МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Навчально-науковий інститут «Інститут державного управління»
Кафедра права, національної безпеки та європейської інтеграції

Кваліфікаційна робота магістра
на тему

ФОРМУВАННЯ МЕХАНІЗМІВ УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ В ТОЧЦІ БІФУРКАЦІЇ: УКРАЇНСЬКИЙ ДОСВІД ГІБРИДНОЇ ВІЙНИ

Виконав студент 2 курсу,
групи ППГЗ-3-24
Спеціальності 281 «Публічне управління та адміністрування»
Освітньо-професійної програми
«Публічна політика та управління в умовах гібридних загроз»
_____ Олександр ТЕЛІНКЕВИЧ

Науковий керівник роботи:
кандидат наук з державного управління,
доцент
_____ Михайло БІЛОКОНЬ

Харків – 2025

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному світі система міжнародних відносин зазнає суттєвих змін, що мають характер біфуркації – нестабільного переходу між альтернативними траєкторіями розвитку. Це породжує нові виклики, зокрема для країн, які перебувають на геополітичних межах та мають обмежений ресурсний потенціал для стратегічного реагування. Україна стала прикладом держави, що змушена функціонувати у постійно змінному безпековому середовищі, на тлі гібридної агресії з боку Російської Федерації.

Гібридна війна проти України поєднує військові, інформаційні, економічні та політичні інструменти, що суттєво трансформують структуру загроз. У таких умовах національна безпека перестає бути лише інституційною категорією, натомість стає адаптивною системою, що потребує перегляду підходів до управління, координації між суб’єктами, стратегічного планування та прогностичного реагування.

Актуальність теми зумовлена необхідністю вдосконалення механізмів управління національною безпекою України з урахуванням біфуркаційного характеру міжнародної обстановки та комплексних викликів гібридної війни. Теоретичне осмислення процесів біфуркації, а також практичний аналіз трансформації української безпекової системи дає змогу запропонувати ефективні управлінські рішення.

Стан наукової розробки проблеми. Актуальність обраної теми підтверджується науковими позиціями вітчизняних дослідників. Зокрема, у працях М.П. Стрельбицького та Л.М. Стрельбицької розкрито правові та організаційні механізми реагування на гібридні загрози. В.Ф. Загурська-Антонюк аналізує державне управління безпекою в умовах геополітичної трансформації. У дослідженнях О.І. Крюкова та Н. Нижник акцент зроблено на інституційній спроможності суб'єктів забезпечення безпеки. Узагальнене осмислення проблематики знайшло відображення у монографіях та наукових

доповідях, присвячених трансформації державної політики в контексті гібридної агресії.

Мета дослідження полягає у визначенні шляхів удосконалення системи управління національною безпекою України в умовах гібридної війни та нестабільного міжнародного середовища.

Для досягнення поставленої мети визначено наступні *завдання:*

– проаналізувати концептуальні підходи до розуміння феномену національної безпеки в сучасному світі;

– дослідити процеси біфуркації в міжнародних відносинах та їх вплив на виникнення загроз національній безпеці;

– розкрити сутність гібридної війни як виклику безпековій системі України;

– оцінити трансформаційні процеси в системі національної безпеки України внаслідок гібридної агресії;

– запропонувати шляхи вдосконалення механізмів управління національною безпекою з урахуванням сучасних викликів.

Об'єктом дослідження є система управління національною безпекою України.

Предметом дослідження є формування механізмів управління національною безпекою в точці біфуркації в контексті українського досвіду гібридної війни.

Методологічне підґрунтя роботи ґрунтується на сучасних наукових засадах публічного управління та адміністрування, що дозволяє глибоко аналізувати динаміку змін в системі національної безпеки в умовах біфуркації та гібридної війни.

Методи дослідження. Для досягнення мети дослідження та вирішення поставлених завдань використано комплекс загальнонаукових та спеціальних методів, застосування яких здійснювалося диференційовано відповідно до специфіки кожного етапу дослідження.

Загальнонаукові методи: аналіз та синтез – для систематизації теоретичних

знань про природу національної безпеки та гібридної війни; індукція та дедукція – при формулюванні узагальнень щодо стратегій безпеки; порівняльно-аналітичний метод – для співставлення підходів різних країн до управління безпекою.

Спеціальні методи: доктринально-правовий аналіз – для оцінки нормативної бази в сфері національної безпеки; метод структурно-функціонального аналізу – при дослідженні інституційної спроможності суб'єктів безпеки.

Практичне значення отриманих результатів. Результати дослідження мають прикладне значення для формування ефективної системи управління національною безпекою України в сучасних умовах. На основі аналізу: обґрунтовано напрями вдосконалення механізмів координації між суб'єктами безпеки; запропоновано рекомендації з підвищення інституційної спроможності; визначено стратегічні пріоритети державної політики у сфері безпеки в умовах гібридної загрози.

Отримані результати можуть бути використані: в роботі державних органів, що формують політику у сфері національної безпеки; при підготовці аналітичних матеріалів та стратегічних документів; у навчальному процесі закладів вищої освіти з галузі «Публічне управління та адміністрування».

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ В УМОВАХ БІФУРКАЦІЇ

1.1 Концептуальні підходи до розуміння національної безпеки та її еволюція в сучасному світі

Поняття «безпека» завжди займало ключове місце в системі цінностей людства, і це закономірно з огляду на первинну потребу людини в захисті себе, свого середовища та способу життя. Тому генезис терміна має давню історію та охоплює кілька етапів соціального та філософського осмислення – від античності до сучасності.

Перші уявлення про безпеку виникли ще в добу античної філософії. Зокрема, у трактаті «Держава» Платон визначає безпеку як засіб запобігання шкоди державі. На його думку, охоронці (воїни) виконують функцію захисту як від зовнішніх загроз, так і від внутрішнього порушення порядку: вони мають забезпечувати моральний контроль над громадянами та перешкоджати проявам зла. Платон фактично формує концепт соціально організованої системи безпеки, яка діє в рамках визначених правил, законів і справедливості. У його підході вже простежується усвідомлення важливості поєднання інтересів особи, громади та держави в контексті захисту життєво важливих інтересів [1].

Інший давньогрецький мислитель Арістотель у праці «Політика» також торкається теми безпеки. Він наголошує, що держава з демократичними засадами управління має більше можливостей для забезпечення безпеки громадян. За Арістотелем, політія – форма правління, в основі якої лежить домінування «середнього елемента» – забезпечує найбільшу стабільність та безпеку порівняно з іншими типами державного устрою. Особливу увагу він приділяє ролі законів у забезпеченні суспільного порядку та самозбереження

спільноти, а також наголошує на пріоритетності безпеки держави над індивідуальною безпекою окремої особи [2].

До теми безпеки звертається і римський політик та філософ Марк Туллій Ціцерон, який підкреслює, що прагнення до захисту є вродженою рисою всіх живих істот. Він зазначає, що природою закладено інстинкт самозбереження: захист себе від загроз і набуття необхідного для життя – це універсальні ознаки безпеки, які проявляються на рівні особистості, родини, громади та держави [3].

Із цього випливає висновок: поняття «безпека» як соціально-філософська категорія зародилося в межах античної думки. В умовах постійних війн, територіальних конфліктів та змін політичного устрою, воно розглядалося як фундаментальна умова існування держави та засіб збереження її цілісності й порядку. Очевидним було: ізольованість індивіда чи громади створює передумови для вразливості, а отже – об'єднання навколо спільної ідеї захисту стало основою безпекової свідомості.

Подальший етап у розвитку ідей про безпеку припадає на період Середньовіччя, коли на перший план виходять не лише державні інститути, а й релігійна влада. Церква, поряд із феодальними структурами, відіграє значну роль у формуванні уявлень про безпеку. У цей період безпека починає розглядатися крізь призму внутрішніх загроз – конфліктів, змов, втрати лояльності. Відомим прикладом тогочасного осмислення поняття є слова з листа єпископа Ш. Фульберта до герцога А. Гільома: «Безпека – це значить не видавати його таємниць та не шкодити безпеці його укріплень» [4]. Це свідчить про формування перших принципів конфіденційності, вірності та структурованого підходу до захисту домену влади.

Одним з основоположників теорії політичного реалізму, який зроби значний внесок у розуміння безпеки в міжнародних відносинах є Ганс Моргентау, професор Чиказького університету, зі своєю науковою роботою «Politics Among Nations» (1948 р.), яка стала класикою у цій галузі. Розгля- немо більш детально основні ідеї Г. Моргентау про безпеку та його бачення її видів (табл. 1.1).

Таблиця 1.1 – Ключові концепти безпеки у теорії Г. Моргентау та відповідні її види

Основні положення теорії	*Відповідні види безпеки*
Безпека як результат боротьби за владу	
Моргентау стверджував, що міжнародні відносини детерміновані постійним суперництвом між державами за владу та вплив. Саме прагнення до розширення політичної сили обумовлює безпекову поведінку держав.	Міжнародна безпека
Реалізується через систему альянсів, блоків, колективних оборонних структур та міжнародних організацій. Її мета – досягнення балансу і стабільності в глобальному політичному просторі.	
Примат національних інтересів	
Національні інтереси – основа зовнішньої політики. Держава повинна захищати власні інтереси в межах міжнародної системи, що є прямим проявом забезпечення її безпеки.	Національна безпека
Стосується захисту суверенітету, територіальної цілісності та внутрішньої стабільності. Має пріоритетний статус серед усіх видів безпеки.	
Політичний реалізм проти морального ідеалізму	
Політика повинна враховувати реальні умови та природу людини, яка є недосконалою. Мораль не може домінувати над прагматизмом влади, оскільки часто суперечить інтересам держав.	Економічна безпека
Захист економічних інтересів держави: доступ до ресурсів, стабільність фінансової системи, економічне зростання як компонент загальної безпеки.	
Концепт балансу сил	
Для підтримання міжнародної безпеки необхідно забезпечити баланс між державами – жодна не повинна домінувати. Це запобігає агресії та створює умови для миру.	Системна безпека (глобальна рівновага)
Передбачає рівномірний розподіл впливу між державами, що гарантує багатополярність і зменшує ризики конфліктів.	

Джерело: складено автором за матеріалами [12]

Насамперед варто зауважити, що поняття «національна безпека» має багатовимірний та багатогранний характер, відображаючи не лише різні сфери суспільного життя, а й різні підходи до його осмислення залежно від фахової спеціалізації. Так, юристи, військові, економісти, політологи та представники інших галузей науки по-різному трактують сутність і зміст цієї категорії, виходячи з власної професійної оптики та методологічної бази. Навіть за умови загального світоглядного консенсусу, такі розбіжності залишаються суттєвими [2].

Національна безпека як явище – це комплексне багаторівневе утворення,

що включає ієрархію структур, інтересів та механізмів, які функціонують на різних рівнях – від повсякденного, побутового сприйняття до глибокого теоретичного аналізу. Вона поєднує у собі взаємопов'язані елементи політичної, економічної, правової, воєнної, інформаційної безпеки тощо. Таким чином, її аналіз потребує системного підходу, який дозволяє охопити опосередковані та прямі зв’язки між складниками цієї системи [3, с. 25].

У концентрованому вигляді концепція національної безпеки становить собою узагальнену систему офіційно прийнятих засад та позицій держави і суспільства щодо життєво важливих цінностей, стратегічних інтересів та механізмів їх захисту від внутрішніх і зовнішніх загроз. Ефективна політика у сфері безпеки можлива лише за умови чіткого розуміння та підтримки суспільством визначених державою інтересів, а також наявності ефективних шляхів, засобів і методів їх реалізації в межах системи публічного управління [4, с. 35].

Очевидним є той факт, що безпека – базова умова існування держави та ключовий чинник стабільності суспільства. Її неспроможність гарантувати цю фундаментальну цінність призводить до занепаду державних інституцій, втрати суверенітету та суспільного деструктиву. Як зазначають дослідники, економічна стабільність, правова організація, громадянська згуртованість є важливими компонентами життєдіяльності, однак лише гарантована захищеність від ключових загроз надає цим компонентам реальну цінність [1, с. 15].

Цікавим є історичний аспект еволюції терміна «національна безпека». На державному рівні це поняття вперше було використано у 1904 році в посланні президента США Теодора Рузвельта до Конгресу, в якому він аргументував необхідність анексії зони Панамського каналу на підставі національних інтересів. Відтоді поняття «національна безпека» стало важливим об’єктом міждисциплінарних досліджень – спочатку в рамках політичної науки, а згодом і в юридичній сфері [2].

У сучасному науковому дискурсі національну безпеку переважно визначають як стан захищеності життєво важливих інтересів особистості,

суспільства та держави від можливих загроз різного походження. При цьому під інтересами розуміють, насамперед, комплекс потреб, реалізація яких забезпечує сталий розвиток та функціонування суб'єкта безпеки – будь то окрема людина, соціальна група чи національна держава [5].

У сучасному науковому дискурсі все частіше наголошується на тому, що національну безпеку не слід трактувати винятково як стан захищеності від загроз. Такий підхід є обмеженим і не враховує глибину соціального, культурного та ідентифікаційного виміру цього явища. Наприклад, В. А. Ліпкан розглядає національну безпеку як особливий простір буття особистості, нації, держави, культури, традицій, звичаїв, природних і духовних ресурсів. Він наголошує, що безпека не лише об’єднує людей між собою, але й пов’язує їх із історичною спадщиною та довкіллям. Мова йде про збереження матеріальних і духовних основ національного розвитку, а також про органічне поєднання прагнення до захищеності з інституційною здатністю її гарантувати – як з боку державних, так і недержавних акторів [6, с. 10].

Подібний підхід пропонує й О. С. Власюк, який у праці «Національна безпека України: еволюція проблем внутрішньої політики» розглядає безпеку як спосіб самозбереження українського народу, що набув державної організації у формі суверенної держави. Такий спосіб забезпечує вільне існування, право на саморозвиток, а також ефективний захист від внутрішніх і зовнішніх викликів. Дослідник визначає національну безпеку як систему державно-правових і суспільних гарантій стабільності життєдіяльності, розвитку громадянського суспільства, захисту базових цінностей та законних інтересів українського народу [1, с. 25].

На думку Т. І. Блистіва, В. Т. Колесника, П. Я. Пригунова та К. В. Карпової, національна безпека не є статичним станом, а повинна розглядатися як динамічний процес, пов'язаний із розвитком і трансформацією держави. Відповідно, систему забезпечення безпеки слід осмислювати як механізм реалізації цього процесу – через адаптацію до змін, реагування на нові загрози та стратегічне прогнозування [7, с. 15].

У «Політичній енциклопедії» поняття національної безпеки трактується як здатність держави зберігати свою цілісність, суверенітет та життєві основи суспільного устрою – політичні, соціальні, економічні, культурні – а також виступати як самостійний суб'єкт міжнародних відносин [8, с. 489]. Це визначення наголошує на інституційній та функціональній складовій безпеки у глобальному вимірі.

Справді, концептуальні підходи до трактування національної безпеки значно різняться залежно від методології, фахової дисципліни та політичного контексту. Проте ключовою спільною рисою в більшості визначень є акцент на захисті життєво важливих інтересів особистості, суспільства і держави.

На рівні законодавства поняття «національна безпека України» вперше зафіксовано в Декларації про державний суверенітет України (1990 р.) [9]. Згідно із Законом України «Про національну безпеку України» від 21 червня 2018 р. № 2469-VIII, її визначено як стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів від реальних та потенційних загроз [10].

