

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ, ПРАВА ТА
МІЖНАРОДНИХ ВІДНОСИН
КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН І ПОЛІТИЧНОГО
МЕНЕДЖМЕНТУ**

**Максименко Ангеліна Ігорівна
(студентки групи ПО-1)**

КВАЛІФІКАЦІЙНА РОБОТА

**«Гібридні війни та проксі-конфлікти як виклик системі глобальної та
державної безпеки»**

(представлена на здобуття ступеня вищої освіти «бакалавр»
галузі знань 05 «Соціальні та поведінкові науки»
спеціальності 052 «Політологія»)

Допускається до захисту
протокол № _____
від _____
в.о. завідувача кафедри
міжнародних відносин
і політичного
менеджменту
д.е.н., доц.
Ірина ГРАБЧУК

(підпис)

Науковий керівник
к.політ.н.,доц. Ігор ПАЩЕНКО

(підпис)

Рецензент
к.філос.н.,доц. Оксана ЛИТВИНЧУК

(підпис)

**Житомир
2025**

Я, Максименко Ангеліна Ігорівна, цим засвідчую, що представлена до захисту кваліфікаційна робота виконана на основі власних наукових досліджень. Текст не містить доробку інших дослідників без відповідних посилань на їх праці.

Я попереджена про те, що буду недопущена до захисту, а в разі отримання диплому – буду позбавлена його відповідно до чинного законодавства України.

ЗМІСТ

ВСТУП	4
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ГІБРИДНИХ ВОЄН	7
1.1. Міжнародна безпека: еволюція та структура поняття	7
1.2. Система та ієрархія національної безпеки	15
1.3. Поняття та характеристики гібридних війн та проксі-конфліктів	21
Висновки до розділу 1	25
РОЗДІЛ 2. ОСНОВНІ ПРОБЛЕМИ СИСТЕМ МІЖНАРОДНОЇ ТА КОЛЕКТИВНОЇ БЕЗПЕКИ В ЕПОХУ ГІБРИДНИХ ВІЙН ТА ПРОКСІ-КОНФЛІКТІ	29
2.1. Система підтримання миру в рамках ООН в часи гібридних загроз	29
2.2. Діяльність ОБСЄ в контексті гібридних війн та проксі-конфліктів	34
2.3. Регіональні безпекові організації в епоху гібридних війн та проксі-конфліктів	40
Висновки до розділу 2	47
РОЗДІЛ 3. ОСНОВНІ ПРОБЛЕМИ СИСТЕМ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ЕПОХУ ГІБРИДНИХ ВІЙН ТА ПРОКСІ-КОНФЛІКТІВ	49
3.1. Системи національної безпеки країн-членів НАТО при протидії гібридній агресії	49
3.2. Системи національної безпеки позаблокових країн при протидії гібридній агресії	55
3.3. Засоби та інструменти протидії гібридній агресії та запобігання проксі-конфлікту в структурі національної безпеки України	61
Висновки до розділу 3	60
ВИСНОВКИ ТА ПРОПОЗИЦІЇ	74
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	77

ВСТУП

Актуальність обраної теми дослідження. У сучасному світі міжнародні відносини зіштовхуються з новими викликами, що призводять до появи нетрадиційних форм загроз і конфліктів. Зростання гібридних війн і проксі-протистоянь стало серйозною проблемою як для глобальної, так і для національної безпеки. Такі конфлікти характеризуються поєднанням військових і невійськових засобів впливу — зокрема кібератак, кампаній дезінформації, хакерської активності, елементів гібридної пропаганди та економічного тиску. Аналіз загроз міжнародній і національній безпеці в умовах гібридних війн і проксі-конфліктів є надзвичайно актуальним. По-перше, подібні форми протистояння суттєво впливають на політичну стабільність, економічну динаміку та соціальну стійкість окремих держав і регіонів. Вони створюють реальні ризики для національного суверенітету, територіальної цілісності та глобальної системи безпеки.

По-друге, активізація гібридних війн і проксі-конфліктів ставить під загрозу усталені принципи міжнародного права, зокрема недоторканність кордонів і перевагу мирного врегулювання спорів. У таких умовах виникає нагальна потреба у переосмисленні та адаптації чинних правових норм до реалій сучасних загроз. По-третє, глибоке усвідомлення причин, характеру та наслідків гібридних і опосередкованих конфліктів є визначальним чинником для формування дієвих стратегій забезпечення національної та глобальної безпеки. Дослідження цієї проблематики сприятиме виявленню слабких місць у системах безпеки, дозволить розробити ефективні превентивні механізми та оперативні заходи реагування. Окрім того, стрімке зростання впливу кіберпростору та цифрових технологій зумовлює посилену увагу до питань кібербезпеки та захисту критичної інфраструктури держав.

Гібридні війни та проксі-конфлікти активно використовують кібератаки як один із ключових інструментів досягнення стратегічних цілей. Ґрунтовне вивчення цієї проблематики є необхідним для формування ефективних підходів

до кібербезпеки, посилення захисних механізмів та забезпечення загальної стійкості держав і міжнародних організацій перед кіберзагрозами. Особливої актуальності ця тема набуває для України, яка з 2014 року перебуває в умовах гібридної війни, розв'язаної російською федерацією. У межах даного дослідження розглядаються окремі елементи системи національної безпеки України, спрямовані на протидію гібридним загрозам і запобігання проксі-конфліктам. Отже, дана робота має безпосереднє практичне значення для України та сприяє зміцненню безпеки в усьому регіоні. Таким чином, актуальність обраної теми полягає в необхідності всебічного аналізу й осмислення викликів міжнародної та національної безпеки в умовах гібридних та опосередкованих конфліктів. Результати дослідження стануть важливим внеском у вдосконалення стратегічних підходів, державної політики та механізмів міжнародної співпраці задля підвищення рівня безпеки, стійкості та миру в сучасному світі.

Аналіз останніх досліджень та публікацій. У рамках написання кваліфікаційної роботи у нагоді стали праці наступних вітчизняних та зарубіжних фахівців : Брежнєвої Т. В. «Стійкість як ключовий елемент колективної оборони НАТО»[37], в цій роботі було досліджено проблему стійкості в середині НАТО, вагома частина роботи присвячена протистоянню гібридним загрозам в контексті колективної безпеки та європейського регіону загалом. Монографія Д. Паламарчук «Національна безпека» [41], в цій великій роботі висвітленні майже всі елементи національної безпеки, її структура, функції, а основне, що висвітлено вразливі місця системи національної безпеки перед новітніми формами агресії, такі як гібридні війни та проксі-конфлікти.

Монографія за редакцією Власюка О. С. «Україна у системі міжнародної безпеки» [46], в цій монографії більше висвітлюється саме проблема України як суб'єкта міжнародної безпеки який активно бореться з гібридними загрозами, наводиться приклади які характеризують проблему гібридних війн та проксі-конфліктів як загроз для системи міжнародної та регіональної безпеки, а також досліджуються методи та практики удосконалення національної безпеки

України в цій сфері. Мамфорда Е. «Proxy Warfare» [56], основа цієї роботи полягає в дослідженні самого явища гібридних війн, методів ведення та застосування, але також наводяться приклади протидії таким загрозам. Прабхакаран П. «National Security: Imperatives And Challenges» [57], це дослідження присвячено сучасній системі національної безпеки, особливо цікавими є визначення, щодо викликів для цієї системи, вказується, що гібридні війни та проксі-конфлікти є одними з основних загроз сучасності і боротьба з ними є складним процесом який потребує стратегічного та оперативного концепту, і багатьох інших. Але окремі аспекти зазначеної проблеми залишаються дещо недостатньо висвітлені в науковій літературі.

Мета. Дослідити, основні проблеми міжнародної та національної безпеки в контексті сучасних загроз, теоретичну складову проблем, роботу міжнародних та регіональних безпекових організацій і проблеми національної безпеки окремих країн в цій сфері.

Завдання. Для досягнення даної мети варто виділити такі завдання:

1. Окреслити основні теоретичні засади дослідження: визначити еволюцію та структуру поняття «міжнародна безпека»; виокремити систему та ієрархію національної безпеки.

2. Проаналізувати діяльність міжнародних організацій на прикладі ООН та ОБСЄ, щодо протидії гібридній агресії, а також виокремити регіональні безпекові організації в цьому плані.

3. Спробувати систематизувати стратегії сектору національної безпеки в різних країнах світу: країнах-членах НАТО; позаблокових країнах.

4. Дослідити методи попередження і ліквідування гібридних війн і проксі-конфліктів в системі національної безпеки України.

Об'єкт дослідження – сьогодення система міжнародної безпеки та системи національної безпеки деяких країн.

Предмет дослідження – проблеми та прогалини в системі міжнародної безпеки та секторах національної безпеки в сфері боротьби з гібридними загрозами та проксі-конфліктами.

Практичне значення дослідження. Розробка стратегій протидії гібридним війнам та проксі-конфліктам: Дослідження також містить аналіз сучасних стратегій протидії гібридним війнам та проксіконфліктам. Результати цього дослідження можуть бути використані для розробки більш ефективних стратегій протидії цим явищам. Практичні рекомендації, які будуть включені в дане дослідження, можуть стати основою для розробки політики та стратегій безпеки відповідних держав і міжнародних організацій.

Кваліфікаційна робота складається зі вступу, трьох розділів, висновків та пропозицій, списку використаних джерел. Основний зміст викладено на 76 сторінках друкованого тексту, у тому числі 1 рисунок, список використаних джерел налічує 57 найменувань.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ГІБРИДНИХ ВОЄН

1.1. Міжнародна безпека: еволюція та структура поняття

У процесі визначення поняття «міжнародна безпека» доцільно насамперед звернутися до класичних підходів, які тривалий час використовувалися у працях багатьох науковців. Складність у формулюванні цього терміна полягає в тому, що історично він належав переважно до сфери військової термінології. Однак із розвитком політичних наук і, зокрема, теорії міжнародних відносин, поняття набуло ширшого змісту. Серед найбільш вживаних дефініцій варто виокремити такі:

I. Міжнародна безпека розглядається як система міжнародних відносин, заснована на дотриманні всіма державами загальновизнаних норм і принципів міжнародного права, що унеможливорює вирішення конфліктів і суперечностей шляхом застосування сили або загрози її застосування [28].

II. Це система взаємовідносин між державами, що функціонує на основі міжнародного права й виключає силові методи вирішення спорів, зокрема шляхом тиску або воєнної агресії [27].

III. Також міжнародна безпека може бути визначена як сукупність міжнародних угод та договорів, які забезпечують підтримання миру через визнання суверенітету, недоторканності кордонів, територіальної цілісності держав і відмову від сили або загрози її застосування під час врегулювання суперечок [29].

З практичного погляду використання терміна «міжнародна безпека» тісно пов'язане з розвитком багатосторонньої дипломатії. Першою історичною спробою обговорення цієї категорії на міждержавному рівні стала Гаазька конференція 1899 року, де вперше було порушено питання кодифікації норм, пов'язаних із міжнародною безпекою. Хоча ця ініціатива не досягла значного практичного результату, вона стала важливим прецедентом у напрямі

формування правових основ для регулювання воєнних конфліктів і заклала підґрунтя як для подальших наукових розвідок, так і для практичних кроків у галузі міжнародної безпеки.

Подальший розвиток ідеї міжнародної безпеки був тісно пов'язаний із діяльністю Ліги Націй — першої міждержавної організації, метою якої було сприяння міжнародному співробітництву, збереженню миру та запобігання конфліктам. Ця організація, створена за результатами Паризької мирної конференції 1919–1920 років з ініціативи 28-го президента США Вудро Вільсона [50], мала на меті не лише підтримання миру, але й забезпечення прав національних меншин та врегулювання територіальних суперечок, що виникли після Першої світової війни.

Паралельно з діяльністю Ліги Націй, у 1928 році було укладено Пакт Бріана – Келлога — міжнародну угоду, відому також як Паризька угода про відмову від війни як інструмента національної політики. Хоча ця угода була підписана незалежно від Ліги Націй, вона відіграла значну роль у формуванні концептуальних засад міжнародної безпеки. Пакт, підписаний 27 серпня 1928 року у Парижі представниками 15 держав, став результатом ініціативи французького міністра закордонних справ Арістиди Бріана та держсекретаря США Френка Келлога [43]. Він був покликаний юридично закріпити відмову від війни як засобу зовнішньої політики, тим самим закладаючи основи для подальшого розвитку нормотворчості у сфері міжнародної безпеки.

Розглядаючи процес кодифікації норм міжнародного права в контексті забезпечення міжнародної безпеки, слід звернути увагу на дві важливі міжнародні угоди — Конвенції про визначення агресії, підписані у 1933 році. Обидві ці конвенції були зареєстровані як офіційні міжнародні документи в рамках Ліги Націй і тривалий час вважалися одними з найбільш авторитетних джерел права у сфері безпеки. Саме ці документи започаткували спробу нормативного визначення агресії як міжнародного злочину, що суттєво вплинуло на подальшу правову практику.

Ці конвенції справили значний вплив на формування Статуту Організації Об'єднаних Націй — фундаментального міжнародного правового акту, який закріпив принципи недопущення агресивної війни. Відповідно до положень Статуту, держави-члени ООН зобов'язані утримуватися від використання сили у своїх міжнародних відносинах, оскільки це суперечить основним засадам діяльності Організації. Таким чином, норма про заборону агресії стала загальновизнаним міжнародним стандартом.

У Статуті ООН ці принципи отримали чітке юридичне закріплення, насамперед у Розділі I, Статтях 1 та 2. У цих положеннях визначено, що метою Організації є:

«...підтримувати міжнародний мир та безпеку і з цією метою вживати ефективних колективних заходів для запобігання та усунення загрози миру й придушення актів агресії, або інших порушень миру, і проводити мирними засобами, відповідно до принципів справедливості та міжнародного права, залагоджування або розв'язання міжнародних конфліктів або ситуацій, що можуть призвести до порушення миру» [4].

Крім того, Статут закріплює обов'язок держав:

– «розв'язувати свої міжнародні суперечки мирними засобами таким чином, щоб не наражати на загрозу міжнародний мир та безпеку і справедливість» [4];

– «утримуватися в своїх міжнародних відносинах від погрози силою або її застосування як проти територіальної недоторканності або політичної незалежності будь-якої держави, так і якимось іншим чином, несумісним із Цілями Об'єднаних Націй» [4];

– «забезпечити, щоб держави, які не є її Членами, діяли відповідно до цих Принципів, оскільки це може виявитися необхідним для підтримки міжнародного миру й безпеки» [4].

Створення зброї масового ураження, насамперед ядерної, докорінно змінило уявлення про міжнародну безпеку та сам феномен війни. Вже наприкінці XX століття стало очевидно, що національна безпека більше не може

розглядатися ізольовано: вона тісно пов'язана з міжнародною безпекою, а її забезпечення значною мірою залежить від глобального безпекового середовища. У 1980-х роках активізувався розвиток нових концепцій всеосяжної міжнародної безпеки, що свідчить про динамічну еволюцію цієї сфери в межах міжнародних відносин.

Сучасна наука та аналітичні методи переконливо доводять, що підтримання національної безпеки неможливе виключно за допомогою військових інструментів, навіть за наявності потужного озброєння. У рамках поняття «міжнародна безпека» дослідники дедалі частіше акцентують увагу на таких аспектах, як збереження миру, попередження воєн і запобігання збройним конфліктам. При цьому універсальної концепції міжнародної безпеки не існує ані в теорії, ані в історичній практиці — вона завжди залежить від конкретних історичних, політичних, регіональних і технологічних умов.

Натомість наукова думка сформувала класифікацію безпекових вимірів, яка відображає структурну складність поняття безпеки: йдеться про регіональну, екологічну, глобальну, національну та інші форми безпеки. Їх об'єднує те, що кожна з них має як історичне, так і нормативно-правове підґрунтя.

Зокрема, поняття «глобальна безпека» у межах міжнародної безпеки означає систему заходів і механізмів, спрямованих на запобігання загрозам планетарного масштабу, які становлять небезпеку для всього людства. Глобальні загрози — це явища, які зачіпають усі цивілізації, країни та народи без винятку, і можуть мати катастрофічні соціально-економічні, екологічні або біологічні наслідки. До таких належать загроза знищення людства, деструктивні процеси, що впливають на існування цілих націй і культур.

Глобальними вважають ті проблеми, які охоплюють увесь світ, здатні викликати глибокі та часто незворотні втрати, й розв'язання яких потребує скоординованої міжнародної взаємодії. До сучасних глобальних проблем відносять політичні, етнічні, демографічні, економічні, соціальні, продовольчі та екологічні виклики. Усередині цих категорій вирізняють більш специфічні

аспекти, зокрема проблеми етнічних конфліктів, енергетичну безпеку, доступ до якісної освіти та охорони здоров'я тощо [49].

Формування політики глобальної безпеки є неможливим без залучення основних суб'єктів міжнародних відносин, включаючи держави, міжнародні організації, транснаціональні корпорації, громадянське суспільство та наукові установи. Глобальна безпека як концепт є порівняно новим явищем у системі міжнародної безпеки — вперше термін набув поширення у 1960-х роках. З часом ця категорія набула автономного змісту, що відрізняється від класичних підходів до міжнародної безпеки: йдеться про охоплення універсальних проблем людства, які мають міждержавний або наддержавний характер.

Політика глобальної безпеки охоплює широкий спектр сфер і проявляється на різних часових та просторових рівнях. Серед ключових напрямів виділяють:

- Екологічну безпеку, яка включає питання деградації земель, глобального потепління, озонових дір, руйнування екосистем, техногенних катастроф, гео- та геліоактивності, а також проблеми регулювання викидів у промисловості [49].
- Економічну безпеку, що охоплює кризу ресурсів, глобальну конкурентоспроможність, процеси інтеграції та дезінтеграції світових ринків, нерівномірний розподіл благ між «старими» та «новими» економіками, а також перспективи сталого розвитку [49].
- Енергетичну безпеку, пов'язану з енергетичними кризами, ризиками експлуатації атомних електростанцій, наслідками виведення АЕС з експлуатації та аваріями, зокрема в Чорнобилі (1986) і Фукусімі (2011) [49].
- Медичну безпеку, що включає контроль за народжуваністю, демографічні програми, боротьбу з епідеміями й пандеміями (SARS, H1N1, COVID-19), а також питання старіння населення [49].
- Космічну безпеку, яка стосується проблем космічного сміття, забруднення орбіти, а також переходу до ноосферно-космічного етапу розвитку цивілізації [49].

- Озброєння та контроль над ним, зокрема моніторинг поширення ядерних технологій і діяльності країн так званого «атомного клубу» [49].
- Філософські та природничо-наукові аспекти, зокрема межі людського пізнання природи, концепції самозародження матерії тощо [49].
- Політичну безпеку, яка включає гармонізацію економічної політики між державами, уніфікацію законодавства та адаптацію національних інституцій до умов глобалізованого світу [49].
- Індустріальну трансформацію, пов'язану з переходом до постіндустріального суспільства та Третьої промислової революції [49].
- Соціальну безпеку, що включає питання демографічного переходу, продовольчу безпеку, перенаселення, експорт демократичних цінностей, асиміляційні процеси в межах глобалізації, а також технологічну й цивілізаційну модернізацію [49].
- Технологічну безпеку, яка охоплює глобальні процеси інформатизації, наслідки технологічного прогресу та обмеження сучасних технологій [49].

Доцільним є поглиблене вивчення політичного виміру глобальної безпеки, оскільки в сучасних умовах він суттєво виходить за рамки традиційно військових підходів. Політика глобальної безпеки дедалі частіше охоплює аспекти економічної взаємозалежності та інституційної інтеграції, що відображає нову реальність міжнародних відносин у ХХІ столітті.

Одним із ключових чинників забезпечення стабільності як на національному, так і на глобальному рівні є взаємопристосування економічних моделей і господарських механізмів різних держав. Усі учасники світового економічного процесу, особливо ті, що глибоко інтегровані у глобальну економіку, змушені узгоджувати свої внутрішні політики з міжнародними нормами та стандартами. Це не лише сприяє формуванню передбачуваного середовища для міжнародної співпраці, а й знижує ризики виникнення міждержавних конфліктів на економічному ґрунті.

