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

КООРДИНАЦІЯ ДІЯЛЬНОСТІ ЦЕНТРАЛЬНИХ ТА МІСЦЕВИХ ОРГАНІВ ВЛАДИ У ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ : ІНТИТУЦІЙНИЙ АСПЕКТ

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

Науковий керівник роботи:
доктор юридичних наук, професор
_____ Лариса ВЕЛИЧКО

Харків – 2025

ЗМІСТ

ВСТУП

Актуальність теми. В сучасному світі гібридні загрози стали домінуючою формою геополітичного протистояння, здатною підривати суверенітет держав, дестабілізувати суспільство та створювати критичні виклики для національної безпеки без формального оголошення війни.

Наша держава з 2014 року перебуває під систематичним гібридним тиском Російської Федерації, а повномасштабне вторгнення 24 лютого 2022 року продемонструвало всю складність гібридної агресії, яка поєднує військові дії з інформаційними операціями, кібератаками, економічним тиском та підривною діяльністю. Органи публічної влади України опинилися перед необхідністю одночасного реагування на різнорідні загрози, що вимагає безпрецедентної координації між центральним та місцевим рівнями управління.

Слід зазначити, що наявна національна система координації органів влади у протидії гібридним загрозам формувалася переважно реактивно, без достатнього стратегічного планування та чіткого розподілу відповідальності. Відсутність ефективних координаційних механізмів між центральними органами виконавчої влади та органами місцевого самоврядування, функціональне дублювання повноважень, недостатня міжвідомча взаємодія та обмежені ресурси до сих пір створюють серйозні перешкоди для комплексної протидії гібридним викликам.

Актуальність даного дослідження обумовлена нагальною потребою узагальнення унікального досвіду воєнного часу, виявлення гострих проблем інституційної координації та розробки науково обґрунтованих рекомендацій щодо вдосконалення системи взаємодії різних рівнів влади у протидії гібридним загрозам. Ефективна координація центральних та місцевих органів влади є необхідною умовою не лише для перемоги в поточній війні, але й для довгострокового забезпечення стійкості України до гібридних викликів, зміцнення державності та успішної євроінтеграції.

Стан наукової розробки проблеми. Проблематика гібридних загроз та механізмів протидії їм перебуває у фокусі наукової уваги багатьох українських та зарубіжних дослідників, однак комплексні дослідження інституційних механізмів координації центральних та місцевих органів влади у протидії гібридним загрозам в Україні досі залишаються фрагментарними.

Розглядаючи концептуальні засади гібридних загроз та гібридної війни, слід звернути увагу на роботи В.П. Горбуліна, який визначає гібридну війну як комплексне застосування військових та невійськових засобів для досягнення стратегічних цілей без формального оголошення війни. Є.В. Магда аналізує російські гібридні технології проти України, досліджуючи інформаційні, економічні та політичні компоненти агресії. Л.І. Шипілова в своїх наукових працях вивчає специфіку протидії гібридним загрозам у секторі безпеки і оборони України та пропонує певні шляхи вдосконалення інституційної спроможності.

Серед теоретичних засад координаційної діяльності у сфері національної безпеки слід виділити роботи Г.П. Ситника, який аналізує систему забезпечення національної безпеки та місце координації в ній та О.М. Суходолі, яка досліджує механізми координації органів виконавчої влади у сфері національної безпеки.

В.С. Абрамов приділяє увагу інституційним засадам національної безпеки, обґрунтовуючи необхідність чіткого розподілу повноважень між різними рівнями влади. Натомість, О.І. Власюк досліджує національну безпеку в умовах гібридної війни та координацію зусиль держави і суспільства.

Цікавими також вбачаються дослідження децентралізації та її впливу на систему національної безпеки. Так, В.Б. Авер’янов аналізує проблеми координації в системі органів виконавчої влади України, а О.М. Батанов досліджує конституційно-правові засади місцевого самоврядування та його роль у забезпеченні безпеки на місцевому рівні.

В.М. Куйбіда та А.Ф. Ткачук приділяють багато уваги практичним аспектам децентралізації та новим повноваженням органів місцевого самоврядування у сфері безпеки громад, а Р.М. Плющ - координації діяльності

органів місцевого самоврядування у надзвичайних ситуаціях.