Водночас чинне законодавство окреслює велику кількість загроз у політичній, економічній, соціальній, екологічній, інформаційній та інших сферах. Проблемою залишається те, що нормативно-правова база не розмежовує реальні та потенційні загрози, хоча їх природа і рівень впливу можуть суттєво відрізнятись. Це ускладнює механізми реагування і управлінського впливу. Тому головним завданням суб'єктів забезпечення національної безпеки є постійний моніторинг внутрішніх і зовнішніх процесів, прогнозування ризиків, виявлення і оцінка дестабілізуючих чинників та конфліктів, аналіз причин їх виникнення й потенційних наслідків [11, с. 17].

Принципово важливою передумовою для глибокого осмислення сутності національної безпеки є чітке розмежування її суб’єктів та об’єктів. Відповідне визначення дозволяє не лише структурно окреслити сферу безпеки, а й ефективно реалізовувати її на практиці.

Ключовим суб’єктом національної безпеки виступає держава, яка згідно з

положеннями Конституції України (статті 3, 27–29) зобов'язана гарантувати безпеку кожного громадянина як у межах країни, так і за її кордонами. Захист життя, здоров'я, честі, гідності та особистої недоторканності громадян є не лише правовою нормою, а й основною функцією державності. Реалізація завдань у сфері безпеки здійснюється через систему органів державної влади – законодавчої, виконавчої та судової – у взаємодії з інститутами громадянського суспільства, недержавними організаціями та самими громадянами [12].

Об'єктами національної безпеки є, передусім, особа, суспільство і держава. Це означає, що до них належать:

– права, свободи та інтереси громадян;

– духовні, культурні та матеріальні цінності суспільства;

– конституційний устрій, суверенітет і територіальна цілісність держави.

Показники ефективності системи національної безпеки формуються на основі оцінки таких чинників, як рівень розвитку демократичного суспільства, стан правової системи, стабільність внутрішньополітичної ситуації, наявність національної стратегії розвитку, єдність та згуртованість громадян, здатність політичних сил до реалізації загальнодержавних цілей [13, с. 58–59].

Для належної реалізації захисних функцій щодо зазначених об'єктів створюється відповідна нормативно-правова база, що регламентує взаємовідносини у сфері національної безпеки. Вона охоплює:

– формування державної політики у сфері безпеки;

– визначення компетенцій органів публічного управління;

– участь приватних структур у безпековій діяльності;

– створення інституційних механізмів контролю та координації.

Система забезпечення національної безпеки є багатокомпонентною – вона включає державні органи, громадські інститути, бізнес-структури та індивідуальних виконавців, діяльність яких координується відповідно до стратегічних завдань і наявних викликів. В умовах зростаючих загроз та нестабільності її ефективне функціонування залежить від здатності реагувати на

ризики, прогнозувати наслідки та забезпечувати стійкість ключових сфер суспільного життя [14, с. 57].

Проблематика забезпечення національної безпеки України є складною й багатоаспектною, а її дослідження потребує міждисциплінарного підходу. Враховуючи масштабність цієї категорії, охопити всі її складники в рамках одного наукового дослідження надзвичайно складно. Саме тому в українському науковому середовищі сформувалася широка спільнота дослідників, які аналізують окремі напрями та підходи до гарантування безпеки – від воєнної та політичної до екологічної, інформаційної та соціальної.

Зокрема, дослідник Ю. Хатнюк присвятив свої праці аналізу актуальних загроз національній безпеці України. У своїх роботах він акцентує на політичних, економічних, воєнних, екологічних і інформаційних викликах, що впливають на стабільність держави. Науковець підкреслює, що для адекватного реагування на багаторівневі загрози необхідно реалізовувати *системний підхід*, який передбачає не лише захист інституцій, але й забезпечення національних інтересів та базових цінностей [14]. Такий підхід дозволяє інтегрувати функції різних суб'єктів безпеки в єдину координовану модель реагування.

Вагомим кроком у переосмисленні концепту безпеки стало оприлюднення у 2021 році аналітичного звіту групи українських науковців, присвяченого формуванню моделі безпеки людини. Це дослідження ґрунтується на міжнародних підходах до гуманітарного захисту, адаптованих до українських реалій, і включає такі компоненти, як:

– гарантування основних прав і свобод,
– забезпечення економічної стабільності,
– доступ до якісної освіти та медичних послуг,
– захист від дискримінації, насильства й соціального виключення.

Автори звіту зазначають, що «реконцептуалізація безпеки демонструє поступове зміщення фокусу – від традиційного захисту державної цілісності до людиноцентричного бачення, де в центрі уваги перебуває особистість і громада». Такий підхід не заперечує важливості державної безпеки, але розширює коло

зацікавлених сторін, що набувають суб'єктності у визначенні безпекових пріоритетів. Це особливо актуально в умовах сучасних глобальних викликів – пандемій, зміни клімату, соціальної нерівності та транснаціональних конфліктів, які вже давно виходять за межі традиційних державних кордонів [15].

Отже, сучасна наукова думка в Україні демонструє еволюцію безпекових концепцій – від жорстко-державоцентричних до відкритих, адаптивних, людинозорієнтованих моделей. У процес забезпечення безпеки дедалі більше залучаються не лише державні органи, а й місцеві громади, громадянське суспільство, бізнес, міжнародні організації та профільні асоціації. Такий підхід відкриває нові горизонти для реалізації стратегій національної та гуманітарної безпеки у взаємодії з глобальними процесами (табл. 1.2).

Таблиця 1.2 – Сучасні концептуальні підходи до розуміння безпеки: характеристика, представники, переваги та недоліки

Назва підходу	*Характеристика*	*Представники*	*Переваги*	*Недоліки*
Традиційний	Орієнтований на державоцентричну модель безпеки, фокусується на військовій силі та обороні держави від зовнішніх загроз	Реалісти: Ганс Моргентау, Кеннет Уолтц	Надає чіткі засоби для захисту територіальної цілісності та суверенітету	Ігнорує нетрадиційні загрози – екологічні, економічні, соціальні
Ліберальний	Робить акцент на міжнародній співпраці, ролі міжнародних інституцій у гарантуванні стабільності	Ліберали: Джон Ікенберрі, Роберт Кеохейн	Сприяє розвитку міжнародного порядку, колективної безпеки та міждержавного діалогу	Може бути слабким у протидії агресії з боку авторитарних режимів
Конструктивістський	Вивчає вплив ідей, ідентичностей, норм та соціального контексту на безпекову політику	Конструктивісти: Александр Вендт, Марта Фіннемор	Враховує культурні, соціальні, когнітивні чинники формування безпеки	Важко операціоналізувати та кількісно оцінити вплив зазначених чинників

Критичний	Спрямований на вивчення глибинних структур нерівності та владних відносин, що формують контексти загроз	Критичні теоретики: Кен Бут, Річард Він Джонс	Дає змогу аналізувати причини вразливості, маргіналізації та структурного насильства	Часто абстрактний, складний для практичної імплементації

Продовження таблиці 1.2

Назва підходу	*Характеристика*	*Представники*	*Переваги*	*Недоліки*
Екологічний	Розглядає екологічні виклики (зміна клімату, забруднення довкілля) як чинники глобальної небезпеки	Ульріх Бек, Роберт Фальк	Акцентує увагу на довгостроковій стійкості та екоцентричних ризиках	Недостатньо враховує військові та геополітичні чинники
Гуманітарний	Ставить у центр уваги захист прав людини, гідності та базових свобод	Мері Калдор, Емма Ротшильд	Розширює рамки безпеки до людиноцентричного рівня; актуальний у миротворчих процесах	Може ускладнювати реалізацію в авторитарних або кризових контекстах
Економічний	Пов’язує безпеку з економічними чинниками: доступом до ресурсів, стабільністю ринків, рівнем розвитку	Джозеф Най, Сьюзен Стрендж	Дає змогу враховувати матеріальні підвалини стабільності та захист економічних інтересів	Ризикує недооцінити нематеріальні чинники – культурні, соціальні, воєнні

Джерело: складено автором за матеріалами [9, 14, 15]

На нашу думку, представлена палітра сучасних підходів до розуміння безпеки відображає глибоку еволюцію цієї концепції та демонструє необхідність її адаптації до нових викликів, які постають у глобальному, національному та індивідуальному вимірах. Застосування цих теоретичних рамок дозволяє формувати інтегровані, гнучкі та контекстуально чутливі стратегії забезпечення безпеки, здатні відповісти на виклики сьогодення.

Сучасне уявлення про безпеку охоплює різноманітні теоретичні підходи, кожен із яких має власну концептуальну базу, переваги та обмеження. Їхнє

застосування можливе залежно від рівня загроз, характеру ситуації та специфіки суб'єкта безпеки.

На глобальному рівні зберігається актуальність традиційного підходу, який фокусує увагу на військовій силі, обороні та суверенітеті. Він є ключовим у протидії геополітичним загрозам та міжнародним конфліктам. Ліберальний підхід, у свою чергу, підкреслює роль міжнародних інституцій і міждержавної співпраці у формуванні умов миру та стабільності. Конструктивістський підхід вносить додаткову глибину, досліджуючи вплив ідей, норм та ідентичностей на міжнародні відносини.

На національному рівні критичний підхід дозволяє висвітлити соціальні та політичні нерівності, які можуть становити латентні загрози державній стабільності. Екологічний аспект безпеки набуває особливої ваги у контексті кліматичних змін, енергетичних криз та техногенних катастроф. Гуманітарний підхід концентрується на дотриманні прав людини, соціальній справедливості та недискримінації – ці складники є фундаментальними для сталого розвитку та суспільного добробуту.

На індивідуальному рівні все більшого значення набуває економічний вимір безпеки, який розглядає доступ до ресурсів, стабільність доходу, можливість самореалізації та захист у кризових умовах. Економічна безпека – це підґрунтя особистої стійкості та соціальної включеності.

Таким чином, сучасна концепція безпеки є багатовимірною, полірівневою та динамічною, що дозволяє враховувати широкий спектр ризиків, включаючи не лише зовнішні загрози, але й внутрішні фактори нестабільності.

1.2 Процеси біфуркації в системі міжнародних відносин та механізми управління національною безпекою в умовах нестабільності

Система національної безпеки (СНБ) належить до таких типів систем, які

постійно зазнають впливу багатьох зовнішніх та внутрішніх чинників. Її ключовою характеристикою є динамічність, що проявляється у здатності адаптуватися, реагувати на зміни середовища та перебудовувати власну структуру відповідно до актуальних викликів. Відтак недоцільно вважати ефективною таку систему, яка залишається статичною та не змінює параметрів функціонування внаслідок взаємодії з оточенням.

З позицій системного підходу, відкриті системи – до яких належить і система національної безпеки – не можуть мати наперед визначеної, детермінованої траєкторії розвитку. Їхня поведінка формується в умовах невизначеності, складності та альтернативності. Особливо це актуалізується у моменти, коли система стикається з критичними викликами, що спричиняють зміну її параметрів. Саме стан вибору напрямку розвитку, що виникає в результаті дії чинників різної природи, в системному аналізі отримав назву точки біфуркації.

У межах теорії криз це поняття відіграє визначальну роль, оскільки саме в точці біфуркації система опиняється перед альтернативами, які можуть призвести як до її оновлення, так і до руйнування. Такий стан неочевидності, нестабільності та вибору – є проявом ідентичності, самобутності та унікальності кожної системи, в тому числі системи національної безпеки.

Зважаючи на те, що СНБ покликана охоплювати широкий спектр сфер – від безпеки держави та суспільства до захисту громадян, економіки, інформаційного простору тощо – вона постійно перебуває під впливом флуктуацій, тобто непередбачуваних змін у політичному, соціальному, військовому або екологічному середовищі. Тому дослідження поведінки системи в точках біфуркації має надзвичайно високу практичну значущість, оскільки дає змогу оцінити наслідки трансформацій та визначити траєкторії адаптації.

Як зазначають О.О. Богданов і Ю.В. Яковець, криза – це не просто порушення стабільності, а перехідний стан системи, що відкриває простір для переоцінки та реконфігурації її основ. У цьому контексті теорія криз, яка описує логіку зародження, розвиток і наслідки критичних зламів, розглядається як

складова загальної теорії систем, засади якої були сформульовані Богдановим ще у 1921 році [6; 7].

Спираючись на положення цієї теорії, доцільно здійснити аналіз впливу загроз різного характеру на систему національної безпеки України, а також окреслити можливі сценарії її розвитку в умовах біфуркаційного вибору. Це, своєю чергою, створює підґрунтя для формування механізмів моніторингу, менеджменту ризиків, стратегічного планування та реагування на кризи.

Синергетична теорія національної безпеки на основі концепції біфуркацій дозволяє осмислити динамічну природу еволюції СНБ як відкритої нелінійної системи, яка постійно змінюється під дією багатофакторних викликів. Біфуркації виступають не лише точками вибору, а й механізмами адаптації, що формують нову конфігурацію системи через оновлення або трансформацію її елементів. Саме циклічність біфуркацій і виконувані ними функції є основою структурного оновлення та стабілізації безпекових систем.

Таблиця 1.3 – Фази циклу біфуркацій в еволюції СНБ

Фаза циклу	*Характеристика*
Стабільність (нижня)	Система досягає рівноважного стану, початкова стабільність перед кризою
Зниження захищеності	Втрата ефективності застарілих алгоритмів, часткова дестабілізація
Депресія	Баланс старих і нових алгоритмів, часткова протидія, втрата ефективності системи
Оживлення	Активація нових елементів, зростання ефективності, зниження ентропії
Стрімкий підйом	Кульмінація оновленої системи, стабілізація параметрів, підтвердження дієздатності
Стабільність (верхня)	Закріплення нової моделі, завершення циклу, зародження передумов нової кризи

Джерело: систематизовано автором

Цикл може бути деформованим під впливом зовнішніх флуктуацій, але має властивість відновлення після стабілізації системосередовища.

Таблиця 1.4 – Основні функції біфуркації як елементу синергетичної

динаміки СНБ

Функція біфуркації	*Зміст*
Усунення застарілих елементів	Елімінація недієвих алгоритмів системи, які втратили функціональність
Формування противаг	Забезпечення рівноваги між організаційним і самоорганізаційним контуром безпеки
Підготовка нового алгоритмічного середовища	Створення умов для запуску та функціонування оновлених елементів у системі
Акумуляція модифікованих елементів	Збереження потенційно адаптованих компонентів для переходу у нову структуру
Конструювання оновленої моделі СНБ	Відбір, трансформація та інтеграція елементів, що формують новий функціональний контур

Джерело: систематизовано автором

Функції біфуркації виступають каталізаторами системного оновлення, зростання ефективності, гнучкості та стійкості національної безпеки.

Цикл біфуркацій та функції, які він виконує у межах еволюції СНБ, становлять фундаментальний інструментарій аналізу кризових процесів та перехідних фаз безпекової системи. Біфуркація – це не тільки точка ризику, а й можливість: трансформація, переоцінка, інновація та відновлення системи. Відтак, синергетичний підхід забезпечує наукову основу формування адаптивної, прогнозованої та сталої системи національної безпеки, здатної реагувати на виклики різного характеру в умовах нестабільності.