Особливе значення у цьому контексті має гармонізація інституційних структур — процес, що реалізується, зокрема, через участь держав у діяльності міжнародних організацій, таких як Світова організація торгівлі (СОТ), Міжнародний валютний фонд (МВФ), Європейський Союз (ЄС), Організація Об'єднаних Націй (ООН) тощо. Координація дій у сферах торгівлі, фінансів, енергетики, екології та правового регулювання дозволяє країнам не лише ефективніше реагувати на кризові ситуації, а й знижувати вразливість до гібридних загроз.

Такий підхід зменшує можливості для застосування економічного тиску як інструмента політичного впливу, зокрема в контексті гібридних війн. Інституційна співпраця посилює довіру між державами, підвищує рівень прозорості політики та створює додаткові механізми для мирного врегулювання суперечностей. У підсумку, політична складова глобальної безпеки стає не лише елементом стримування агресії, а й інструментом формування конструктивного, збалансованого та безпечного міжнародного середовища.

Важливою складовою є також узгодження національної та міжнародної економічної політики, що передбачає спільне реагування на глобальні виклики, включаючи фінансові кризи, енергетичну нестабільність, кліматичні ризики та продовольчу безпеку. Узгоджена політика дає змогу уникати суперечностей між державами, знижуючи ймовірність конфліктів на економічному ґрунті. Крім того, уніфікація господарського законодавства сприяє формуванню єдиного правового простору, в якому інвестиції захищені, а правові механізми врегулювання спорів — ефективні та справедливі. Усе це перетворює економіку на інструмент не боротьби, а співпраці, підсилюючи фундамент глобальної безпеки.

Таким чином, сучасна політика глобальної безпеки не може існувати без комплексної взаємодії економічних, правових та інституціональних механізмів, які забезпечують умови для сталого розвитку, зміцнення міжнародної довіри та мінімізації ризиків гібридних загроз і проксі-конфліктів. Усе це створює підґрунтя для формування більш стійкої системи міжнародних відносин.

Водночас важливо враховувати, що загрози безпеці нерідко мають яскраво виражену регіональну специфіку, а тому питання регіональної безпеки становить невід'ємну складову загальної архітектури міжнародної безпеки. Однак політика глобальних акторів має обмежений вплив на специфічні процеси в окремих регіонах [25]. Регіональна безпека — це форма міжнародної безпеки, яка реалізується у межах певного географічного простору. Хоч вона подібна за суттю до міжнародної безпеки, однак має низку відмінностей, пов'язаних із локальними традиціями, співвідношенням сил та особливостями політичного ландшафту.

По-перше, забезпечення регіональної безпеки часто здійснюється як міжнародними організаціями (наприклад, ОБСЄ), так і через регіональні інтеграційні об'єднання, такі як Організація Африканської Єдності (ОАЄ). Регіональні структури безпеки виступають ключовими суб'єктами у врегулюванні конфліктів, запобіганні ескалації загроз і розбудові миру. По-друге, ефективна підтримка безпеки в регіоні потребує залучення та координації зусиль багатьох держав [56].

У цьому контексті поняття «регіон» у сфері безпеки варто розуміти як групу держав, об'єднаних спільною системою безпеки, що функціонує в межах конкретного географічного простору і орієнтована на реагування на характерні для нього загрози. Із завершенням епохи «Холодної війни» традиційні межі регіонів зазнали трансформацій. Наприклад, Близький і Середній Схід, що раніше розглядалися як окремі регіони, у сфері безпеки нині дедалі частіше об'єднуються в концепт Великого Близького Сходу. Подібні інтеграційні зрушення простежуються й в Азіатсько-Тихоокеанському регіоні. Водночас деякі країни, як-от Туреччина, можуть одночасно належати до кількох безпекових регіонів — європейського, євразійського тощо [26].

Окрему увагу заслуговує аналіз рівня «напруженості» регіонів, тобто ступеня складності в забезпеченні в них безпеки. Існує умовний поділ на стабільні регіони (наприклад, Європа) та регіони з високим конфліктним потенціалом (як-от Африка, Близький Схід). У цьому контексті особливої

актуальності набуває пострадянський простір, де військово-політична нестабільність, поява нових авторитарних режимів і прагнення до силового перерозподілу сфер впливу створюють загрозу як для окремих країн, так і для всього регіону.

Після розпаду СРСР теорія міжнародної безпеки почала приділяти більше уваги субрегіональному виміру. Йдеться про відносно компактні зони з тісними економічними, політичними та безпековими зв'язками — наприклад, Балтійський чи Чорноморський субрегіони. Вивчення таких утворень дозволяє краще зрозуміти специфіку локальних викликів та засобів їх нейтралізації.

Отже, міжнародна безпека — це динамічне та багатогранне поняття, яке постійно змінюється під впливом глобальних, регіональних і локальних процесів. Його розвиток обумовлений як науковими підходами в галузі міжнародних відносин, політології, історії та військової науки, так і еволюцією практичних механізмів протидії сучасним загрозам.

1.2. Система та ієрархія національної безпеки

Національна безпека трактується як здатність держави своєчасно і ефективно виявляти, запобігати та нейтралізувати реальні й потенційні загрози своїм національним інтересам. У широкому значенні вона охоплює захист фундаментальних інтересів особистості, суспільства та держави, а також забезпечення сталого розвитку та стабільного функціонування соціально-політичних, економічних і правових систем [51].

Для забезпечення національної безпеки необхідним є чітке визначення та систематизація основних понять, що використовуються в цій галузі. У рамках сучасної теорії національної безпеки виділяють цілий комплекс термінів, зокрема: національні інтереси, стратегія національної безпеки, загрози національній безпеці, система національної безпеки, забезпечення національної безпеки, сектор безпеки тощо.

Ключові елементи національної безпеки:

- Національні інтереси — це сукупність матеріальних, інтелектуальних, духовних і культурних цінностей, що мають першочергове значення для збереження державного суверенітету, територіальної цілісності, політичної стабільності, а також поступального розвитку держави. Вони визначають стратегічні потреби суспільства й держави та є орієнтиром для політики у сфері безпеки [20].

- Загрози національній безпеці — це реальні або потенційні чинники (явища, процеси, дії), що можуть завдати шкоди життєво важливим інтересам держави та суспільства. Вони охоплюють широкий спектр — від воєнних і терористичних до економічних, інформаційних та екологічних [20].

- Воєнна організація держави включає сукупність державних органів і військових формувань, що функціонують на основі національного законодавства. Основна мета їхньої діяльності — забезпечення обороноздатності та захисту держави від зовнішніх і внутрішніх загроз. Їх функціонування здійснюється під демократичним цивільним контролем з боку суспільства [20].

- Правоохоронні органи — це структура державного управління, яка наділена повноваженнями забезпечувати дотримання законності, охорону прав і свобод громадян, боротьбу зі злочинністю, а також здійснювати правопорядок на всій території держави [20].

Принципи забезпечення національної безпеки:

1. Пріоритет прав і свобод людини та громадянина — уся безпекова діяльність повинна відповідати основоположним правам і свободам, закріпленим у Конституції [20].

2. Верховенство права — діяльність усіх суб'єктів системи національної безпеки має здійснюватися виключно в межах правового поля [20].

3. Мирне врегулювання конфліктів — держава зобов'язується надавати перевагу договірним, дипломатичним і ненасильницьким засобам врегулювання суперечностей [20].

4. Оперативність реагування на загрози — держава повинна забезпечувати своєчасні дії щодо виявлення та нейтралізації ризиків, що загрожують національним інтересам [20].

5. Чітке розмежування повноважень між органами державної влади — розмежування компетенцій сприяє ефективній координації дій усіх суб'єктів національної безпеки [20].

6. Демократичний цивільний контроль над воєнною організацією — один із базових елементів, що гарантує підзвітність і підконтрольність силових структур суспільству [20].

7. Інтеграція у міжнародну систему колективної безпеки — активна участь у міжнародних механізмах безпеки дозволяє зміцнювати власну безпекову систему через багатостороннє співробітництво [20].

Аналізуючи типи національної безпеки, доцільно зосередитись на категоріях внутрішньої та зовнішньої безпеки, які є тісно взаємопов'язаними складовими загальної безпекової системи держави. Ці поняття активно використовуються як у публіцистичній, так і в науковій літературі, хоча й не мають чітко визначеного юридичного закріплення в основних нормативно-правових актах, зокрема в Законі України «Про основи національної безпеки України». Внутрішня безпека означає рівень захищеності національних інтересів від загроз, джерелами яких є внутрішні чинники: процеси, явища або дії (чи бездіяльність) фізичних та юридичних осіб, що перебувають на території держави та під її юрисдикцією. Її забезпечення значною мірою залежить від можливостей державної влади, здатності інституцій вчасно реагувати на виклики, ефективності механізмів контролю й стабільності політичної, економічної, соціальної та духовної сфер. У свою чергу, зовнішня безпека визначається як рівень захищеності національних інтересів від загроз, що походять із-за меж державної території і не підлягають прямому впливу національної юрисдикції. До таких загроз належать дії іноземних суб'єктів, міжнародні кризи, зовнішньополітичний тиск, збройна агресія або міжнародний тероризм. Їхня інтенсивність, характер і тривалість часто визначаються не лише

внутрішніми можливостями держави, а й конфігурацією міжнародної системи, місцем країни в ній, наявністю або відсутністю союзників, а також здатністю міжнародних безпекових структур реагувати на виклики. При цьому внутрішня безпека значною мірою впливає на здатність держави забезпечувати зовнішню, адже внутрішня дестабілізація послаблює позиції на міжнародній арені. Аналіз системи національної безпеки вимагає також урахування її поділу за сферами життєдіяльності суспільства й держави. Такий поділ хоча й не завжди має чітке наукове підґрунтя, проте широко використовується в законодавстві, державних стратегіях та управлінських документах. У цьому контексті національна безпека охоплює політичну, економічну, енергетичну, воєнну, екологічну, інформаційну та державну безпеку. Ці складові тісно переплітаються, формуючи цілісну систему, здатну реагувати на багатовекторні загрози, що виникають унаслідок змін внутрішнього стану держави або міжнародної ситуації. Таким чином, національна безпека є динамічним поняттям, яке охоплює як внутрішні, так і зовнішні аспекти життєдіяльності держави, вимагаючи комплексного, міждисциплінарного підходу до її вивчення, формування політики та реалізації відповідних заходів.

Серед іноземних публікацій найбільш ґрунтовний підхід до класифікації елементів національної безпеки представлено у праці індійського науковця та публіциста Прабхакарана Палері «National Security: Imperatives and Challenges» (2008). У цій роботі автор виділяє розширену систему складників національної безпеки, серед яких: військова безпека, економічна безпека, безпека ресурсів, прикордонна безпека, демографічна безпека, безпека на випадок катастроф, енергетична безпека, геостратегічна безпека, інформаційна безпека, продовольча безпека, безпека здоров'я, етнічна безпека, екологічна безпека, кібербезпека та геномна безпека [46].

Палері сформулював ці категорії, спираючись на те, що кожна з них має представляти собою цілісну концепцію, що є універсальною у застосуванні, має соціальне значення на макрорівні та справляє прямий вплив на повсякденне життя людини. На його думку, ці елементи мають бути постійно вразливими до

загроз, функціонувати безперервно від моменту свого формування до сучасного існування (навіть у разі періодичних проявів), а також відповідати сучасному уявленню про «природну безпеку», що набула широкого поширення в новітньому політичному дискурсі. Водночас автор критично оцінює вживання певних термінів, які часто з'являються у публічних обговореннях тематики безпеки, зокрема «тероризм» чи «соціальне забезпечення», вважаючи їх такими, що не відповідають принципу концептуальної цілісності [46].

Одним із ключових елементів структури національної безпеки є система національної безпеки, яка відображає ієрархію та логіку організації всіх процесів у сфері захисту державних інтересів. До її складових належать, зокрема, об'єкти національної безпеки, під якими розуміють національні матеріальні та духовні цінності, інтереси особи, суспільства й держави. Не менш важливу роль відіграє корпус чинного національного законодавства, що визначає пріоритети державної політики у сфері безпеки та закріплює офіційні підходи, принципи й механізми захисту національних інтересів. Важливими елементами системи є також сукупність зовнішніх і внутрішніх факторів, які впливають на стан національної безпеки. До них відносять не лише динамічні змінні, такі як тенденції, статистичні показники чи стратегічні цілі, а й системи зовнішнього впливу, включаючи міжнародні структури безпеки, їхню діяльність, пріоритети та наслідки реалізованих політик.

Суб'єктами забезпечення національної безпеки виступають органи державної влади та місцевого самоврядування, інститути громадянського суспільства, окремі громадяни, а також засоби масової інформації. Сукупність інструментів, які перебувають у розпорядженні держави — політичних, економічних, воєнних, інформаційних — формують арсенал засобів забезпечення безпеки. До них належать збройні сили, спеціальні служби, підприємства оборонно-промислового комплексу, дипломатичні механізми, державні резерви та інші ресурси, здатні ефективно реагувати на загрози. Окрему категорію становлять національні джерела загроз — це фізичні та юридичні

особи, чия діяльність чи бездіяльність може перешкоджати реалізації національних інтересів та підривати безпекову архітектуру держави [46].



Рис.1.1. Структура та ієрархія національної безпеки

Отже, структура та ієрархія національної безпеки на сучасному етапі є достатньо дослідженими в теоретичному та прикладному аспектах, однак актуальність подальшого осмислення цієї теми зберігається, з огляду на постійне оновлення загроз та трансформацію глобального і регіонального безпекового середовища. На завершення цього розділу доцільно підсумувати основні положення, зосередившись на ключових елементах структури та ієрархії національної безпеки.

Перш за все, можна виділити базові складові, до яких належать політичні, економічні та концептуально-світоглядні компоненти. Саме на їх основі вибудовується внутрішньо стійка система безпеки, що забезпечує стабільне функціонування суспільства, держави та захист прав і свобод громадян. Ці

елементи формують фундамент ідеологічної, правової та організаційної основи всієї системи національної безпеки.

Іншим важливим аспектом є інструментарій, під яким слід розуміти сукупність засобів, методів, стратегій, концепцій, тактик і механізмів, що використовуються для досягнення цілей у сфері безпеки. Цей «арсенал» охоплює як внутрішньополітичні, так і зовнішньополітичні ресурси, спрямовані на виявлення, стримування та нейтралізацію загроз, а також на збереження належного рівня захищеності національних інтересів у різних сферах суспільного життя.

Не менш значущим елементом у структурі національної безпеки є апарат управління та прийняття рішень, до якого входять інституції, уповноважені на розроблення та реалізацію державної політики у сфері безпеки. Йдеться про координаційні, аналітичні, силові та виконавчі структури, діяльність яких спрямована на своєчасне реагування на загрози, формування стратегій протидії, а також організацію заходів з ліквідації наслідків потенційних або реальних кризових ситуацій як на регіональному, так і на загальнодержавному рівні.

Таким чином, національна безпека є системним утворенням із чітко вибудованою ієрархією, що ґрунтується на поєднанні базових ціннісних орієнтирів, ефективного інструментарію впливу та функціонування керівних органів державної влади. Саме комплексна взаємодія цих складників дозволяє забезпечити сталість розвитку держави та збереження її суверенітету в умовах сучасних глобальних викликів.

1.3. Поняття та характеристики гібридних війн та проксі-конфліктів

Гібридні війни та проксі-конфлікти не є абсолютно новими явищами в міжнародних відносинах, однак їх активізація в умовах ХХІ століття та поглиблення теоретичного осмислення з боку науки про міжнародні відносини сприяли формуванню окремого напрямку досліджень, який набув актуальності не лише в академічному середовищі, а й серед політичних еліт, військових стратегів і фахівців із безпеки. У контексті трансформації світового порядку та ускладнення архітектури міжнародних відносин, нові виклики постали перед державами й іншими суб'єктами глобальної політики. Зокрема, суттєвою загрозою сьогодні виступають так звані «тихі війни» — конфлікти, що ведуться без офіційного оголошення, із застосуванням засобів прихованого, непрямого впливу, включно з використанням проксі-сил.

Особливу небезпеку становить те, що саме гібридні та проксі-конфлікти активно використовуються недемократичними державами з ревізіоністськими або імперіалістичними амбіціями, які прагнуть змінити існуючий баланс сил, уникаючи прямого зіткнення з сильнішими противниками. На практиці явища гібридної війни вже стали буденними в риториці політиків, військових, журналістів, експертів з національної безпеки. Уряди створюють спеціалізовані підрозділи, аналітичні центри та міжвідомчі експертні групи, що займаються вивченням, прогнозуванням і протидією системним гібридним загрозам. Більш того, в структурі збройних сил провідних країн з'являються командування, що спеціалізуються саме на гібридних конфліктах, інформаційних і психологічних операціях, кібербезпеці та асиметричних тактиках, що підтверджує високий рівень усвідомлення загроз, пов'язаних із такими типами війни.

Основною метою гібридної війни може слугувати досягнення стратегічних або тактичних національних інтересів однієї держави шляхом підриву стабільності іншої держави, ослаблення її міжнародних позицій або навіть повного виведення з геополітичної гри. У таких випадках мова йде не лише про наступальну форму гібридної агресії, а й про оборонну тактику, яку може

використовувати держава-жертва. Якщо проти неї ведеться гібридна війна, вона, як правило, виробляє власну систему реагування, стримування і протидії, адаптовану до складних та багатовекторних викликів.

Для розуміння феномену гібридної війни доцільно почати з аналізу її визначення. В сучасній науковій та експертній літературі існує велика кількість дефініцій цього поняття, що зумовлено його відносною новизною та складністю класифікації. Попри це, одним із найбільш влучних є таке визначення: «Гібридна війна — війна з поєднанням в застосуванні конвенційної зброї, партизанської війни, тероризму та злочинної поведінки з метою досягнення певних політичних цілей, основним інструментом якої є створення державою-агресором в державі, обраній для агресії, внутрішніх протиріч та конфліктів з подальшим їх використанням для досягнення політичних цілей агресії, які досягаються звичайною війною» [48].

У ширшому розумінні гібридна війна — це сукупність заздалегідь підготовлених та оперативно реалізованих заходів військового, дипломатичного, інформаційного, економічного та правового характеру, спрямованих на досягнення стратегічних цілей без обов'язкового ведення масштабних бойових дій. Однією з характерних рис є відсутність потреби у створенні принципово нових систем озброєння чи технічних засобів, адже агресор здебільшого використовує наявні засоби — військові, пропагандистські, фінансові, кібертехнологічні — в нестандартних, часто комбінованих формах.

До складу гібридної війни входить цілий спектр гібридних загроз: від традиційних військових операцій до нестандартних форм, таких як масові кібератаки, підривна діяльність у фінансовій, енергетичній чи інформаційній сферах, кампанії дезінформації, масштабний тероризм, а також маніпулятивне використання етнічних, релігійних або соціальних протиріч. У сукупності ці засоби створюють багаторівневу конфігурацію впливу, метою якої є дестабілізація, деморалізація, ослаблення або повне підпорядкування держави-мішені [35].

Авжеж, сучасні події в міжнародних відносинах не лише доповнюють, але й трансформують уявлення про характер і динаміку гібридних конфліктів. Яскравим прикладом є повномасштабне вторгнення Російської Федерації в Україну у 2022 році, яке вже стало предметом міжнародного аналізу й, без сумніву, залишиться в центрі наукової уваги ще багато років. Однак варто пам'ятати, що цей акт відкритої агресії став продовженням восьмирічної гібридної війни, яку Росія вела проти України з 2014 року, використовуючи широке коло інструментів — від інформаційних кампаній до економічного шантажу та дестабілізації регіонів Донбасу й Криму.

