наративів, зниження довіри до опонента та мобілізації власної аудиторії. Одним із ключових методів є створення викривленого образу реальності через маніпуляції фактами, емоціями та цінностями. Пропаганда часто ігнорує або спотворює реальні події, замінюючи їх фейками чи вигаданими версіями. Цей метод спрямований на створення альтернативної реальності для цільової аудиторії. У пропаганді часто використовується метод дискредитації тих, хто не погоджується з офіційною позицією. Це дозволяє ізолювати опонентів, маргіналізувати їх і перешкодити формуванню альтернативної думки. Пропагандистські методи створення образу

жертви, перекладання відповідальності, ігнорування фактів та стигматизації незгодних демонструють високий рівень маніпуляції свідомістю. Вони використовуються для виправдання агресії, підтримки контролю над масами та підриву довіри до опонентів. Для ефективної протидії таким методам необхідно впроваджувати освітні програми з медіаграмотності, розвивати незалежні ЗМІ та посилювати міжнародну співпрацю у боротьбі з дезінформацією [23].

Росія активно використовує інформаційні технології в рамках гібридної війни, зокрема спеціальні пропагандистські акції, спрямовані на дестабілізацію ситуації в Україні та маніпуляцію свідомістю громадян. Для прикладу, це висвітлення подій Революції Гідності, а саме те що російська пропаганда подавала Майдан як «державний переворот», фінансований Заходом, дискредитуючи прагнення українців до демократії. Наступним яскравим прикладом є пропаганда про Донбас, де активно використовувалися наративи про «геноцид» російськомовного населення на Донбасі, щоб виправдати збройну агресію. Також анексія Криму, це створення образу «законного повернення» Криму до РФ через спотворення історичних фактів та маніпуляцію міжнародним правом. Застосування цих методів пропаганди дозволяє РФ досягати певних результатів у гібридній війні, але водночас викликає зростання обізнаності у суспільстві про маніпулятивні техніки. Протидія таким кампаніям вимагає комплексного підходу, що включає підвищення медіаграмотності населення, створення ефективної системи розвінчування фейків, активну інформаційну політику з боку держави та міжнародних партнерів. У нашій ситуації політичний шлях вирішення конфлікту повинен бути ключовим. Для цього уряд країни та міжнародні організації, такі як ООН повинні прикладати зусилля, щоб виявляти можливі конфлікти. Для цього вони повинні проводити моніторинг у різних галузях міжнародних відносин, соціальній сфері у конкретній країні, заздалегідь проводити законодавчу роботу для забезпечення прав національних меншин і т.д.

Тому, організація функціонування в умовах гібридної боротьби потребує інноваційного переосмислення, гнучкості та адаптації до передумов, котрі постійно перемінюються. Важлива зосередженість у Стратегічному оборонному

бюлетені виділяється сучасним методам здійснення воєнних дій. Орієнтування на кіберпростір ворога, здійснення запобіжних заходів, налаштованих на порушення функціонування кіберінфраструктури ворога. Кіберозахист держави – захист особистий цифрових структур та гібридної інфраструктури. Мережоцентричний засіб підходу, а саме застосування новітніх інформаційних інновацій для раціональної координації дій у реальному часі, об'єднання розвідки, військових підрозділів та керівництво в одну інформаційну систему [24].

Дана Стратегія визначає активне запровадження запобіжних методів, котрі допомагають вчасно виявляти та нейтралізувати гібридні небезпеки. Це включає як фізичну оборону, так ефективне функціонування в інформаційному та кіберпросторі. Нормативний акт звертає увагу на важливому значенні співпраці між певними складовими сил оборони та їх інтеграції у одну цілісну систему, котра може працювати швидко та ефективно. Поділ стратегічних ресурсів має забезпечувати важливість захисту національних інтересів, а також погоджену взаємодію між воєнними та цивільними угрупуваннями.

Підсумовуючи, варто зазначити, що Стратегічний оборонний бюлетень показує новий підхід до політики України у сфері оборони, котрий визначає глобальні тенденції у воєнній політиці, гібридні небезпеки та сутність інформаційних технологій. Цей підхід дозволяє реалізовувати стабільність країни та адаптацію до передумов, в котрих пряма сутичка з сильнішим ворогом міняється асиметричними та непрямими діями, застосовуючи потенціал громадського суспільства, технології й моральну перевагу [25, с.9-10]. Потреба нормативного здійснення протидії гібридним небезпекам, котрі виникають перед нашою державою, а також змінний характер вдосконалення національного законодавства потребує грунтовної концептуалізації, постійного вивчення та переосмислення нормативних засад. Тому, за останні роки у умовах воєнної агресії наша держава створила велике систему законодавства у сфері захисту національної безпеки, протидії гібридним загрозам, порядку мобілізації, тощо. Даний підхід до створення нормативно-правової основи різниться структурним

методом, не лише врегульовує загальні галузі потенційних загроз, але і досліджуючи їх у постійному зв’язку з міжнародною спільнотою, їх правовою основою та врахуванням чинників незалежності та законності нашої країни [26].

Також, іншою керівною властивістю нормативного законодавства України в даній галузі є налаштованість не тільки на охорону раціонального розвитку держави та життєдіяльності громадського суспільства, а й на захисті демократичного розвитку, прав та свобод людини, характерних українському суспільству цінностей та ознак.

РОЗДІЛ 3
ВДОСКОНАЛЕННЯ ПРАВОВИХ МЕХАНІЗМІВ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

3.1 Вдосконалення національного законодавства у сфері протидії гібридним загрозам

У цьому розділі варто зазначити, що діюча нормативно-правова основа України у галузі протидії гібридним небезпекам на сьогодні має тільки обмежену кількість законів та положень, котрі налаштовані на оборону державного суверенітету та інформаційного захисту. Серед котрих варто зазначити наступні важливі нормативно-правові акти: Закон України «Про внесення змін до деяких законів України щодо регулювання правового режиму на тимчасово окупованій території України» [27], Закон України «Про національну безпеку України» [11], тощо. Однак, існуюча нормативна основа вимагає покращення та доопрацювання для більш раціональної боротьбі сучасним гібридним небезпекам.

Сучасна практика Європейського Союзу та Сполучених Штатів Америки у боротьбі з гібридним небезпеками дає Україні практичні та стратегічні чинники для поліпшення національного законодавства. Тому, враховуючи вищезазначені приклади сучасності Україна могла б визначити та затвердити у законодавстві правові резолюції та нормативні акти, котрі б визнавали національні процеси протидії гібридним загрозам. Також можна у нас сформувати одні фактори та норми комунікаційної політики для зменшення відношення міжнародної пропаганди на громадську позицію. Як приклад, потрібно зміцнити міжнародну співпрацю та обмін інформацією з Європейським Союзом та США для правильнішого моніторингу та оперативного втручання на гібридні загрози у світі [15].