Біфуркація, як критичний момент у розвитку системи, свідчить про її якісний перехід – від усталеної моделі функціонування до трансформації чи оновлення. У контексті синергетичного аналізу біфуркація є не лише точкою вибору, а ознакою еволюційної здатності системи, її відкритості до змін, здатності реагувати на нові виклики та адаптуватися до умов зовнішнього середовища.

Біфуркаційні процеси мають власну внутрішню динаміку, що проявляється у проходженні системою кількох послідовних стадій:

Латентна фаза – приховане визрівання передумов біфуркації. Система ще зберігає стабільність, але накопичені протиріччя вже сигналізують про необхідність змін. Цей етап відповідає завершенню старого циклу розвитку та зародженню нового.

Фаза обвалу – період інтенсивного загострення внутрішніх суперечностей, міжсистемної конкуренції та послаблення загального потенціалу безпеки. У цей момент активізуються нові елементи системи, які претендують на домінування у майбутній конфігурації.

Фаза пом’якшення – початок збалансування старих і нових підсистем. Система набуває тимчасової рівноваги, відкриваючи простір для оновлення та подальшої стабілізації. Формуються передумови для апогею розвитку нового циклу.

Тривалість кожного етапу є неоднаковою та залежить від рівня

адаптивності системи, масштабів флуктуацій і здатності до самоорганізації. Утім, загальна траєкторія розвитку є незворотною, оскільки еволюція системи безпеки, як і будь-якої складної відкритої системи, відбувається за принципом поступового переходу через критичні точки змін.

Біфуркації – явище універсальне, оскільки властиве будь-якій складній системі, що прагне розвитку. Без регулярного проходження через критичні точки, системи втрачають здатність адаптуватися, стають жертвами ригідності й деградації.

Прикладом може слугувати дестабілізація біполярної системи безпеки, що існувала протягом Холодної війни. Після її колапсу припущення щодо встановлення універсальної глобальної моделі безпеки не справдилися. Монополярний світовий устрій, де США претендували на роль єдиного гаранта глобальної стабільності, виявився нестійким. Події 11 вересня 2001 року стали ознакою кризи монополярної системи, хоча не тотального краху СНБ США, а радше краху ілюзії її універсальності.

Інші історичні приклади – колапс СНБ СРСР, СФРЮ, Філіппін – підтверджують, що кожна система безпеки має власну траєкторію еволюції, власну критичну точку і не може бути тотожною іншій. Джерела кризи, її динаміка та наслідки є ексклюзивними для кожної державної моделі.

Відтак, біфуркації слід розглядати одночасно як загальну закономірність розвитку систем і як індивідуальний феномен, що залежить від конкретних обставин, структурного контексту та стратегічних рішень.

Ураховуючи індивідуальну природу кожної біфуркації, її багатовимірність і контекстуальну обумовленість, постає необхідність у здійсненні класифікації біфуркацій. Такий підхід дозволяє не лише зрозуміти їхню природу, а й забезпечити ефективну реакцію системи у точці вибору. Біфуркації у межах системи національної безпеки можуть бути класифіковані за такими критеріями (табл. 1.5.).

Таблиця 1.5 – Класифікація біфуркацій у системах

Критерій класифікації	*Вид біфуркації*	*Характеристика / опис*
За об’єктом впливу	Суспільні	Формуються через масові настрої, реакцію громадян, соціальну динаміку
	Біологічні / природні	Виникають у живих чи неживих системах: пандемії, стихійні лиха, техногенні аварії
	Соціоприродні	На стику суспільства і довкілля: зміна клімату, екологічні катастрофи
За характером прояву	Структурні	Передують суттєвим змінам у системі або її демонтажу
	Ізольовані / резонансні	Виникають самостійно або викликають ланцюгову реакцію з іншими біфуркаціями
	Циклічні / випадкові	Як частина еволюційного циклу або результат стихійного впливу
За тривалістю	Короткострокові	Мають швидкий перебіг, завершуються у короткі терміни
	Середньострокові	Тривають проміжний період часу, супроводжуються частковими трансформаціями
	Довгострокові	Охоплюють декілька фаз розвитку, призводять до глибинної перебудови системи

Джерело: систематизовано автором

Біфуркації рідко існують ізольовано. Їх взаємодія здатна викликати інноваційні або дестабілізаційні процеси, які посилюють або послаблюють загальний потенціал системи національної безпеки. При одночасному виникненні біфуркацій у кількох підсистемах (економічній, військовій, інформаційній), можливе утворення синергетичного ефекту, що спричиняє системне оновлення або, навпаки, системну кризу [20].

Біфуркація, як процес, завжди має початок, розвиток і завершення. Завершення біфуркаційної фази – це не кінець системи, а перехід до постбіфуркаційного періоду, в якому можливе конструктивне оновлення за наявності усвідомленого механізму реагування.

– ідентифікація передумов кризи;
– оцінка характеру змін та флуктуацій;
– відбір застарілих елементів для деактивації;
– активізація елементів нової конфігурації;
– модернізація придатних структур системи;

– формування стійкої оновленої конфігурації СНБ.

Важливо: універсальних алгоритмів виходу з біфуркації не існує, оскільки кожна система має унікальну структуру, зовнішнє середовище та логіку реагування. Тому єдино вірним є побудова загального механізму, який включає чітко сформульовані цілі, функції, принципи та методи, що забезпечують системну селекцію та адаптацію.

Біфуркації – це не тільки криза, а можливість для оновлення і якісного розвитку системи національної безпеки. Їх класифікація дозволяє глибше зрозуміти природу зламів та знайти відповідні механізми реагування. Саме через управління біфуркаціями система здатна зберігати стійкість, адаптивність і стратегічну дієздатність у складному глобальному середовищі[18].

Система національної безпеки (СНБ) може розглядатися як постійний динамічний процес, у якому реалізується механізм виходу із біфуркаційних точок. Такий підхід дозволяє осмислити розвиток СНБ не як одноразову реакцію на загрозу, а як творчу систему трансформацій і рішень, здатну адаптуватись до змін та формувати нову траєкторію еволюції[26].

Як зазначалося раніше, кожна біфуркація має свій початок і завершення, після чого система переходить до нового рівня функціонування або ж трансформується в якісно нову конфігурацію. Характер постбіфуркаційного розвитку залежить від тієї фази циклу, на якій виникла біфуркація:

Якщо біфуркація припадає на фазу поширення – перехід відбувається стрімко, з інтенсивним приростом потенціалу, а кожен наступний піковий стан перевищує попередній.

Якщо вона виникає на етапі стабільності – розрив між піками поступово зменшується, стабілізація проходить плавніше.

Якщо точка біфуркації фіксується в нижній фазі стабільності – процес відновлення ускладнюється, біфуркація триває довше, а пік нового циклу може бути нижчим за попередній.

Це підтверджує існування двоякої природи біфуркацій – вони можуть бути як конструктивними, відкриваючи шлях до розвитку, так і деструктивними, що

призводять до стагнації або занепаду системи.

Кожна система має ядро ключових елементів – так звані системостворюючі компоненти, руйнування яких неминуче спричиняє її колапс. Проте кожна система має унікальний набір таких елементів, що визначає її спадковість та внутрішню ідентичність. Це означає, що при впливі на систему різного роду флуктуацій вона не завжди зазнає критичних втрат – адаптується, змінює окремі механізми або напрями функціонування, зберігаючи внутрішній каркас[25].

Ця здатність поєднувати динамічність зовнішніх проявів та стійкість ключових структур отримала назву фрактальності. Вона відображає просторову інваріантність системи – тобто її здатність зберігати стабільність у мінливому середовищі через повторювані, але унікальні сценарії біфуркацій. Таким чином, кожна біфуркація є персоніфікованим відображенням стану та взаємодії елементів конкретної системи, індикатором її життєдіяльності, стійкості та потенціалу розвитку.

РОЗДІЛ 2
ОСОБЛИВОСТІ ГІБРИДНОЇ ВІЙНИ ЯК ВИКЛИКУ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

2.1 Сутність та еволюція гібридної війни: від глобального феномена до українського контексту

Під кінець XX століття у протистоянні між державами з'явився новий формат, який часто іменують війною четвертого покоління, що по суті є гібридним конфліктом. Головна мета такого протистояння полягає в розпалюванні та підтримці внутрішніх конфліктів у країні-мішені. При цьому агресор демонстративно відхрещується від своєї участі, старанно приховуючи реальну динаміку подій та тих, хто стоїть за ними[22, с. 345].

Потужність гібридної війни проявляється в її спроможності впливати на всі сфери життя атакованої країни: від військової та дипломатичної до психологічної, фінансової, соціальної, ідеологічної та інформаційної. Типовий підхід передбачає застосування цих напрямів у різних комбінаціях, що дозволяє максимально виснажити опонента. Ключовою рисою є існування єдиного центру координації, який здійснює повний контроль над регулярними та нерегулярними силами (включно з пропагандистськими структурами, терористичними та кримінальними групами).

Завдяки конфлікту між Росією та Україною, за останні роки термін «гібридна війна» набув особливої актуальності як у наукових колах, так і в офіційних документах. За одним із визначень, гібридна загроза означає застосування противником різнопланових комбінацій військових і невійськових інструментів впливу на державу, що передбачає залучення як державних, так і недержавних суб'єктів [28].

Важливо відзначити, що концепцію «гібридної війни» вперше

сформулював генерал Джеймс Н. Меттіс у вересні 2005 року. Ця ідея була більш детально висвітлена ним у співавторстві з Ф. Гоффманом у статті «Майбутня війна: зліт гібридних воєн», опублікованій у листопаді того ж року[31].

Вся складність боротьби з проявами гібридної війни полягає в тісному поєднанні її ознак. Інформаційна війна має на меті працювати з інформацією, тоді як психологічна оперує емоціями, щоб максимально вплинути на світогляд особи чи групи, надаючи йому необхідного для ініціатора конфлікту змісту.

Таблиця 2.1 – Основні витоки гібридної війни

Витоки	*Сутність*
Політичні	Вплив на політичну систему, фінансування партій, підтримка сепаратистських рухів та «агентів впливу» для зміни правлячого режиму.
Ідейно-пропагандистські	Ведення ідеологічної війни проти тих, хто інакше сприймає політичні цінності та спрямованість суспільного розвитку, просування масштабних пан-ідей («русского мира», «китайського відродження»).
Науково-технологічні	Активне використання технічних засобів масового впливу (ЗМІ, інтернет) для нав'язування своєї позиції та політичних поглядів.
Мас-медійні	Маніпулювання свідомістю та насадження чіткої позиції, що відповідає політичному замовленню зовнішньої сили; перетворення журналістики на інструмент інформаційної боротьби.
Воєнні	Прямі збройні зіткнення.
Збройно-комерційні	Збільшення виробництва зброї та її розповсюдження для торгівлі з недержавними та терористичними угрупованнями.
Культурні	Поширення «мілітарної культури» та ідеї силового вирішення конфліктів, що формує відповідну поведінку індивідів.
Морально-віктимні	Маніпулювання історичними фактами та викривлення образів героїв через ЗМІ з метою знищення національної ідеології.
Конфесійні	Сприяння релігійним розколам для отримання додаткових важелів впливу на соціально-політичне середовище, як це спостерігається в Україні.
Спортивно-конфронтаційні	Використання спорту як інструменту політичного впливу та демонстрації переваг однієї країни над іншою.
Спеціальні	Діяльність розвідувальних служб, що використовують шпигунство, шантаж, дезінформацію та терористичні акти для досягнення поставлених цілей.

Джерело: сформовано автором

Аналіз перелічених витоків свідчить, що гібридна війна – це чіткий, заздалегідь спланований багатовекторний процес, який у кінцевому підсумку здатний призвести до зміни політичного керівництва, режиму чи курсу країни.

«Гібридний» характер конфлікту полягає в комбінації використання збройних сил з нетрадиційними методами, що створює «сіру зону» в рамках міжнародного права. Це ускладнює кваліфікацію дій, встановлення відповідальності та їх регулювання згідно з чинними законами та звичаями війни.

Концепція «гібридних воєн» була вперше сформульована у вересні 2005 року генералом Джеймсом Н. Меттісом, а згодом деталізована Ф. Гоффманом у його праці «Майбутня війна: зліт гібридних воєн». Гоффман припускав, що майбутні конфлікти не будуть обмежуватися одним видом опору, а навпаки, противники одночасно використовуватимуть усі доступні методи, створюючи таким чином мультимодальні або «гібридні» війни[32].

З організаційного погляду, гібридні конфлікти можуть поєднувати ієрархічні політичні структури з децентралізованими або мережевими тактичними одиницями. Щодо засобів, вони також є гібридними за своєю формою та застосуванням. Противники, як-от держави чи фінансово підтримувані угруповання, можуть володіти сучасним військовим потенціалом, поєднуючи його з тероризмом та кібервійнами.

У гібридних конфліктах, поряд із регулярними арміями, виникає широке коло нових учасників. Ці суб'єкти включають нерегулярні повстанські групи, злочинні формування, транснаціональні терористичні організації, приватні військові компанії, спеціальні підрозділи та військові контингенти міжнародних об'єднань. Така багатовекторність значно ускладнює процес ідентифікації сторін конфлікту, а також застосування до них відповідних норм міжнародного права.

Згідно з концепцією Ф. Гоффмана, гібридні війни є комплексною стратегією, яка об'єднує різноманітні режими ведення бойових дій. Ця синергія досягається шляхом інтеграції традиційних, нетрадиційних тактик, дій нерегулярних військових формувань, організації терористичних актів та злочинних заворушень. Така діяльність може здійснюватися різними підрозділами або навіть одним і тим же, але завжди під оперативним та тактичним керівництвом, що координується на головному театрі операцій для

досягнення максимального ефекту. Ця координація забезпечує синергію на будь-якому рівні ведення бойових дій[33].

Гоффман підкреслює, що для успішного ведення гібридної війни необхідні невеликі підрозділи з рішучими та винахідливими командирами, які готові діяти в умовах невизначеності. Вони повинні володіти відповідним озброєнням і екіпіруванням, що дозволяє випереджати противника. Основною проблемою в майбутньому, на думку Гоффмана, буде забезпечення захисту з урахуванням різноманітності методів і засобів нападу[34].

Сучасні інформаційні технології значно сприяють противнику, покращуючи підготовку бойовиків та обмін досвідом. Це дозволяє їм швидко засвоювати тактичні та технічні нововведення, що становить серйозну загрозу. З огляду на це, межі між «правильною» та «неправильною» війною стають дедалі більш розмитими.

Навіть недержавні актори отримують доступ до зброї, яка раніше була прерогативою держав. Водночас самі держави все частіше вдаються до нетрадиційних стратегій, використовуючи будь-які, навіть нелегітимні методи і прийоми. Це суперечить етичним застереженням Іммануїла Канта, який наголошував на неприпустимості використання вбивць, отруйників та підбурювання до зради, що може підірвати довіру в майбутньому. У гібридній війні, однак, подібні методи є частиною арсеналу.

Дослідження НАТО Multiple Futures (2004) підтвердило тенденцію до використання гібридних методів у міжнародній безпеці. Генерал-майор у відставці Франк ван Каппен зазначає, що гібридна війна – це поєднання класичних бойових дій з використанням нерегулярних збройних формувань. Ці недержавні виконавці можуть виконувати завдання, які держава не може здійснити сама, оскільки вона зобов'язана дотримуватися Женевської та Гаазької конвенцій. Таким чином, «брудна робота» перекладається на плечі недержавних формувань, що дозволяє державі-агресору уникати відповідальності[40].