Саме гібридна агресія Росії стала каталізатором глибокого дослідження цього феномену як у західному, так і в українському науковому дискурсі. На основі досвіду України були створені аналітичні моделі, розроблені військові концепції протидії, засновані експертні платформи та спеціалізовані підрозділи в системі національної безпеки. Наразі характеристика гібридних війн вже є відносно систематизованою, і в цьому контексті можна виокремити кілька основних елементів, які становлять її структуру.

Політико-дипломатичний компонент спрямований на підрив міжнародної легітимності країни-жертви, погіршення її іміджу на міжнародній арені, обмеження контактів з іншими державами та міжнародними організаціями. Економічний складник включає деструктивні дії щодо фінансової системи, валютні маніпуляції, санкційні атаки, економічне шантажування, блокування зовнішньої торгівлі. Інформаційно-психологічний елемент реалізується через поширення дезінформації, маніпулятивних наративів, фейкових новин, провокаційних меседжів, спрямованих на дестабілізацію громадської думки, підрив морального духу населення та формування умов для внутрішньої деструкції. Кіберкомпонент полягає у здійсненні кібератак на критичну інфраструктуру, зламі державних інформаційних систем, втручанні у виборчі процеси, шпигунстві, кібершантажі.

Енергетичний вимір гібридної війни включає контроль над поставками енергоносіїв, маніпуляції ринками газу, нафти, електроенергії, а також створення штучних енергетичних криз для впливу на політику країни-жертви. Військовий елемент передбачає залучення нерегулярних збройних формувань, парамілітарних структур, приватних військових компаній, а також підтримку повстанських угруповань з метою дестабілізації внутрішньої ситуації. Внутрішньополітичний інструментарій охоплює створення та просування маріонеткових політичних сил, підкуп та шантаж представників влади, політичне шпигунство, проникнення в органи державного управління.

У цьому контексті також важливо зупинитися на менш дослідженому, але не менш важливому явищі — проксі-конфліктах. На відміну від гібридних воєн, що здебільшого асоціюються з багатовекторними, комбінованими методами впливу, проксі-війни мають чітко виражену воєнно-політичну структуру. Вітчизняна наукова література поки що приділяє недостатньо уваги цьому феномену, зокрема через те, що проксі-війни часто помилково ототожнюються або підміняються поняттями гібридного конфлікту. Насправді ж проксі-конфлікти мають власну природу, масштаби та логіку.

Класичне визначення, подане Карлом Дойчем ще у 1964 році, визначає проксі-війну як міжнародний конфлікт між двома державами, які реалізують свої інтереси на території третьої країни, використовуючи її ресурси, внутрішні суперечності та збройні формування, під прикриттям підтримки або втручання у внутрішній конфлікт цієї країни [44]. Проксі-війна фактично дозволяє впливовим державам уникнути прямого військового зіткнення, делегуючи бойові дії або інші активні дії місцевим чи регіональним силам. Це робить її особливо привабливою для держав, які прагнуть мінімізувати власні втрати, але зберегти контроль над ситуацією або утвердити свої геополітичні амбіції.

Точного й універсально визнаного визначення поняття «проксі-війна» у науковій літературі досі не існує. Це пояснюється складністю, багат шаровістю та змінністю цього явища залежно від історичних і політичних обставин.

Класичне визначення, сформульоване Карлом Дойчем у 1964 році, хоча й стало підґрунтям для подальших досліджень, зазнає критики з боку сучасних авторів, зокрема А. Мамфорда. Останній вважає, що модель Дойча, створена в умовах Холодної війни, надмірно зосереджується на державних суб'єктах і не враховує впливу недержавних акторів, які відіграють дедалі більшу роль у сучасних збройних конфліктах [44].

Значний внесок Мамфорда у теорію проксі-війни полягає в тому, що він сформулював дев'ять критичних питань (на основі розвідки Якова Бар-Сіман-Това), які допомагають глибше осмислити сутність цього феномену. Відповідаючи на них, Мамфорд уточнює, що обов'язковою рисою проксі-війни є непряме втручання зовнішньої сили, а не її безпосередня участь. Симетрія зовнішнього впливу не є визначальною: достатньо, щоб хоча б одна сторона конфлікту діяла в інтересах третьої держави. Важливо також, що сам факт проксі-війни рідко публічно визнається країнами-спонсорами, які надають перевагу термінам на кшталт «підтримка», «допомога», «кооперація» тощо.

На відміну від традиційних військових союзів, де учасники готові нести однакові ризики та жертви, проксі-війна передбачає навпаки — небажання держави-спонсора зазнавати втрат, натомість використовується чужа територія, ресурси та людські життя. Мамфорд підкреслює суб'єктивність інтерпретації: для визнання війни проксі-конфліктом недостатньо лише факту допомоги, важливо також оцінити наміри, мотивацію та рівень контролю над учасником, що виступає в ролі проксі. Цікавою є також його думка, що навіть невеликі держави можуть використовувати проксі-механізми, не усвідомлюючи масштабних наслідків. У цьому контексті він наводить приклад США, які у 2003 році в Іраку, на його думку, певною мірою діяли як проксі-сила Ірану, не усвідомлюючи складної геополітичної конфігурації.

Окремо Мамфорд проводить межу між проксі-війною та таємною операцією: якщо держава безпосередньо втручається, навіть приховано, то йдеться радше про секретну військову акцію, а не класичну проксі-модель. Проте

обидва явища часто переплітаються, адже проксі-війни нерідко потребують прикриття, а отже — і засобів прихованого впливу.

Не менш важливим є питання наслідків застосування інструментарію проксі-конфліктів. Мамфорд наголошує на небезпеці залежності: під час Холодної війни низка африканських країн, залучених у проксі-війни, фактично потрапила у стан залежності від СРСР чи США. Такі держави хоча й зберігали формальну незалежність, але втрачали політичну та економічну самостійність, що мало довгострокові наслідки. Крім того, ідея, що проксі-війна — це «ефективний спосіб» швидкого завершення конфлікту, є хибною. Насправді, участь зовнішніх акторів лише затягує конфлікт, оскільки програючій стороні надаються ресурси для продовження опору, що перетворює війну на затяжне й руйнівне протистояння. Це створює ситуацію «балансу насильства», коли жодна зі сторін не здатна перемогти, але й не припиняє бойові дії.

Також варто звернути увагу на те, що проксі-війни зазвичай не мають розширення театру бойових дій, оскільки залучені сторони свідомо уникають прямої ескалації. Проте якщо розширення відбувається, то, як зазначає Мамфорд, зазвичай це відбувається несподівано, без прямого контролю й часто супроводжується новими геостратегічними ризиками. При цьому в основі проксі-конфліктів часто лежить логіка «ворог мого ворога — мій союзник», що, з одного боку, спрощує об'єднання сил, але з іншого — створює вкрай нестабільні альянси, засновані не на спільних цінностях, а на ситуативному співпадинні інтересів.

У підсумку, проксі-війна як форма сучасного міжнародного конфлікту має багатовимірну природу, що виходить за межі простої формули «війна чужими руками». Її інструменти, наслідки, логіка впливу та типологія учасників вимагають глибокого аналізу з урахуванням нових викликів безпеки, ролі недержавних акторів та трансформації міжнародної системи.

Однак, як демонструє практика, проксі-війни нерідко супроводжуються так званим «зворотним ударом» (англ. *blowback* — термін, що використовується в аналітичній термінології ЦРУ), коли наслідки зовнішнього втручання

виявляються несподіваними, небажаними та довготривалими для країни-спонсора. Це відбувається в тих випадках, коли інтереси зовнішнього актора й сил, які він підтримує, збігаються лише ситуативно. Прикладом цього явища, на думку Мамфорда, є рішення США під час війни в Афганістані забезпечити антиурядові повстанці — моджахедів — протиповітряними ракетами «Стінгер». Незважаючи на спроби американців згодом вилучити ці ракети, вони поширилися далеко за межі Афганістану, зокрема у зони конфліктів на Балканах і в Палестині.

Ще одним проявом blowback стало те, що після закінчення війни в Афганістані ці ж моджахеди заклали фундамент для створення осередків ісламського фундаменталізму, включно з формуванням руху «Талібан», який згодом став реальним політичним і військовим чинником у регіоні. Американські політики недооцінили можливі наслідки такого повороту подій: навіть у 1998 році Збігнєв Бжезінський риторично запитував: «Що було важливіше у світовій історії: Талібан чи падіння радянської імперії? Декілька перезбуджених ісламістів чи визволення Центральної Європи...?» — не усвідомлюючи, що наслідки цієї підтримки невдовзі втіляться в одному з найтрагічніших актів терору — атаках 11 вересня 2001 року [44].

Отже, викладені вище теоретичні положення становлять значну наукову цінність у контексті осмислення змісту й природи ключових понять: «міжнародна безпека», «національна безпека», «гібридна війна» та «проксі-конфлікт». Їх уточнення й розвиток у працях сучасних дослідників формують методологічне підґрунтя для подальшого наукового аналізу та критичного переосмислення глобальних і регіональних загроз. Це дає змогу не лише глибше опрацювати зазначену тематику в академічному просторі, але й застосовувати ці знання на практиці — у сфері державної політики, міжнародної дипломатії та безпекових стратегій.

Висновки до розділу 1

У першому розділі розкрито комплексну природу понять міжнародної та національної безпеки, а також сучасні форми конфліктів, зокрема гібридні війни та проксі-конфлікти. Поняття міжнародної безпеки еволюціонувало від військової доктрини до багатовимірної системи, що включає правові, політичні та інституційні механізми, спрямовані на запобігання конфліктам і забезпечення стабільності у світі. Особливу увагу приділено ролі міжнародних організацій, таких як Ліга Націй, ООН, а також концепціям глобальної безпеки, що стали актуальними у другій половині XX століття. Визначено, що міжнародна безпека включає в себе як глобальний, так і регіональний рівні. Глобальна безпека охоплює питання, пов'язані із загрозами всьому людству — екологічними, енергетичними, технологічними, соціальними та іншими, і вимагає координації зусиль більшості міжнародних акторів. Регіональна безпека натомість має свої особливості залежно від конфігурації регіону, геополітичних інтересів та наявності загроз, що притаманні конкретному простору.

У частині, присвяченій національній безпеці, акцент зроблено на її визначенні як здатності держави захищати свої національні інтереси, протистояти зовнішнім і внутрішнім загрозам, а також забезпечувати стійкий розвиток. Систему національної безпеки охарактеризовано як багаторівневу структуру, яка охоплює безпеку у політичній, економічній, військовій, інформаційній, екологічній, енергетичній та інших сферах. Розкрито роль суб'єктів забезпечення безпеки, включаючи органи влади, військові структури, громадянське суспільство, ЗМІ. Зроблено акцент на пріоритеті прав людини, верховенстві права, демократичному цивільному контролі та міждержавній кооперації у сфері безпеки.

Важливою складовою дослідження стали гібридні війни та проксі-конфлікти — явища, що відображають нову природу воєн та міжнародних конфліктів у XXI столітті. Гібридна війна — це поєднання традиційних військових дій із кібератаками, економічним тиском, інформаційними

кампаніями та використанням внутрішніх протиріч у державі-жертві. Проксі-війни, в свою чергу, є формою непрямого військового протистояння, коли зовнішні держави реалізують свої інтереси через підтримку третіх сторін у внутрішніх конфліктах інших країн. Обидва явища є прикладами сучасних загроз, які можуть бути важко ідентифіковані та ефективно нейтралізовані за допомогою традиційних механізмів безпеки.

РОЗДІЛ 2. ОСНОВНІ ПРОБЛЕМИ СИСТЕМ МІЖНАРОДНОЇ ТА КОЛЕКТИВНОЇ БЕЗПЕКИ В ЕПОХУ ГІБРИДНИХ ВІЙН ТА ПРОКСИ-КОНФЛІКТИ

2.1. Система підтримання миру в рамках ООН в часи гібридних загроз

Організація Об'єднаних Націй (ООН) є найважливішою універсальною міжнародною організацією сучасності, покликаною підтримувати та зміцнювати міжнародний мир і безпеку, сприяти мирному співіснуванню держав і розвитку співробітництва між ними. Її роль у сучасній системі міжнародних відносин є визначальною, оскільки саме ООН виступає головним майданчиком для діалогу, врегулювання конфліктів та прийняття колективних рішень на глобальному рівні [36]. Хоча ідея створення організації, здатної запобігати війнам і сприяти збереженню миру, з'явилася задовго до ООН, попередні спроби були переважно неефективними. Найбільш відомим прикладом стала Ліга Націй, заснована у 1919 році. Попри високі очікування, ця структура не змогла запобігти спалахам воєн і збройних конфліктів, зокрема агресії нацистської Німеччини, що зрештою призвело до її розпаду в 1946 році.

Поштовхом до створення ООН стала Друга світова війна, яка, попри свою руйнівну силу та глобальні втрати, водночас сприяла консолідації людства навколо ідеї потреби в новій міжнародній архітектурі безпеки. Проте на момент її створення концепція гібридних загроз не була сформульована, і відповідно, не знайшла відображення в Статуті ООН. Це пояснюється як відсутністю чіткого розуміння природи новітніх конфліктів, так і тим, що міжнародне право того часу було зосереджене переважно на класичних формах міждержавних війн. Навіть у Женевських конвенціях 1949 року, де йдеться про застосування їхніх положень у випадках збройного конфлікту, не надається юридичного значення формальному оголошенню війни, що є важливим у контексті гібридних війн, які часто відбуваються без офіційної декларації [6].

З моменту свого заснування ООН відіграє ключову роль у гарантуванні міжнародного миру, використовуючи широкий набір інструментів – від дипломатичних зусиль до економічного тиску та миротворчих операцій. Особливе значення має система миротворців ООН, яка стала одним з основних інструментів реагування на конфлікти. Проте в умовах трансформації характеру загроз миротворча діяльність ООН стикається з новими викликами. Гібридні війни, які включають кібератаки, кампанії дезінформації, економічний тиск, використання недержавних акторів та інших нестандартних інструментів, вимагають переосмислення існуючих механізмів безпеки, оскільки традиційні підходи не завжди є ефективними в умовах асиметричних конфліктів.

У цьому контексті важливо також згадати про юридичну категорію «агресії», яка регулюється міжнародним правом і безпосередньо стосується мандату ООН у сфері миру та безпеки. Згідно з Резолюцією 3314 Генеральної Асамблеї ООН від 14 грудня 1974 року, агресія визначається як застосування збройної сили державою проти суверенітету, територіальної недоторканності чи політичної незалежності іншої держави або будь-яким іншим чином, що несумісний зі Статутом ООН. Зазвичай акт агресії вважається таким, коли саме держава-агресор першою застосовує збройну силу [1].

Проблематика гібридних загроз полягає насамперед у їх складній природі та труднощах з ідентифікацією, оскільки такі загрози передбачають використання як державних, так і недержавних акторів, взаємодія між якими часто має прихований, непрозорий і багаторівневий характер. У сучасних умовах гібридні загрози набувають дедалі більш системного характеру й становлять серйозний виклик для глобальної безпеки, оскільки поєднують елементи військової сили, економічного тиску, інформаційних операцій, кіберзагроз та внутрішньої дестабілізації. Особливістю таких загроз є їхня асиметричність та здатність завдавати шкоди без формального початку бойових дій, що робить їх складними для виявлення та протидії на ранніх етапах.

Система миротворчої діяльності ООН історично була орієнтована на реагування на класичні загрози миру, включаючи міждержавні конфлікти та

внутрішні громадянські війни. Проте з огляду на зростання ролі гібридних загроз постала необхідність адаптації миротворчого потенціалу ООН до нових викликів. Для ефективного реагування в умовах гібридних конфліктів потрібен комплексний підхід, що поєднує військові, дипломатичні та цивільні засоби. До таких засобів належать оперативний обмін розвідданими, моніторинг кіберпростору, боротьба з дезінформацією, а також захист критичної інфраструктури.

Однією з найбільших проблем є те, що джерелом гібридної загрози можуть виступати самі держави-члени ООН, які, користуючись інструментами проксі-впливу та інформаційного маніпулювання, уникають прямої відповідальності. Це створює колізії як в організаційно-політичному, так і в міжнародно-правовому вимірах, унеможливаючи оперативне прийняття санкцій чи інших колективних рішень проти агресора. У відповідь на це деякі дослідники пропонують застосовувати стратегії стримування, зокрема дипломатичне викриття агресора, демонстрацію єдності міжнародної спільноти, встановлення чітких "червоних ліній" щодо втручання у справи інших держав, посилення обізнаності про ворожу діяльність у структурах ООН та інших глобальних форумах [30].

Відповіддю ООН на гібридні виклики стало впровадження нових ініціатив. Зокрема, створено Інтегровану службу навчання, що займається підготовкою миротворців до реагування на нестандартні загрози. Також організація розробляє новітні технології для підвищення ситуаційної обізнаності, в тому числі в кіберпросторі, та активно розвиває партнерство з регіональними структурами, такими як Африканський Союз, Європейський Союз та ОБСЄ, з метою забезпечення колективної протидії гібридним викликам. Утім, вагомим стримуючим фактором залишається надмірна бюрократизація діяльності ООН, що ускладнює оперативне ухвалення рішень та нормативну адаптацію до нових загроз.

Ще однією критичною проблемою є відставання міжнародно-правової кодифікації щодо гібридних форм конфліктів. Незважаючи на наявність

потужної нормативної бази з протидії тероризму, яка включає Резолюції Ради Безпеки ООН №1373 (2001), №1624 (2005), №1267 (1999), №1333 (2000), №1390 (2002), №1735 (2006), №2178 (2014), а також документи, присвячені запобіганню поширенню зброї масового знищення (Резолюції №1540 (2004) і №1673 (2006)), та основні конвенції ООН щодо боротьби з фінансуванням тероризму, ці акти не охоплюють усього спектру гібридної агресії. Відсутність чіткої правової дефініції ускладнює притягнення агресора до відповідальності та підриває ефективність колективної безпеки, яку прагне забезпечити ООН. Таким чином, подолання гібридних загроз вимагає як інституційного реформування миротворчої системи, так і розробки нових універсальних міжнародно-правових норм, які б адекватно відображали сучасну динаміку конфліктів.

Важливим моментом у контексті реагування міжнародної спільноти на події на сході України у 2014–2015 роках є парадоксальна пасивність ключових органів ООН, зокрема Ради Безпеки та Генеральної Асамблеї. Попри очевидні прояви гібридної агресії, включаючи спонсорування екстремізму, озброєння незаконних формувань і застосування тактики дестабілізації, жодного фундаментального документу на рівні ООН ухвалено не було. Причиною цього частково є тривалий процес погодження нової універсальної Конвенції про боротьбу з міжнародним тероризмом, яка мала б запровадити єдиний механізм відповідальності в умовах транснаціональної загрози. Хоча над її текстом працює спеціальна робоча група, процес її прийняття затягнувся на роки, попри гостру потребу в оперативних міжнародно-правових рішеннях [47].

Насправді, термін «міжнародний тероризм» став у центрі правового тлумачення гібридних загроз у системі ООН. Це, однак, не завжди коректно з точки зору практичної кваліфікації таких дій. Наприклад, відповідно до Резолюції РБ ООН №1373 (2001), держави зобов'язані криміналізувати фінансування терористичної діяльності, заморожувати активи, що використовуються для терористичних цілей, та укладати міжнародні угоди для боротьби з тероризмом. Для координації виконання цієї резолюції створено Контртерористичний комітет, який об'єднує 15 країн-членів Ради Безпеки [47].

Проте правовий інструментарій, спрямований переважно проти класичних форм тероризму, не враховує специфіку нових форм гібридної агресії, в яких межа між воєнними, інформаційними, економічними та політичними засобами суттєво розмита.

Окрім цього, система ООН стикається з низкою політичних, організаційних та ресурсних проблем у боротьбі з гібридними загрозами. Зокрема, відсутність узгодженого бачення серед держав-членів щодо визначення суті гібридних викликів та методів реагування на них перешкоджає розробці спільної стратегії. Складнощів додає і той факт, що джерелом гібридної загрози можуть бути самі держави-члени ООН, що унеможливорює ефективне реагування в межах чинної інституційної архітектури. Ресурсне обмеження ООН також знижує її здатність адаптуватися до нового безпекового ландшафту.