На мій погляд, інтеграція сучасних підходів до зміцнення інформаційної безпеки є надзвичайно важливим елементом забезпечення стійкості України в

умовах тривалої гібридної агресії. Вивчення міжнародного досвіду, зокрема практик Європейського Союзу, дозволяє краще розуміти природу гібридних загроз і адаптувати національну політику до нових викликів.

Хочу зазначити шляхи відносно покращення законодавства у галузі боротьби з гібридним конфліктами:

- по-перше, це формування системної нормативно-правової основи для боротьби з гібридним загрозам;
- варто створити новий спеціальний Закон України «Про протидію гібридні війни в Україні», котрий буде закріплювати терміни, процедури та основи реагування на гібридні конфлікти. Даний закон повинен визначати повне коло повноважень установ державної влади та певні методи оборони національних інтересів;
- формування нової Стратегії протидії сучасним гібридним війнам;
- формування та затвердження Стратегії, котра буде головні засади, сфери та напрями боротьби з гібридним загрозам. Даний нормативний документ має включати різні галузі, включаючи інформаційну, кібернетичну та економічну охорону, та охоплювати сучасні рекомендації для державних органів та приватного сектору відносно протидії гібридним конфліктам.
- покращення структури оборони критично важливих об’єктів;
- запровадження методів відносно оборони структур, котрі можуть бути метою для інформаційних та кібернетичних небезпек. Це охоплює формування процедур фіксування безпеки даних об'єктів, швидкого реагування на методи та постійного здійснення аналізу ризикових факторів [14].

Також вважаю, що здійснення освітніх та наукових методів, налаштованих на створення нормативної культури у молодому осередку та загалом у громадському суспільстві. Тлумачення прав та свобод надасть можливість виховати повагу до прав оточуючих, що є керівним елементом національної стабільності до гібридних небезпек. Навчання має посприяти вихованню у молодого покоління поваги до прав інших осіб, їх способу життя, здоров'я та гідності.

Також потрібно, щоб українські військові навчальні заклади активно розвивали програми підготовки спеціалістів з кібербезпеки та протидії гібридним загрозам. В умовах сучасних загроз, зокрема з боку державних та недержавних акторів, навчання з виявлення та нейтралізації кібератак набуває особливої важливості. Основні напрямки навчання та підготовки кібер спеціалістів включають виявлення та нейтралізація кібератак. Кібер спеціалісти повинні бути здатні виявляти потенційні загрози на ранніх етапах, використовувати сучасні інструменти для аналізу загроз та своєчасно реагувати на атаки, щоб мінімізувати їхній вплив на критичну інфраструктуру та інформаційні системи. У свою чергу захист даних та інформаційних систем є основним завданням кіберспеціалістів. Це включає в себе впровадження засобів шифрування, багаторівневих систем безпеки, виявлення вразливостей і запобігання несанкціонованому доступу до систем.

Розробка ефективних стратегій кібероборони є критично важливою для забезпечення національної безпеки. Кіберспеціалісти навчаються створювати комплексні плани реагування на кіберзагрози, впроваджувати заходи для захисту стратегічних об'єктів та забезпечувати безпеку в умовах кіберконфлікту [32, с.98].

Враховуючи сучасну глобальну політичну ситуацію, стандарти НАТО з кібербезпеки є важливим елементом навчання. Вони визначають базові принципи кібероборони, методи захисту та взаємодії між країнами для забезпечення спільної безпеки у кіберпросторі. Кіберспеціалісти мають вивчати методи аналізу новітніх кіберзагроз, визначати потенційні вразливості в інформаційних системах та розробляти ефективні засоби для протидії цим загрозам. Кіберспеціалісти також отримують навчання для проведення кібероперацій, зокрема активних заходів для захисту національних інтересів у кіберпросторі, включаючи реалізацію заходів для упередження та усунення наслідків атак. Цей тип підготовки є критичним для підтримки інформаційної безпеки та забезпечення ефективного захисту національних інтересів в умовах постійно зростаючих кіберзагроз [28].

Аналітична робота є одним із ключових елементів протидії гібридним загрозам, зокрема в умовах сучасних конфліктів, де інформаційна війна, пропаганда та кібератаки відіграють важливу роль. Підготовка розвідників та аналітиків, а також фахівців у галузі стратегічних комунікацій, передбачає освоєння низки навичок, які дозволяють швидко та ефективно реагувати на різноманітні загрози.

Підготовка спеціалістів повинна включати навчання методам збору розвідувальної інформації з відкритих і закритих джерел. Це може бути як традиційне спостереження, так і використання сучасних технологій, зокрема інструментів збору інформації з інтернет-ресурсів, соціальних мереж, а також аналітики великих даних. В умовах гібридної війни медіа грамотність є необхідною для кожного громадянина, а особливо для військовослужбовців. Це дозволяє оцінювати інформацію критично та правильно реагувати на інформаційні маніпуляції. Навчання медіа грамотності включає розпізнавання неправдивих або маніпулятивних повідомлень, а також правильне використання соціальних мереж та інформаційних платформ для комунікації. Стратегічні комунікації мають на меті не лише захист від інформаційних атак, але й формування правильного іміджу на міжнародній арені. Підготовка в цій сфері включає вміння вести переговори, розв'язувати кризові ситуації через засоби масової інформації, а також організовувати ефективну комунікацію з громадськістю, щоб уникнути паніки та забезпечити стійкість до інформаційних атак [29].

Таким чином, підготовка аналітиків, розвідників та спеціалістів зі стратегічних комунікацій є важливою складовою протидії гібридним загрозам, що дозволяє ефективно реагувати на змінювані умови сучасного конфлікту та забезпечити національну безпеку.

Важливо зазначити, що підготовка фахівців для протидії гібридним загрозам включає також реформування інституцій та налагодження міжвідомчої взаємодії. Найперше, в Україні повинні формуватися специфічні підрозділи, котрі будуть детально займатись протидією гібридним загрозам, кібербезпекою

та інформаційною боротьбою. Це надасть можливість забезпечити цілеспрямовану підготовку фахівців та покращити раціональність реагування на загрози. Також наступним важливим напрямом є зміцнення взаємодії між відомствами. Зрозуміло, що ефективна протидія гібридним загрозам потребує тісної координації між різними відомствами — військовими, розвідувальними, правоохоронними та дипломатичними органами. Для цього в Україні розробляються та впроваджуються механізми спільної роботи та обміну інформацією [30].