Серед зарубіжних науковців слід відмітити Franka Hoffmana, який створив фундаментальну концепцію гібридної війни, систематизувавши характеристики сучасних конфліктів та обґрунтувавши необхідність міжвідомчої координації у відповідь на них. James J. F. Forest детально досліджує інституційні механізми протидії гібридним загрозам у країнах НАТО, розробивши методологію аналізу координаційних структур. Michael Mazarr досліджує стратегічну конкуренцію в умовах гібридного протистояння та роль різних рівнів влади у забезпеченні стійкості держави, а Margaret E. Kosal аналізує координацію урядових та неурядових акторів у протидії гібридним викликам, підкреслюючи важливість багаторівневого управління. Hanna Smith досліджує досвід протидії гібридним загрозам у країнах Балтії, виявивши успішні практики координації центральної та місцевої влади.

Загалом, аналіз наукової літератури свідчить, що українські дослідники зосереджуються в більшості на концептуальних, правових та інституційних засадах протидії гібридним загрозам у цілому, тоді як зарубіжні науковці приділяють більшу увагу практичним механізмам координації різних рівнів влади та міжвідомчої взаємодії.

Незважаючи на значну кількість досліджень окремих аспектів досліджуваної проблеми, на цей час відсутні комплексні роботи, які б системно аналізували саме механізми координації центральних та місцевих органів влади у протидії гібридним загрозам в Україні в умовах воєнного стану. Практично відсутні дослідження, які узагальнюють український досвід координаційної діяльності у період 2022-2025 років та пропонують науково обґрунтовані рекомендації щодо оптимізації інституційних механізмів координації. Саме заповнення цієї прогалини обумовлює актуальність і практичну значущість даного дослідження.

Метою роботи є комплексний інституційний аналіз механізмів координації центральних та місцевих органів влади у протидії гібридним загрозам в Україні та розробка науково обґрунтованих практичних рекомендацій

щодо їх стратегічної оптимізації.

Для досягнення поставленої мети визначено наступні *завдання:*

– узагальнити концептуальні підходи до розуміння гібридних загроз та координаційної діяльності у сфері національної безпеки, уточнити термінологічний апарат дослідження;

– дослідити міжнародний досвід координації центральних та місцевих органів влади у протидії гібридним викликам шляхом компаративного аналізу практик різних країн;

– проаналізувати нормативно-правові та організаційні основи координації діяльності органів влади у сфері національної безпеки України, визначити структуру, повноваження та механізми взаємодії відповідних органів;

– вивчити практику взаємодії різних рівнів влади у відповідь на гібридні загрози, виявити проблеми та досягнення української моделі координації;

– оцінити ефективність інституційних механізмів координації діяльності органів влади та виявити проблемні зони функціонування системи їх взаємодії;

– розробити рекомендації щодо оптимізації взаємодії центральних та місцевих органів влади в умовах гібридних загроз.

Об'єктом дослідження є процеси координації центральних та місцевих органів влади у протидії гібридним загрозам.

Предметом дослідження є інституційні механізми координації діяльності центральних та місцевих органів влади у протидії гібридним загрозам в Україні.

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.

Так, *метод термінологічного аналізу* застосовано для уточнення понятійно-категоріального апарату дослідження, розмежування понять «гібридна загроза», «гібридна війна», «координація», «взаємодія», що дозволило

створити чітку термінологічну основу роботи; *метод теоретичного узагальнення* використано для систематизації наукових підходів до розуміння гібридних загроз та координаційної діяльності і формулювання власних теоретичних висновків щодо природи координаційних механізмів; *системний підхід* застосовано для дослідження координації органів влади як цілісної системи взаємопов'язаних елементів публічної політики у сфері національної безпеки, що, в свою чергу, дозволило виявити ключові взаємозв'зки між різними компонентами системи (підрозділ 1.1).

Компаративний метод використано для порівняльного аналізу міжнародного досвіду координації органів влади у протидії гібридним загрозам, виявлення спільних та відмінних рис різних національних моделей, що дало змогу ідентифікувати успішні практики для адаптації в українських умовах; *метод кейс-стаді* застосовано для поглибленого аналізу конкретних прикладів успішних практик координації в країнах ЄС, НАТО та інших демократичних державах, що забезпечило розуміння практичного застосування теоретичних концепцій (підрозділ 1.2).

Інституційний аналіз використано для дослідження формальних та неформальних інститутів координації діяльності органів влади, їх структури, повноважень та взаємодії, що дозволило виявити інституційні прогалини та дублювання функцій (підрозділи 2.1, 2.2); *структурно-функціональний аналіз* застосовано для визначення ролей та функцій центральних і місцевих органів влади у системі протидії гібридним загрозам, що допомогло ідентифікувати проблеми координації; *нормативно-правовий аналіз* використано для вивчення законодавчої бази координації органів влади у сфері національної безпеки, виявлення прогалин та суперечностей у правовому регулюванні, що стало основою для формулювання законодавчих рекомендацій (підрозділ 2.1).