Використання асиметрії є ключовою характеристикою гібридних війн. У правовій площині це означає, що агресор використовує прогалини в міжнародному праві, щоб послабити можливості держави-жертви для адекватної відповіді. Поєднуючи це з інформаційним, дипломатичним або військовим тиском, країна-агресор досягає стратегічної переваги. Існує два ключових підходи до зменшення цієї асиметрії в межах чинного міжнародного права. По-перше, Стаття 51 Статуту ООН дозволяє державі реагувати силою у разі акту агресії, а глава VII надає Раді Безпеки повноваження на вжиття примусових заходів у випадку загрози миру. НАТО й ЄС також адаптують своє правове поле: наприклад, НАТО публічно заявило про готовність вважати кібератаки формою збройного нападу, що потребує колективної відповіді згідно зі статтею 5 Вашингтонського договору.

По-друге, міжнародне право дозволяє державам використовувати широкий спектр «несилових» механізмів реагування на гібридну агресію. До них належать санкції, блокування фінансових потоків, кіберзахист, інформаційна протидія, реформи сектору безпеки, боротьба з корупцією, побудова спроможностей на рівні державних інституцій, диверсифікація джерел енергії та ресурсів, а також застосування «м'якої сили» через дипломатію та культурну політику. Таким

чином, вже наявна правова база створює передумови для комплексного і, що важливо, гнучкого реагування на гібридні загрози в межах міжнародного правопорядку [57].

На сьогоднішній день глобальна система міжнародних відносин зазнає суттєвих трансформацій. Концепція національної держави, яка традиційно виступала основою світового порядку, поступово змінюється під тиском внутрішніх і зовнішніх викликів. Етнополітична нестабільність, повстанські рухи, масові заворушення охоплюють майже третину країн-членів ООН, у той час як національні кордони стають дедалі вразливішими. Валютні системи контролюються центральними банками, імпорт і міграційні потоки порушують державний суверенітет, а явища транснаціонального тероризму, нелегальної торгівлі наркотиками та зброєю створюють загрозу стабільності та безпеці.

В умовах такого безладдя формується нова парадигма політичного мислення — концепція постнаціональної держави. Її поява свідчить про необхідність переосмислення традиційних уявлень щодо державного суверенітету, безпеки та ролі держави у забезпеченні національних інтересів. Для адекватного реагування на сучасні глобальні виклики, а також для формування ефективної стратегії національної безпеки, вкрай важливо мати глибоке розуміння змін, які відбуваються в політичній, соціально-економічній, культурній та ідеологічній сферах.

Особливої уваги потребує участь миротворчих місій ООН у збройних конфліктах, що мають риси гібридних війн. Ілюстративним прикладом виступає ситуація в Лівані після ізраїльського вторгнення 1982 року. Громадянська війна в цій країні відбувалася на тлі глибокого релігійного та політичного поділу суспільства (приблизно 59,7 % мусульман і 39 % християн), а також наявності зовнішніх військових сил. У вакуумі влади сформувався недержавний актор — Хезболла, який отримував військову, фінансову та ідеологічну підтримку з боку Ірану. Використовуючи слабкість державного апарату та підтримку частини шіїтського населення, ця організація закріпилася в південному Лівані, реалізуючи як соціальні функції, так і збройну боротьбу проти Ізраїлю.

Після виведення ізраїльських військ у 2000 році та сирійських — у 2005-му, держава залишалася ослабленою, що дозволило Хезболлі продовжити нарощування впливу. У 2006 році збройний напад на ізраїльських солдатів спровокував війну тривалістю 34 дні, що супроводжувалася масовими руйнуваннями. Цей конфлікт є класичним прикладом гібридної війни між суверенною державою та добре організованим недержавним актором із зовнішньою підтримкою. У відповідь на ситуацію, ООН розгорнула в регіоні одну з найбільших своїх місій — Тимчасові сили ООН у Лівані (UNIFIL), які налічують понад 12 400 військовослужбовців, що здійснюють моніторинг, сприяють стабілізації та підтримують зусилля ліванської армії [24].

Таким чином, гібридні загрози виступають серйозним викликом для міжнародного миру та безпеки. Миротворча система ООН має адаптувати свої підходи до сучасної безпекової динаміки, що потребує інтеграції військових, цивільних і дипломатичних інструментів. Попри наявні ініціативи щодо посилення потенціалу миротворчих місій, зокрема в контексті реагування на гібридні виклики, все ще відчувається гостра потреба в розширенні міжнародної співпраці, оптимізації ресурсного забезпечення та розробці нових стратегій протидії цим загрозам.

2.2. Діяльність ОБСЄ в контексті гібридних війн та проксі-конфліктів

ОБСЄ, як регіональна організація з безпеки, заснована під час холодної війни, з самого початку покликана сприяти миру, стабільності та співпраці на європейському континенті. Впродовж багатьох років вона активно працювала у сферах запобігання конфліктам, моніторингу виборів, захисту прав людини та підтримки країн з перехідною економікою. Проте в умовах зростання нових форм загроз, таких як гібридні війни та проксі-конфлікти, ОБСЄ зіштовхнулася з серйозними труднощами в ефективному реагуванні.

Останнім часом як глобальні, так і регіональні міжнародні інституції, включаючи ОБСЄ, розпочали активний пошук ефективних механізмів

реагування на новітні безпекові виклики. Наприклад, 12 грудня 2016 року на засіданні Ради Безпеки ООН, присвяченому транснаціональному характеру сучасного тероризму та потребі посилення співпраці між державами, було прийнято резолюцію щодо удосконалення інструментів правової взаємодії в зборі та обробці доказів терористичної діяльності. Аналогічний документ був ухвалений ОБСЄ у листопаді того ж року [24].

Участь ОБСЄ в реагуванні на гібридні конфлікти підтверджена її діяльністю під час агресії росії проти України у 2014–2022 роках. Цей конфлікт став яскравим прикладом для аналізу ефективності дій ОБСЄ в умовах сучасних викликів. Зокрема, гібридна війна проти України продемонструвала неготовність і недостатню рішучість як глобальних, так і регіональних інституцій, включаючи ОБСЄ, в ефективному врегулюванні збройних конфліктів, що в свою чергу призвело до втрати ними значної частини міжнародного авторитету [34].

У рамках гібридних загроз та опосередкованих конфліктів ОБСЄ виконує кілька важливих функцій для підтримки миру в регіоні. Зокрема, одним із її основних напрямів діяльності є здійснення моніторингу ситуації в зонах конфлікту. Представники місій ОБСЄ працюють на місцях, збираючи інформацію про порушення режиму припинення вогню, права людини та інші загрози безпеці. У випадку України, ОБСЄ була ключовим інструментом спостереження за дотриманням угод про відведення важкого озброєння та припинення бойових дій. Ще одним важливим напрямом діяльності організації є сприяння діалогу між сторонами конфлікту. ОБСЄ неодноразово ініціювала переговори між Україною та росією з метою досягнення мирного врегулювання конфлікту на Донбасі.

ОБСЄ також брала участь у посередницьких процесах у конфліктах на Балканах та в регіоні Кавказу. Водночас, гібридна експансія росії відбувається на тлі загального ослаблення ефективності міжнародних і регіональних механізмів безпеки. Сьогодні ОБСЄ перебуває у стані інституційної кризи, зокрема через блокування її зусиль з урегулювання російсько-українського конфлікту самою російською стороною [34].

Попри це, організація намагається діяти проактивно в нових сферах безпеки, зокрема протидії дезінформації. Так, Офіс представника ОБСЄ з питань свободи ЗМІ здійснює моніторинг медіапростору та просуває стандарти відповідальної журналістики. ОБСЄ також бере участь у реалізації освітніх програм з медіа-грамотності, спрямованих на підвищення спроможності громадян виявляти фейкову інформацію та протистояти інформаційним маніпуляціям. У цій сфері організація досягла помітного прогресу.

Як частина ширшої стратегії стримування російської гібридної агресії, ЄС та ОБСЄ запровадили низку контрзаходів. Зокрема, у 2014 році було погоджено спільну санкційну політику щодо росії, ухвалено відповідні резолюції в межах ЄС, ОБСЄ та ПАРЄ з осудом агресії проти України. У березні 2015 року Європейська рада ухвалила рішення про необхідність боротьби з російською дезінформацією, а влітку того ж року в структурі Служби зовнішніх дій було створено спеціальну групу – East StratCom Task Force – для координації стратегічних комунікацій і підтримки позицій ЄС та ОБСЄ в інформаційному просторі [34].

Особливо показовим моментом у контексті ролі ОБСЄ стала її позиція під час так званих «виборів» 2 листопада 2014 року на окупованих територіях Донецької та Луганської областей. Попри статус офіційної міжнародної структури зі спостереження за виборами, ОБСЄ не відрядила туди жодної місії, засвідчуючи тим самим нелегітимність процесу. Водночас, проросійські праворадикальні сили з Європи прибули до окупованих територій, щоб створити ілюзію міжнародної підтримки. Ба більше, у той самий період було створено штучну організацію під назвою АБСЄ (Асоціація безпеки та співробітництва в Європі), яка мала імітувати легітимність ОБСЄ, що ще раз підтверджує спроби росії дискредитувати міжнародні механізми безпеки та нав'язати альтернативну парадигму [34].

Імітація справжньої міжнародної легітимності через створення фальшивих структур, таких як АБСЄ (Асоціація безпеки та співробітництва в Європі), що навмисно перегукується назвою ОБСЄ, має на меті не лише висміювання

останньої, але й навіювання сумнівів щодо авторитетності справжніх спостерігачів. А. Шеховцов у своєму дослідженні навів перелік із 44 осіб, які були залучені в якості фальшивих «спостерігачів» на цих псевдовиборах, серед яких єдиним французом був Жан-Люк Шафхаузер [34].

Щодо гібридної агресії росії проти України, ключовим кроком у відповідь стало створення Спеціальної моніторингової місії ОБСЄ в Україні (СММУ). Це була незброєна цивільна місія, започаткована 21 березня 2014 року на прохання уряду України та на основі консенсусного рішення всіх 57 держав-учасниць ОБСЄ. Початковий склад місії становив 100 осіб зі строком мандату шість місяців. Зі зростанням напруженості чисельність місії було збільшено до 500 осіб, а згодом і до 1291 (814 міжнародних та 447 місцевих працівників). Однак після повномасштабного вторгнення росії в Україну в лютому 2022 року російська делегація заблокувала подальше продовження мандату місії, і її діяльність була згорнута [14].

Попри певні досягнення, ОБСЄ стикається з рядом системних проблем у реагуванні на гібридні війни та проксі-конфлікти. Найгострішою з них є відсутність єдності серед держав-учасниць щодо розуміння природи цих загроз. Частина країн наполягає на необхідності адаптації існуючих правових і інституційних механізмів до нових викликів, тоді як інші вважають, що поточна система міжнародного права є достатньою. Така розбіжність у підходах ускладнює вироблення спільної позиції, що знижує ефективність організації. Водночас нерідко спостерігається ігнорування деякими країнами окремих рішень ОБСЄ через небажання визнавати їх обов'язковими.

Іншою проблемою є брак ресурсів. ОБСЄ значною мірою залежить від фінансових внесків держав-учасниць, деякі з яких останнім часом скорочують фінансування, що суттєво обмежує можливості організації в реалізації своїх місій, особливо в гарячих точках. Така ситуація ускладнює забезпечення належного технічного забезпечення, логістики та залучення кваліфікованого персоналу.

Критичну оцінку діяльності ОБСЄ висловлювали і деякі українські посадовці. Так, колишній керівник Луганської обласної військово-цивільної адміністрації Геннадій Москаль заявив, що місія ОБСЄ часто виглядає як організація, яка імітує активність, не приносячи реальної користі, й навіть допускав наявність прихильників росії серед її складу. За його словами, працівники ОБСЄ рідко з'являлися в зоні бойових дій, натомість частіше їх можна було побачити у ресторанах і пивбарах [53].

Загалом, характеристика місій та операцій ОБСЄ свідчить про її широку присутність у нестабільних регіонах Європи. Польові операції організації покликані надавати державам-членам практичну допомогу у виконанні зобов'язань, що випливають з рішень ОБСЄ, та сприяти нарощуванню національного потенціалу, зокрема через реалізацію конкретних проєктів. До основних напрямів її діяльності належать: підтримка реформ правоохоронних органів, захист прав національних меншин, правова експертиза, сприяння дотриманню принципів верховенства права, свободи ЗМІ, а також просування принципів толерантності, недискримінації тощо [55].

Окремі польові структури також здійснюють моніторинг ситуації на місцях, що дозволяє ОБСЄ реалізовувати механізми раннього попередження, запобігання конфліктам та брати участь у постконфліктному відновленні. Для цього місії активно співпрацюють із державними адміністраціями, громадянським суспільством, міжнародними організаціями на регіональному і національному рівнях. Така взаємодія сприяє координації зусиль, забезпеченню взаємодоповнюваності та підвищенню ефективності роботи в межах спільних ініціатив. Важливою інституційною одиницею в цій системі є Центр із запобігання конфліктам ОБСЄ (ЦПК), який відповідає за планування, реструктуризацію та закриття місій. ЦПК виконує аналітичні, координаційні функції, а також формулює політичні рекомендації [55].

Водночас аналіз діяльності польових місій ОБСЄ у контексті гібридних конфліктів виявляє низку структурних обмежень. Насамперед це відсутність механізмів юридичної відповідальності та інституційного реагування на порушення міжнародного права в умовах гібридної агресії. ОБСЄ не має повноважень на примусове втручання у внутрішні справи держав-членів, а також обмежена у можливостях впливу на третіх акторів, задіяних у гібридних конфліктах.

Для ефективного подолання цих викликів необхідне посилення співпраці між державами-учасниками ОБСЄ, зокрема у напрямі спільної розробки механізмів правової відповідальності за дії у гібридних війнах. Одночасно організація повинна ініціювати розширення фінансування своїх операцій, збільшення ресурсної бази, модернізацію кадрового складу, що дасть змогу забезпечити ефективність реалізації місій.

Особливо важливою є інтеграція зусиль ОБСЄ з іншими міжнародними структурами — насамперед Європейським Союзом та НАТО. Спільна розробка стратегічних підходів до реагування на нові форми конфліктів дозволить забезпечити стійкість міжнародного безпекового порядку та зменшити ризики ескалації нестабільності в європейському регіоні.

Таким чином, у контексті гібридних війн і проксі-конфліктів потенціал ОБСЄ залишається надзвичайно важливим для забезпечення миру й стабільності.

Програми моніторингу, діалогу та посередництва, реалізовані організацією, уже допомогли знизити напруженість у ряді зон конфлікту. Проте наявні проблеми — брак ресурсів, політична фрагментованість та обмежені інституційні повноваження — потребують додаткових зусиль і політичної волі для їх подолання. Лише за таких умов ОБСЄ зможе повною мірою реалізувати свій потенціал у протидії гібридним загрозам.

2.3. Регіональні безпекові організації в епоху гібридних війн та проксіконфліктів

У сучасній міжнародній системі простежується стійке зростання кількості гібридних війн і проксі-конфліктів, які становлять серйозні виклики для національної й регіональної безпеки. У цьому контексті регіональні організації безпеки набувають вирішального значення як суб'єкти, здатні протидіяти новітнім формам загроз, зберігати стабільність та забезпечувати безпечне середовище для своїх членів. Цей розділ присвячено аналізу ролі організацій регіональної безпеки в умовах гібридних загроз, виявленню їх потенціалу, інституційних переваг та обмежень, а також окресленню основних викликів, з якими стикаються такі структури.

Система колективної безпеки, що формується в межах як глобальних, так і регіональних альянсів, передбачає спільні зусилля держав для запобігання загрозам миру, придушення агресії та врегулювання конфліктів. Її ефективність визначається передусім здатністю об'єднаних країн протистояти потенційному агресору, створюючи коаліцію з переважаючими ресурсами та міць. На відміну від ізольованої протидії, в межах колективної безпеки агресор, як правило, несе значно вищі ризики через ймовірність зустріти організовану протидію з боку кількох держав [22].

Крім того, важливою функцією організацій колективної безпеки є сприяння створенню середовища, сприятливого для миру та стабільності. Це досягається шляхом забезпечення обміну інформацією, що зменшує підозри щодо експансіоністських намірів інших країн, а також створенням міжнародних форумів для діалогу, які сприяють зміцненню спільних цінностей та взаємної довіри. Відкритість і транспарентність, які супроводжують діяльність таких інституцій, значно знижують рівень стратегічної непевності, що часто стає джерелом конфліктів у міжнародних відносинах.

Також колективна безпека відіграє важливу роль у врегулюванні так званих дилем безпеки, коли держави змушені нарощувати оборонний потенціал у відповідь на дії інших акторів. В умовах ефективно функціонуючої системи колективної безпеки потреба у надмірному зосередженні ресурсів на наступальних спроможностях суттєво зменшується. Це пов'язано з тим, що кожна держава, яка входить до альянсу, робить внесок у спільну безпеку, зокрема — у протидію агресору. У результаті знижується ймовірність невірної тлумачення намірів, а отже — й загроза превентивних або ескалаційних дій, які нерідко стають каталізатором збройних конфліктів [22].

Регіональні організації безпеки становлять важливу форму багатосторонньої співпраці, спрямованої на забезпечення миру та стабільності в межах певного географічного регіону. Вони різняться між собою за сферою діяльності, складом учасників та функціональним наповненням. Серед таких структур варто відзначити Організацію Північноатлантичного договору (НАТО), Африканський Союз (АС), Асоціацію держав Південно-Східної Азії (АСЕАН) та інші. Особливу увагу привертає європейський безпековий простір, де одночасно діють декілька організацій колективної безпеки, зокрема ОБСЄ, НАТО та Організація Договору про колективну безпеку (ОДКБ), остання з яких має міжрегіональний характер [42].

НАТО, на відміну від багатьох інших регіональних структур, має ефективний механізм реалізації рішень завдяки наявності у своєму розпорядженні значних військових потужностей та розвиненої інфраструктури.

Важливою особливістю є також обов'язковість дотримання єдиних технічних стандартів у збройних силах держав-членів, що забезпечує високий рівень взаємодії. Інституційні переваги Альянсу включають централізовану командну структуру, логістичні засоби та потужні механізми збору й обробки інформації. Усе це дає змогу координовано й ефективно застосовувати військову силу в разі потреби, на відміну від інших регіональних організацій, які подібних спроможностей не мають [42].

У цілому, регіональні організації безпеки відіграють ключову роль у протидії сучасним викликам безпеці, зокрема гібридним і проксі-загрозам. Вони створюють інституційні платформи для політичного діалогу, зміцнення довіри, обміну інформацією та координації зусиль між державами-членами. Наприклад, ОДКБ декларує свою активну участь у забезпеченні стабільності в Центральній Азії, зокрема у боротьбі з тероризмом, екстремізмом та незаконним обігом наркотиків. Утім, ефективність її дій залишається предметом критики, зважаючи на обмежену здатність до оперативного реагування та політичну залежність від окремих учасників.

Паралельно з цим, Європейський Союз, попри початковий економічний характер своєї інтеграції, також трансформувався в актора безпеки. Події в колишній Югославії стали каталізатором для формування Спільної безпекової та оборонної політики ЄС. Усередині Союзу завдяки глибокій інтеграції створено унікальне середовище, у якому збройний конфлікт між його членами є фактично неможливим. Водночас ЄС почав докладати зусиль для розбудови стабільності за межами власного кордону, зокрема через миротворчі місії, участь у врегулюванні конфліктів, а також у розбудові інституцій країн-партнерів [39].