Отже, підготовка кадрів для протидії гібридним загрозам є критично важливою для національної безпеки України. Інтеграція євроатлантичних стандартів, співпраця з НАТО та впровадження сучасних методик навчання дозволяють створити високоефективну систему захисту від складних і багатогранних загроз. Україна продовжує розвивати свій потенціал у цій сфері, що є важливим кроком на шляху до зміцнення її безпеки та стійкості перед новими викликами. Тому, врахування та затвердження вищезазначених нормативно-правових положень та запровадження цих методик надають нашій державі здатність раціональніше боротися з гібридним загрозам, вдосконалити оборону державних та національних інтересів, а також покращити рівень інформаційної стабільності громадського суспільства. Покращення нормативно-правової бази та вдосконалення нормативної культури надасть можливість зміцнити обороноздатність України та її готовність до боротьби з новітнім викликам.

3.2 Міжнародне співробітництво як ключовий елемент у боротьбі з гібридними загрозами

У даному питанні хочу зазначити, сьогодні протидія гібридним загрозам є одним із ключових напрямків безпекової політики багатьох країн та міжнародних організацій, і практика Європейського Союзу, НАТО та Сполучених Штатів Америки в цьому питанні є особливо важливим для України. Враховуючи

складність гібридних загроз, такі країни та організації розробили стратегічні документи та нормативно-правові акти, налаштовані на захист національної безпеки, інформаційного простору та стійкості суспільства.

Варто зазначити основні нормативні міжнародні акти в сфері протидії гібридним небезпекам. У Європейському Союзі до них відносять по-перше Резолюцію «Стратегічні комунікації Європейського Союзу як протидія пропаганді третіх сторін», саме цей нормативний акт включає керівні основи Європейського Союзу відносно протидії пропаганді, котра попадає від третіх країн та налаштована на маніпуляції громадською думкою в державах Євросоюзу. Головна увага приділяється створенню стійких комунікацій, котрі повинні протидіяти дезінформаційним групам, налаштованим на розкол та розкол суспільства в Європі. По-друге, це «Спільні принципи протидії гібридним загрозам – відповідь Європейського Союзу», даний акт закріплює координаційні процеси між державами-учасниками ЄС та методи з покращення потужностей ЄС давати відсічі гібридним небезпекам, котра охоплює кіберзахист, боротьбу з дезінформацією та покращення загальної інформаційної стійкості [31].

Слід виділити, що у Сполучених Штатах Америки це Резолюція Конгресу «Про рішуче засудження дій Російської Федерації під керівництвом В. Путіна, котрим було запроваджено політику агресії проти сусідніх країн з ціллю політичного та економічного домінування», даний акт показує офіційну позицію Конгресу США щодо гібридної агресії з боку Росії та засуджує її намагання відношення на внутрішні справи сусідніх країн через різні форми гібридних загроз, охоплюючи дезінформацію та кібератаки. Також згадаю і про нормативний акт «Про боротьбу з іноземною дезінформацією та пропагандою», котрий був направлений на формування механізмів для боротьби іноземній дезінформації, котра має на завданні має маніпулювання громадською думкою в США. Згідно до даного законопроекту визначені ресурси для розвідки, аналізу та інформаційних кампаній, налаштовані на захист американського сучасного суспільства від іноземного тиску [32].

Європейський Союз визначає гібридні загрози як велику комбінацію

традиційних та нетрадиційних засобі, налаштованих на уразливі місця країн з ціллю завдання шкоди без переходу до відкритої агресії. Дані фактори можуть включати маніпулювання інформацією, кібератаки, використання законодавчих чи економічних механізмів для примусу, а також залучення соціально чутливих аспектів, таких як міграційні кризи. Як показує практика авторитарні режими все частіше реалізовують гібридні засоби для підриву демократичних інститутів, посилення внутрішньої поляризації суспільств і реалізації власних геополітичних цілей. Наприклад, кампанії з дезінформації спрямовані на підрив довіри до урядів і громадських інституцій, а кіберзагрози націлені на критично важливу інфраструктуру. Економічний тиск і маніпуляції з постачанням ресурсів стають інструментами контролю, а юридичні механізми використовуються для легітимізації таких дій на міжнародній арені [33, с.9-10].

На моє переконання, формування та запровадження ефективних стратегій протидії даним загрозам дозволить Україні не тільки краще захистити себе, а й посилити співпрацю з міжнародними партнерами. Це включає адаптацію стандартів ЄС у сфері інформаційної безпеки, формування стійких інститутів державного управління і підвищення обізнаності суспільства щодо гібридних викликів. Впровадження таких підходів зміцнить стійкість держави, підвищить рівень безпеки та сприятиме захисту демократичних цінностей.

Гібридні загрози, які включають втручання в демократичні процеси через дезінформаційні кампанії, маніпуляцію соціальними медіа, радикалізацію, вербування та використання проксі-акторів, є одним із ключових викликів для сучасних держав. Їхня мета — підірвати довіру до демократичних інститутів, дестабілізувати суспільство і досягнути політичних, економічних чи геополітичних переваг без прямого застосування сили [28].

Український досвід протидії таким загрозам став унікальним кейсом для міжнародної спільноти, особливо після початку військової агресії Російської Федерації у 2014 році. Росія використала широкий арсенал гібридних дій: масштабні інформаційні кампанії, кібератаки на критично важливу інфраструктуру, економічний тиск через маніпуляцію енергетичними ресурсами

та військову ескалацію. Це спонукало Україну розвивати власні механізми стійкості та спротиву [34].

Країни ЄС та США, зіштовхнувшись із подібними загрозами, змогли швидко оцінити свої вразливості та ухвалити законодавчі й стратегічні документи, спрямовані на протидію гібридним атакам. Наприклад, у ЄС було ухвалено Резолюцію «Стратегічні комунікації Європейського Союзу як протидія пропаганді третіх сторін» та концепцію «Спільні принципи протидії гібридним загрозам». У США прийнято законопроєкти, спрямовані на боротьбу з іноземною дезінформацією та пропагандою, які визначають механізми реагування на загрози з боку держав, що використовують гібридні інструменти [35, с.95].

Наша держава може та має застосувати міжнародну практику для посилення власної національної оборони. Інтеграція даних підходів може охоплювати:

1. Вдосконалення нормативно-правової бази, формування нормативних актів, аналогічних до європейських і американських, налаштованих на захист демократичних процесів, інформаційної сфери та критичної інфраструктури.

2. Зміцнення інформаційної безпеки, підвищення рівня кіберзахисту, створення національних механізмів моніторингу і боротьби з дезінформацією.

3. Освітні кампанії, формування медіа грамотності серед населення, щоб зменшити вразливість суспільства до маніпулятивного контенту.