Метод документального аналізу застосовано для вивчення офіційних документів, стратегій, програм, звітів органів влади щодо координаційної діяльності у протидії гібридним загрозам, що забезпечило емпіричну базу дослідження (підрозділи 2.1, 2.2); *метод моніторингу* використано для

відстеження та аналізу практики координації між центральними та місцевими органами влади у період 2022-2025 років, що забезпечило актуальність емпіричних даних; *метод експертних інтерв'ю* застосовано для збору первинної інформації від практиків, які безпосередньо залучені до координаційної діяльності у сфері протидії гібридним загрозам, що додало практичну складову до теоретичного аналізу (підрозділ 2.2).

Проблемно-орієнтований аналіз застосовано для виявлення та систематизації ключових викликів і проблем функціонування механізмів координації, що дозволило структурувати виявлені недоліки; *SWOT-аналіз* використано для комплексної оцінки сильних і слабких сторін існуючої системи координації, можливостей та загроз її розвитку, що забезпечило стратегічне бачення перспектив розвитку; *метод експертних оцінок* застосовано для оцінювання ефективності різних координаційних механізмів та практик взаємодії органів влади, що дозволило розмістити рекомендації за пріоритетністю (підрозділ 3.1).

Метод стратегічного планування використано для визначення пріоритетних напрямів удосконалення системи координації з урахуванням обмежених ресурсів та актуальних викликів; *метод моделювання* застосовано для розробки моделі оптимізованої системи координації центральних та місцевих органів влади у протидії гібридним загрозам; *метод прогнозування* використано для визначення перспективних тенденцій розвитку гібридних загроз та відповідних координаційних механізмів; *метод системного синтезу* застосовано для формулювання комплексу рекомендацій щодо вдосконалення координаційної діяльності (підрозділ 3.2).

Комплексне застосування зазначених методів дозволило забезпечити всебічність, об'єктивність та науковість дослідження інституційних механізмів координації центральних та місцевих органів влади у протидії гібридним загрозам в Україні.

Практичне значення отриманих результатів. Результати дослідження мають конкретне практичне застосування у декількох ключових сферах:

У науково-дослідній сфері матеріали роботи становлять теоретико-методологічну основу для подальших наукових досліджень в означеній сфері та збагачують академічну дискусію новими кейсами, створює базу для міжнародних порівняльних досліджень.

У практичній діяльності державних органів результати дослідження можуть бути враховані Радою національної безпеки і оборони України в якості аналітичної основи при розробці та вдосконаленні стратегічних документів з питань національної безпеки та координації діяльності органів влади, зокрема при оновленні Стратегії національної безпеки України.

Кабінет Міністрів України, Офіс Президента України, центральні органи виконавчої влади можуть врахувати запропоновані практичні рекомендації щодо вдосконалення механізмів координації з органами місцевого самоврядування, а Секретаріат Кабінету Міністрів України може застосовувати результати дослідження при розробці нормативно-правових актів з питань координації діяльності органів виконавчої влади, зокрема при підготовці постанов та розпоряджень уряду.

Виявлені проблеми координації між центральним та місцевим рівнями влади дозволять органам державної влади цілеспрямовано зосередити зусилля на усуненні конкретних інституційних недоліків через створення ефективних координаційних механізмів.

Узагальнені практики координаційної взаємодії можуть бути трансформовані у методичні рекомендації для працівників органів публічної влади та посадових осіб місцевого самоврядування.

У навчальному процесі матеріали дослідження можуть бути інтегровані закладами вищої освіти при викладанні дисциплін «Національна безпека», «Публічне управління та адміністрування», «Місцеве самоврядування», «Державна політика у сфері національної безпеки», збагачуючи їх актуальними українськими кейсами координаційної діяльності в умовах гібридної війни.

Результати дослідження можуть бути включені до програм підготовки та підвищення кваліфікації публічних службовців у Національному агентстві

України з питань державної служби, ННІ «Інституті державного управління» Харківського національного університету імені В.Н. Каразіна, зокрема для керівників органів виконавчої влади та органів місцевого самоврядування.

Узагальнені практики координації складають основу практичних занять, воркшопів та тренінгів з питань протидії гібридним загрозам для різних цільових аудиторій.

Матеріали роботи можуть бути також використані при підготовці навчально-методичних посібників, монографій, наукових статей з проблематики координації органів влади у протидії гібридним загрозам, при розробці нових освітньо-професійних програм магістрів публічного управління та адміністрування, а також підготовки фахівців у сфері національної безпеки, формуючи навчальні плани та програми дисциплін.