Регіональні організації безпеки також мають сильні сторони, які роблять їх добре придатними для вирішення гібридних війн і конфліктів за дорученням. По-перше, вони краще розуміють місцевий контекст і динаміку, що має вирішальне значення для виявлення основних причин конфліктів і розробки відповідних заходів. По-друге, вони мають легітимність і авторитет, щоб діяти як посередники та фасилітатори мирних процесів. По-третє, вони забезпечують

форум для зміцнення довіри та впевненості між державами-членами, що має вирішальне значення для вирішення проблем безпеки, які вимагають колективних дій.

Регіональні організації безпеки стикаються з низкою проблем під час реагування на гібридні війни та конфлікти. По-перше, багато з них мають обмежені ресурси та технічні можливості, що ускладнює оперативне та ефективне реагування на складні й багатовимірні загрози. Наприклад, окремі організації не володіють достатніми військовими або розвідувальними засобами, аби своєчасно виявляти та нейтралізовувати прояви гібридної агресії. По-друге, внутрішні політичні розбіжності або відсутність консенсусу серед держав-членів значно знижують ефективність їхнього функціонування. Ілюстративним прикладом є ситуація в Раді співробітництва арабських держав Перської затоки (GCC), яка опинилася в глибокій внутрішній кризі під час дипломатичного конфлікту з Катаром.

По-третє, зусилля регіональних організацій часто ускладнюються через зовнішнє втручання потужних держав, що переслідують власні інтереси у відповідних регіонах. Це призводить до розбалансування безпекових механізмів і перешкоджає ефективному врегулюванню конфліктів. Загальна оцінка сучасних загроз, зокрема гібридних, дозволяє зробити кілька висновків: по-перше, зростає небезпека внутрішньодержавних конфліктів; по-друге, залишається імовірність масштабних міждержавних воєн на Європейському континенті; по-третє, зберігається ризик гібридних атак з боку тоталітарних режимів Близького Сходу, Азії та російської федерації. Водночас з'являються нові виклики, що підривають стабільність і сталий соціально-економічний розвиток сучасних суспільств [39].

Системний аналіз у політичній науці дав змогу глибше дослідити архітектуру регіональної безпеки, охоплюючи її ключові компоненти — військово-політичні, соціально-економічні, соціокультурні, політико-інституційні тощо. Дослідницький акцент зміщується до вивчення ефективності державно-політичних інститутів у контексті забезпечення національної та

регіональної безпеки. У роки «холодної війни» значна частина теоретичних засад залишалася недостатньо розробленою, що пояснювалося домінуванням ядерного стримування як головної парадигми. Унаслідок цього особлива увага приділялася ідеї, що саме природа демократичних громадянських суспільств визначає їхню схильність до мирного співіснування [41].

Традиційна парадигма регіональної безпеки, заснована на переважно військовому підході до територіального захисту, сьогодні виявляється недостатньою в умовах гібридних загроз, які поєднують класичні та нетрадиційні засоби — кібератаки, пропаганду, дезінформацію, використання іррегулярних формувань. Це вимагає формування нової парадигми регіональної безпеки, більш комплексної, адаптивної й міждисциплінарної.

Однією з таких сучасних концепцій є «безпека людини» — підхід, який акцентує не лише на захисті держави, а передусім на безпеці окремих осіб і спільнот. Ця концепція охоплює широкий спектр загроз — від економічної вразливості та екологічної нестабільності до системних порушень прав людини. Вона визнає взаємозалежність традиційних і нетрадиційних загроз та передбачає їх вирішення за допомогою інтегрованих інструментів.

Прикладом реалізації такої парадигми є діяльність Асоціації держав Південно-Східної Азії (АСЕАН), яка обрала модель безпеки людини, зосереджену на соціально-економічному розвитку, забезпеченні стійкості та екологічної безпеки. До країн, які застосовують колективні моделі регіональної безпеки, належать також держави Північноатлантичного альянсу, АНЗЮС, АСЕАН, а з певними обмеженнями — країни Африканського Союзу та інші [41].

Ще однією важливою сучасною парадигмою регіональної безпеки є концепція кооперативної безпеки, яка акцентує увагу на необхідності багатосторонньої співпраці та постійного діалогу між державами для ефективного реагування на безпекові виклики. Цей підхід ґрунтується на усвідомленні того, що сучасні загрози мають транснаціональний характер і не можуть бути нейтралізовані виключно односторонніми зусиллями. Яскравим прикладом втілення цього підходу є діяльність Шанхайської організації

співробітництва (ШОС), яка координує зусилля своїх країн-членів у протидії тероризму, незаконному обігу наркотиків і загрозам кібербезпеки в регіоні Центральної Азії.

Третя нова парадигма, що набуває дедалі більшого поширення, — це концепція стійкості. Вона передбачає підвищення здатності суспільств, державних інституцій і регіональних утворень адаптуватися до загроз, протистояти їм і відновлюватися після криз. Цей підхід визнає, що сучасні загрози, особливо гібридні, часто є непередбачуваними, мають каскадний вплив та охоплюють одночасно кілька сфер — безпекову, економічну, соціальну. Європейський Союз активно впроваджує підхід до стійкості, розробляючи стратегії з протидії гібридним викликам, що охоплюють кіберзагрози, дезінформацію, енергетичну вразливість тощо.

Перевагою нових підходів до регіональної безпеки є їхня комплексність. По-перше, вони визнають і враховують взаємозв'язки між традиційними (військовими) і нетрадиційними (інформаційними, економічними, екологічними) загрозами, що дозволяє сформулювати більш ефективні та адаптивні механізми реагування. По-друге, наголошується на важливості регіонального співробітництва, що є критично важливим в умовах глобалізованих викликів, які нерідко виходять за межі окремих держав. По-третє, у центр уваги ставиться стійкість як здатність зберігати функціонування систем навіть під час глибоких криз, що особливо актуально у світі, де загрози можуть виникати раптово та мати ланцюгову реакцію.

Однак існують і значні виклики. Зокрема, потенційна конкуренція між регіональними безпековими структурами може призвести до фрагментації зусиль і підриву кооперативних ініціатив. Тривала напруга між окремими блоками чи державами провокує гонку озброєнь, підвищує ризик конфронтації та створює перешкоди для ефективної колективної відповіді на спільні загрози. Крім того, подібна напруга нерідко поширюється за межі первинного регіону, втягуючи інші країни в боротьбу за геополітичний вплив. Саме такий сценарій спостерігався під час холодної війни, коли уникнення прямого конфлікту між

основними блоками в Європі стало можливим лише ціною серії проксі-війн у нестабільних регіонах світу. Наслідки цих конфліктів і сьогодні залишаються джерелом напруженості та викликів для глобальної системи безпеки [23].

Однак нові парадигми регіональної безпеки не позбавлені суперечностей і низки внутрішніх обмежень. По-перше, багатьом із них бракує необхідних ресурсів, кадрових і технічних можливостей для повноцінного реагування на складні, багатовимірні загрози. По-друге, впровадження таких підходів може наштовхуватись на опір з боку держав або недержавних акторів, зацікавлених у збереженні нестабільності або слабких інституцій у певному регіоні. По-третє, внутрішні політичні суперечності, конфлікт інтересів та ідеологічні розбіжності між державами-членами часто ускладнюють формування спільної позиції, що істотно знижує ефективність регіональних організацій у вирішенні конфліктів.

Узагальнюючи, варто зазначити, що регіональні організації безпеки відіграють ключову роль у протидії гібридним війнам і проксі-конфліктам. Вони надають платформу для діалогу й координації зусиль, краще орієнтуються у специфіці місцевого контексту, а також можуть виступати посередниками й модераторами мирних процесів. Водночас ефективність їх діяльності стримують низка чинників: обмежені ресурси, внутрішня фрагментація, залежність від політичної волі держав-членів і зовнішнє втручання з боку глобальних гравців. Подолання цих викликів потребує не лише розширення інституційної спроможності, а й глибшої міжорганізаційної співпраці, а також політичної підтримки з боку провідних держав світу.

В умовах новітніх викликів глобальної безпеки особливої актуальності набуває пошук і запровадження нових підходів до забезпечення стабільності. Парадигми, що базуються на концептах людської безпеки, кооперативного підходу та стійкості, пропонують більш комплексне бачення безпеки, яке враховує як традиційні, так і нетрадиційні загрози. Вони підкреслюють необхідність регіонального партнерства, відкритого діалогу та гнучких механізмів реагування. Успішне впровадження цих моделей вимагатиме не лише значного політичного ресурсу та фінансування, а й здатності до стратегічного

передбачення, інституційної адаптації та тісної взаємодії між регіональними та глобальними суб'єктами безпеки. Зрештою, дієвість нових парадигм регіональної безпеки визначатиметься тим, наскільки ефективно вони зможуть відповідати на сучасні виклики, сприяти зміцненню миру, стабільності й безпеки у відповідних регіонах.

Висновки до розділу 2

У сучасному світі гібридні загрози та проксі-конфлікти стають визначальними викликами для систем міжнародної та колективної безпеки. Організація Об'єднаних Націй, яка має ключовий мандат на підтримку миру, стикається з потребою адаптації до нових типів загроз, що включають дезінформацію, кіберзлочинність, використання недержавних акторів та приховані методи впливу. Недостатня швидкість правової кодифікації новітніх загроз, розмитість термінології та розбіжності в підходах держав-членів обмежують ефективність миротворчих операцій ООН. Хоча ініціативи щодо модернізації місій і партнерства з регіональними організаціями мають потенціал, без політичної волі та достатніх ресурсів ці заходи залишаються фрагментарними.

ОБСЄ, як регіональна структура безпеки, демонструє спроможність до моніторингу конфліктів, сприяння діалогу та протидії дезінформації. Водночас обмежений мандат, залежність від консенсусу та вплив окремих держав-членів (зокрема російської федерації) істотно ускладнюють її роботу в гібридних конфліктах. Приклад Спеціальної моніторингової місії в Україні показує як потенціал, так і межі можливостей ОБСЄ в умовах сучасних конфліктів.

Регіональні безпекові організації — НАТО, ЄС, ОДКБ, АСЕАН та інші — відіграють критичну роль у реагуванні на гібридні виклики. Вони мають кращу обізнаність із локальним контекстом, легітимність серед держав регіону та більшу гнучкість у реагуванні. Проте ефективність цих організацій часто стримується внутрішніми суперечностями, браком ресурсів, а іноді й зовнішнім тиском. Для відповіді на нові форми конфліктів вони змушені переходити до нових парадигм безпеки: безпеки людини, кооперативної безпеки та концепції стійкості.

У підсумку, система міжнародної та регіональної безпеки вимагає суттєвого оновлення: інституційної реформи, узгодження підходів до гібридних загроз, модернізації правових рамок та зміцнення міжорганізаційної взаємодії.

Лише комплексний, гнучкий і скоординований підхід дозволить ефективно протистояти викликам гібридної війни та проксі-конфліктів, захистити держави та громадян від нових форм агресії.

РОЗДІЛ 3. ОСНОВНІ ПРОБЛЕМИ СИСТЕМ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ЕПОХУ ГІБРИДНИХ ВІЙН ТА ПРОКСІКОНФЛІКТІВ

3.1. Системи національної безпеки країн-членів НАТО при протидії гібридній агресії

Організація Північноатлантичного договору (НАТО) завжди відігравала ключову роль у підтриманні безпеки, насамперед на європейському континенті. Від моменту створення і до завершення періоду холодної війни основним завданням Альянсу було стримування Радянського Союзу. Однак після розпаду СРСР і завершення біполярної конфронтації НАТО розпочала процес глибокої трансформації відповідно до нових безпекових викликів. Безсумнівно, для більшості країн-членів Альянсу збереження цього військово-політичного об'єднання відповідало їхнім стратегічним інтересам.

Так, для Сполучених Штатів Америки НАТО залишалося дієвим інструментом впливу на архітектуру безпеки в Європі. Зі свого боку, держави Західної Європи сприймали Альянс як гаранта стабільності в умовах політичних трансформацій та нового геополітичного порядку. Розпад Радянського Союзу істотно змінив баланс сил, а отже, і характер загроз, що постали перед європейськими країнами. В нових умовах, на тлі зростання кількості конфліктів асиметричного характеру, зокрема гібридних, держави-члени НАТО були змушені переосмислити свої системи національної безпеки.

Гібридна агресія, що поєднує елементи класичної воєнної сили з кібератаками, дезінформаційними кампаніями, економічним тиском і підривною діяльністю, потребує комплексної та скоординованої відповіді. Усвідомлюючи необхідність спільних дій, країни-члени Альянсу активізували співпрацю в межах НАТО з метою посилення інституційної спроможності протидіяти новим типам загроз. У цьому контексті особливе значення має розвиток стратегій колективної та національної стійкості.

Одним із важливих інструментів у цій площині є регулярне проведення оцінювання рівня стійкості держав-членів Альянсу. Такі оцінювання дають змогу визначати як досягнення, так і вразливі сфери, що потребують додаткової уваги. У 2022 році НАТО ухвалила щорічний Аналіз стійкості, який започаткував новий цикл планування й огляду в цій сфері. У документі наведено інтегральну оцінку стану колективної стійкості Альянсу, а також визначено рівень виконання вимог у семи базових галузях. На основі висновків Аналізу розробляються конкретні заходи, спрямовані на усунення виявлених прогалин і підвищення рівня стійкості в масштабах Альянсу [2].

Доктрина колективної оборони НАТО, яка базується на принципах спільної відповідальності за безпеку, є однією з ключових платформ європейських країн для реагування на сучасні загрози. Основою цієї доктрини є Стаття 5 Вашингтонського договору, згідно з якою напад на одного члена Альянсу розглядається як напад на всіх. У контексті гібридної агресії, що набуває дедалі більш комплексного характеру, НАТО забезпечує скоординовану взаємодію держав-членів через механізми обміну розвідувальною інформацією, спільного оперативного планування та швидкого реагування. Саме в цьому контексті поняття "криза", що використовується в офіційних документах НАТО, дедалі частіше інтерпретується як форма гібридної загрози на її початкових етапах.

Запобігання конфліктам і реагування на кризи є одним із трьох базових завдань Альянсу, поряд із колективною обороною та безпековою співпрацею. У Стратегічній концепції НАТО 2022 року чітко окреслено готовність Альянсу діяти для запобігання та вирішення конфліктів, які можуть впливати на безпеку його членів. У цьому контексті НАТО реалізує широкий спектр програм з підготовки та розбудови потенціалу, орієнтованих на посилення стійкості як у державах-партнерах, так і всередині самого Альянсу. За десятиліття діяльності НАТО накопичила унікальний досвід у сфері кризового менеджменту, який охоплює планування, координацію, логістичне забезпечення та ведення багатонаціональних миротворчих операцій [2].

У сучасних умовах безпеки зростає усвідомлення необхідності розглядати стійкість не лише як допоміжний інструмент, а як самостійний напрям діяльності НАТО нарівні з колективною обороною та кризовим реагуванням. Такий підхід закріплений у ряді стратегічних документів Альянсу, зокрема в Аналізі стійкості, ухваленому в 2022 році, який започаткував новий цикл планування та моніторингу прогресу у сфері підвищення стійкості членів НАТО [33].

З урахуванням динаміки змін безпекового середовища НАТО адаптує свою політику до нових викликів, пов'язаних із гібридною війною. Значну увагу приділено інтеграції кібербезпеки, інформаційних операцій, захисту критичної інфраструктури та підвищенню національної стійкості в оборонне планування. Яскравим прикладом таких зусиль є ініціатива «Посилена передова присутність» (Enhanced Forward Presence, eFP), у межах якої у Східній Європі розгорнуто багатонаціональні бойові групи з метою стримування потенційної агресії та оперативного реагування на гібридні загрози.

Європейські держави, у свою чергу, гармонізують свої безпекові стратегії з політикою НАТО, розробляючи комплексні міжвідомчі рамки, що поєднують військові, дипломатичні, інформаційні та економічні інструменти. Це сприяє не лише ефективному захисту національного суверенітету, а й укріпленню трансатлантичної єдності. В особливий спосіб акцент зроблено на забезпеченні кібербезпеки — найбільш уразливого сегменту сучасного безпекового простору.

Європейські країни активно розвивають кіберпідрозділи у структурах національної безпеки, запроваджують механізми обміну оперативною інформацією, інвестують у науково-дослідницькі розробки в галузі інформаційного захисту. НАТО, у свою чергу, виступає платформою для обміну передовими практиками та стандартизації кіберзахисту серед держав-членів. Усе це дає підстави стверджувати, що Альянс не лише зберігає свою актуальність у нових безпекових умовах, а й є ключовим гравцем у протидії гібридним викликам XXI століття.

Стрімкий розвиток інформаційно-комунікаційних технологій значно ускладнив завдання національних спецслужб та інших органів безпеки щодо

захисту від кібератак. Це вимагає постійного удосконалення систем захисту критичної військової та цивільної інфраструктури. У відповідь на ці виклики НАТО реалізує низку заходів, спрямованих на посилення кіберстійкості та інформаційної безпеки держав-членів.

Зокрема, в рамках Альянсу:

- створено спеціалізовані команди швидкого кіберреагування;
- укладено Меморандум про порозуміння між НАТО та державами-членами щодо захищених каналів обміну інформацією в умовах кризових ситуацій;
- активізовано діяльність Центру передового досвіду з кіберзахисту НАТО в Таллінні, який займається як розробкою технічних рішень для протидії шкідливому програмному забезпеченню, так і підготовкою профільних фахівців;
- започатковано співпрацю з малими та середніми компаніями, що розробляють інноваційні рішення у сфері кібертехнологій;
- ухвалено документ «Зобов'язання щодо кіберзахисту» (саміт НАТО у Варшаві, 2016 р.), яким країни-члени підтвердили готовність до колективного розвитку кіберспроможностей [7].

Одним із ключових напрямів забезпечення кіберстійкості є боротьба з дезінформацією. У сучасних умовах інформаційної війни європейські держави інвестують у кампанії з підвищення медіаграмотності, формування критичного мислення у громадян, а також освітні ініціативи, спрямовані на підвищення обізнаності про загрози гібридного характеру. НАТО, у свою чергу, в межах стратегічної комунікації протидіє дезінформаційним впливам, сприяє прозорості дій та підтримує довіру громадськості до демократичних інституцій.

Варто підкреслити, що реалізація союзницької співпраці у сфері гібридної безпеки в значній мірі зосереджена в рамках НАТО. Це зумовлено не лише стратегічною позицією Вашингтона як гаранта трансатлантичної єдності, але й прагненням не допустити створення паралельних структур, які могли б послабити вплив Альянсу на європейську безпеку.

У грудні 2015 року міністри закордонних справ країн-членів НАТО ухвалили Стратегію реагування на прояви гібридної війни, що стала одним із центральних компонентів реалізації «Плану дій щодо забезпечення готовності». Основні положення цієї стратегії передбачають:

- удосконалення системи обміну розвідданими та механізмів раннього попередження про гібридну активність, насамперед з боку Російської Федерації;
- поєднання традиційних та нетрадиційних засобів у протидії гібридним загрозам, у тому числі за участі державних і недержавних акторів;
- розробку набору індикаторів для оцінки рівня загрози та формування сценаріїв кризового реагування;
- можливість застосування Статті 5 Вашингтонського договору у випадку гібридної агресії;
- розширення співпраці з міжнародними партнерами, зокрема Європейським Союзом, для формування спільної платформи протидії гібридній війні [8].

У цьому контексті особливої уваги заслуговує досвід взаємодії НАТО та ЄС. Попри спроби поглибити співпрацю, вона часто наштовхується на дублювання функцій та конкуренцію за вплив. Наприклад, обидві організації паралельно впроваджували концепції сил швидкого реагування — ЄС сформував бойові групи чисельністю до 1500 осіб, тоді як НАТО створило власні сили оперативного реагування. Подібна ситуація спостерігалась і в місії в Дарфурі (Судан), де замість координації дій домінувало суперництво. Це свідчить про існування різного бачення ролі обох інституцій, що ускладнює реалізацію спільних безпекових ініціатив.