4. Міжнародна співпраця, яка буде включати обмін практикою та інтеграція у глобальні й регіональні ініціативи з протидії гібридним загрозам [36].

Вважаю, що нормативна адаптація даних методів надасть можливість Україні зміцнити власну стійкість, захистити демократичні процеси та ефективніше протистояти сучасним викликам. Гібридні загрози формують суттєві виклики для міжнародного права, зокрема у галуззях регулювання збройних протистоянь, права на самооборону, обґрунтованості превентивних заходів та реалізації контрзаходів. Маніпулятивний характер та непрозорість даної тактики руйнують звичні правові норми, адже стираються кордони між

станом війни та миру, а також між діяльністю державних і недержавних суб'єктів. Особливу небезпеку становить можливість викривленого або маніпулятивного тлумачення звичаєвого міжнародного права, що здатне підірвати ефективність правового регулювання міжнародних відносин.

Гібридні операції нерідко налаштовані на дестабілізацію функціонування країни, що є безпосереднім порушенням міжнародного права. Використання цих засобів країни суперечить їхнім зобов'язанням діяти добросовісно та додержуватись міжнародних норм. Крім того, такі дії є порушенням норм невтручання у внутрішні справи суверенних країн, котрий залишається ключовою основою сучасного міжнародного правопорядку. На сьогодні, гібридні загрози не переходять кордонів відкритої агресії, вони структуровано підривають методи мирного врегулювання спорів, визначених у Статуті ООН та інших міжнародних договорах. Дана тактика сильно ускладнює координацію дій міжнародної спільноти, зменшує нормативно-правові процеси запобігання конфліктам та формує нові загрози для глобальної стабільності та безпеки.

Відповідно до пункту 2 статей 8–11 Європейської конвенції з прав людини (ЄКПЛ), заходи протидії гібридним загрозам мають бути чітко визначені законом, спрямовані на легітимну мету та відповідати вимогам, необхідним для функціонування демократичного суспільства. У випадку масштабних гібридних чи невійськових атак європейські держави можуть застосовувати положення статті 17 ЄКПЛ, яка забороняє зловживання правами та безпосередньо пов'язана з принципом добросовісності в міжнародному праві [37]. Крім того, стаття 15 ЄКПЛ дозволяє державам-учасницям тимчасово призупиняти виконання своїх зобов'язань за Конвенцією в умовах надзвичайного стану. Водночас це не поширюється на основоположні права, такі як право на життя, заборона тортур, рабства, смертної кари, подвійного покарання та принцип nulla poena sine lege («немає покарання без закону») [37].

На сьогодні НАТО є першою організацією, котра нормативно закріпила визначення гібридних загроз. В той час найбільш вдосконалена нормативно-правова система протидії таким загрозам сьогодні працює в Європейському

Союзі (ЄС) та його державах-учасниках. Починаючи з 2016 року, Європейська Комісія спільно з Верховним представником ЄС із закордонних справ і політики безпеки розробили широкий набір заходів у рамках Спільної рамкової програми 2016 року щодо протидії гібридним загрозам («Спільна структура протидії гібридним загрозам – відповідь Європейського Союзу»). Дана програма включає значну кількість галузей політики та налаштована на забезпечення системного реагування [38].

Також хочу наголосити, що Hybrid Fusion Cell (HFC) відіграє керівну роль у структурі протидії гібридним загрозам ЄС. Його завдання полягає в отриманні, аналізі та обміні як конфіденційною інформацією, так і даними з відкритих джерел, що стосуються індикаторів і попереджень про гібридні загрози. Ця інформація надходить від різних зацікавлених сторін у рамках Європейської служби зовнішніх дій (EEAS), включаючи представництва ЄС, Європейську комісію, агентства ЄС, а також держави-члени. У свою чергу, Європейська комісія відповідає за координацію між HFC та національними і європейськими органами [39].

Документ також визначає країнам-членам сформувати національні контактні пункти для аналізу гібридних загроз. Дані пункти будуть раціональній співпраці та дотримання безпечного зв’язку з HFC ЄС.

Для раціональної протидії гібридним загрозам у документі акцентується увага на потреби зменшення вразливостей у даних керівних сферах:

1. Сфера енергетики, диверсифікація засобів енергії, просування методів безпеки для дотримання стабільності ядерної інфраструктури.

2. Безпека транспорту та постачання, системне врегулювання питань безпеки на морі, оборони критичної морської інфраструктури, глобальних ланцюгів постачання, морської торгівлі та природних ресурсів, співпраця між цивільними та військовими учасниками для протидії гібридним загрозам.

Отже, ці методи налаштовані на зміцнення стійкості інфраструктури та громадської суспільства, забезпечуючи ефективну відповідь на виклики гібридних загроз.

Потрібно визнати, що практика майже трьох років воєнних дій в Україні показали відсутність ефективної нормативної підготовки для реагування на критичні випадки настільки великого масштабу. Враховуючи це, важливо звернути увагу на вже наявних нормах міжнародного права та їх частковій імплементації в українську нормативну структуру, щоб захистити Україну від гібридних загроз або, хоча б, підготувати її до оперативного реагування на дані загрози та їх результати [40].

Повертаючись до вищезазначеного нормативного акту, в ньому визначено перелік методів для здійснення безпеки в таких галузях, як сфера кіберпростору, економіка політика, та сфера будівництва тощо. Одним із ключових моментів є тактика взаємовідношення з організацією НАТО. Для прикладу, зазначено певний перелік для щільної роботи між ЄС та НАТО, серед котрих ситуаційна обумовленість, стратегічне спілкування, кібербезпека та запобігання ризикам та реагування на у відповідному порядку. Тому, на сьогодні дуже важливо визначено, що для раціональної роботи ЄС і НАТО має бути однакова інформацію відносно загроз, бо лише через щільну спільну їх діяльність може бути досягнути тих завдань на які вони орієнтовані [41].

Враховуючи те, що наша країна офіційно не є членом НАТО, слід вказати, щоб сучасне наше нормативно-правове регулювання також включало тактику взаємної роботи з НАТО та іншими світовими установами та організаціями для боротьби з гібридним небезпеками. Дана тактика повинна бути детально визначено в нормативних актах, котрі регламентують співпрацю України з міжнародними союзниками.

Також потрібно ще раз наголосити увагу, що у ближчому майбутньому звіти діяльності Європейського Союзу можуть стати дієвими також для українського громадського суспільства, проте у воєнний час це може формувати новітні загрози для структури національної безпеки. Водночас, на національному рівні мають бути сформовані спеціальні комісії для аналізу гібридних загроз. У мирний час до складу таких комісій слід залучати експертів з публічними цінностями, проте в умовах війни їх особи мають лишатися конфіденційними.