Гібридна війна є сучасним феноменом у сфері безпеки, що характеризується поєднанням традиційних та нетрадиційних методів ведення

конфлікту. Цей термін підкреслює «гібридність» (змішаність) форм ведення бойових дій, де конвенційні військові операції тісно переплітаються з неконвенційними інструментами.

Згідно з формулюванням Філіпа Карбера, гібридна війна охоплює вісім ключових чинників, які поділяються на військові та невійськові. Військова складова включає[41]:

– використання традиційних конвенційних сил;
– застосування сил спеціальних операцій;
– залучення нетрадиційних неконвенційних сил;
– використання проксі-сил (сил-представників).
– Невійськова складова є не менш важливою і містить:
– політичні чинники;
– економічні чинники;
– дії в кіберпросторі;
– операції в медіа-просторі, які включають пропаганду та інформаційні війни.

Всі ці елементи тісно переплітаються та взаємодіють для досягнення стратегічних цілей агресора. Це поєднання створює так звану «сіру зону» в міжнародному праві, що ускладнює ідентифікацію, кваліфікацію та регулювання конфлікту згідно зі стандартними законами та звичаями війни. Такий підхід дозволяє державі-агресору маскувати свою участь у конфлікті та уникати міжнародної відповідальності.

Таблиця 2.2 – Класифікація методів гібридної війни

Традиційні методи війни	*Нетрадиційні методи війни*
Регулярні збройні сили	Партизанські методи
Чітка державна належність	Тероризм
Дипломатія	Підбурювання повстань
Економічні санкції	Участь криміналітету
Комплексна логістика	Кіберінформаційна війна
Розвинені технології	Низька інтенсивність
Домінування вогневої сили	Використання нерегулярних збройних формувань
Дотримання «правил війни»	Недотримання «правил війни»

Джерело: сформовано автором

Серед ключових ознак гібридної війни, окрім військових компонентів, слід виділити застосування економічних і дипломатичних інструментів, кібератаки та інформаційно-психологічні операції. Як зазначає політолог Євген Магда, до характерних рис гібридних загроз належать: використання інформаційної зброї, залучення недержавних акторів, застосування терористичних методів, ігнорування норм військового права та етики, а також активне використання економічного та психологічного тиску і пропаганди[37, с. 268].

Ведення гібридної війни надає державі-агресору значні переваги. Цей підхід дозволяє досягати політичних цілей з мінімальним залученням або навіть без використання конвенційних збройних сил. Такий тип конфлікту є відносно низьковитратним і часто дозволяє уникнути відповідальності перед міжнародною спільнотою за воєнні злочини та інші порушення міжнародного права.

Гібридна війна має комплексний набір компонентів, що дозволяють здійснювати одночасний вплив на противника в різних сферах. Серед визначальних складових гібридних війн виділяють інформаційну, ідеологічну, психологічну, економічну, політичну, дипломатичну, військову, технологічну, ресурсну та енергетичну.

Особливе місце займає економічний компонент, значення якого суттєво зросло в епоху глобалізації. Історія свідчить про різноманітність методів економічного протистояння, починаючи від фальсифікації грошових знаків, як це було під час наполеонівських війн, і закінчуючи сучасними фінансовими інструментами. Нинішні методи включають пряме блокування фінансових рахунків окремих осіб чи урядів, а також непрямі заборони, такі як блокування доступу до міжнародних платіжних систем, наприклад, SWIFT, що було застосовано проти іранських банків у 2018 році[36, с. 64].

Однією з ключових складових гібридної війни, особливо для України, є енергетичний аспект. Використання енергетичних ресурсів як інструменту політичного тиску є прямим відображенням впливу держави на світові події. З розвитком технологій та розширенням економічних зв’язків з’являються нові

форми ресурсного протиборства, такі як транспортна, енергетична та навіть водна блокада, що можуть призводити до екоциду на цілих територіях. Прикладами таких дій є спроба відведення вод річки Йордан у 1967 році, яка стала однією з причин Шестиденної війни, або кібердиверсії проти енергосистеми Венесуели у 2019 році.

Культурно-цивілізаційна складова також є важливою мішенню гібридних операцій. У цьому контексті акцент зміщується на форму, використовуючи маніпулятивні образи, тоді як зміст втрачає пріоритет. Сучасна масова культура часто характеризується спрощеним поданням інформації, що не вимагає значних інтелектуальних зусиль від аудиторії та базується на емоційному впливі.

Гібридні загрози також можуть включати використання міграційних потоків як інструменту впливу на інші держави. Прикладом може слугувати використання «транзитними країнами», такими як Туреччина, мігрантів, здебільшого молодих чоловіків із низьким рівнем освіти, для тиску на країни Європейського Союзу.

У контексті сучасних конфліктів важливим елементом є так звана «юридична війна». Вона включає подання позовів до міжнародних судів, формування доказової бази для подальших правових кроків та застосування санкцій. Юридичні аспекти конфліктів є критично важливими, оскільки вони формують міжнародну підтримку, впливають на громадську думку та політичний контекст.

Інформаційна війна є одним із ключових інструментів гібридного конфлікту. Американські фахівці визначають її елементи як: добування розвідувальної інформації, здійснення дезінформаційних кампаній, проведення психологічних операцій, фізичне руйнування інформаційних ресурсів, зараження комп’ютерними вірусами та проникнення в інформаційні мережі. У гібридних війнах цей аспект є визначальним, оскільки дозволяє агресору маніпулювати громадською думкою, дестабілізувати комунікаційні системи та спотворювати сприйняття подій[38, с. 236].

Не менш важливим є психологічний тиск, що є поширеним методом

впливу на свідомість населення. Його інструментарій включає шантаж, залякування, погрози репресіями та вбивствами, а також поширення відомостей про реальні чи вигадані загрози. Серед поширених технологій тиску слід виділити шахрайство, блеф, політичні ігри, провокації та поширення чуток. Провокація є особливо ефективним методом у сучасних конфліктах, оскільки дозволяє спонукати противника до дій, які є стратегічно невигідними для нього.

Мета інформаційної та психологічної війни є спільною: підрив морального духу противника, введення його в оману та досягнення перемоги з мінімальними людськими втратами і матеріальними витратами. Важливо, що цей вид протистояння значно менш ресурсозатратний порівняно з класичними військовими діями. Водночас, він вимагає значних інтелектуальних ресурсів, оскільки успішність залежить від ретельного планування, аналізу вразливих сторін противника та розробки комплексних заходів впливу для досягнення максимального синергетичного ефекту.[39, с. 134]

Більшість дослідників відзначають, що сучасні воєнно-політичні конфлікти, включно з гібридними війнами, характеризуються асиметричністю, локальністю та непередбачуваністю, виявляючись у різких переходах від деескалації до ескалації. Такі конфлікти є важкокерованими, оскільки одночасно відбувається їхня інтернаціоналізація, що залучає дедалі ширше коло держав та їхніх національних інтересів.

Особливою рисою сучасних конфліктів є те, що їхніми прямими учасниками все частіше виступають не лише держави, а й різноманітні недержавні актори: соціальні спільноти, економічні та кримінальні організації, діяльність яких набуває вираженого політичного характеру.

З огляду на ці аспекти, термінологічна сутність «гібридної війни» визначається як соціально-політичне явище, що має характерні ознаки сучасного воєнно-політичного конфлікту. Це політична суперечність, у ході якої вирішуються різнобічні протиріччя – економічні, територіальні, демографічні, етнічні, національні, релігійні, ідеологічні тощо. Їхнє вирішення досягається не тільки за допомогою військової сили, але, в першу чергу, із залученням

широкого спектру невійськових засобів впливу.

2.2 Вплив гібридної війни на трансформацію системи національної безпеки України

Протягом тривалого періоду Україна перебуває в умовах постійних гібридних загроз, що формує не лише її незалежність, але й визначає саме існування нації. З моменту відкритої агресії Російської Федерації у 2014 році та перетину державних кордонів, країна зіткнулася з комплексом викликів, що свідчать про системне застосування гібридних методів ведення війни. Ці гібридні загрози охоплюють широкий спектр дій – від збройної агресії, інформаційно-психологічних операцій та кібератак до економічного тиску і політичної дестабілізації. Багатовекторність і комплексний характер цих загроз значно ускладнюють розробку чіткої та ефективної стратегії протидії, що вимагає впровадження сучасних підходів до аналізу та нейтралізації загроз національній безпеці[41].

Незаконна анексія Автономної Республіки Крим Росією у 2014 році стала переломним моментом, продемонструвавши застосування гібридних методів у повному обсязі. Ця агресія, що відбулася в період ослаблення України, мала на меті задовольнити загарбницькі наміри, посіяти розбрат та посилити власний вплив. Гібридний характер конфлікту, що базувався на відсутності прямої збройної конфронтації, виявився у масованому тиску як на українське суспільство, так і на міжнародну спільноту. Після 2014 року світ став свідком ескалації на Донбасі, що включала[42]:

– Початок весни 2014: масові проросійські виступи на Сході України.

– Квітень 2014: проголошення самопроголошених «ДНР» і «ЛНР», спроби створення «Новоросії».

У цих подіях було застосовано широкий інструментарій гібридних

методів: координація ворожих агентів під виглядом «ополченців», інформаційні операції для дискредитації української влади, а також інтенсивні кібератаки.

Таблиця 2.3 – Порівняння інтенсивності та природи загроз 2014 року та після 2022 року

Характеристики	*2014 рік*	*2022-Сьогодення*
Характер агресії	Росія діяла через «маріонеткові утворення», уникаючи прямої участі.	Відкрита повномасштабна агресія, що супроводжується активним використанням гібридних елементів.
Основні методи	Провокації, пропаганда та «гібридна війна» у її класичному, замаскованому розумінні.	Продовження інформаційних операцій, кібератаки на критичну інфраструктуру, енергетичний тиск, спроби розколу суспільства.
Еволюція методів	Акцент робився на маскуванні конфлікту як «громадянського».	Хоча дії є відкритими, гібридні інструменти постійно використовуються для впливу на українське суспільство через теми мобілізації, втрат та економічних труднощів.
Нові форми загроз	Відносно обмежений інструментарій.	Залучення штучного інтелекту та бот-мереж, підрив гуманітарної безпеки, посилення пропаганди серед біженців.
Масштаб війни	Переважно замаскована, локальна війна.	Глобальний та багаторівневий конфлікт, що стосується не лише фронту, а й тилу, цивільного населення та міжнародної спільноти.

Джерело: систематизовано автором

З позицій синергетичного підходу, деталізованого у першому розділі, ці події є не просто «переломним моментом», а класичним проявом системної кризи. Попередні роки функціонування держави можна ідентифікувати як латентну фазу накопичення внутрішніх деструктивних протиріч та зростання зовнішніх загроз. Застосовані російською федерацією гібридні методи, зокрема інформаційні операції та приховані військові дії, виступили як потужна зовнішня флуктуація, що остаточно вивела українську систему національної безпеки зі стану відносної (хоча й деградуючої) рівноваги. Таким чином, 2014 рік став для України точкою біфуркації – критичним моментом, який унеможливив повернення до попередньої, пострадянської моделі безпеки і поставив державу перед екзистенційним вибором однієї з альтернативних траєкторій: або

дезінтеграція та втрата суверенітету, або докорінна трансформація інститутів та мобілізація для опору

Хронологічний аналіз подій свідчить, що агресивні дії проти України не обмежувалися суто військовими інструментами. Навпаки, з плином часу політичний компонент гібридних загроз набуває зростаючого значення. Це проявлялося у підтримці проросійських політичних рухів, спрямованих на дестабілізацію внутрішньої ситуації, спробах втручання у виборчі процеси, поширенні дезінформації, що підривала легітимність української влади, а також у маніпуляціях навколо питань національної ідентичності та історичних цінностей.

Отже, аналіз гібридних загроз вимагає не лише військово-стратегічної оцінки, а й глибокого розуміння політичних, економічних і соціальних механізмів, що застосовуються для досягнення стратегічних цілей агресора.

У цьому контексті важливого значення набуває дослідження як прямих, так і непрямих гібридних атак, сутність яких полягає у нав'язуванні суспільству чужих наративів. Ці наративи, що створювалися шляхом маніпуляцій щодо «спільної історичної долі» та «братерських народів», насправді мали на меті нівелювати національну ідентичність та суверенітет української державності. Крім того, ключовою складовою політичної гібридної агресії стала експлуатація економічної та соціальної залежності, яка маскувалася під гаслами «дружби народів» і «взаємовигідної співпраці».

Інституційна система забезпечення національної безпеки України формувалася протягом останніх десятиліть під впливом як внутрішніх політичних трансформацій, так і зовнішніх загроз. Після 2014 року, з початком російської агресії, система набула нового змісту – вона стала орієнтованою на реагування на гібридні виклики, що включають інформаційні та кібератаки, терористичну діяльність, політичну дестабілізацію, економічний тиск, енергетичні загрози тощо. Основу цієї системи становлять державні органи, які реалізують політику безпеки на стратегічному, оперативному та тактичному рівнях[43].

Таблиця 2.4 – державні органи, які реалізують політику безпеки на стратегічному, оперативному та тактичному рівнях

Орган	*Роль у протидії гібридним загрозам*
Рада національної безпеки і оборони України (РНБО)	Ключовий координаційний орган. Визначає пріоритети політики безпеки, координує діяльність органів влади, розробляє стратегії та доктрини. Ініціювала ухвалення Доктрини інформаційної безпеки (2017) та Стратегії кібербезпеки (2021).
Служба безпеки України (СБУ)	Виконує функції контррозвідки, боротьби з тероризмом. Роль у кібербезпеці та виявленні ІПСО (інформаційно-психологічних операцій) значно зросла. Нейтралізує шпигунські мережі, викриває диверсії та бореться з внутрішніми колаборантами.
Міністерство оборони України та Генеральний штаб ЗСУ	Забезпечують воєнну безпеку. Відповідають за стратегічне планування, розвиток сил оборони та міжнародне співробітництво. Адаптуються до характеру війни, впроваджуючи цифрові платформи та безпілотні технології.
Міністерство внутрішніх справ України	Координує діяльність Національної поліції, Державної прикордонної служби, Нацгвардії та ДСНС. Відіграє критичну роль у громадській безпеці, боротьбі з ДРГ (диверсійно-розвідувальними групами) та цивільному захисті.
Міністерство цифрової трансформації України	Новий гравець в архітектурі безпеки. Відповідає за розвиток цифрової інфраструктури, кіберпростору та електронного урядування. У 2022-2023 роках брало участь у створенні кіберзахисної інфраструктури та ІТ-військ.
Громадянське суспільство	Волонтерські організації, медіа та експерти. Забезпечують додаткову стійкість системи, протидіють дезінформації, сприяють обміну даними та допомагають у підготовці стратегій безпеки.

Джерело: систематизовано автором

Інституційна система національної безпеки України нині є багаторівневою, гнучкою та інтегрованою, проте не позбавленою викликів. Серед основних проблем – обмежене фінансування, дублювання повноважень, фрагментованість міжвідомчої взаємодії та потреба у гармонізації із західними стандартами. Разом з тим, процес її еволюції триває, а війна стала каталізатором глибоких змін, які, за належного управління, можуть суттєво зміцнити державну безпеку[45].