Таким чином, ефективна протидія гібридним загрозам у XXI столітті передбачає не лише інституційну адаптацію НАТО та модернізацію його оперативних структур, але й потребує справжньої стратегічної синергії з боку інших міжнародних акторів, передусім ЄС, на основі прозорості, координації і довіри.

Проте процес стратегічної координації між НАТО та Європейським Союзом у сфері безпеки залишається ускладненим низкою факторів. Однією з головних перешкод є те, що не всі держави-члени ЄС водночас є членами Північноатлантичного альянсу. Попри те, що переважна більшість таких країн беруть активну участь у консультаціях з питань безпеки в межах двосторонніх і багатосторонніх форматів, а також у постійно діючих структурах співпраці між ЄС та НАТО, окремі держави, як-от Мальта та Кіпр, залишаються поза повноцінною взаємодією. Зокрема, після їхнього вступу до Європейського Союзу у 2004 році так і не були укладені угоди про обмін секретною інформацією з НАТО, що значно обмежує їхню участь у формуванні спільної безпекової політики. Хоча представники цих країн і залучаються до неофіційних зустрічей з питань регіональної безпеки, подібний формат не забезпечує рівноправного доступу до ухвалення рішень, що, безумовно, послаблює потенціал спільної відповіді на сучасні виклики [5].

У підсумку можна стверджувати, що національні безпекові системи країн Європи, побудовані в рамках НАТО, відіграють вирішальну роль у протидії гібридній агресії. Завдяки ефективному використанню механізмів колективної оборони, розробленню інтегрованої політики безпеки, посиленню кіберзахисту та реалізації стратегічних комунікаційних ініціатив, держави-члени Альянсу спромоглися створити адаптивні, взаємопов'язані та стійкі моделі реагування на загрози гібридного характеру. Інтеграція оборонних ресурсів, аналітичного потенціалу й розвідувальної інформації в рамках Північноатлантичного альянсу підвищує рівень готовності до кризи, зміцнює національну безпеку кожної держави-члена та сприяє загальній стабільності на європейському континенті.

3.2. Системи національної безпеки позаблокових країн при протидії гібридній агресії

Фінляндія, до приєднання до НАТО, демонструвала приклад ефективної політики «всеохопної безпеки», яка ґрунтувалася на високій інтеграції цивільного та військового компонентів системи національної безпеки. Особливу увагу приділяли кіберзахисту, стратегічним комунікаціям, протидії дезінформації, а також готовності до широкого спектра кризових ситуацій. Швеція та Швейцарія традиційно дотримуються політики нейтралітету, проте активно інвестують у зміцнення власного оборонного потенціалу, розбудову інформаційної безпеки та підтримку системи територіальної оборони.

Сінгапур, як малий, але високотехнологічний суб'єкт міжнародних відносин, зробив ставку на інноваційні технології, кібербезпеку, аналітичні центри та стратегічне прогнозування. Тут держава контролює ключові вузли інформаційної інфраструктури, а національна система безпеки включає потужний сектор громадянської освіти з медіаграмотності. Аналогічно, Японія застосовує підхід інтегрованої безпеки, що передбачає зміцнення обороноздатності, модернізацію збройних сил і посилення безпеки критичної інфраструктури в умовах кіберзагроз і стратегічного тиску з боку Китаю та Північної Кореї.

Нідерланди, Ірландія та Нова Зеландія, попри різні геополітичні умови, реалізують моделі, в яких безпекова політика є тісно пов'язаною з питаннями демократичного врядування, інклюзивності, прав людини та екологічної безпеки. Водночас Велика Британія та Австралія, маючи міцні союзницькі зв'язки, особливо зі США, орієнтуються на проактивні стратегії стримування, включаючи участь у глобальних кіберкоаліціях, розвідспільнотах (як-от Five Eyes) та посилення оперативної сумісності з партнерами.

Спільними рисами державної політики у сфері безпеки в позаблокових та умовно нейтральних країнах є поєднання класичних і новітніх інструментів реагування: від конституційного закріплення принципів стійкості й стратегічної

автономії до впровадження національних стратегій кіберзахисту, розвитку інформаційної стійкості суспільства, інституційної децентралізації відповідальності за безпеку та активізації дипломатичної взаємодії на двосторонньому рівні.

Цей досвід демонструє, що навіть у відсутність офіційної участі в регіональних безпекових блоках, держава може формувати ефективну модель протидії гібридній агресії. Водночас ці країни визнають необхідність адаптації безпекової політики до глобальних трансформацій та зростаючої взаємозалежності загроз, що потребує балансу між стратегічною автономією та міжнародною кооперацією. В умовах розмитих кордонів між війною та миром, безпекою і розвитком, лише комплексні, гнучкі й адаптивні моделі державної політики можуть забезпечити належний рівень національної стійкості.

Наприклад, Індія створила комплексну розвідувальну мережу для виявлення та реагування на гібридні загрози в режимі реального часу, використовуючи як людський інтелект, так і передові технології спостереження. Щоб протистояти гібридній агресії, Індія зосередилася на посиленні своїх кіберспроможностей. Країна інвестувала в розробку надійної інфраструктури кібербезпеки для захисту критично важливих інформаційних мереж від кібератак. Індія також бере активну участь у двосторонніх і багатосторонніх партнерствах для покращення обміну інформацією та співпраці у протидії гібридним загрозам. Крім того, зусилля Індії з оборонної модернізації зосереджені на розробці передових технологій і систем спостереження для виявлення та нейтралізації нетрадиційних загроз. Приклад протистояння гібридній агресії Індія має в результаті довготривалого конфлікту з Пакистаном.

Витоки конфлікту сягають ще 1947 року, коли князівство Джамму і Кашмір ділили між Індією і Пакистаном. Більшість колишня британської території відійшла до Індії. Проблема полягала в тому, що її населяли здебільшого мусульмани, які тяжіли до Ісламабаду, але тодішній очільник Кашміру був індуїстом і приєднав князівство до Індії. З того часу етнічні та релігійні конфлікти тут не вщухають [12].

Такий підхід дозволив Фінляндії сформувати ефективну модель протидії гібридним загрозам, яка охоплює як «жорсткі» елементи обороноздатності, так і «м'які» інструменти, пов'язані з комунікацією, просвітою населення, підвищенням довіри до інституцій та забезпеченням прозорості у сфері безпеки. Своєчасна модернізація системи цивільної оборони, регулярне проведення багаторівневих тренувань і наявність чітко визначених протоколів реагування стали фундаментом стійкості фінського суспільства до інформаційно-психологічного тиску та кіберзагроз. До того ж, особливу увагу було приділено освітнім кампаніям із підвищення медіаграмотності, що знижувало ефективність дезінформаційних впливів з боку агресора.

Таким чином, як досвід Індії, так і приклад Фінляндії демонструють, що незалежно від участі в оборонних союзах, держави здатні формувати ефективну державну політику у сфері захисту від гібридної агресії. При цьому важливою умовою успіху є поєднання воєнних, дипломатичних, інформаційних та громадських інструментів із широким залученням суспільства до процесу забезпечення національної безпеки. З огляду на це, навіть позаблокові держави мають потенціал для створення адаптивних і стійких систем реагування на багатовимірні загрози сучасного безпекового середовища. Водночас у контексті триваючих гібридних конфліктів і наростання ролі інформаційного фронту стає очевидним, що успішне протистояння гібридній агресії вимагає не лише національних зусиль, а й розвитку ефективного міжнародного партнерства, обміну досвідом і координації зусиль на глобальному рівні.

Фінляндія також інвестувала у вдосконалення своїх можливостей кібербезпеки для захисту критичної інфраструктури від кібервтрутень. Активна участь країни в міжнародних організаціях, таких як Європейський Союз і НАТО, наприклад програма «Партнерство заради миру», дозволяє їй користуватися перевагами механізмів колективної безпеки та платформ обміну інформацією. Ще у 2016 році Комітет національної безпеки в уряді Фінляндії оновив список дій, які він вважає загрозливими та ймовірними методами гібридної війни.

Раніше фінські військові традиційно вважали найбільшими загрозами національній безпеці тероризм і війну з іншими країнами [18].

Сінгапур, позаблокова країна, розташована в геополітично нестабільному регіоні, розробила комплексну систему національної безпеки для протидії гібридній агресії. Визнаючи взаємопов'язаний характер гібридних загроз, підхід Сінгапуру до безпеки поєднує військове стримування, ефективне управління та стратегічне партнерство.

Сінгапур інвестував значні кошти в можливості збору та аналізу розвідувальних даних, щоб швидко виявляти гібридні загрози та реагувати на них. Країна також розробила передові заходи кібербезпеки для захисту критичної інфраструктури, боротьби з кампаніями дезінформації та забезпечення цілісності інформаційних мереж.

Сінгапур бере активну участь у регіональних форумах з питань безпеки та військових навчаннях, щоб покращити оперативну сумісність зі своїми партнерами та обмінятися передовим досвідом у протидії гібридній агресії. Наприклад, Сінгапур та Україна співпрацюють в сфері кібербезпеки, ще у 2018 році Міністр внутрішніх справ України Арсен Аваков та віцепрем'єр-міністр з питань нацбезпеки Сінгапуру Тео Чі Хін домовилися про співпрацю між кіберполіцейськими двох країн. Також Аваков повідомив, що провів зустріч із міністром внутрішніх справ Сінгапуру Касівісванатаном Шанмугамом, в ході якої були обговорені спільні гібридні загрози у сучасному світі та досягнуто домовленості про спеціальну співпрацю підрозділів кіберполіції [17]. Географічне розташування та політичний ландшафт Австрії роблять її сприйнятливою до тактики гібридної війни.

У відповідь на виклики сучасного безпекового середовища, Швейцарія активізувала зусилля у напрямі розвитку міжвідомчої взаємодії та посилення кіберзахисту. Зокрема, створено Центр кібербезпеки, який координує захист ключових галузей інфраструктури, розроблено національну стратегію кіберзахисту, а також запроваджено програми підготовки населення до кризових ситуацій. Особливу увагу приділено збереженню принципу збройного

нейтралітету, що є традиційною основою зовнішньої політики Швейцарії, водночас із поступовою адаптацією системи національної безпеки до нових реалій гібридного протистояння.

Водночас Швейцарія приділяє значну увагу інформаційній безпеці, боротьбі з дезінформацією та захисту демократичних інституцій. Було посилено співпрацю з європейськими партнерами щодо моніторингу медіапростору, вдосконалення цифрових технологій та розширення потенціалу стратегічних комунікацій. Зростаючий обсяг кіберінцидентів, а також активізація дій недержавних акторів, що можуть діяти в інтересах третіх країн, примушує Швейцарію переосмислювати власну концепцію безпеки та готуватися до кризових сценаріїв нового типу.

У підсумку досвід Австрії та Швейцарії свідчить про те, що навіть країни з нейтральним або позаблоковим статусом не можуть залишатися осторонь глобальних безпекових трансформацій. Їхні моделі реагування на гібридні загрози формуються на основі національних інтересів, політики активного нейтралітету, стратегічної гнучкості та інституційної адаптивності. При цьому критично важливими чинниками ефективності є здатність до міжвідомчої координації, своєчасне оновлення стратегічних документів і розвиток партнерських відносин у сфері кібер- та інформаційної безпеки.

Найактуальнішою проблемою для Швейцарії залишається міграційна криза. У цьому контексті деякі політики наголошують на необхідності зміни пріоритетів при формуванні безпекової політики на користь підтримки поліцейських та прикордонних сил, а не армії. Ще одним важливим завданням в сфері національної безпеки є виявлення серед населення країни прибічників терористичних угруповань та боротьба з вербувальниками терористів. Пряма терористична загроза Швейцарії знаходиться на низькому рівні, оскільки країна не є пріоритетною ціллю джихадистів. Російська агресивна політика теж напряду не загрожує Швейцарії, втім її вплив на міжнародне середовище представляє довготривалий вимір стратегічного оточення держави. Швейцарські

експерти вважають, що наслідки конфронтації рф та Заходу залишатимуться актуальними протягом десятиліть.

Основним завданням швейцарських збройних сил визначається оборона території держави та обмежена участь в миротворчих операціях [38].

Швеція також зміцнює міжвідомчу взаємодію шляхом інтеграції завдань у сфері безпеки між урядовими структурами, зокрема Міністерством оборони, Міністерством юстиції та Службою безпеки (Säkerhetspolisen). Створення інституційної платформи для стратегічного управління ризиками, що виходять за межі традиційної військової загрози, стало ключовим кроком у забезпеченні гнучкої та всебічної відповіді. Значну увагу також приділено співпраці з громадянським суспільством і приватним сектором, зокрема в галузі кібербезпеки та інформаційної гігієни.

З 2017 року в Швеції активно впроваджується концепція «загальної оборони» (Totalförsvaret), яка охоплює не лише збройні сили, а й усі елементи суспільства, включно з державними установами, бізнесом і населенням. Ця концепція передбачає розбудову стійкості як до відкритих воєнних дій, так і до підривної діяльності в умовах «сірої зони». Оновлений підхід до безпеки орієнтований не лише на оборону, а й на попередження, виявлення і пом'якшення впливу гібридних загроз ще до ескалації кризи.

Національна стратегія безпеки Швеції також містить положення щодо посилення стійкості інформаційного простору, протидії зовнішньому втручанням в демократичні процеси та забезпечення безпеки виборів. У цьому контексті особливе місце займає співпраця з іншими скандинавськими та європейськими державами, а також участь у міжнародних ініціативах з протидії дезінформації, таких як «Європейська обсерваторія цифрових медіа» (EDMO).

Таким чином, навіть перебуваючи в статусі позаблокової держави до 2023 року, Швеція вибудувала комплексну та багаторівневу систему безпеки, орієнтовану на адаптацію до гібридних викликів. Її досвід демонструє, що позаблокова країна може ефективно реагувати на нові форми загроз шляхом зміцнення внутрішньої стійкості, розвитку аналітичного та дослідницького

потенціалу, розбудови партнерських відносин і гнучкого підходу до політики безпеки.

Позаблокові країни стикаються з особливими проблемами під час протидії гібридній агресії через свою нейтральну позицію та обмежений військовий потенціал. Однак за допомогою комплексних систем національної безпеки ці країни можуть ефективно боротися з багатовимірною природою гібридних загроз. Використовуючи розвідувальні мережі, покращуючи можливості кібербезпеки, зміцнюючи стійкість і залучаючись до стратегічних партнерств, країни, що не входять у блоки, можуть розробити надійний захист для оборони своїх інтересів національної безпеки у все більш складному та взаємопов'язаному світі.

3.3. Засоби та інструменти протидії гібридній агресії та запобігання проксі-конфлікту в структурі національної безпеки України

Очевидним є той факт, що сьогодні, в епоху глобальних викликів і загроз, світ переживає новий етап геополітичного протиборства між провідними країнами світу за ресурси, комунікації, ринки збуту, розширення сфер впливу та інше. Можна з упевненістю сказати, що Україна зразка 2013-2014 років не була готова до викликів гібридної війни, оскільки отримані внаслідок розпаду СРСР у 1991 році можливості рік за роком Україна втрачала, не маючи рішучості покінути із радянським минулим, передусім у сфері державного управління.

Все це призвело до зависання в певному «пострадянському вакуумі». Така нерішучість призвела до того, що в Україні за допомогою агентів впливу, тобто певних маніпуляторів, у науковій та блогосфері стали поширюватися різноманітні інтерпретації концепції «failed state», в якій усіяко із застосуванням маніпулятивних технологій обґрунтовується неможливість реалізації Україною свого суверенітету, і фактично готувалась наукова та теоретична база для доведення факту неспроможності України та української політичної нації мати власну незалежну та суверенну соборну державу. Тому

будь-які анексії та паради суверенітетів або сепаратизмів трактуються як природна відповідь на неспроможність державної влади України управляти всією країною, задовольняти національні інтереси, а не потреб окремих осіб з числа олігархату [32]. Все це призвело до того, що у 2014 році проти України був застосований метод гібридної війни з боку російської федерації. Ця боротьба триває і на сьогоднішній день [32].

Гібридна агресія та проксі-конфлікти створюють значні виклики національній безпеці, вимагаючи ефективних засобів та інструментів протидії таким загрозам. Україна, розташована на геополітичному роздоріжжі, стикалася з численними випадками гібридної за останні роки. Після аналізу російської гібридної агресії (з 2014 року до сьогодні) можна дійти висновку, що вона є гібридною за своїм характером і змішаною за діями, технікою та методами, зміною ролі цивільного населення, місцевих громадських рухів і політичних організацій та перетворення їх на активних учасників вимушеного протистояння.

Перш ніж загострювати увагу на конкретних викликах, які стоять перед Україною, треба дати визначення даних понять, та описати їх структурні елементи. Законодавче визначення поняття національної безпеки наводиться у однойменному Законі України «Про Національну безпеку України», за яким під даним терміном розуміють захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. Тобто ми можемо побачити, що національна безпека України є багатокомпонентним та багатоаспектним поняттям, і для її активної практичної реалізації повинні тісно співпрацювати майже всі внутрішні та зовнішні державні системи [52].

Однак, важливою складовою російсько-української гібридної війни є не лише використання російською федерацією військової стратегії зі знищення української державності, але й систематичне руйнування політичних інститутів України. Це створює загрозу для національної безпеки країни. Більше того, росія активно проникала в українські владні структури та активно здійснювала політику рекрутингу в армії та спецслужбах. Говорячи про самі методи,

інструменти та рекомендації, щодо покращення системи національної безпеки, зараз будуть наведені конкретні приклади секторів національної безпеки які можуть бути зв'язані з відбиванням гібридної агресії. Покращення служб зовнішньої розвідки і ситуаційна обізнаність. Україна визнає критичну роль розвідки та ситуаційної обізнаності у протидії гібридній агресії.

Посилення розвідувальних можливостей, у тому числі розвідувальних мереж, сигнальної розвідки та розвідки на основі відкритих джерел (OSINT), дозволяє своєчасно виявляти та оцінювати гібридні загрози. Відстежуючи дії супротивників, аналізуючи їхні наміри та виявляючи вразливі місця, Україна може активно реагувати на потенційні гібридні атаки чи «тригери» проксі-конфлікту.

При своєчасному розкритті планів підготовки гібридної війни з метою протидії формується відповідна довгострокова військово-політична стратегія, створюється спеціальний національний (коаліційний) орган для координації зусиль розвідки на всіх рівнях, від стратегічного до тактичного, виробляються принципові підходи щодо ефективного та прихованого використання сил спеціальних операцій і нанесення ударів високоточною зброєю. Ретельно визначаються райони, які можуть бути охоплені гібридною війною, попередньо вивчаються всі їх характеристики.

При плануванні та організації розвідки важливо розуміти, що в сучасних умовах перемога у війні не обов'язково полягає в повному розгромі збройних сил протилежної сторони, в їх фактичному знищенні або взятті в полон, окупації або встановленні тотального контролю над територією противника. Сенса гібридної війни полягає в дезінтеграції військового організму держави-жертви агресії, в руйнуванні основних елементів державної влади, в досягненні тотального контролю над свідомістю населення, що вимагає наявності централізованої системи протидії цьому виду конфлікту.

Синергетичний ефект застосування гібридних загроз обумовлює їх особливу небезпеку для всієї системи забезпечення національної безпеки країни, що вимагає своєчасного розкриття загроз розвідкою на основі науково

обґрунтованого прогнозування сенсу і цілей дій противника, визначення сил та засобів гібридної агресії, об'єктів впливу загроз.

Головне завдання полягає у своєчасному розкритті підготовчих заходів супротивника по розв'язуванню гібридної агресії, комплексу гібридних загроз, які планується використати для підривання безпеки країни. Успішне рішення головної задачі опирається на комплекс розвідувальних завдань, що стоять перед усіма видами розвідки і контррозвідки. Завдання охоплюють сфери діяльності супротивника, в яких формуються стратегії підривних дій, створюються необхідні ресурси, встановлюються канали зв'язку і взаємодії. Загальна цільова установка по руйнуванню держави-жертви агресії розробляється і узгоджується країною-агресором на рівні урядових органів, керівництва транснаціональних корпорацій, фінансовобанківських структур, окремих впливових осіб.