Дані комісії або особливі органи мають реалізовувати постійний моніторинг та аналіз гібридних загроз. Звичайно, що Служба безпеки України вже займається даною діяльністю у відповідності до повноважень, котрі їм були надані, однак європейська практика значно збільшила б структуру національної безпеки в протидії таким загрозам [42].

Окремо варто звернути увагу на Стратегію безпеки ЄС, затверджену у 2020 році. Вона відрізняється від попередніх стратегій «Безпечна Європа в кращому світі» (2003 р.) та «Сильніша Європа. Глобальна стратегія зовнішньої політики та політики безпеки Європейського Союзу» (2016 р.) тим, що в новій стратегії набагато більше уваги зосереджено гібридним загрозам. Для прикладу, у другій частині Стратегії, що називається «Боротьба з загрозами, що розвиваються», більш детально вивчається проблематика, що пов'язана з боротьбою з гібридним загрозам [15].

Також на сьогодні важливим є питання прикордонного впливу, особливо в розумінні взаємовідносин з Білоруссю. На сьогодні, Білорусь активно підтримує політику росії, надавши плацдарм для першої хвилі атак на початку 2022 року та надалі продовжує забезпечувати та російські війська, здійснюючи спільні навчання та передислокацію військової сили. Даний прикордонний тиск вимагає від України відводити військову силу з інших стратегічно важливих напрямків через велику ймовірність нових провокацій та атак зі сторони Білорусі, в тому числі враховуючи вторгнення російських диверсійно-розвідувальних груп та партизанів. Тому, ці питання частково вирішуються в межах угоди про функціонування Європейського Союзу, тому Україні потрібно на нормативному рівні закріпити тактику та подальші дії прикордонної політики щодо держав-сусідів, деякі з котрих підтримують агресивну гібридну політику проти нашої країни [43].

Враховуючи на високу активність Європейського Союзу у боротьбі гібридним загрозам та суттєвість їхньої практики для України, слід зазначити, що ООН у даному розумінні показує менш раціональні та ефективні тактики. ООН, як серйозна організація, котра мала б охороняти Україну від гібридних

атак Кремля, переважно покладається на санкційну політику та велику стурбованість внаслідок незаконних військових дій на території України. Однак, дана тактика є недостатньо ефективною, адже підтримка агресора з боку інших країн та здатність РФ замінювати санкційні продукції говорять про те, що економічні санкції не тільки можуть мати ефективний вплив на велику країну, таку як росія [44].

Женевські конвенції 1949 року та два додаткові протоколи до них 1977 року, котрі протягом десятиліть забезпечували керівні принципи ведення звичайних воєн через jus in bello (міжнародне право, що регулює поведінку під час війни), не дають точних та належних правил для випадків, що пов'язаних з гібридними військовими діями. У сучасному світі гібридних небезпек, котрі поєднують як військові, так і невійськові методи, закони війни є розпливчастими, і їх реалізація не завжди ефективна. Тому методи, визначені ООН та Женевськими конвенціями, проявляються не ефективними для деескалації зіткнень у «сірій зоні», де переважають не відкриті військові дії, а різні засоби маніпуляцій, перекручування фактів, економічних санкцій, кібернападів та інших гібридних засобів здійснення воєнних дій. В даному розумінні тактика ООН вимагає перезавантаження, в тому числі, через адаптацію міжнародних положень до нових реалій сучасних гібридних загроз, котрі зумовлюють потребу більш конкретної реакції та нових підходів для зупинення конфліктів у «сірих зонах» [45].

Однією з основних проблематик, котра ускладнює правильну боротьбу гібридним загрозам, є непублічність дій у сірій зоні та активне залучення не офіційних структур, котрі реалізовують різні маніпуляційні дії або велику дезінформації. Дані утворення дуже часто функціонують поза рамками звичайних методів світового правопорядку, що унеможливлює ідентифікацію агресора та аналіз гібридної загрози. Також у міжнародному гуманітарному праві наявна конфліктність між державним суверенітетом та правами особи. Як вказав Руссо, збільшення акценту в міжнародному праві з суверенітету на гуманітарні норми завдало до появи розриву між звичайним миром та військовими діями,

котрі активно застосовуються державними та недержавними учасниками для реалізації операцій, що не постійно включають військові дії, але і гібридні випадки [48, с.112].

Даний фактор також підриває загальну повагу до законодавства, в тому числі щодо дієвості міжнародного гуманітарного права прав та свобод людини. Від давніх-давен міжнародне право стало предметом постійного контролю, котрий іноді завдає до його неефективного тлумачення та застосування для виправдання дій як певних країн, так і не офіційних учасників. В умовах сучасного інформаційного простору, в тому числі через великий розвитком соціальних мереж, нормативні правові норми стають предметом маніпуляцій, та законодавство часто застосовується як методо для оскарження дій опонентів або виправдання власних.

Відносно НАТО, хоча принцип колективної безпеки - напад на одного члена є нападом на всіх є основою Альянсу, гібридні загрози залишаються частково поза цим механізмом. Дані випадки викликають труднощі в рамках застосування даного принципу в умовах сучасних гібридних загроз, де напад не завжди є чітко визначеним або традиційним. Відповідно, хоча країни-члени можуть отримати допомогу, питання більш активного втручання або колективної оборони може бути не так однозначно вирішене, особливо коли загроза не включає класичні військові дії. Це підкреслює необхідність адаптації стратегій НАТО до нових типів загроз та їх визначення в правовому контексті [45, с.207].

Сучасне міжнародне гуманітарне право та міжнародні утворення поступово формують певні дієві методи боротьби з гібридними небезпеками, визнаючи, що вони є великою частиною сучасних конфліктів у нинішньому світі. Україна активно реалізовує правові інструменти для боротьби з таким загрозам, наприклад, через звернення до міжнаціональних судових органів, щоб здійснити нормативну підтримку у врегулюванні конфліктів, розпочатими гібридними методами, особливо зі сторони Росії.

Створення ефективного механізму протидії гібридним загрозам з боку РФ вимагає системного підходу, який охоплює короткострокові та довгострокові цілі.

Встановити такий метод захисту території України на кордоні, щоб у РФ не було здатності накопичувати технікою окуповані території. І у майбутньому, в довгостроковій перспективі повністю звільнити усю територію України від московських окупантів. Великий перелік санкцій лишається найбільш розповсюдженим методом міжнародного впливу на агресора. Європейський Союз та ООН активно реалізовують санкції проти Російської Федерації з ціллю змінити її політичнну ситуацію та припинити всі агресивні дії. Санкції охоплюють заморожування великих грошових активів, обмеження у видачі віз для російських посадовців та компаній, що мають прямий зв'язок з гібридними атаками на Україну [46, с.97].