Сучасна система національної безпеки України функціонує в умовах тривалої гібридної агресії з боку Російської Федерації, що охоплює не лише військову, але й інформаційну, політичну, економічну, енергетичну, кібернетичну та психологічну сфери. У зв’язку з цим постає необхідність системного перегляду підходів до гарантування безпеки держави та

впровадження комплексних реформ, здатних забезпечити стійкість і гнучкість у протидії гібридним викликам. На основі аналізу сучасного стану системи національної безпеки України пропонуються наступні рекомендації[46, с. 274]:

Формування цілісної державної стратегії протидії гібридним загрозам.

Україна потребує єдиного стратегічного документу, що визначатиме комплексний підхід до протидії гібридній агресії. Така стратегія має враховувати міжвідомчу координацію, роль громадянського суспільства, інформаційні, кібернетичні та економічні виміри загроз. Необхідно: розробити Оновлену концепцію національної безпеки України, в якій гібридна війна буде визначена як окрема форма загрози; передбачити механізми превентивного реагування, а не лише реактивних дій; встановити чіткі протоколи взаємодії між секторами оборони, внутрішніх справ, СБУ, РНБО, Міні Цифри та іншими.

Посилення кібербезпеки та цифрової стійкості.

З огляду на постійні кібератаки на українські державні органи, критичну інфраструктуру та об’єкти енергетики, варто: розширити повноваження Державної служби спеціального зв’язку та захисту інформації, створивши постійно діючу мережу моніторингу загроз; запровадити обов’язкову кібербезпекову сертифікацію для всіх державних установ та стратегічних підприємств; підтримувати розвиток власного програмного забезпечення та зменшувати залежність від іноземних технологій; розвивати систему реагування на інциденти (CSIRT) з оперативною аналітикою.

Зміцнення інформаційної безпеки та стратегічної комунікації.

Інформаційний фронт є одним із найважливіших у гібридній війні. Тому Україні слід: створити Єдиний центр стратегічних комунікацій, що забезпечуватиме швидке реагування на дезінформаційні кампанії; проводити медіаграмотні кампанії серед населення, особливо в регіонах, де існує вразливість до ворожого впливу; посилити державну підтримку незалежних ЗМІ, які дотримуються журналістських стандартів; запровадити моніторинг ворожого контенту в соцмережах за участю фахівців з OSINT та залученням міжнародних партнерів.

Переосмислення системи військово-цивільної взаємодії та територіальної оборони.

Повномасштабна війна показала необхідність глибокої інтеграції цивільних ресурсів у систему оборони. Для цього слід: переформатувати підготовку резервістів за моделлю країн Балтії (зокрема, створення добровольчих загонів при громадах); розробити локальні плани безпеки для кожної територіальної громади; створити структури кризового управління на місцях із чітко розписаними обов'язками під час надзвичайних ситуацій; залучати громадян до постійних навчань і тренувань, особливо у прикордонних областях.

Реформа системи національної безпеки у сфері освіти і науки.

Наукова спільнота, освітні заклади та експертні центри мають стати основою аналітичної, концептуальної та прогностичної підтримки безпеки. Рекомендується: створити державну програму дослідження гібридних загроз за участю університетів, think-tank ів, аналітичних центрів; підтримувати наукові розробки у сфері соціальної психології, інформаційних технологій, комунікацій; включити дисципліни з національної безпеки, кібер гігієни та критичного мислення в програми старших класів та університетів.

Міжнародне співробітництво і євроатлантична інтеграція.

Україна повинна поглиблювати співпрацю з партнерами у сфері безпеки, зокрема: активніше брати участь у спільних навчаннях НАТО та ЄС, з акцентом на протидію гібридним загрозам; використовувати технічну допомогу з кібербезпеки від партнерів для модернізації інфраструктури; створити спільні центри обміну інформацією про загрози з країнами Балтії, Польщею, Фінляндією; ініціювати навчальні програми для фахівців сектору безпеки за підтримки країн НАТО.

Енергетична та економічна безпека як фундамент стійкості.

Гібридна війна часто проявляється у формі енергетичного шантажу, диверсій чи фінансових атак. Тому Україна має: збільшити енергонезалежність через розвиток альтернативної енергетики; запровадити механізми захисту

критичної інфраструктури (електростанцій, логістичних вузлів, підприємств оборонпрому); посилити фінансову розвідку для боротьби з відмиванням грошей, що фінансують деструктивні мережі; стимулювати внутрішнє виробництво стратегічно важливої продукції: медичної, оборонної, ІТ-сфери.

Гуманітарна політика та внутрішня згуртованість.

Суспільна стійкість – це не лише технології, а й відчуття справедливості, рівності, довіри до держави. Тому потрібно: забезпечити ефективну політику реінтеграції окупованих територій, включно з інформаційною, культурою та освітньою підтримкою; підвищити рівень державної підтримки ветеранів, військовослужбовців та їхніх родин; забезпечити рівний доступ до публічних послуг у всіх регіонах, особливо в прикордонних та постраждалих зонах; підтримувати національну ідентичність через культуру, мову, мистецтво.

Реальність гібридних загроз вимагає від України не лише оновлення законодавчої бази, але й створення принципово нової моделі безпеки – адаптивної, інтегрованої, превентивної. Національна безпека повинна стати справою не лише силових структур, а всього суспільства. Виконання запропонованих рекомендацій дозволить Україні сформувати ефективну, стійку та сучасну систему безпеки, здатну протистояти як традиційним, так і новітнім формам агресії.

РОЗДІЛ 3
ШЛЯХИ ВДОСКОНАЛЕННЯ МЕХАНІЗМІВ УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ УКРАЇНИ

3.1 Стратегічне планування та інституційна спроможність суб'єктів забезпечення національної безпеки

У сучасних умовах безпеки гібридні загрози набули статусу ключового чинника, що істотно змінює концепцію національної безпеки. Збройна агресія Російської Федерації проти України, яка розпочалася у 2014 році, продемонструвала неефективність традиційних засобів захисту перед новими викликами, що поєднують відкриті бойові дії з прихованими, асиметричними методами впливу – зокрема інформаційними, кібернетичними, економічними, політичними та психологічними операціями (джерело). В таких умовах стратегічне управління та формування безпекової політики потребують нових характеристик: адаптивності, здатності до прогнозування, оперативного реагування та багаторівневої взаємодії [49].

Створення дієвих стратегій національної безпеки в умовах гібридної війни вимагає комплексного аналізу як зовнішніх, так і внутрішніх загроз, а також глибокого осмислення сутності сучасних конфліктів (джерело). Україна, яка перебуває на передовій боротьби з гібридною агресією, змушена постійно пристосовуватися до нових форм загроз, вдосконалювати інституційні механізми та залучати всі доступні ресурси – від дипломатичних інструментів і розвідувальних структур до громадянської активності та цифрових технологій безпеки [36].

Інституційна система національної безпеки України формувалася протягом останніх десятиліть під впливом внутрішніх політичних змін і зовнішніх викликів. Після початку російської агресії у 2014 році вона зазнала

суттєвих змін, зосередившись на протидії гібридним загрозам, серед яких – інформаційні та кібернетичні атаки, терористичні акти, політична дестабілізація, економічний тиск і загрози в енергетичній сфері. Основу цієї системи становлять державні інституції, що реалізують політику безпеки на стратегічному, оперативному та тактичному рівнях.

Для глибшого розуміння структури системи національної безпеки доцільно застосовувати класифікацію суб'єктів за різними критеріями: юридичною (адміністративно-правовою) природою, функціональним призначенням (горизонтальний підхід), зв'язком з державою (державні та недержавні суб'єкти), характером взаємодії з державними структурами (прямі та непрямі зв'язки). Найбільш інформативною вважається класифікація за юридичною природою та рівнем повноважень, тобто вертикальна класифікація, яка дозволяє чітко визначити правовий статус і специфіку взаємодії суб'єктів у сфері безпеки.

Інституційна система національної безпеки України формувалася протягом останніх десятиліть під впливом внутрішніх політичних змін і зовнішніх викликів. Після початку російської агресії у 2014 році вона зазнала суттєвих змін, зосередившись на протидії гібридним загрозам, серед яких – інформаційні та кібернетичні атаки, терористичні акти, політична дестабілізація, економічний тиск і загрози в енергетичній сфері. Основу цієї системи становлять державні інституції, що реалізують політику безпеки на стратегічному, оперативному та тактичному рівнях.

Для глибшого розуміння структури системи національної безпеки доцільно застосовувати класифікацію суб'єктів за різними критеріями: юридичною (адміністративно-правовою) природою, функціональним призначенням (горизонтальний підхід), зв'язком з державою (державні та недержавні суб'єкти), характером взаємодії з державними структурами (прямі та непрямі зв'язки). Найбільш інформативною вважається класифікація за юридичною природою та рівнем повноважень, тобто вертикальна класифікація, яка дозволяє чітко визначити правовий статус і специфіку взаємодії суб'єктів у

сфері безпеки.

У межах цієї класифікації виділяють три основні групи суб'єктів:

1. Державні органи, які здійснюють заходи щодо забезпечення національної безпеки. Держава виступає ключовим елементом механізму безпеки, оскільки саме вона формулює завдання перед суспільством, захищає його інтереси та створює відповідні механізми для їх реалізації [5, с. 88].

Державні органи – це організовані колективи та посадові особи, які діють на основі права, приймають і реалізують загальнообов'язкові рішення [9, с. 33]. Вони виконують функції з виявлення, запобігання та нейтралізації загроз, мають державно-владні повноваження, що дозволяє їм ухвалювати рішення у сфері безпеки відповідно до норм адміністративного права.

2. Органи місцевого самоврядування, які, хоча й мають автономію, є важливими суб'єктами публічного адміністрування. Вони реалізують управлінські функції на місцевому рівні, приймають рішення з питань місцевого значення, що можуть впливати на загальний рівень національної безпеки. Їхній внесок полягає у впровадженні місцевих програм безпеки, співпраці з державними органами та участі в профілактиці правопорушень [5, с. 88].

3. Суб'єкти громадянського суспільства, які сприяють усуненню причин асоціальної поведінки, підтримують права і свободи людини, демократію, соціальну справедливість і солідарність. Як зазначає С.І. Спільник, громадянське суспільство передбачає самоврядність, верховенство права, вільний ринок, доступ до культурних надбань і умови для реалізації творчого потенціалу кожної особи. Його участь у забезпеченні безпеки проявляється через громадський контроль, реалізацію соціальних ініціатив та просування цінностей сталого розвитку[33].

Відповідно до положень Закону України «Про основи національної безпеки України» від 19 червня 2003 року №964-IV (який наразі втратив чинність), у статті 4 було визначено перелік суб'єктів, що здійснюють функції у сфері забезпечення національної безпеки. До них належали:

– Президент України;

– Кабінет Міністрів України;
– Верховна Рада України;
– Рада національної безпеки і оборони України;
– Міністерства та інші центральні органи виконавчої влади;
– Національний банк України;
– Суди загальної юрисдикції;
– Прокуратура України;
– Національне антикорупційне бюро України;
– Місцеві державні адміністрації та органи місцевого самоврядування;
– Збройні сили України;
– Державна прикордонна служба України;
– Служба зовнішньої розвідки України;
– Служба безпеки України;
– Інші військові формування, створені відповідно до чинного законодавства;
– Органи та підрозділи цивільного захисту;
– Громадяни України та об'єднання громадян (Право і безпека. 2020. №2 (77), с. 34).

Такий широкий перелік суб'єктів свідчить про комплексний характер системи національної безпеки, яка охоплює як державні інституції, так і громадські структури, що можуть брати участь у реалізації безпекової політики. Це також підтверджує важливість міжсекторальної взаємодії в умовах сучасних викликів.

Згідно з чинним Законом України «Про національну безпеку України» від 21 червня 2018 року №2469-VIII, сектор безпеки і оборони визначається як комплексна система, що включає органи державної влади, Збройні Сили України, інші військові формування, створені відповідно до законодавства, розвідувальні та правоохоронні структури, спеціалізовані державні органи з правоохоронними функціями, оборонно-промисловий комплекс, сили цивільного захисту, а також громадські об'єднання і громадян, які добровільно

долучаються до процесу забезпечення національної безпеки. Уся діяльність цих суб'єктів підлягає демократичному цивільному контролю та спрямована на захист національних інтересів держави (Закон України №2469-VIII).

Відповідно до положень статті 12 цього Закону, сектор безпеки і оборони України структурно складається з чотирьох взаємопов'язаних компонентів:

– Сили безпеки – до них належать розвідувальні та правоохоронні органи, державні органи спеціального призначення з правоохоронними функціями, а також сили цивільного захисту (ст. 1);

– Сили оборони – включають Збройні Сили України, інші військові формування, розвідувальні та правоохоронні органи, а також органи спеціального призначення, що виконують оборонні функції (ст. 1);

– Оборонно-промисловий комплекс – як інституційна складова, що забезпечує технічну та матеріальну підтримку сектору оборони;

– Громадські об'єднання та громадяни, які добровільно беруть участь у заходах із забезпечення національної безпеки (Закон України №2469-VIII).

У частині 2 статті 12 Закону України «Про національну безпеку України» також визначено перелік ключових інституцій, що входять до складу сектору безпеки і оборони. Серед них:

– Міністерство оборони України;
– Збройні Сили України;
– Державна спеціальна служба транспорту;
– Міністерство внутрішніх справ України;
– Національна гвардія України;
– Національна поліція України;
– Державна прикордонна служба України;
– Державна міграційна служба України;
– Державна служба України з надзвичайних ситуацій;
– Служба безпеки України;
– Управління державної охорони України;
– Державна служба спеціального зв'язку та захисту інформації

України;

– Апарат Ради національної безпеки і оборони України;

– Розвідувальні органи України;

– Центральний орган виконавчої влади, відповідальний за формування та реалізацію державної військово-промислової політики (Закон України №2469-VIII) (табл. 3.1).

Таблиця 3.1 – Порівняльна таблиця суб'єктів національної безпеки України

Категорія	*Закон України «Про основи національної безпеки України» (2003, №964-IV)*	*Закон України «Про національну безпеку України» (2018, №2469-VIII)*
Вищі органи влади	Президент України, Верховна Рада України, Кабінет Міністрів України	Згадуються окремо у ст. 13 як керівництво, але не включені до сектору безпеки і оборони
Координаційні органи	Рада національної безпеки і оборони України	Апарат РНБО включено до сектору безпеки і оборони
Центральні органи виконавчої влади	Міністерства та інші ЦОВВ	Міністерство оборони, МВС, центральний орган з військово-промислової політики
Судова система	Суди загальної юрисдикції	Не згадуються
Правоохоронні органи	Прокуратура України, СБУ, НАБУ	СБУ, Національна поліція, Державна міграційна служба, Управління держохорони
Військові формування	Збройні Сили України, інші військові формування	ЗСУ, Національна гвардія, Держспецслужба транспорту
Прикордонна та розвідка	Державна прикордонна служба, Служба зовнішньої розвідки	ДПСУ, розвідувальні органи України
Цивільний захист	Органи і підрозділи цивільного захисту	ДСНС, сили цивільного захисту
Фінансові інституції	Національний банк України	Не згадується
Антикорупційні органи	НАБУ	Не згадується окремо
Місцеве самоврядування	Місцеві державні адміністрації та органи місцевого самоврядування	Не включені до переліку сектору безпеки і оборони
Громадянське суспільство	Громадяни України, об'єднання громадян	Громадські об'єднання та громадяни (включені в ч.1 ст.12, але не в ч.2)
Оборонно-промисловий комплекс	Не згадувався	Включено як окрема складова сектору безпеки і оборони

Джерело: [35]

Рада національної безпеки і оборони України (РНБО) виступає центральним координаційним органом у сфері національної безпеки та оборони. Її функціональне призначення полягає у визначенні пріоритетних напрямів державної політики, узгодженні дій виконавчих органів влади в умовах надзвичайного або воєнного стану, а також у розробці стратегічних документів – доктрин, концепцій та оборонних планів. В умовах збройного конфлікту роль РНБО значно посилилася: її рішення стали основою для президентських указів щодо мобілізації, запровадження санкцій, забезпечення інформаційної безпеки та кіберзахисту. Зокрема, саме РНБО ініціювала прийняття Доктрини інформаційної безпеки України (2017) та Стратегії кібербезпеки (2021), які стали відповіддю на новітні загрози (Закон України №2469-VIII).