Тому, важливим завданням розвідки є добування планів дій країни-агресора з дестабілізації адміністративно-політичної, соціально-економічної і культурносвітоглядної сфер, які передбачають створення на території країни-жертви розподілених мережевих структур з високою мірою самостійності і здатністю до самосинхронізації, каналів їх забезпечення : фінансових, матеріально-технічних, інформаційних, кадрових, створення складів зброї, боєприпасів, засобів зв'язку, підбирання місць для підготовки бойовиків тощо. Також важливим завданням розвідки є виявлення умов підготовки спецоперацій противника, спрямованих на прискорення процесів розвалу держави і замаскованих під дипломатичні демарші, економічні санкції, інформаційні «вкидання», диверсійні акти проти важливих об'єктів [16].

Створення Україною Спільного розвідувального центру у 2019 році покращило координацію розвідки та співпрацю між різними силовими відомствами. Цей централізований розвідувальний центр покращує обізнаність про ситуацію в країні, забезпечуючи більш ефективну відповідь на гібридні загрози. Окреме питання це діяльність російських розвідувальних служб на території України, яка має на меті діяти відразу по декількох напрямках, це і збір інформації з обмеженим доступом, вербування місцевого населення, підривна

діяльність. Дієво протидіяти цьому можна буде коли Служба безпеки України трансформується у виключно контртерористичний та контррозвідувальний орган, по прикладу хоча би британської MI5, яка займається виключно 3 функціями: боротьба з тероризмом, шпіонажем та розповсюдженням зброї масового ураження.

Таким чином цілком слушною є ідею виведення зі складу СБУ підрозділу «К» (Головне управління боротьби з корупцією та організованою злочинністю), з передачею повноважень даного відділу ДБР, Національній поліції чи новоствореному Бюро економічної безпеки. Це зменшить кількість кадрів, фінансування, та сфокусує СБУ дійсно на нагальних проблемах, а не на питаннях господарських злочинів [52].

Кібербезпека та інформаційні операції. Гібридна агресія часто включає кіберпростір та інформаційні операції для маніпулювання громадською думкою, поширення дезінформації та порушення критичної інфраструктури. Україна визнає важливість надійних заходів кібербезпеки та активних інформаційних операцій для протидії гібридним загрозам. Використання кіберпростору як виміру асиметричної агресії є явищем порівняно новим і менш опрацьованим з точки зору розуміння рівня загроз та можливої протидії.

Як відзначає Д.Дубов, начальник відділу інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень, дискусія щодо сприйняття природи кібератак та відповідей на них почалася в 2010-2011 роках. У 2011 році був прийнятий документ «Талліннське керівництво із застосування міжнародного законодавства у кіберсфері», а в 2012 році НАТО визнало кіберпростір новим театром воєнних дій. Однак у практичній площині реагування є досить проблематичним, оскільки важко довести причетність конкретних країни чи груп до здійснення атак [9].

Передовсім, як відзначають експерти, активність російських спецслужб у кіберпросторі України до 2013 року не була відчутною. Водночас уже був відомий досвід здійснення росією кібератак проти Естонії та Грузії. А в 2013 році українські спеціалісти почали фіксувати низку АРТ-атак, спрямованих на збір

таємної інформації чи інформації з обмеженим доступом. У більшості атак аргументовано підозрюються російські спецслужби та контрольовані ними хакерські спільноти [31].

Створення в Україні Національного координаційного центру кібербезпеки (NC4) у 2017 році посилює здатність країни захищатися від кібератак. NC4 співпрацює з міжнародними партнерами та розробляє комплексні стратегії кібербезпеки для захисту критичної інфраструктури, державних систем і даних громадян.

На даний момент потрібно більше зосереджувати увагу на: підвищення захищеності критичної інформаційної інфраструктури та стійкості її функціонування, розвиток механізмів виявлення та попередження кіберзагроз та ліквідації наслідків їх прояву, підвищення захищеності громадян та територій від наслідків надзвичайних ситуацій, спричинених інформаційно-технічним чи військовим впливом на об'єкти критичної інформаційної інфраструктури.

Певна річ, захист критичних галузей, які функціонують на базі широко розповсюджених інформаційних систем, наприклад телекомунікацій або охорони здоров'я, також має приділятися значна увага, але, на нашу думку, сучасні засоби забезпечення кібербезпеки при грамотному їх використанні здатні значно знизити ризики, що виходять від самих різних загроз: починаючи від звичайних шкідливих програм і до складних таргетованих атак. У промислових інформаційних системах ці методи просто непридатні через безліч причин [40].

Зміцнення стійкості та соціальної згуртованості. Розвиток стійкості в суспільстві має вирішальне значення для протидії гібридній агресії та запобігання конфліктам, пов'язаним з іншими. Україна зосереджується на посиленні суспільної згуртованості, просуванні демократичних цінностей і протидії кампаніям дезінформації, які спрямовані на використання розбіжностей. Після окупації Криму та агресії РФ на Сході України виникли нові виклики в сфері захисту прав і свобод людини. Експерти вказують, що сьогодні ключовими проблемними факторами у цій сфері є окупація, воєнні дії і гальмування реформ.

Вони пов'язані зі «зневагою до верховенства права та прав людини, популізмом, який породжує політичну корупцію та безвідповідальність влади, запевнення великих груп політиків та громадських активістів, що складні проблеми можна вирішити простими шляхами, зокрема, за рахунок застосування сили і примусу» [3].

В Україні відзначаються прояви таких гібридних впливів, як використання квазі-громадських організацій, медіа та соціальних мереж для дестабілізації міжнаціональних відносин, експлуатація теми політики пам'яті та соціокультурних питань.

Наприклад, у травні 2017 року в деяких регіонах було розгорнуто зовнішню рекламну кампанію «Опозиційного блоку» з провокативними гаслами, які стимулювали ескалацію конфліктів: «Требуем остановить репрессии и наступление нацизма», «Требуем прекратить войну» тощо. В червні 2016 року повідомлялося про намагання створення Бессарабської народної республіки [10].

Український уряд, організації громадянського суспільства та навчальні заклади співпрацюють, щоб підвищити обізнаність про гібридні загрози, дезінформацію та важливість критичного мислення. Освітні програми та громадські кампанії сприяють медіаграмотності та громадянській активності, зміцнюючи стійкість суспільства проти тактики гібридної війни. Боротьба за молодь в контексті згуртованості, вона є дуже важливою. Тому що старше покоління, воно вже є зі своїми сформованими якимись думками, сформованими позиціями. Є великий спектр, який ми вже не згуртуємо ніколи. Згуртувати треба тих, кого ще можливо згуртувати [13].

Покращення сектору правоохоронної системи в контексті гібридної агресії. Гібридна агресія ставить перед націями складні виклики, долаючи традиційні кордони війни та безпеки. Щоб подолати цю багатогранну загрозу, уряди повинні зосередитися на зміцненні своїх правоохоронних систем. У цьому розділі підкреслюється важливість посилення правоохоронного сектору в ширшому контексті гібридної війни. Тривалий час правоохоронна система

поступово деградувала, перетворюючись на каральний орган у руках авторитарного й низькоморального керівництва.

До служби в правоохоронних органах потягнулися люди, які планували власне збагачення саме за рахунок використання свого службового становища. Загальна ситуація в державі не сприяла тому, щоб у рядах правоохоронної системи затримувалися професійні, компетентні, моральні і відповідальні кадри. Низький рівень фінансового та матеріально-технічного забезпечення спонукав правоохоронців до пошуку додаткових заробітків, що призводило до процвітання корупції, «кришування», сприяння незаконній діяльності. Корумпованість силових відомств більшість (56,8%) українських експертів назвали першим за важливістю фактором для початку агресії росії проти України [15].

Важливе значення у втраті правоохоронними органами здатності протистояти гібридним загрозам мало проникнення агентури держави-агресора до системи правопорядку та безпеки держави. Зокрема, за свідченням голови СБУ у 2006- 2010 роках Валентина Наливайченка, «Альфа» й інші підрозділи СБУ станом на лютий 2014 року були інфільтровані російською ідеологією та агентурою настільки, що до кінця квітня 2014 року були переконані – росія не агресор, а росіяни є братами. Тому в Криму вірними присязі залишилися близько 30% співробітників СБУ [19].

У світлі унікальних характеристик гібридної агресії правоохоронні органи повинні надати пріоритет розробці спеціалізованих навчальних програм. Ці програми мають бути зосереджені на покращенні розуміння концепцій, тактики та методів гібридної війни серед персоналу правоохоронних органів. Ці знання дозволять їм виявляти гібридні загрози в межах своєї юрисдикції та ефективно реагувати на них.

Проблема вдосконалення державного управління правоохоронними органами в умовах гібридної війни ще недостатньо досліджена і потребує більш детального вивчення та обговорення. Протистояти гібридним загрозам Україна зможе лише кардинально реформувавши власну систему правоохоронних

органів у напрямку посилення можливості як вертикальної координації дій усіх правоохоронних структур так і горизонтальних зв'язків між ними. Модернізація механізмів державного управління правоохоронними органами на сучасному етапі розвитку держави має проводитись поетапно, з урахуванням вимог сьогоденності та міжнародного досвіду. На першому етапі необхідно затвердження концепції реформи правоохоронних органів, із визначенням періодів та термінів, потрібних ресурсів, індикаторів та критеріїв оцінювання результатів.

На другому етапі необхідно прийняття загального закону про правоохоронні органи, розроблення законодавчої бази у відповідності вимогам цього закону, зокрема відповідних положень про роботу правоохоронних органів.

На третьому етапі має відбутися реалізація реформи. Вдосконалення системи державного управління правоохоронними органами в цих умовах має бути спрямоване на забезпечення керівництва ним як цілісною системою, що побудована на наступних принципах: чіткої регламентації діяльності кожного правоохоронного органу з метою уникнення дублюючих та неpritаманих функцій; налагодження співробітництва та ефективних стратегічних комунікацій між правоохоронними органами; застосуванні адаптивних стратегій управління, які передбачають залучення незалежних експертних організацій; залучення громадянського суспільства до прийняття найбільш важливих стратегічних рішень з питань забезпечення внутрішньої безпеки, співпраця з населенням та місцевими громадами; суттєвого підвищення рівня професійності та відповідальності працівників, що підвищуватиме довіру суспільства до правоохоронної системи; забезпечення необхідного рівня фінансового, матеріальнотехнічного та соціального забезпечення працівників, що гарантує їм гідне місце і роль у суспільстві.

У результаті реформування правоохоронна система має перетворитися на суспільно-орієнтовану структуру, побудовану на сервісній моделі діяльності органів правопорядку, позбавитися репресивних функцій та бути орієнтованою

на вирішення проблем населення в рамках загальновизнаного у світі підходу партнерських відносин. Загальний успіх у протидії гібридній війні буде залежати від здатності правоохоронних органів продемонструвати населенню держави та у першу чергу – окупованих районів, переваги української моделі розвитку з ефективною системою верховенства права, високими соціальними та демократичними стандартами, ефективним державним управлінням. Таким чином, новими функціями правоохоронних органів у сучасних умовах мають стати оновлена діяльність задля забезпечення цілісності та стабільності держави, а також захист від новітніх загроз та здатність до реагування на новітні виклики [37].

Еволюція характеру гібридної агресії вимагає постійного вдосконалення правоохоронного сектору. Зосереджуючись на навчанні, зборі та аналізі розвідданих, технологічному прогресі та міжнародній співпраці, уряд України може посилити свою здатність ефективно протистояти гібридним загрозам. Зміцнення правоохоронної системи є життєво важливим для захисту національної безпеки, збереження стійкості суспільства та збереження верховенства права перед обличчям гібридної агресії. Протидія гібридній агресії та запобігання проксі-конфліктам є першочерговими для національної безпеки України.

Покращуючи можливості розвідки, зміцнюючи кібербезпеку, сприяючи стійкості суспільства та покращення сектору правоохоронної системи, Україна прагне пом'якшити вплив тактики гібридної війни. Ці засоби та інструменти разом із постійною адаптацією та інноваціями сприятимуть збереженню суверенітету, стабільності та національної безпеки України перед обличчям гібридних загроз, що розвиваються.

Підсумовуючи матеріал викладений в розділі, ера гібридних воєн і проксі-конфліктів створює значні виклики для систем національної безпеки в усьому світі. Ці виклики включають швидкий розвиток технологій, складність гібридних загроз і потребу в покращенні координації та співпраці між державами.

Розширення можливостей розвідки, інвестиції в передові технології, сприяння міжнародній співпраці та розробка комплексних стратегій є важливими для систем національної безпеки задля ефективної протидії гібридній агресії та запобігання проксіконфліктам. Вирішуючи ці основні проблеми, країни можуть підвищити свою стійкість, захистити свій суверенітет і захистити свою національну безпеку перед обличчям загроз, що розвиваються, розвивалися і будуть розвиватися.

Висновки до розділу 3

Розділ 3 присвячений аналізу ключових проблем систем національної безпеки в умовах гібридних війн та проксиконфліктів. У результаті проведеного дослідження встановлено, що традиційні підходи до забезпечення національної безпеки виявилися недостатніми для ефективного протистояння новітнім загрозам, які набувають багатовимірною і водночас прихованого характеру. Гібридна агресія поєднує в собі як традиційні військові методи, так і нові форми – кіберзлочинність, інформаційні кампанії, економічний та політичний тиск, що вимагає перегляду стратегій захисту на рівні держав.

Країни-члени НАТО демонструють високий рівень адаптації до гібридних загроз завдяки колективним механізмам реагування, єдиній політиці кіберзахисту, налагодженій співпраці між розвідувальними службами та постійному вдосконаленню стратегії стримування. Позаблокові держави, які не мають колективних безпекових гарантій, змушені формувати власні моделі національної безпеки, адаптовані до геополітичного становища, внутрішніх ресурсів і ступеня вразливості. Приклади Фінляндії, Індії, Швейцарії, Швеції та інших країн засвідчують, що ефективна протидія гібридним загрозам можлива навіть за відсутності членства в оборонних альянсах, за умови стратегічного планування, розвитку розвідувальних можливостей, кіберзахисту, медіаграмотності та міжвідомчої координації.

Окрему увагу приділено Україні, яка, як держава, що вже тривалий час перебуває в умовах гібридної війни з російською федерацією, змушена в короткі терміни модернізувати свої інституції безпеки. Показано, що ключовими напрямками зміцнення національної безпеки України є розвиток розвідувального потенціалу, реформування СБУ та правоохоронної системи, посилення кіберзахисту, стратегічні комунікації, а також підвищення рівня соціальної згуртованості та стійкості суспільства. Наголошено, що гібридна війна не обов'язково передбачає класичне зіткнення армій, а її головна мета —

дестабілізація політичної системи, підрив довіри до влади та роз'єднання громадянського суспільства.

Узагальнюючи викладене, можна стверджувати, що протидія гібридній агресії потребує не лише силового інструментарію, а й комплексного міжгалузевого підходу, що включає політичні, економічні, інформаційні, дипломатичні та соціальні заходи. Успішна протидія таким загрозам можлива лише за умови політичної волі, стратегічного бачення та тісної взаємодії на міжнародному рівні. Системи національної безпеки повинні розвиватися динамічно, враховуючи новітні виклики, та бути спроможними адаптуватися до непередбачуваних сценаріїв гібридної агресії.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

В роботі розглянуто проблеми міжнародної та національної безпеки в епоху гібридних війн та проксі-конфліктів. Дослідження зосереджувалися на теоретичних та практичних аспектах цих проблем, а також на оцінці та аналізі використаних досліджень. Щодо теоретичних аспектів, було розглянуто концепцію гібридних війн та їх вплив на міжнародну та національну безпеку. Зазначено, що гібридні війни характеризуються поєднанням військових та невійськових методів ведення конфлікту, таких як інформаційна війна, кібератаки, фінансовий тиск та інші.

Висвітлено важливість адаптації національних систем безпеки, на прикладі позаблокових держав та України, до нових загроз та необхідність розвитку міжнародного співробітництва для протидії гібридним загрозам. У практичній частині були проаналізовані дослідження, які звертаються до проблеми гібридних війн та проксі-конфліктів. Виявлено, що багато досліджень фокусуються на ролі кібербезпеки та інформаційної війни в контексті гібридних загроз.

Висвітлено значення обміну розвідувальною інформацією та співпраці між державами в контексті протидії гібридним загрозам. Оцінюючи використані дослідження, слід зазначити їх значний внесок у розуміння проблеми гібридних війн та проксі-конфліктів. Вони надали необхідні теоретичні засади та підходи до практичних досліджень, які можуть бути використані для розвитку стратегій та політик безпеки на національному та міжнародному рівнях.

Однак, варто відзначити, що деякі аспекти проблеми міжнародної та національної безпеки в епоху гібридних війн та проксі-конфліктів залишаються недостатньо дослідженими. Наприклад, важливо дослідити більш детально вплив економічних факторів та економічної залежності на безпеку держав, а також роль громадської думки та медіа в контексті гібридних загроз. З метою вирішення розглянутих у роботі проблем, висновки та пропозиції включають наступні пункти:

1. Посилення міжнародного співробітництва: З метою ефективної протидії гібридним загрозам, важливо розвивати міжнародне співробітництво та обмін інформацією між державами. Вироблення спільних стратегій та механізмів координації може покращити здатність держав протидіяти гібридним загрозам.

2. Розвиток кібербезпеки та захисту інформації: У зв'язку з ростом кіберзагроз та інформаційної війни, необхідно залучати більше ресурсів до розвитку кібербезпеки та захисту інформації. Це включає покращення технічних засобів захисту, підвищення кваліфікації фахівців та розробку політик та норм, спрямованих на протидію кіберзагрозам.

3. Розширення області досліджень: Необхідно залучати більше ресурсів та зусиль для дослідження та розуміння проблеми гібридних війн та проксі-конфліктів. Це може включати проведення більш детального аналізу економічних аспектів безпеки, розробку стратегій ефективної комунікації та управління громадською думкою, а також вивчення впливу новітніх технологій, таких як штучний інтелект та кіберфізичні системи, на безпеку.

4. Збалансований підхід до безпеки: Важливо підходити до питання безпеки в комплексному та збалансованому способі. Це означає поєднання військових та невійськових засобів протидії загрозам, залучення дипломатичних та політичних інструментів, зміцнення резервів та розвиток регіональних та міжнародних механізмів колективної безпеки.

5. Виховання свідомих громадян: Покращення безпеки також потребує виховання свідомих громадян, які здатні розпізнавати гібридні загрози та вчасно реагувати на них. Це може включати освіту населення про безпекові ризики, розвиток медійної грамотності та посилення критичного мислення. У цілому, проблеми міжнародної та національної безпеки в епоху гібридних війн та проксі-конфліктів є складними та багатограними. Вирішення цих проблем вимагає збільшення співробітництва, розвитку кібербезпеки, розширення області досліджень та застосування збалансованого підходу до безпеки. Ініціативи на національному та міжнародному рівнях, спрямовані на цільову боротьбу з гібридними загрозами, можуть сприяти поліпшенню ситуації Одним із ключових

висновків роботи є те, що загрози, пов'язані з гібридними війнами та проксі-конфліктами, не обмежуються територією окремих країн чи регіонів. Вони мають глобальний характер і вимагають спільних зусиль та міжнародної координації для ефективного протидії.

Створення міжнародних механізмів співробітництва, обмін досвідом та розвідувальною інформацією стануть ключовими елементами у формуванні колективної безпеки. У контексті розглянутих проблем, необхідно звернути увагу на необхідність більш широкого дослідження економічних аспектів безпеки. Гібридні війни та проксі-конфлікти мають значний вплив на економічну стійкість держав, зокрема через залежність від енергетичних ресурсів, міжнародну торгівлю та фінансову систему. Детальне дослідження цих аспектів може допомогти в розробці стратегій зменшення ризиків та підвищення економічної стійкості в умовах гібридних загроз.