Тому, вважаю, що дані методи мають на меті заставити агресора росію зупинити власну тактику, проте підтримка, котру агресор отримує від інших країн, часто знижує раціональність цих санкцій. Це свідчить про те, що міжнародний осередок має зустрічатись з певними складнощами при намаганнях сформувати єдину сильну стратегію для зупинення росії, та тоді коли певні країни не підтримують або навіть знімають дані обтяження. Тому, хоча санкції лишаються важливим інструментом, їх раціональність часто залежить від повноти підтримки міжнародної спільноти.

На мій погляд, реалізація та збільшення санкцій, справді, стало керівним та раціональним методом міжнародного впливу, адже воно забезпечується міжнародною цивілізованою спільнотою та ґрунтується на загальноприйнятих правилах міжнародного гуманітарного права. Дані санкції показують готовність міжнародної спільноти функціонувати спільно проти гібридних загроз та надавати забезпечення державам, котрі страждають від агресії та військового впливу з боку Російської Федерації. Наприклад, санкції надають можливість покращити економічний та політичний тиск на ворога, хоча раціональність даних методів може бути досить обмежена через підтримку зі сторони певних країн. Україна також активно застосовує міжнародну гуманітарну та військову допомогу, котра визнана цивілізованим міжнародним гуманітарним правом. Дана допомога вже надає відбудові деокупованих територій, що є керівним аспектом у

процедурі подолання результатів гібридних атак [49].

Враховуючи на довгі переговори відносно конкретнішого визначення гібридних небезпек, світові організації визнають їх як зростаючу проблематику безпеки. Спільноти, такі як Європейський Союз, вже активно запроваджують законодавчі норми для протидії таким загрозам, наприклад, через санкції, формування комісій та регулярні аналізи та звіти. В той час, інші міжнародні військові спільноти ще перебувають на стадії створення відповідного законодавства [47, с.207].

Головною проблемою лишається те, що гібридні загрози часто попадають в «сірі зони» міжнародного гуманітарного права, де вони можуть бути тлумаченні по-різному в залежності від випадку. Це надає країнам можливість, котрі використовують гібридні методи атак, виправдовувати свої дії, стверджуючи, що порушення норм міжнародного права не відбулося. Проте, у світлі агресії Росії проти України, міжнародна спільнота починає активно працювати над заповненням цього вакууму в юридичному спектрі, для того щоб забезпечити раціональну протидію гібридним загрозам на міжнародному рівні [50].

На сьогодні наша держава може активно застосовувати міжнародний нормативно-правову практику у протидії з гібридними загрозами, зважаючи, на те, що саме Україна стала однією з найбільших жертв таких гібридних атак. Європейський Союз, в тому числі, значно конкретніше, визначив різновиди гібридних загроз та галузі, котрі потребують захисту. Проте, Україна не була повністю готова до низки гібридних атак, скоєних Росією в 2022 році, як у юридичному, так і в практичному аспекті.

Однією з важливих можливостей для України є надання свого власного практичного досвіду для формування міжнародних стратегій боротьби з гібридними загрозами. Враховуючи, що Україна вже багато років є об’єктом таких атак, вона має унікальний досвід і знання, які можуть стати орієнтиром для інших демократичних держав у майбутньому. Цей досвід може стосуватися як реакції на інформаційні війни, кіберзагрози та економічний тиск, так і організаційних заходів у сфері національної безпеки, що вже активно

застосовуються в Україні. Посилення міжнародного співробітництва та обміну практикою з іншими сучасними країнами надасть нам можливість не тільки покращити свою обороноздатність та дати відсіч будь яким гібридним загрозам, але й створити нову вагому практику у глобальні стратегії щодо протидії цим новітнім викликам та бути як яскравим прикладом для інших країн.

ВИСНОВКИ

Отже, вивчаючи правове регулювання протидії гібридним загрозам можна зробити наступні висновки:

У сучасному цивілізованому гібридні небезпеки, справді, не мають будь якої прив'язки до території чи географії розташування, що робить їх ще більш складними для протидії та реагування. Кіберпростір та глобалізація тільки ускладнюють виявлення і протидію цим загрозам, бо такі загрози можуть здійснюватися в будь якому кутку світу і не завжди мають певне визначення агресора чи напрямку атаки.

У першому розділі, було проаналізовано визначення терміну «гібридної загрози», котрий в сучасному розумінні має три головних тлумачення. По-перше, це гібридна загроза це гібридність у певній військовій ситуації, котрі має відношення до особливостей здійснення бойових дій, де переплітаються різноманітні форми та методи військового протистояння. Ця гібридність зумовлює адаптацію військового ворога до ситуації, застосування як традиційного озброєння, так і особливих нетрадиційних засобів ведення війни. По-друге, гібридна загроза це гібридність у методології та тактиці ворона, в цій ситуації гібридні загрози тлумачаться як відповідна стратегія та тактика дій ворона, спрямована на отримання певних політичних завдань. Це охоплює в себе кількість певних методів жорсткого насилля та активних дій, як приклад, це може бути пропаганда, кібероперації, інформаційні атаки та сильний економічний вплив. По-третє, гібридна загроза це певна гібридність у відношенні сил, котрі формує та забезпечує певна країна, гібридність означає вид сили та продуктів, потрібних для дотримання безпеки.

У другому розділі встановлено, що нинішні реалії воєнних дій показали, що в Україні відсутні нормативні процедури для оперативного втручання на кризові випадки, взаємопов’язані з гібридними атаками. Імплементація наявний положень міжнародного гуманітарного права в українське законодавство може сильно покращити готовність держави до похожих загроз. Це надасть Україні можливість бути краще зібраною та готовою для зупинення гібридних атак або

зменшення їхніх результатів.

У третьому розділі, встановлено, що посилення міжнародного співробітництва та обміну практикою з іншими сучасними країнами надасть нам можливість не тільки покращити свою обороноздатність та дати відсіч будь яким гібридним загрозам, але й створити нову вагому практику у глобальні стратегії щодо протидії цим новітнім викликам та бути як яскравим прикладом для інших країн.

Підсумовано, що властивість гібридної війни також полягає в тому, що вона потребує реалізації комплексного підходу, котрий включає не лише військові методи, але і масштабний засобів керівництва: таких як юридичних, організаційних-нормативних, комунікаційних та психологічних. Тому, взаємодія між державною владою та населенням є ключовим методом для раціонального управлінського реагування на такі атаки. Тут важливим є не лише оперативне та чітке прийняття рішень, але й можливість здійснити забезпечити стабільність та досвід серед громадян навіть у умовах, коли йде активне застосування інформаційних маніпуляцій та соціально-психологічних методів.