Служба безпеки України (СБУ) виконує завдання у сфері контррозвідувальної діяльності, протидії тероризму та охорони державної таємниці. У контексті сучасних викликів її роль у забезпеченні кібербезпеки та виявленні інформаційно-психологічних операцій значно зросла. СБУ реалізує оперативно-розшукові заходи, спрямовані на нейтралізацію шпигунських структур, викриття диверсійної діяльності та боротьбу з внутрішніми колаборантами. Після початку повномасштабної агресії 24 лютого 2022 року повноваження СБУ були розширені, що стало предметом дискусій щодо необхідності посилення демократичного контролю над її діяльністю (Закон України №2469-VIII).

Міністерство внутрішніх справ України (МВС) виконує функцію координаційного центру для таких ключових структур, як Національна поліція, Державна прикордонна служба, Національна гвардія та Державна служба України з надзвичайних ситуацій. Ці органи забезпечують громадську безпеку, здійснюють боротьбу з диверсійно-розвідувальними групами, контролюють державний кордон і реалізують заходи цивільного захисту. Особливо важливою є діяльність Національної гвардії, яка бере участь у стабілізації ситуації на тимчасово окупованих територіях, підтримуючи правопорядок після гібридних

атак (Закон України №2469-VIII).

Міністерство цифрової трансформації України стало новим інституційним елементом у системі національної безпеки. Його компетенція охоплює розвиток цифрової інфраструктури, формування безпечного кіберпростору, впровадження електронного урядування та реалізацію політики відкритих даних. У 2022–2023 роках Мінцифра спільно з Держспецзв'язку активно працювала над створенням кіберзахисної інфраструктури, формуванням ІТ-військ та цифровою мобілізацією населення. Український досвід у створенні «армії дронів» та залученні ІТ-волонтерів (зокрема, ініціативи Anonymous Ukraine та ІТ-армія) набув міжнародного визнання як унікальний приклад цифрового спротиву (Закон України №2469-VIII).

Громадянське суспільство відіграє важливу роль у підвищенні стійкості національної безпеки. Волонтерські організації, незалежні медіа та експертні спільноти активно співпрацюють з державними інституціями, сприяючи протидії дезінформації, забезпечуючи оперативний обмін інформацією та беручи участь у розробці стратегічних документів. Зокрема, такі організації, як Центр протидії дезінформації та VoxUkraine, здійснюють моніторинг інформаційного простору, виявляють фейки та нейтралізують пропагандистські наративи (Закон України №2469-VIII).

Сучасна інституційна система національної безпеки України характеризується багаторівневою структурою, високою адаптивністю та інтеграційною здатністю. Водночас вона стикається з низкою системних викликів, серед яких – недостатній рівень фінансування, дублювання функцій між окремими органами, фрагментарність міжвідомчої координації та потреба у приведенні національних механізмів у відповідність до стандартів країн-членів НАТО та ЄС.

Попри ці труднощі, трансформація системи безпеки триває. Повномасштабна війна стала потужним стимулом для її оновлення, спричинивши глибокі структурні та функціональні зміни. За умови ефективного управління ці процеси мають потенціал значно посилити здатність держави до

захисту національних інтересів та забезпечення стабільності.

Комплексний підхід до протидії гібридним загрозам передбачає консолідацію зусиль усіх ключових секторів державного управління – політичного, оборонного, інформаційного, економічного, дипломатичного та кібернетичного – з метою формування узгодженої та ефективної системи реагування. У контексті національної безпеки України це означає активізацію міжвідомчої співпраці між такими структурами, як Служба безпеки України, Рада національної безпеки і оборони, Міністерство оборони, Міністерство внутрішніх справ, Державна служба спеціального зв'язку та захисту інформації, а також Міністерство цифрової трансформації.

Важливу роль у реалізації цього підходу відіграють інститути громадянського суспільства та міжнародні партнери, які сприяють не лише оперативному реагуванню на загрози, а й їхньому попередженню. Це досягається шляхом розвитку аналітичних механізмів, систем раннього виявлення, інформаційної гігієни, законодавчих ініціатив та посилення захищеності критичної інфраструктури.

Сучасна доктрина національної безпеки України визнає, що її забезпечення є спільною відповідальністю державних органів, місцевого самоврядування та громадянського суспільства. Такий підхід відображає принцип багатосекторної взаємодії, що дозволяє ефективно реагувати на сучасні виклики у сфері безпеки.

Серед різних класифікацій суб'єктів національної безпеки найбільш обґрунтованою з теоретичного та практичного погляду є класифікація за юридичною (адміністративно-правовою) природою та рівнем повноважень. Цей підхід дозволяє охопити широке коло учасників безпекового процесу та чітко визначити їхню роль у системі.

Окремо слід розглянути вплив суб'єктів міжнародного права, зокрема міжнародних організацій, на забезпечення національної безпеки. Хоча вони не є частиною національної правової системи, їхня роль реалізується через механізми міжнародного співробітництва та виконання Україною міжнародних

зобов’язань. У цьому контексті національні органи публічної служби взаємодіють з представниками міжнародних структур, що дозволяє інтегрувати зовнішні ресурси та досвід у національну систему безпеки.

3.2 Механізми координації, взаємодії та прогнозування загроз в умовах гібридної війни

У сучасному світі, що перебуває в стані глобальних викликів і загроз, спостерігається новий виток геополітичного суперництва між провідними державами за контроль над ресурсами, комунікаційними каналами, ринками збуту та сферами впливу. У цьому контексті можна стверджувати, що Україна у період 2013–2014 років виявилася неготовою до викликів гібридної війни. Можливості, отримані після розпаду Радянського Союзу у 1991 році, поступово втрачалися через відсутність політичної волі для остаточного розриву з радянською спадщиною, особливо у сфері державного управління.

Така інституційна нерішучість спричинила формування умов, які можна охарактеризувати як «пострадянський вакуум». У результаті, за участі агентів впливу, в науковому середовищі та блогосфері почали поширюватися маніпулятивні трактування концепції «failed state». Ці інтерпретації, використовуючи технології інформаційного впливу, намагалися довести неспроможність України реалізувати власний суверенітет, формуючи теоретичне підґрунтя для заперечення здатності української політичної нації до існування як незалежної, суверенної та соборної держави [52].

У цьому дискурсі анексії, сепаратистські рухи та «паради суверенітетів» подаються як нібито логічна реакція на неспроможність української державної влади ефективно управляти країною та задовольняти національні інтереси, що, натомість, підмінюються приватними інтересами представників олігархічних кіл [52].

Події 2014 року стали переломним моментом, коли проти України було застосовано інструменти гібридної війни з боку Російської Федерації. Цей конфлікт триває й досі, набуваючи нових форм і масштабів.

Гібридна агресія та проксі-конфлікти становлять серйозну загрозу для національної безпеки, оскільки вимагають комплексних і ефективних механізмів протидії. Україна, яка географічно розташована на перетині стратегічних інтересів, зазнала численних проявів гібридного впливу протягом останніх років. Аналізуючи дії Росії з 2014 року, можна дійти висновку, що ця агресія має гібридний характер, поєднуючи різноманітні методи – від військових і інформаційних до політичних і соціальних. Особливістю є залучення цивільного населення, місцевих активістів та політичних структур, які перетворюються на учасників конфлікту, часто – вимушено [51].

Перш ніж перейти до аналізу конкретних викликів, що постають перед Україною, необхідно окреслити базові поняття та їхню структуру. Закон України «Про національну безпеку України» визначає національну безпеку як стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів від реальних і потенційних загроз. Це свідчить про те, що національна безпека є багатовимірним і складним поняттям, реалізація якого потребує узгодженої роботи всіх внутрішніх і зовнішніх державних інституцій [53].

Одним із ключових елементів російсько-української гібридної війни є не лише застосування Російською Федерацією військових засобів з метою підриву української державності, а й цілеспрямоване руйнування політичних інститутів України. Така діяльність становить серйозну загрозу для національної безпеки держави. Зокрема, Росія здійснювала активне проникнення у владні структури України, а також реалізовувала політику вербування кадрів у Збройних Силах та спеціальних службах [48].

У контексті обговорення методів, інструментів та рекомендацій щодо вдосконалення системи національної безпеки, доцільно звернутися до конкретних прикладів секторів, які відіграють важливу роль у протидії гібридній

агресії. Це охоплює як військові та правоохоронні структури, так і інститути цифрової трансформації, інформаційної безпеки, громадянського суспільства та міжнародного партнерства. Їхня взаємодія є критично важливою для формування стійкої системи реагування на багатовимірні загрози [42].

Удосконалення зовнішньої розвідки та розвиток ситуаційної обізнаності є одним із ключових напрямів підвищення ефективності національної безпеки України в умовах гібридної війни. Держава визнає стратегічне значення розвідувальної діяльності як інструменту раннього виявлення та оцінки загроз. Зокрема, йдеться про розширення можливостей агентурної розвідки, сигнальної розвідки, а також використання методів збору інформації з відкритих джерел (OSINT).

Завдяки системному моніторингу дій противника, аналізу його намірів та виявленню вразливих точок, Україна здатна оперативно реагувати на потенційні гібридні атаки, а також на провокації, що можуть призвести до проксі-конфліктів. Такий підхід дозволяє не лише зміцнити обороноздатність, а й забезпечити проактивне управління ризиками у сфері безпеки.

Своєчасне виявлення планів підготовки гібридної агресії є критично важливим для формування ефективної військово-політичної стратегії протидії. У таких умовах створюється спеціалізований національний або коаліційний орган, який координує діяльність розвідувальних структур на всіх рівнях – від стратегічного до тактичного. Визначаються базові принципи застосування сил спеціальних операцій, а також сценарії використання високоточної зброї. Особливу увагу приділяють аналізу територій, які потенційно можуть стати об’єктами гібридного впливу, з урахуванням їхніх соціальних, політичних та інфраструктурних характеристик [46].

У сучасній війні перемога не обов’язково означає фізичне знищення збройних сил противника чи окупацію території. Гібридна стратегія передбачає дезінтеграцію військово-адміністративної системи держави-жертви, руйнування її інституційної основи та встановлення контролю над свідомістю населення. Це вимагає централізованої системи протидії, здатної оперативно реагувати на

багатовимірні загрози [47].

Синергетичний ефект гібридних атак полягає в їх здатності одночасно впливати на різні компоненти системи національної безпеки. Тому розвідка має діяти на основі науково обґрунтованих прогнозів, визначаючи наміри противника, його ресурси, засоби впливу та потенційні об’єкти атаки. Головним завданням є виявлення підготовчих заходів, які можуть бути використані для дестабілізації держави.

Комплекс розвідувальних і контррозвідувальних завдань охоплює аналіз сфер діяльності агресора, де формуються стратегії підриву, створюються ресурси, налагоджуються канали зв’язку та координації. Загальна мета – руйнування державності жертви – формується на рівні урядових структур країни-агресора, а також за участі транснаціональних корпорацій, фінансових установ і впливових осіб. Розвідка повинна виявляти плани дестабілізації адміністративно-політичної, соціально-економічної та культурно-ідеологічної сфер, включаючи створення автономних мережевих структур, каналів їх забезпечення, складів озброєння, місць підготовки бойовиків тощо.

Окремим напрямом є виявлення умов підготовки спеціальних операцій, які маскуються під дипломатичні дії, економічні санкції, інформаційні кампанії або диверсії проти критичних об’єктів інфраструктури. Їхнє своєчасне розкриття є запорукою збереження державної цілісності та стабільності [50].

Створення у 2019 році Спільного розвідувального центру стало важливим кроком у напрямі посилення координації між силовими структурами України. Завдяки централізованому управлінню розвідувальною діяльністю вдалося підвищити рівень ситуаційної обізнаності, що, своєю чергою, сприяє більш оперативному та ефективному реагуванню на гібридні загрози [51].

Окрему загрозу становить діяльність російських розвідувальних служб на території України, яка здійснюється у кількох напрямках: збір конфіденційної інформації, вербування місцевих жителів, організація підривних акцій. Протидія таким діям потребує реформування Служби безпеки України, зокрема її трансформації у спеціалізований контррозвідувальний та контртерористичний

орган. Прикладом може слугувати британська служба MI5, яка зосереджується виключно на трьох функціях: боротьбі з тероризмом, шпигунством та запобіганні поширенню зброї масового ураження [50].

У цьому контексті доцільною виглядає пропозиція щодо виведення зі структури СБУ підрозділу «К» – Головного управління боротьби з корупцією та організованою злочинністю – з передачею його повноважень іншим правоохоронним органам, таким як Державне бюро розслідувань, Національна поліція або новостворене Бюро економічної безпеки. Такий крок дозволить оптимізувати кадровий склад, зменшити фінансове навантаження та зосередити діяльність СБУ на пріоритетних загрозах, пов'язаних із національною безпекою, а не на розслідуванні господарських правопорушень.

У межах гібридної агресії особливе місце займає використання кіберпростору та інформаційних операцій, які спрямовані на маніпулювання суспільною свідомістю, поширення дезінформації та порушення функціонування критичної інфраструктури. Україна визнає стратегічну важливість впровадження ефективних заходів кіберзахисту та активного ведення інформаційної боротьби як ключових інструментів протидії сучасним загрозам.

Застосування кіберпростору як складової асиметричної агресії є відносно новим явищем, яке ще не повністю осмислене з точки зору рівня небезпеки та можливих механізмів реагування. Як зазначає Д. Дубов, керівник відділу інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень, дискусії щодо природи кібератак та відповідей на них активізувалися у 2010–2011 роках. У 2011 році було ухвалено «Талліннське керівництво щодо застосування міжнародного права у кіберсфері», а вже у 2012 році НАТО офіційно визнало кіберпростір новим театром воєнних дій [49].

Проте на практиці реагування на кіберзагрози залишається складним завданням, оскільки довести причетність конкретної держави або організованої групи до здійснення атак надзвичайно важко. Це створює додаткові виклики для формування правових і оперативних механізмів протидії, що потребують

міжнародної координації та технологічної модернізації [9].

Як зазначають фахівці, до 2013 року активність російських спецслужб у кіберпросторі України залишалася малопомітною. Водночас уже тоді був зафіксований досвід здійснення Російською Федерацією масштабних кібератак проти інших держав, зокрема Естонії та Грузії. Починаючи з 2013 року, українські кіберфахівці почали виявляти серію цілеспрямованих APT-атак (Advanced Persistent Threats), метою яких був несанкціонований доступ до конфіденційної інформації або даних з обмеженим доступом. У більшості випадків обґрунтовано підозрюються російські спецслужби та пов'язані з ними хакерські угруповання [31].