Аналіз кейсів української координаційної практики може бути використаний у навчальному процесі як практичний матеріал для вивчення сучасних викликів національній безпеці на конкретних прикладах.

Апробація результатів дослідження. Основні положення та результати дослідження обговорювалися на засіданнях кафедри права, національної безпеки та європейської інтеграції ННІ «Інституті державного управління» Харківського національного університету імені В.Н. Каразіна і можуть бути використані в подальшому в науковій діяльності кафедри.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ КООРДИНАЦІЇ ДІЯЛЬНОСТІ ОРГАНІВ ВЛАДИ У ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

1.1 Концептуальні підходи до розуміння гібридних загроз та координаційної діяльності органів влади у сфері національної безпеки

Гібридні загрози, що еволюціонували від традиційних форм міждержавного протистояння до складних багатовекторних впливів у XXI столітті, становлять фундаментальний виклик для сучасних демократичних держав та вимагають переосмислення базових підходів до національної безпеки.

Концептуалізація гібридних загроз у теорії публічного управління та міжнародних відносин, що відбувалася поступово протягом останніх двох десятиліть, набула чіткості після російської агресії проти Грузії у 2008 році та особливо після анексії Криму і початку війни на Донбасі у 2014 році [28].

Термін «гібридна війна», введений у науковий обіг американським військовим аналітиком Френком Хоффманом у середині 2000-х років, первісно описував комбінацію конвенційних та іррегулярних методів ведення бойових дій, але згодом розширив своє значення, охопивши значно ширший спектр невійськових інструментів впливу [47]. Сучасне розуміння гібридних загроз, сформульоване у документах НАТО та ЄС, включає координоване використання військових, економічних, інформаційних, кібернетичних, дипломатичних та інших інструментів для досягнення стратегічних цілей без формального оголошення війни [8].

Теоретичне осмислення феномену гібридних загроз базується на синтезі різних наукових дисциплін, включаючи теорію міжнародних відносин, воєнну науку, публічне управління, комунікативістику та кібербезпеку. Класична реалістична парадигма міжнародних відносин, що фокусувалася на військовій

силі як основному інструменті державної політики, виявилася недостатньою для пояснення складних багатовимірних впливів, характерних для гібридних кампаній. Конструктивістський підхід, розроблений у працях Олександра Вендта та інших теоретиків, наголошує на ролі ідей, норм та ідентичностей у формуванні міжнародної реальності та надає більш адекватну рамку для розуміння інформаційної та ідеологічної складових гібридних загроз [14], а теорія складних систем, запозичена з природничих наук, допомагає концептуалізувати гібридні загрози як нелінійні, адаптивні феномени, що характеризуються емерджентними властивостями та непередбачуваними ефектами взаємодії різних компонентів.

Ключовими характеристиками гібридних загроз, що відрізняють їх від традиційних форм конфлікту, є багатовимірність, амбівалентність, прихованість джерела, експлуатація вразливостей демократичних систем, адаптивність до контрзаходів противника та синергія різних компонентів впливу. Багатовимірність гібридних загроз, що проявляється в одночасному використанні військових, економічних, інформаційних, кібернетичних, дипломатичних інструментів у скоординованій кампанії, вимагає відповідної багатосекторальної відповіді з боку цільової держави [59].

Амбівалентність гібридних загроз розмиває традиційні межі між війною та миром, внутрішніми та зовнішніми загрозами, державними та недержавними акторами, створюючи «сіру зону» невизначеності, яка ускладнює прийняття адекватних політичних рішень. Прихованість джерела гібридного впливу через використання проксі-груп, приватних військових компаній, кібератак з анонімних джерел дозволяє агресору уникати відповідальності та ускладнює міжнародну відповідь через проблеми атрибуції.

Експлуатація вразливостей демократичних систем, включаючи свободу слова, відкритість кордонів, політичну поляризацію, медіаплюралізм, є принциповою особливістю гібридних загроз, що використовують демократичні цінності проти самих демократій. Адаптивність гібридних кампаній до контрзаходів противника через постійне вивчення та коригування підходів

створює динамічне протиборство, де жодна сторона не може покладатися на статичні стратегії захисту. Синергія компонентів гібридної загрози означає, що комбінований ефект різних інструментів перевищує суму їхніх окремих впливів завдяки координації та взаємному підсиленню.