Таким чином, під час написання моєї роботи було досягнуто мети та завдання роботи, проаналізовано теоретичні засади правового регулювання протидії гібридним загрозам, визначення їх характеристику та нормативно-правову основу щодо протидії. Також мною було проаналізовано правові механізми протидії гібридним загрозам у міжнародній практиці, вивчено український досвід правового регулювання боротьби з російською гібридною та повномасштабною агресією. Також мною було зазначено шляхи вдосконалення національного законодавства у сфері протидії гібридним загрозам та врахування міжнародного військового досвіду.

Для України, як незалежної держави, котра активно стикається з гібридною агресією з боку Росії, важливо не тільки застосовувати міжнародний досвід, але і вдосконалювати свою концептуальну основу відносно протидії таким загрозам. Це охоплює дослідження не тільки теоретичних методів нових типів конфліктів, але і створення організаційної бази для дослідження та адаптації стратегій

гібридного протиборства, враховуючи світовий досвід.

Тому, вивчення та подальша розробка таких концепцій можуть стати базою для створення більш раціональної національної стратегії безпеки, котра буде здатна забезпечити Україні стійкість у протистоянні сучасним викликам глобальних і гібридних загроз.

СПИСОК ДЖЕРЕЛ ПОСИЛАННЯ

1. Конституція України: Закон від 28.06.1996 №254к/96-ВР. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 17.11.2024 року).

2. Про основи національного спротиву : Закон України № 41. Дата оновлення : 20.06.2024 року, URL: https://zakon.rada.gov.ua/laws/show/1702-20#Text (дата звернення: 17.11.2024 року).

3. Пирожков С. І., Божок Є. В., Хамітов Н. В. Національна стійкість (резильєнтність) країни: стратегія і тактики випередження гібридних загроз. Вісник НАН України. 2021. No 8. С. 74–82. (дата звернення: 17.11.2024 року).

4. Гбур З. В. Актуальні гібридні загрози економічній безпеці України. Інвестиції: практика та досвід. 2018. No 7. С. 97–99. (дата звернення: 17.11.2024 року).

5. Концепція забезпечення національної системи стійкості : Рішення Ради Національної безпеки і оборони України. Дата оновлення: 20 серпня 2021 року, URL: https://zakon.rada.gov.ua/laws/show/n0065525-21#n2 (дата звернення: 17.11.2024 року).

6. Спільна структура протидії гібридним загрозам – відповідь Європейського Союзу, URL: https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en (дата звернення: 17.11.2024 року).

7. Платформа Україна – НАТО з аналізу практики протидії гібридній війні в Україні, URL: https://www.nato.int/cps/uk/natohq/topics_37750.htm (дата звернення: 17.11.2024 року).

8. Данилюк О. В. Міжвідомче та міжнародне співробітництво при виявленні та протидії гібридним загрозам. К. : 7БЦ, 2021. 192 с. (дата звернення: 17.11.2024 року).

9. Підсумкова декларації саміту НАТО, котрий проходив у Шотландії у вересні 2014 року, URL: https://www.nato.int/cps/uk/natohq/official_texts_227678.htm (дата звернення:

17.11.2024 року).

10. Стратегічний порядок денного ЄС на 2024–2029 роки», URL: https://dixigroup.org/strategichnyj-poryadok-dennyj-yes-na-2024-2029-roky/ (дата звернення: 17.11.2024 року).

11. Про національну безпеку України : Закон України №31. Дата оновлення: 09.08.2024 року, URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 17.11.2024 року).

12. Вєдєнєєв Д.В., Семенюк О.Г. Система державних установ з розробки теорії протидії гібридним загрозам у країнах ЄС і НАТО, 2022 рік, URL: http://www.lsej.org.ua/6_2022/11.pdf (дата звернення: 17.11.2024 року).

13. Про основні засади забезпечення кібербезпеки України : Закон України № 2163-VIII.Дата оновлення: 28.06.2024 року, URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 17.11.2024 року).

14. Про Стратегічний оборонний бюлетень України : Рішення Ради Національної безпеки і оборони України. Дата оновлення: 21.09.2021 року, URL: https://zakon.rada.gov.ua/laws/show/n0063525-21#Text (дата звернення: 17.11.2024 року).

15. Стратегія безпеки ЄС 2020, URL: https://dialog.lviv.ua/strategiya-yevropa-2020-u-tsentri-lyudina/ (дата звернення: 17.11.2024 року);

16. Женевська конвенція про захист цивільного населення під час війни від 12 серпня 1949 року, URL: https://zakon.rada.gov.ua/laws/show/995_154#Text (дата звернення: 17.11.2024 року).

17. Бакай А. Є. Платформа Україна-НАТО як механізм реформування системи медичного забезпечення в надзвичайних ситуаціях. Інвестиції: практика та досвід. 2018. No 16. С. 127–131. (дата звернення: 17.11.2024 року).

18. Гібридна війна: in verbo et in praxi монографія Донецький національний університет імені Василя Стуса / під. заг. ред. проф. (дата звернення: 17.11.2024 року).

19. Хагельстам А. Співпраця заради протидії гібридним загрозам. URL:

https://www.nato.int/docu/review/uk/articles/2018/11/23/spvpratsya-zaradi protid-gbridnim-zagrozam/index.html (дата звернення: 17.11.2024 року).

20. Кресін О. В. Визнання, регулювання та забезпечення протидії гібридним загрозам у НАТО та ЄС. *Правова держава.* 2022. Вип. 33 (у друці).

21. Протидія гібридним загрозам в Українському законодавстві, Кресін О., 2022 рік, URL: https://www.researchgate.net/publication/361681661_Protidia_gibridnim_zagrozam_v_ukrainskomu_zakonodavstvi (дата звернення: 17.11.2024 року).

22. Лопатченко І. М. Застосування соціальних мереж як сучасного механізму взаємодії органів влади і громадськості. *Вісник Національної академії Державної прикордонної служби України.* Серія : Державне управління. 2018. Вип. 4. URL: http://nbuv.gov.ua/UJRN/Vnadpsdu_2018_4_6 (дата звернення: 17.11.2024 року).

23. Вєдєнєєв Д. В., Семенюк О. Г. Розвиток концептуальних і науково-практичних поглядів на сутність неконвенційної (гібридної) конфліктності. Монографія. К. : «АртЕк», 2021. 228 с.

24. Резнікова О. О. Розбудова національної стійкості: концептуальні підходи, передові світові практики. 2019. URL: https://niss.gov.ua/sites/default/files/2019-11/roa_presentation_niss_v01.pdf (дата звернення: 17.11.2024 року);.