Відповіддю на зростання кіберзагроз стало створення у 2017 році Національного координаційного центру кібербезпеки (NC4), який суттєво посилив здатність України протистояти кібератакам. Центр здійснює координацію між державними структурами, співпрацює з міжнародними партнерами та розробляє комплексні стратегії кіберзахисту, спрямовані на охорону критичної інфраструктури, державних інформаційних систем та персональних даних громадян [21].

На сучасному етапі розвитку системи національної безпеки України особливу увагу слід приділяти посиленню захисту критичної інформаційної інфраструктури та забезпеченню її стабільного функціонування. Важливими напрямами є вдосконалення механізмів виявлення кіберзагроз, їхнього попередження та ефективної ліквідації наслідків. Також необхідно підвищувати рівень захищеності населення та територій від наслідків надзвичайних ситуацій, що можуть бути спричинені інформаційно-технічним або військовим впливом на об'єкти критичної інфраструктури [40].

Окрему увагу слід приділяти захисту галузей, які функціонують на основі широко застосовуваних інформаційних систем – зокрема телекомунікацій та сфери охорони здоров'я. При цьому варто зазначити, що сучасні засоби кіберзахисту, за умови їх грамотного використання, здатні суттєво знизити ризики, пов'язані з різними типами загроз – від простих шкідливих програм до

складних цілеспрямованих атак [44].

Водночас у промислових інформаційних системах застосування таких методів є обмеженим або навіть непридатним через специфіку їхньої архітектури, вимоги до безперервності роботи та інші технічні особливості. Це створює додаткові виклики для формування ефективної моделі кіберзахисту в промисловому секторі [45].

Зміцнення суспільної стійкості та соціальної згуртованості є ключовим чинником у протидії гібридній агресії та запобіганні внутрішнім конфліктам. Україна активно працює над консолідацією суспільства, утвердженням демократичних принципів і протидією інформаційним кампаніям, спрямованим на загострення соціальних розбіжностей. Такий підхід дозволяє зменшити вразливість населення до маніпуляцій та сприяє формуванню єдиного національного простору.

В Україні фіксуються численні прояви гібридного впливу, серед яких – використання псевдогромадських організацій, медіаресурсів та соціальних мереж для дестабілізації міжетнічних відносин, маніпуляції темами історичної пам’яті та соціокультурної ідентичності. Наприклад, у травні 2017 року в окремих регіонах країни було проведено зовнішню рекламну кампанію політичної сили «Опозиційний блок» із провокативними гаслами, що сприяли ескалації суспільної напруги: «Требуем остановить репрессии и наступление нацизма», «Требуем прекратить войну». А в червні 2016 року повідомлялося про спробу ініціювання створення так званої «Бессарабської народної республіки» [10].

Російські засоби масової інформації активно висвітлюють ситуацію у сфері міжрелігійних відносин в Україні, зокрема, переходи релігійних громад з Української православної церкви Московського патріархату (УПЦ МП) до Української православної церкви Київського патріархату (УПЦ КП) подаються як порушення прав віруючих УПЦ МП. Експерти зафіксували випадки поширення дезінформації, зокрема чуток про загрозу закриття або підпалів храмів УПЦ МП, як це було, наприклад, у Білгороді-Дністровському Одеської

області, що створювало ризики конфліктного загострення [11].

У травні 2017 року також з’явилася інформація про наміри УПЦ МП адаптувати свої статути за моделлю Російської православної церкви, що передбачало надання єпархіальним управлінням повноважень контролювати всі аспекти життя релігійних організацій. Додаткове напруження в релігійному середовищі спричинили законопроекти №4128 та №4511, які викликали негативну реакцію з боку УПЦ МП [11].

В Україні активно розвивається міжсекторальна співпраця між урядовими структурами, громадянським суспільством та освітніми установами з метою підвищення рівня обізнаності населення щодо гібридних загроз, дезінформаційних кампаній та важливості критичного мислення. Освітні ініціативи та громадські проєкти сприяють формуванню медіаграмотності, активної громадянської позиції та загальної стійкості суспільства до маніпулятивних технологій, що застосовуються в межах гібридної війни.

Особливу увагу слід приділяти молодіжному середовищу, адже саме молодь є найбільш відкритою до формування нових цінностей, поглядів і моделей поведінки. Як зазначають експерти, старші покоління вже мають усталені переконання, які складно змінити, тоді як молодь залишається ключовою цільовою групою для формування згуртованого, стійкого та свідомого громадянського суспільства. Саме тому стратегічно важливо зосередити зусилля на згуртуванні тих, хто ще здатен до переосмислення та активної участі в суспільних процесах [13].

У контексті гібридної агресії, яка виходить за межі традиційного розуміння війни та безпеки, особливої актуальності набуває питання зміцнення правоохоронного сектору. Гібридні загрози є багатовимірними, тому ефективна протидія їм вимагає модернізації та очищення системи внутрішньої безпеки держави.

Протягом тривалого часу правоохоронна система України зазнавала поступової деградації, перетворюючись із інструмента правопорядку на репресивний механізм, що обслуговував інтереси авторитарного та морально

дискредитованого керівництва. До її лав нерідко вступали особи, які розглядали службу як засіб особистого збагачення, використовуючи службове становище у власних інтересах. Водночас загальна соціально-політична ситуація не сприяла утриманню в системі професійних, етичних і відповідальних кадрів.

Недостатнє фінансування та слабка матеріально-технічна база змушували працівників шукати додаткові джерела доходу, що сприяло поширенню корупційних практик, «кришування» та підтримці незаконної діяльності. За результатами опитувань, більшість українських експертів (56,8%) вважають саме корумпованість силових структур одним із ключових чинників, що сприяв початку агресії Російської Федерації проти України [15].

Одним із ключових чинників, що сприяв ослабленню здатності правоохоронних органів України протистояти гібридним загрозам, стало проникнення агентури держави-агресора до системи правопорядку та безпеки. За свідченням Валентина Наливайченка, який очолював Службу безпеки України у 2006–2010 роках, на початку 2014 року окремі підрозділи СБУ, зокрема «Альфа», були настільки інфільтровані російською ідеологією та агентурними елементами, що до кінця квітня того ж року значна частина співробітників не сприймала Росію як агресора, а росіян – як ворогів. У результаті, в умовах анексії Криму, лише близько 30% співробітників СБУ залишилися вірними присязі [19].

З огляду на специфіку гібридної агресії, правоохоронні органи мають зосередити зусилля на розробці та впровадженні спеціалізованих освітніх програм. Такі програми повинні бути спрямовані на поглиблення знань персоналу щодо концептуальних засад, тактичних прийомів та методів ведення гібридної війни. Це дозволить правоохоронцям своєчасно ідентифікувати гібридні загрози у межах своєї компетенції та ефективно реагувати на них, забезпечуючи стабільність і безпеку держави [19].

Проблематика реформування державного управління у сфері правоохоронних органів в умовах гібридної війни залишається недостатньо дослідженою та потребує глибшого аналізу. Ефективна протидія гібридним

загрозам можлива лише за умови системної трансформації правоохоронного сектору, зокрема шляхом посилення вертикальної координації між структурами та розвитку горизонтальних зв'язків між ними.

Модернізація управлінських механізмів у правоохоронній сфері має здійснюватися поетапно, з урахуванням актуальних викликів та міжнародного досвіду. На першому етапі необхідно затвердити концепцію реформи, визначивши її етапи, ресурси, індикатори та критерії оцінювання. Другий етап передбачає ухвалення загального закону про правоохоронні органи та розробку відповідної нормативної бази. Третій етап – практична реалізація реформи [37].

Удосконалення державного управління правоохоронними органами має базуватися на таких принципах:

– чітке регламентування функцій кожного органу для уникнення дублювання повноважень;

– налагодження стратегічної комунікації та міжвідомчої співпраці;

– впровадження адаптивних управлінських стратегій із залученням незалежних експертів;

– участь громадянського суспільства у прийнятті ключових рішень щодо внутрішньої безпеки;

– розвиток партнерських відносин із населенням та місцевими громадами;

– підвищення професійного рівня та відповідальності працівників;

– забезпечення належного фінансового, матеріально-технічного та соціального забезпечення персоналу [38].

У результаті реформи правоохоронна система має трансформуватися у суспільно-орієнтовану структуру, що функціонує за сервісною моделлю, позбавлена репресивних функцій і спрямована на вирішення проблем громадян. Успіх у протидії гібридній агресії значною мірою залежатиме від здатності правоохоронних органів продемонструвати переваги української моделі розвитку – з ефективним верховенством права, високими соціальними стандартами та якісним державним управлінням. Нові функції правоохоронних

органів мають включати забезпечення стабільності держави, захист від новітніх загроз та здатність реагувати на сучасні виклики [39].

Постійна трансформація форм і методів гібридної агресії вимагає безперервного вдосконалення правоохоронного сектору України. Зосередження на професійній підготовці кадрів, розвитку аналітичних спроможностей, впровадженні сучасних технологій та розширенні міжнародного співробітництва дозволяє державі підвищити ефективність реагування на багатовимірні загрози. Зміцнення правоохоронної системи є критично важливим для забезпечення національної безпеки, підтримання суспільної стійкості та утвердження верховенства права в умовах гібридного протистояння.

Протидія гібридній агресії та запобігання проксі-конфліктам залишаються пріоритетними завданнями у сфері безпеки. Україна, модернізуючи розвідувальні механізми, посилюючи кіберзахист, формуючи згуртоване громадянське суспільство та реформуючи правоохоронні органи, прагне мінімізувати вплив гібридних інструментів. Поєднання цих заходів із постійною адаптацією до нових викликів і впровадженням інноваційних рішень сприятиме збереженню державного суверенітету, політичної стабільності та загальної безпеки країни в умовах ескалації гібридних загроз.

Узагальнюючи, можна стверджувати, що сучасна епоха гібридних війн і проксі-конфліктів формує складні виклики для систем національної безпеки у глобальному вимірі. Ці виклики охоплюють стрімкий технологічний прогрес, багатовимірність гібридних загроз, а також нагальну потребу в удосконаленні механізмів координації та міждержавної взаємодії.

Для ефективної протидії гібридній агресії та запобігання проксі-конфліктам державам необхідно зосередитися на розширенні розвідувальних спроможностей, інвестуванні в інноваційні технології, активізації міжнародного співробітництва та розробці комплексних стратегій безпеки. Такий підхід дозволить зміцнити національну стійкість, забезпечити захист суверенітету та гарантувати стабільність у контексті постійно еволюціонуючих загроз.

ВИСНОВКИ

У процесі дослідження проблематики національної безпеки України в умовах гібридної агресії всі поставлені завдання були реалізовані комплексно та послідовно:

1. Проведено аналіз концептуальних підходів до розуміння феномену національної безпеки в сучасному світі. Дослідження виявило еволюцію цієї категорії: від традиційних, державоцентричних та мілітаризованих поглядів (що асоціюються з класичним реалізмом) до сучасних багатовимірних концепцій. Було обґрунтовано, що сьогодні національна безпека є комплексною системою, яка охоплює не лише оборонний, але й політичний, економічний, інформаційний, екологічний та, що важливо, гуманітарний виміри. Виокремлення ключових елементів, змісту та структури дозволило сформувати цілісне уявлення про безпекову систему держави, довівши ефективність саме комплексного підходу як базової моделі забезпечення національної цілісності в умовах сучасних загроз.

2. Досліджено процеси біфуркації в міжнародних відносинах та їх вплив на виникнення загроз національній безпеці. Встановлено, що сучасна міжнародна система перебуває у стані фазового переходу, або «точці біфуркації», що характеризується високою нестабільністю та невизначеністю траєкторій розвитку. Для системи національної безпеки такі процеси виступають водночас й як екзистенційна загроза, що руйнує застарілі механізми, й як унікальна можливість для докорінного оновлення та адаптації.

3. Розкрито сутність гібридної війни як виклику безпековій системі України та систематизовано основні теоретичні засади гібридної війни та гібридних загроз. Гібридна війна визначена як цілеспрямована стратегія агресора, що комбінує конвенційні військові дії з широким спектром невійськових інструментів: політичним тиском, економічними диверсіями, інформаційно-психологічними операціями та кібератаками. Застосування

порівняльного та емпіричного методів дозволило розкрити багатовимірність цього явища, його еволюцію від прихованих операцій 2014 року до повномасштабного застосування у 2022-му. Специфіка гібридної війни полягає у створенні «сірої зони», що розмиває межі між станом війни та миру, та у фокусуванні на дестабілізації держави-жертви зсередини.

4. Проведено оцінку трансформаційних процесів в системі національної безпеки України внаслідок гібридної агресії та простежено динаміку гібридної агресії проти України у період з 2014 по 2024 роки. Гібридна агресія виступила каталізатором вимушеної, але глибокої трансформації сектору безпеки і оборони України. Було виокремлено основні форми ворожого впливу – інформаційну, військову, кібернетичну, медійну, культурну та економічну – що дозволило глибше зрозуміти характер сучасних загроз. Аналіз державної політики, нормативно-правової бази та інституційних механізмів (зокрема, ролі РНБО, СБУ, ЗСУ, МВС та нової ролі Мінцифри) виявив позитивні зрушення в адаптації до нових викликів. Водночас було окреслено системні проблеми, пов’язані з недостатньою міжвідомчою координацією, фрагментарністю стратегічних рішень та нагальною потребою в посиленні превентивних механізмів. Особливо наголошено на критичній важливості інформаційної безпеки та стратегічних комунікацій, де, попри певні успіхи, залишаються суттєві вразливості до дезінформаційних кампаній ворога.

Розглянуто зовнішньополітичну діяльність України як інструмент зміцнення національної безпеки. Особливу увагу приділено інтеграції до НАТО та ЄС, міжнародній підтримці та стратегічному партнерству. Доведено, що зовнішня політика відіграє важливу роль у протидії гібридним загрозам.

5. Запропоновано шляхи вдосконалення механізмів управління національною безпекою України. Обґрунтовано необхідність реформування правоохоронного сектору, посилення розвідувальних спроможностей, розвитку кібербезпеки, зміцнення соціальної згуртованості та впровадження адаптивних стратегій управління з урахуванням міжнародного досвіду.

Узагальнюючи результати дослідження, можна стверджувати, що

ефективна протидія гібридній агресії потребує системного оновлення безпекової архітектури України, інтеграції зусиль держави, суспільства та міжнародних партнерів, а також постійної адаптації до нових викликів.

На основі комплексного аналізу сучасного стану системи національної безпеки України, а також результатів проведеного дослідження, сформульовано низку рекомендацій, спрямованих на підвищення ефективності протидії гібридним загрозам.

Розробка інтегрованої державної стратегії протидії гібридній агресії. Україна потребує єдиного стратегічного документа, який би визначав системний і міжвідомчо узгоджений підхід до протидії гібридним викликам. Така стратегія має охоплювати всі ключові виміри – інформаційний, кібернетичний, економічний – та передбачати активну участь громадянського суспільства. Доцільним є оновлення Концепції національної безпеки України з чітким визначенням гібридної війни як окремої форми загрози. Важливо закласти механізми превентивного реагування, а не обмежуватися лише реактивними заходами. Необхідно також встановити чіткі протоколи взаємодії між основними суб'єктами безпеки – Міністерством оборони, МВС, СБУ, РНБО, Міністерством цифрової трансформації та іншими відповідальними структурами.