Крім того, важливо звернути увагу на роль громадської думки та медіа в контексті гібридних війн та проксі-конфліктів. Зловживання медійним простором та маніпуляція громадською думкою можуть стати ефективними інструментами в руках акторів, що здійснюють гібридні атаки. Посилення медійної грамотності та розвиток стратегій ефективної комунікації можуть зменшити вразливість суспільства перед гібридними загрозами.

Загалом, у цій дипломній роботі автор проаналізував проблеми міжнародної та національної безпеки в епоху гібридних війн та проксіконфліктів. Результати досліджень свідчать про серйозні загрози, з якими зіткнулися сучасні держави та міжнародна система в цілому. Висновки вказують на необхідність змін у підходах до безпеки, як на теоретичному, так і на практичному рівні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Визначення агресії: резолюція від 14.12.1974. № 995_001-74. [Електронний ресурс]. - Режим доступу: https://zakononline.com.ua/documents/show/169633_169633
2. Щорічний звіт Генерального секретаря за 2022 рік. Офіційна інтернетсторінка НАТО. 21 березня 2023. [Електронний ресурс]. - Режим доступу: https://www.nato.int/cps/en/natohq/opinions_212795.htm?selectedLocale=uk#sg4
3. Права людини в Україні 2016. [Електронний ресурс]/ Українська Гельсінська спілка з прав людини. – Режим доступу: https://helsinki.org.ua/wp-content/uploads/2016/12/HumanRight2016-sokr_web.pdf
4. Статут ООН. Департамент громадської інформації ООН. Київ. [Електронний ресурс]. - Режим доступу: https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/UN%20Charter_Ukrainian.pdf
5. Щорічна доповідь за 2002 рік щодо діяльності ОБСЄ. Відень. 2003. ОБСЄ.
6. Final Report on the Meaning of Armed Conflict in International Law. The Hague Conference (2010). Use of Force. [Електронний ресурс]. - Режим доступу: [http://www.ila-20hq.org/download.cfm/docid/2176DC63-%20D268%E2%80%93934133%E2%80%93938989A664754F9F87%20\(Last%20accessed:%2030.09.2016\).](http://www.ila-20hq.org/download.cfm/docid/2176DC63-%20D268%E2%80%93934133%E2%80%93938989A664754F9F87%20(Last%20accessed:%2030.09.2016).)
7. NorthAtlantic Treaty Organization. Cyber Defence Pledge. [Електронний ресурс]. –Режим доступу: https://www.nato.int/cps/su/natohq/official_texts_133177.htm
8. North Atlantic Treaty Organization. Warsaw Summit Communiqué, 9.7.2016. [Електронний ресурс]. – Режим доступу: https://www.nato.int/%20cps/en/natohq/official_texts_133169.htm

9. Військова відповідь на кібератаки Кремля? І так, і ні. [Електронний ресурс]. Укрінформ. – Режим доступу : <https://www.ukrinform.ua/rubrictechnology/2251563-vijskova-vidpovid-nakiberataki-kremla-i-tak-i-ni.html>

10. Голова СБУ пояснив, навіщо ФСБ знадобилось обмінювати сепаратистів з Одеси. [Електронний ресурс]/«5 канал». – Режим доступу: <https://www.5.ua/suspilstvo/holova-sbu-poiasnyvnavishcho-fsbznadobylos-obminiuvaty-separatystiv-z-odesy-117784.html>

11. Десятки тисяч віруючих підписали звернення до Верховної Ради. [Електронний ресурс]/ УПЦ МП. – Режим доступу: <http://news.church.ua/2017/05/15/desyatki-tisyach-viruyuchixpidpisalizvernennya-do-verhovnoji-radi/>

12. Індія-Пакистан: ядерної війни поки немає, в розпалі гібридна. Інформаційне агентство «Український інтерес». 04.03.2019. [Електронний ресурс]. - Режим доступу: <https://uain.press/news/world/indiya-pakistan-yadernoyi-vijny-pokynemaye-v-rozpali-gibrydna-1004885>

13. Інтерв'ю з Віктором Міщишиним «Війна та згуртованість суспільства». Інститут Громадського Суспільства. 22.01.2022. – Режим доступу: <https://www.csi.org.ua/news/vijna-ta-zgurtovanist-suspilstva-viktormishhyshyn/>

14. Прес-реліз: Чинний голова та Генеральна секретарка висловили жаль щодо недосягнення консенсусу для продовження дії мандата СММ в Україні. Офіційна інтернет-сторінка ОБСЄ. 31 березня 2022. [Електронний ресурс]. - Режим доступу: <https://www.osce.org/uk/chairmanship/515018>

15. Сприяння розбудові можливостей України гарантувати безпеку суспільства в умовах гібридних загроз. Результати експертного опитування. [Електронний ресурс]. – Режим доступу: https://geostrategy.org.ua/images/%D0%94%D0%BE%D1%81%D0%BB%D1%96%D0%B4%D0%B6%20%D0%B5%D0%BD%D0%BD%D1%8F_%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%20%D1%81%D1%8C%D0%BA%D0%BE%D1%8E.pdf

16. Ткач В. Про роль розвідки в гібридній війні і «дзеркальну проекцію». Інформаційне агентство «ОПК». 01.04.2019. [Електронний ресурс]. - Режим доступу: <http://opk.com.ua/%D0%BF%D1%80%D0%BE-%D1%80%D0%BE%D0%BB%D1%8C-%D1%80%D0%BE%D0%B7%D0%B2%D1%96%D0%B4%D0%BA%D0%D0%B2-%D0%B3%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D1%96%D0%B9-%D0%B2%D1%96%D0%B9%D0%BD%D1%96-%D1%96/>

17. Україна і Сінгапур домовилися про співпрацю між кіберкопами. Інформаційне агентство «Укрінформ». 29.10.2018. [Електронний ресурс]. - Режим доступу: <https://www.ukrinform.ua/rubricsociety/2568057-ukraina-i-singapur-domovilisa-pro-spivpracu-mizkiberkopami.html>

18. Фінляндія через побоювання гібридної війни внесла продаж землі росіянам до списку загроз безпеці. Інформаційне агентство «УНІАН». 03.03.2016. [Електронний ресурс]. - Режим доступу: <https://www.unian.ua/economics/realestate/1282030-finlyandiya-cherezpoboyuvannya-gibridnoji-viyni-vnesla-prodaj-zemli-rosiyanam-do-spiskuzagroz-bezpetsi.html>

19. Як ми втрачали Крим. Свідчення перших осіб України. [Електронний ресурс]/«Українська правда».—Режим доступу: https://www.pravda.com.ua/cdn/graphics/2017/04/jak_my_vtrachaly_krym_svidchennja_pershyh_osib_ukrainy/

20. Національна безпека. Монографія. Д. Паламарчук. Борисфен Інтел. 24 травня 2020.

21. Національна стійкість в умовах мінливого безпекового середовища. Монографія. О. О. Резнікова. – Київ 2022. [Електронний ресурс]. - Режим доступу: https://niss.gov.ua/sites/default/files/2022-03/reznikovaukraineresilience2022_02.pdf

22. Україна у системі міжнародної безпеки. Монографія. За ред. О.С. Власюка. – Київ. Фоліант; Стилос, 2009. – С. 94.

23. ALYSON J. K. BAILES and ANDREW COTTEY. Regional security cooperation in the early 21st century. SIPRI Yearbook 2006: Armaments, Disarmament and International Security. 2006. [Електронний ресурс]. - Режим доступу: <https://www.sipri.org/sites/default/files/YB06ch04.pdf>

24. Гібридна війна і журналістика - проблеми інформаційної безпеки: навчальний посібник. Вид-во НПУ ім. М. П. Драгоманова. Київ. 2018. – 12 с.. [Електронний ресурс]. - Режим доступу: <https://enpuir.npu.edu.ua/bitstream/handle/123456789/25597/Kulias%2012-27.pdf;jsessionid=0D21A2B67B6130AAA69627C2AAE64D3B?sequence=1>

25. Міжнародне право. Особлива частина: навчальний посібник для студентів юр. факультетів та ВНЗ // І. І. Лукашук. Академія правових вчень. Вид. №3. 2005.

26. Міжнародне публічне право: підручник // за ред.. Д. К. Бекашева. 2002.

27. Політична наука: словник-довідник. Санжаревський І. І. Вид №6.. Тамбов. 2016. - 1290 с.

28. Прохоров А. М. Великий енциклопедичний словник. Вид № 3. 2004 . – 1456 с.

29. Соціологія: енциклопедія. Грицанов О. О., Абушенко В. Л.. Мінськ. 2003. – 1312 с.

30. Shifting Paradigm of War: Hybrid warfare. Turkish National Defense University. Istanbul (2017). [Електронний ресурс]. - Режим доступу: <https://www.msu.edu.tr/eng/Documents/Hybrid%20Warfare.pdf>

31. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2016 році». – К.: НІСД, 2016. – 258с.

32. Бахметьев А. Є. Забезпечення національної безпеки України в умовах ведення гібридної війни. НУ «Одеська юридична академія». [Електронний ресурс]. - Режим доступу: <http://dspace.onua.edu.ua/bitstream/handle/11300/21740/%d0%91%d0%b0%d1%85%d0%bc%d0%b5%d1%82%d1%8c%d1%94%d0%b2%20%d0%9>

0.%20%d0%84.%20%d0%97%d0%b0%d0%b1%d0%b5%d1%81%d0%bf
 %d0%b5%d1%87%d0%b5%d0%bd%d0%bd%d1%8f%20%d0%bd%d0%b
 0%d1%86%d1%96%d0%be%d0%bd%d0%b0%d0%bb%d1%8c%d0%bd%
 d0%be%d1%97%20%d0%b1%d0%b5%d0%b7%d0%bf%d0%b5%d0%ba%
 d0%b8%20%d0%a3%d0%ba%d1%80%d0%b0%d1%97%d0%bd%d0%b8
 %20%d0%b2%20%d1%83%d0%bc%d0%be%d0%b2%d0%b0%d1%85%2
 0%d0%b2%d0%b5%d0%b4%d0%b5%d0%bd%d0%bd%d1%8f%20%d0%
 b3%d1%96%d0%b1%d1%80%d0%b8%d0%b4%d0%bd%d0%be%d1%97
 %20%d0%b2%d1%96%d0%b9%d0%bd%d0%b8.pdf?sequence=1&isAllow ed=y

33. Брежнєва Т.В. Стійкість як ключовий елемент колективної оборони НАТО // Стратегічні пріоритети. –2017. –№ 3 (44). –С. 13

34. Гібридна війна Росії – виклик і загрози для Європи. Центр Разумкова. Київ, грудень 2016. [Електронний ресурс]. - Режим доступу: https://razumkov.org.ua/images/Material_Conference/2016_12_14/GIBRIDWAR-FINAL-1-1.pdf

35. Горбулін В. П. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. [Електронний ресурс]. - Режим доступу: https://niss.gov.ua/public/File/2015_book/012315_Gorbulyn.pdf

36. Донеллі Дж. Права людини у міжнародній політиці // переклад з англ.. Т. Завалій. – Львів. 2004. – 280 с.

37. Загорулько А. П. Удосконалення державного управління правоохоронними органами як фактор підвищення їх ефективності в умовах гібридної війни. УДК 355/359.07. Київ. - Режим доступу: http://repositsc.nuczu.edu.ua/bitstream/123456789/7741/1/ilovepdf_com-14-23.pdf

38. Замікула М. О. Безпекова та оборонна політика нейтральних країн Європи в умовах дестабілізації системи міжнародних відносин. Національний інститут стратегічних досліджень. Відділ проблем зовнішньої політики та міжнародної безпеки. 2017. [Електронний ресурс]. - Режим доступу: <https://niss.gov.ua/sites/default/files/2017-07/bezpeka-93fb8.pdf>

39.Іванчик М. Роль міжнародних організацій у системі безпеки країн регіону. ДВНЗ «Ужгородський національний університет». [Електронний ресурс]. - Режим доступу:

<https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/22764/1/%D0%A0%D0%9E%D0%9B%D0%AC%20%D0%9C%D0%86%D0%96%D0%9D%D0%90%D0%A0%D0%9E%D0%94%D0%9D%D0%98%D0%A5%20%D0%9E%D0%A0%D0%93%D0%90%D0%9D%D0%86%D0%97%D0%90%D0%A6%D0%86%D0%99.pdf>

40. Козьмініх А. В. Кібербезпека та кібератаки в умовах гібридної війни. НУ «Одеська юридична академія». [Електронний ресурс]. - Режим доступу: <http://dspace.onua.edu.ua/bitstream/handle/11300/19153/%D0%9A%D0%BE%D0%B7%D1%8C%D0%BC%D1%96%D0%BD%D0%B8%D1%85%20%D0%90%D0%BB%D1%8C%D0%BE%D0%BD%D0%B0%20%D0%92%D1%96%D1%82%D0%B0%D0%BB%D1%96%D1%97%D0%B2%D0%BD%D0%B0.pdf?sequence=1&isAllowed=y>

41. Коломієць О. В. Особливості системи міжнародної безпеки в умовах глобалізації. Автореферат. НУ «Одеська юридична академія». Одеса, - 2015. [Електронний ресурс]. - Режим доступу: <http://dspace.onua.edu.ua/bitstream/handle/11300/2187/%d0%9a%d0%be%d0%bb%d0%be%d0%bc%d1%96%d1%94%d1%86%d1%8c%20%d0%9e.%d0%92..pdf?sequence=1&isAllowed=y>

42. Кучик О. С. Механізми та форми реалізації колективної безпеки у діяльності міжнародних організацій. Наукова стаття. Журнал «Актуальні проблеми міжнародних відносин». Випуск 99 (Частина II). 2011. [Електронний ресурс]. - Режим доступу: https://intrel.lnu.edu.ua/wpcontent/uploads/2015/10/apmv_2011_992__7.pdf

43. Стівен Пінк. Просвітництво сьогодні. Аргументи на користь розуму, науки та прогресу. «Наш формат». – 560 с.

44. Andrew Mumford. Proxy Warfare. John Wiley & Sons, 2013. №. 13.

45. Mikael WIGELL, Harri MIKKOLA, Tapio JUNTUNEN «Best practices in the whole-of-society approach in countering hybrid threats». Policy Department for External Relations Directorate General for External Policies of the Union PE 653.632 - May 2021. [Електронний ресурс]. - Режим доступу: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU\(2021\)653632_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf)

46. Paleri, Prabhakaran (2008). National Security: Imperatives And Challenges. New Delhi: Tata McGraw-Hill. p. 521. ISBN 978-0-07-065686-4. Retrieved 23 September 2010.

47. V. Vlasjuk. HYBRID WAR, INTERNATIONAL LAW AND EASTERN UKRAINE. European political and law discourse. 2015. ISSN 2336-5439. [Електронний ресурс]. - Режим доступу: <https://eppd13.cz/wpcontent/uploads/2015/2015-2-4/04.pdf>

48. Гібридна війна // Вікіпедія. [Електронний ресурс]. - Режим доступу: https://uk.wikipedia.org/wiki/%D0%93%D1%96%D0%B1%D1%80%D0%B8%D0%B4%D0%BD%D0%B0_%D0%B2%D1%96%D0%B9%D0%BD%D0%B0

49. Глобальні проблеми людства // Вікіпедія. [Електронний ресурс]. - Режим доступу: https://uk.wikipedia.org/wiki/%D0%93%D0%BB%D0%BE%D0%B1%D0%B0%D0%BB%D1%8C%D0%BD%D1%96_%D0%BF%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC%D0%B8_%D0%BB%D1%8E%D0%B4%D1%81%D1%82%D0%B2%D0%B0

50. Ліга Націй // Вікіпедія. [Електронний ресурс]. - Режим доступу: https://uk.wikipedia.org/wiki/%D0%9B%D1%96%D0%B3%D0%B0_%D0%9D%D0%B0%D1%86%D1%96%D0%B9

51. Національна безпека // Вікіпедія. [Електронний ресурс]. - Режим доступу: <https://uk.wikipedia.org/wiki/%D0%9D%D0%B0%D1%86%D1%96%D0%B9>

BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%B1
%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0

52. Національна безпека України: Складові елементи та виклики сьогодення. Інтернет-блог «Military». 23 березня 2021. [Електронний ресурс]. - Режим доступу: <https://mil.in.ua/uk/blogs/natsionalna-bezpekaukrayiny-skladovi-elementy-ta-vyklyky-sogodennya/>

53. Організація безпеки та співробітництва в Європі. Україна і ОБСЄ // Вікіпедія. [Електронний ресурс]. - Режим доступу: https://uk.wikipedia.org/wiki/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F_%D0%B7_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8_%D1%96_%D1%81%D0%BF%D1%96%D0%B2%D1%80%D0%BE%D0%B1%D1%96%D1%82%D0%BD%D0%B8%D1%86%D1%82%D0%B2%D0%B0_%D0%B2_%D0%84%D0%B2%D1%80%D0%BE%D0%BF%D1%96#%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B0_%D1%96_%D0%9E%D0%91%D0%A1%D0%84

54. Офіційна інтернет-сторінка Міністерства розвитку громад та територій України. Навчальний посібник «Національна безпека». [Електронний ресурс]. - Режим доступу: <https://www.minregion.gov.ua/wpcontent/uploads/2017/11/Navchalniy-posibnik-GPNB.pdf>

55. Офіційна інтернет-сторінка ОБСЄ. Розділ: Де ми знаходимося. [Електронний ресурс]. - Режим доступу: <https://www.osce.org/ru/wherewe-are>

56. Проблеми безпеки Південно-Східної Європи. [Електронний ресурс]. - Режим доступу: <http://kimo.univ.kiev.ua/CCE/39.htm>

57. MCDC Countering Hybrid Warfare Project. A Multinational Capability Development Campaign project. March 2019. [Електронний ресурс]. - Режим доступу: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf

АНОТАЦІЯ

Максименко Ангеліна Ігорівна «Гібридні війни та проксі-конфлікти як виклик системі глобальної та державної безпеки»– Рукопис.

Кваліфікаційна робота студентки IV - го курсу денної форми навчання на здобуття освітнього рівня бакалавр спеціальності 052 «Політологія». Державний університет «Житомирська політехніка». Факультет національної безпеки, права та міжнародних відносин, Житомир, 2025.

Кваліфікаційна робота складається зі вступу, трьох розділів, висновків та пропозицій, списку використаних джерел. Основний зміст викладено на 76 сторінках друкованого тексту, у тому числі 1 рисунок, список використаних джерел налічує 57 найменувань.

У дипломній роботі досліджено ключові аспекти національної та міжнародної безпеки в контексті новітніх загроз, що набули актуальності в XXI столітті — гібридних війн та проксі-конфліктів. У першому розділі розглянуто еволюцію концепції міжнародної безпеки, проаналізовано структуру та ієрархію національної безпеки, а також надано визначення гібридних воєн і проксі-конфліктів із виокремленням їх основних характеристик.

У другому розділі висвітлено проблеми функціонування глобальних і регіональних систем безпеки в умовах гібридних загроз. Проаналізовано ефективність діяльності ООН, ОБСЄ та інших міжнародних інституцій, їхню здатність адаптуватися до сучасних викликів безпеки, зокрема в умовах протистояння нетрадиційним загрозам.

Третій розділ присвячено аналізу систем національної безпеки окремих країн, як членів НАТО, так і позаблокових держав, з метою виявлення найбільш ефективних інструментів протидії гібридній агресії. Особлива увага приділена українському досвіду побудови національної безпеки у відповідь на багатовекторні гібридні загрози з боку російської федерації.

Результати дослідження дозволяють стверджувати, що в умовах трансформації характеру сучасних конфліктів необхідним є перегляд

традиційних моделей безпеки, посилення координації міждержавних дій та адаптація систем національної оборони до нових викликів.

Ключові слова: *національна безпека, міжнародна безпека, гібридна війна, проксі-конфлікт, НАТО, ООН, ОБСЄ, кібербезпека, інформаційні загрози, стратегія безпеки.*