25. Андрієвський, Т.Г. (2016). Гібридна війна як специфічний тип гібридного конфлікту. Сучасне суспільство. 2(12), 9-10. URL: http://www.irbis-nbuv.gov.ua/cgibin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=cuc_2016_2_3 (дата звернення: 17.11.2024 року).

26. Забезпечення національної безпеки держави в умовах гібридної війни: сучасні реалії та міжнародний досвід, Цебинога В.Ю., 2018 рік, URL https://univd.edu.ua/general/publishing/konf/17_05_2018/pdf/41.pdf (дата звернення: 17.11.2024 року).

27. Про внесення змін до деяких законів України щодо регулювання правового режиму на тимчасово окупованій території України : Закон України №2217-IX. Дата оновлення: 21.04.2022 року, URL: https://zakon.rada.gov.ua/laws/show/2217-20#Text (дата звернення: 17.11.2024 року).

28. Паршикова А. Міжнародний досвід протидії гібридним загрозам: законодавче регулювання та організації з питань стратегічних комунікацій. URL: http://euinfocenter.rada.gov.ua/uploads/documents/29377.pdf (дата звернення: 17.11.2024 року).

29. Коломієць О. Соціокультурний вимір проблеми гібридної війни. *Вісник львівського університету. Серія філос-політолог.* студії. 2023. Вип. 49. С. 62– DOI:https://doi.org/10.30970/PPS.2023.49.7 URL: http://fps-visnyk.lnu.lviv.ua/archive/49_2023/7.pdf (дата звернення: 17.11.2024 року).

30. Міжнародні нормативно-правова засоби протидії гібридним загрозам в умовах агресії рф проти України, Чуб С.В.2022 рік, URL: http://pdu-journal.kpu.zp.ua/archive/4_2022/36.pdf (дата звернення: 17.11.2024 року).

31. Омелянюк С. М. Соціально-психологічні особливості дискурсу військової загрози. Теоретичні і прикладні проблеми психології. 2019. № 3(2). С. 158–162. URL: http://nbuv.gov.ua/UJRN/Tippp_2019_3%282%29__17 (дата звернення: 17.11.2024 року).

32. Світова гібридна війна: український фронт: монографія, за заг. ред. В. П. Горбуліна. К. : НІСД, 2017. 496 с. (дата звернення: 17.11.2024 року).

33. Мартинюк, В., Гончар, М., Чубик, А.,Жук, С., Чижова,О., Максак, Г., Тищенко, Ю., Зварич, О.(2018). Аналітичний документ. Гібридні загрози України і суспільна Безпека. Досвід ЄС і Східного партнерства. Київ: Центр глобалістики «Стратегія XXI». (дата звернення: 17.11.2024 року).

34. Державна прикордонна служба України. Серія: Державне управління. 2018. Вип. 4. С. 34–43. URL: http://nbuv.gov.ua/UJRN/Vnadpsdu_2018_4_6 (дата звернення: 17.11.2024 року).

35. Глосарій з гібридних загроз. За ред. Гришко С.В. Харків : ХНУРЕ, 2021.

113 с. URL: https://warn-erasmus.eu/ua/glossary/ (дата звернення: 17.11.2024 року).

36. Гібридна війна: сутність, виклики та загрози: зб. матер. круглого столу (Київ, 8 липня 2021 р.). Київ: НА СБУ, 2021. URL: https://academy.ssu.gov.ua/uploads/ p_57_28744724.pdf (дата звернення: 17.11.2024 року).

37. Європейська конвенція з прав людини (ЄКПЛ) в редакції від 01.08.2021 року, URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 17.11.2024 року).

38. Гібридні загрози: чи вистоїть Україна? URL: https://yvu.com.ua/gibrydni-zagrozy-chy-vystoyit-ukrayina/ (дата звернення: 17.11.2024 року).

39. Хмель А. Боротьба із гібридними загрозами в ЄС (за нормативно-правовою базою Європейського Союзу). Acta de Historia & Politica : Saeculum XXI.2021/2022. T. III. С. 91–101. (дата звернення: 17.11.2024 року).

40. Місюра, А., Паливода, В. (2018). Концептуальні підходи НАТО та ЄС до забезпечення стійкості держави і суспільства у сфері національної безпеки. URL: https://cutt.ly/fUY2Ian (дата звернення: 17.11.2024 року).

41. Паливода, В. (2020). Центр протидії тероризму та гібридним загрозам при МВС Чеської Республіки. URL: https://cutt.ly/jUY2PEP (дата звернення: 17.11.2024 року).

42. Гібридні загрози: нові виклики та можливості для України, Підгірна В.Н., Гладиш А.В. URL: https://archer.chnu.edu.ua/bitstream/handle/123456789/5705/Pidgirna_Tezy.doc?sequence=1&isAllowed=y (дата звернення: 17.11.2024 року).

43. Світова гібридна війна: український фронт. За ред. Горбуліна В.П. Київ: Інститут стратегічних досліджень, 2017. 496 с. (дата звернення: 17.11.2024 року).

44. Рюле, М., Робертс, К. **(**2010, March 19) Розширення інструментарію НАТО з протидії гібридним загрозам. Retrieved from https://www.nato.int/docu/review/uk/articles/2021/03/19/rozshirennyanstrumentaryu-nato-z-protid-gbridnim-zagrozam/index.html (дата звернення: 17.11.2024 року).

45. Гібридні загрози та гібридні війни: сутність та аспекти взаємодії,

Т.Рева, *Вісник Львівського університету*, серія філос.-політолог.студії. 2022 рік, URL: http://fps-visnyk.lnu.lviv.ua/archive/40_2022/24.pdf (дата звернення: 17.11.2024 року).

46. Гбур З.В. Актуальні гібридні загрози економічній безпеці України. Інвестиції: 100 практика та досвід. 2018. No 7. С. 97–100 (дата звернення: 17.11.2024 року).

47. Зубченко С.О. Сучасний гуманітарний інструментарій протидії гібридній війні РФ проти України. Стратегічні пріоритети. 2017. No 4 (45). С. 207–214. (дата звернення: 17.11.2024 року).

48. Ієрусалимов В. Гібридні ґендерні загрози як елемент дестабілізації діяльності Верховної Ради України. Інформаційна безпека людини, суспільства, держави. 2019. No 2 (26). С. 109–115. (дата звернення: 17.11.2024 року).

49. Воєнні аспекти протидії «гібридній» агресії: досвід України: монографія колектив авторів, за заг. ред. А. М. Сиротенка. К. : НУОУ ім. Івана Черняховського, (2020). 176 с. URL: https://nuou.org.ua/assets/monography/mono_gibr_viin.pdf. (дата звернення: 17.11.2024 року).

50. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. (2016). с. 27-32. URL: http://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf (дата звернення: 17.11.2024 року).