Зміцнення кібербезпеки та цифрової стійкості держави. У зв'язку з постійними кібератаками, що спрямовані на державні органи, критичну інфраструктуру та енергетичні об'єкти, особливої актуальності набуває посилення кіберзахисту. Доцільно розширити функціональні повноваження Державної служби спеціального зв'язку та захисту інформації, створивши постійну систему моніторингу кіберзагроз. Важливим кроком є запровадження обов'язкової сертифікації з кібербезпеки для всіх державних установ і стратегічно важливих підприємств. Слід підтримувати розвиток національного програмного забезпечення з метою зменшення залежності від іноземних технологій. Крім того, необхідно розвивати систему реагування на кіберінциденти (CSIRT), забезпечивши її оперативною аналітичною спроможністю.

Зміцнення інформаційної безпеки та стратегічної комунікації є одним із ключових напрямів протидії гібридній агресії, оскільки інформаційний фронт відіграє вирішальну роль у сучасних конфліктах. З метою посилення спроможності держави до реагування на дезінформаційні кампанії доцільно створити Єдиний центр стратегічних комунікацій, який забезпечуватиме оперативну координацію дій. Важливим є проведення широкомасштабних програм з медіаграмотності серед населення, особливо в регіонах, що є вразливими до зовнішнього інформаційного впливу. Необхідно також посилити державну підтримку незалежних засобів масової інформації, які дотримуються професійних стандартів журналістики, та запровадити системний моніторинг ворожого контенту в соціальних мережах із залученням фахівців з OSINT та міжнародних партнерів.

Переосмислення системи військово-цивільної взаємодії та територіальної оборони стало актуальним у зв’язку з досвідом повномасштабної війни, що продемонстрував необхідність інтеграції цивільних ресурсів у загальну систему оборони. Зокрема, слід реформувати підготовку резервістів за прикладом країн Балтії, передбачивши створення добровольчих формувань при територіальних громадах. Важливим є розроблення локальних планів безпеки для кожної громади, формування структур кризового управління з чітким розподілом функціональних обов’язків у надзвичайних ситуаціях, а також залучення громадян до регулярних навчань і тренувань, особливо в прикордонних регіонах.

Реформування системи національної безпеки у сфері освіти і науки передбачає активне залучення наукової спільноти, освітніх установ та аналітичних центрів до формування концептуальних засад безпекової політики. Доцільним є створення державної програми дослідження гібридних загроз за участю університетів, think-tanків та незалежних експертних платформ. Слід підтримувати наукові розробки у сферах соціальної психології, інформаційних технологій та комунікацій. Важливо також інтегрувати дисципліни з національної безпеки, кібергігієни та критичного мислення до навчальних програм старших класів і закладів вищої освіти, що сприятиме формуванню

стійкого та свідомого громадянського суспільства.

Міжнародне співробітництво та євроатлантична інтеграція є стратегічно важливими напрямами у зміцненні національної безпеки України. Поглиблення партнерства з державами-членами НАТО та ЄС має включати активну участь у спільних навчаннях, особливо з акцентом на протидію гібридним загрозам. Важливим є використання технічної допомоги у сфері кібербезпеки для модернізації національної інфраструктури, створення центрів обміну інформацією про загрози у співпраці з країнами Балтії, Польщею та Фінляндією, а також реалізація навчальних програм для фахівців безпекового сектору за підтримки партнерів з Альянсу.

Енергетична та економічна безпека виступають фундаментальними складовими стійкості держави в умовах гібридної війни. Зважаючи на ризики енергетичного шантажу, диверсій та фінансових атак, Україна має посилити енергонезалежність шляхом розвитку альтернативних джерел енергії, запровадити ефективні механізми захисту критичної інфраструктури – електростанцій, логістичних центрів, підприємств оборонного комплексу. Необхідно також активізувати фінансову розвідку для протидії відмиванню коштів, що використовуються для фінансування деструктивних мереж, та стимулювати внутрішнє виробництво стратегічно важливої продукції – медичної, оборонної, ІТ-сфери.

Гуманітарна політика та внутрішня згуртованість є не менш важливими чинниками безпеки, ніж технологічні рішення. Суспільна стійкість базується на відчутті справедливості, рівності та довіри до державних інституцій. У цьому контексті необхідно забезпечити ефективну політику реінтеграції тимчасово окупованих територій, включаючи інформаційну, культурну та освітню підтримку. Важливим є підвищення рівня державної підтримки ветеранів, військовослужбовців та їхніх родин, забезпечення рівного доступу до публічних послуг у всіх регіонах, особливо в прикордонних та постраждалих зонах, а також підтримка національної ідентичності через культуру, мову та мистецтво.

В умовах ескалації гібридних загроз Україна має не лише оновити

законодавчу базу, а й сформувати нову модель безпеки – адаптивну, інтегровану та превентивну. Національна безпека повинна стати спільною справою не лише силових структур, а й усього суспільства. Реалізація запропонованих рекомендацій дозволить сформувати ефективну, стійку та сучасну систему безпеки, здатну протистояти як традиційним, так і новітнім формам агресії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ананьїн В. О. Національна безпека держави в сучасних умовах : монографія / В. О. Ананьїн, О. В. Ананьїн, В. В. Горлинський ; за заг. ред. В. О. Ананьїна. Київ : КПІ ім. Ігоря Сікорського, 2021. 345 с.

2. Бахметьєв А. Є. Забезпечення національної безпеки України в умовах ведення гібридної війни / НУ «Одеська юридична академія». URL: http://dspace.onua.edu.ua/bitstream/handle/1 (дата звернення: 24.10.2025).

3. Бжезінський З. Велика шахівниця. URL: https://www.ukrlit.ua/lib/bzhezinskiy/html (дата звернення: 24.10.2025).

4. Вєдєнєєв Д., Сегеда С. Історико-теоретичні витоки поглядів на сутність війн (конфліктів) неконвенційного концептуального типу (1970-ті – початок 2000-х рр.). *Воєнно-історичний вісник*. 2022. № 1. С. 161–181.

5. Вєдєнєєв Д. В., Семенюк О. Г. Формування концептуальних та функціональних передумов гібридної конфліктності як загрози національній безпеці України: ретроспективний аналіз : монографія. Київ : ДП «ІНФОТЕХ», 2020. 274 с.

6. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики : Вибр. наук. праці. Київ : НІСД, 2016. 528 с.

7. Гібридна війна. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Гібридна_війна (дата звернення: 24.10.2025).

8. Глобальна та національна безпека / В. І. Абрамов, Г. П. Ситник, В. Ф. Смолянюк та ін. ; за заг. ред. Г. П. Ситника. Київ : НАДУ при Президентові України, 2016. 784 с.

9. Горбулін В. Гібридна війна як ключовий інструмент російської геостратегії реваншу. URL: https://www.gazeta.dt.ua/internal/gibridna-viyna-yak-klynehoviyinstrumentrsiyskoyi-geostrategiyi-revanshu_html (дата звернення: 24.10.2025).

10. Єрмоленко А. Публічність як чинник громадянського суспільства в

Україні за доби глобалізації. *Вісник ХНУВС*. 2022. № 4 (99). С. 106–117.

11. Загуменна Ю. О. Концептуалізація феномену національної безпеки в теоретико-правовій науці: особливості сучасної методології. *Форум права*. 2021. № 1 (66). С. 37–55. DOI: https://doi.org/10.5281/zenodo.4486522 (дата звернення: 24.10.2025).

12. Конституція України : прийнята Верховною Радою України 28.06.1996. URL: http://zakon3.rada.gov.ua/laws/show/254к/96-вр/ed19960628 (дата звернення: 24.10.2025).

13. Концепція національної безпеки України : прийнята Верховною Радою України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=13342&pf35401=24861 (дата звернення: 24.10.2025).

14. Костенко Г. Ф. Теоретичні аспекти стратегії національної безпеки : навч. посіб. Київ : ДЕМІД, 2002. 144 с.

15. Кравченко Н. Інформаційна складова як ключовий аспект гібридної війни. *Acta de Historia & Politica : Saeculum XXI*. 2022. Т. IV. С. 106–118.

16. Лисецький Ю. М., Старовойтенко О. О., Семенюк Ю. В., Павленко Д. Г. Гібридні війни. Компоненти та особливості. *Вчені записки ТНУ імені В. І. Вернадського*. Серія: Державне управління. 2021. Т. 32 (71), № 5. С. 63–70.

17. Ліпкан В. А. Національна безпека України : навч. посіб. / Національна академія внутрішніх справ. Київ : Кондор, 2008. 552 с.

18. Ліпкан В. А. Національна безпека України : монографія. Київ : Кондор, 2013. 437 с.

19. Ліпкан В. А., Ліпкан О. С., Яковенко О. О. Національна і міжнародна безпека в визначеннях та поняттях. Київ : Текст, 2006. 256 с.

20. Магда Є. Гібридна агресія Росії: уроки для Європи. Київ : КАЛАМАР, 2017. 268 с.

21. Національна безпека: світоглядні та теоретико-методологічні засади : монографія / за заг. ред. О. П. Дзьобаня. Харків : Право, 2021. 776 с.

22. Нижник Н. Р., Ситник Г. П., Білоус В. Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : навч. посіб. Ірпінь : Акад.

ДПС України, 2000. 70 с.

23. Подорожна Т. С. Забезпечення інформаційної безпеки України в умовах сучасних викликів та загроз з боку РФ. *Аналітично-порівняльне правознавство*. 2023. № 6. С. 491–497.

24. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-VIII (дата звернення: 24.10.2025).

25. Про Стратегію національної безпеки України : Указ Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020 (дата звернення: 24.10.2025).

26. Редькіна А. Українські національні інтереси й цінності: суспільне усвідомлення та переоцінка. *Політичні дослідження / Political Studies*. 2023. № 1 (5). С. 144–162. URL: http://pd.ipiend.gov.ua/article/view/280397 (дата звернення: 24.10.2025).

27. Результати Вільнюського Саміту 11-12 липня. НАТО у Вільнюсі. 2023 рік. URL: https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/rezultaty-vilnyuskoho-samitu-nato-11-12-lypnya-2023-roku (дата звернення: 24.10.2025).

28. Рущенко І. П. Підривні соціальні технології в структурі гібридної війни. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/315/RUSHCHENKO.pdf?sequence=1&isAllowed=y (дата звернення: 24.10.2025).

29. Ситник Г. П., Орел М. Г. Національна безпека в контексті європейської інтеграції України : підручник / Г. П. Ситник, М. Г. Орел ; за ред. Г. П. Ситника. Київ : Міжрегіональна Академія управління персоналом, 2021. 372 с.

30. Смолянюк В. Ф., Деменко О. Ф., Прибутько П. С. Основи національної безпеки України : навч. посіб. Київ : Паливода А. В., 2017. 140 с.

31. Стрільчук Л. Інформаційна війна як складова сучасних гібридних воєн (на прикладі Грузії та України). *Літопис Волині*. 2023. № 28. С. 235–239.

32. Требін М. Гібридна війна як нова українська реальність. URL: https://www.ukrsocium.org.ua/Arhiv/Stati/us-3_2014/113-127.pdf (дата звернення:

24.10.2025).

33. Федченко О. Аналіз факторів та сучасних загроз інформаційній безпеці держави у контексті забезпечення національної безпеки України. *Journal of Scientific Papers «Social Development and Security»*. 2022. Vol. 12, № 3. С. 128–134.

34. Хатнюк Ю. А. Аналіз сучасних загроз національній безпеці. *Науковий вісник Міжнародного гуманітарного університету*. Серія: Юриспруденція. 2020. № 43. С. 65–68. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/3469 (дата звернення: 24.10.2025).

35. Чекаленко Л. Про поняття «гібридна війна». URL: http://www.viche.info/journal/4615/ (дата звернення: 24.10.2025).

36. Ядуха С. Й., Лисак О. М. Національна безпека України. Її основні аспекти, принципи та загрози. *Вісник Хмельницького національного університету*. Серія: Економічні науки. 2018. № 5 (1). С. 131–136.

37. Antebi L. Artificial Intelligence and National Security in Israel. Tel Aviv, 2021. 142 p.

38. Bazilian M., Goldthau A., Westphal K. Model or Ally? How Europe Can Lead on Energy and Climate. 2019. URL: https://surl.li/gktfvv (last accessed: 24.10.2025).

39. Phillips D. B. Review of Beyond Ukraine: Debating the Future of War, edited by T. Sweijs and J. H. Michaels. *Joint Forces Quarterly*. 2024. 2nd Quarter (Oct.), no. 113. P. 116–118.

40. Brown H. Thinking About National Security: Defense and Foreign Policy in a Dangerous World. Colorado, 1983. 288 p.

41. Buzan B. People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era. 2nd ed. London : Harvester Wheatsheaf, 1991.

42. Casimir Pulaski Foundation. How to Defend Against Hybrid Threats. 2021. URL: https://pulaski.pl/wp-content/uploads/2021/11/FOB16_EN.pdf (last accessed: 24.10.2025).

43. DefencesCoop. NATO seeks to confront the growing ‘pressure of hybrid

war’. 2024. URL: https://defensescoop.com/2024/07/16/nato-confront-growing-pressure-hybridwar-russia-china/ (last accessed: 24.10.2025).

44. DuMont M. Elements of national security strategy. *DOCPLAYER*. URL: https://docplayer.net/183125113-Elements-ofnational-security-strategy-malia-dumont.html (last accessed: 24.10.2025).

45. Harvard Divinity School. "Declaration of the Rights of Man and the Citizen". Religion and Public Life. Harvard University. URL: https://rpl.hds.harvard.edu/faq/declaration-rights-man-and-citizen (дата звернення: 24.10.2025).

46. Heinrich Böll Foundation. Безпека людини: особливості та можливості впровадження в Україні. Human Security: Articles. 2021. Київ : Heinrich Böll Foundation. URL: https://cutt.ly/AeKsmgCq (дата звернення: 24.10.2025).

47. Hoffman F. Hybrid Warfare and Challenges. *Joint Force Quarterly (JFQ)*. 2009. Issue 52 (Forth Quarter).

48. Hoffman F. G. Future Threats and Strategic Thinking. *Infinity Journal*. 2011. Fall. URL: https://www.infinityjournal.com/article/34/Future_Threats_and_Strategic_Thinking/ (last accessed: 24.10.2025).

49. Hoffman F. G. Hybrid vs. compound war. *Armed Forces Journal*. 2009. Oct. URL: http://armedforcesjournal.com/hybrid-vs-compound-war/ (last accessed: 24.10.2025).

50. Hoffman F. Conflict in the 21st Century: The Rise of Hybrid Wars. 2007. URL: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf last accessed: 24.10.2025).

51. Lavigne Ph. Embracing Change. A sense of Urgency. *Joint Forces Quarterly*. 2023. 4th Quarter, no. 111. P. 25–32.

52. Kimmage M. The War in Ukraine and the Origins of the New Global Instability. Oxford University Press, 2024. 279 p.

53. Morgenthau H. Politics Among Nations: The Struggle for Power and Peace. New York : Alfred A. Knopf, 1948.

54. Office of the Historian. "The Declaration of Independence, 1776".

Milestones in the History of U.S. Foreign Relations. U.S. Department of State. URL: https://history.state.gov/milestones/1776-1783/declaration (last accessed: 24.10.2025).