Українські дослідники, аналізуючи досвід протистояння російській агресії, виділяють специфічні риси гібридних загроз у пострадянському просторі, включаючи використання історичної пам’яті та мовних питань як інструментів дестабілізації, експлуатацію етнічних та регіональних розбіжностей, маніпулювання енергетичною залежністю [27]. Проаналізуємо типологію гібридних загроз за сферами впливу та інструментами (таблиця 1.1).

Таблиця 1.1 – Типологія гібридних загроз за сферами впливу та інструментами

Сфера впливу	*Інструменти*	*Цільові об'єкти*	*Індикатори загрози*	*Приклади застосування*
Військова	Іррегулярні формування, приватні військові компанії, «зелені чоловічки»	Територіальна цілісність, суверенітет	Нарощування військ біля кордону, захоплення об'єктів без розпізнавальних знаків	Анексія Криму 2014, «сепаратизм» на Донбасі
Інформаційна	Дезінформація, пропаганда, маніпуляції у соцмережах, фейкові новини	Громадська думка, довіра до інституцій	Координовані кампанії у соцмережах, аномальна активність ботів	Референдум Brexit, вибори США 2016
Кібернетична	DDoS-атаки, зламування систем, витоки даних, шкідливе ПЗ	Критична інфраструктура, держустанови, бізнес	Масові кібератаки, відключення систем	Атаки на Естонію 2007, NotPetya в Україні 2017
Економічна	Енергетичний шантаж, торговельні обмеження, корупційні схеми	Економічна незалежність, критичні сектори	Раптові зупинки постачань, необґрунтовані санкції	«Газові війни» РФ проти України
Дипломатична	Дезінформація на міжнародній арені, дипломатичний тиск, вето	Міжнародна підтримка, репутація держави	Ізоляція на міжнародній арені, блокування рішень	Вето РФ у РадБезу ООН

Джерело: розробка автора.

Представлена типологія гібридних загроз, розроблена на основі аналізу сучасних конфліктів та досліджень провідних аналітичних центрів і демонструє багатовимірний характер цього феномену та необхідність комплексного підходу до протидії. Кожна сфера впливу, виділена у таблиці, характеризується специфічними інструментами, що можуть використовуватися як автономно, так і у синергії з іншими компонентами гібридної кампанії, створюючи мультиплікативний ефект дестабілізації [87].

Військова складова, яка у традиційних конфліктах була домінуючою, у гібридних компаніях часто відіграє підтримуючу роль, створюючи тиск та загрозу ескалації, тоді як основні зусилля спрямовуються на інформаційне, кібернетичне та економічне ослаблення противника. Інформаційний компонент, що набув критичного значення у цифрову епоху, використовує маніпуляції громадською думкою через соціальні мережі та традиційні медіа для підриву соціальної згуртованості та довіри до демократичних інституцій без єдиного пострілу. Кібернетичні атаки на критичну інфраструктуру демонструють вразливість сучасних цифровізованих суспільств та можливість завдати значної шкоди економіці та життєзабезпеченню населення через віртуальні операції, що не залишають традиційних слідів агресії.

Концепція інституційної координації у системі публічного управління, критично важлива для ефективної протидії гібридним загрозам і базується на теорії організаційного дизайну та міжвідомчої взаємодії. Координація, за класичним визначенням Генрі Мінцберга, є процесом узгодження дій різних організаційних одиниць для досягнення спільних цілей та запобігання конфліктам і дублюванню зусиль [5].

У контексті протидії гібридним загрозам, що характеризуються багатовимірністю та складністю, координація набуває особливого значення через необхідність синхронізації зусиль численних державних органів, що традиційно функціонували автономно у своїх секторальних сферах відповідальності [83]. Багатовимірний характер гібридних загроз вимагає залучення не лише силових та оборонних відомств, але й органів, відповідальних

за економічну політику, інформаційну безпеку, цифрову трансформацію, соціальну політику, освіту, культуру, кожен з яких володіє специфічною експертизою та ресурсами [82].

Теоретичні моделі координації у публічному управлінні, розроблені протягом останніх десятиліть, варіюються від ієрархічних, де координація досягається через командну вертикаль та централізоване прийняття рішень, до мережевих, що базуються на горизонтальних зв'язках, добровільній співпраці та спільному виробленні рішень [13]. Ієрархічна модель координації, характерна для військових та силових структур, забезпечує швидкість та чіткість виконання команд, але може бути занадто жорсткою для адаптації до динамічних гібридних загроз, що вимагають креативності та міжсекторальної експертизи [16].

Мережева модель координації, популярна у теорії нового публічного управління, надає більшу гнучкість та інноваційність, але потребує високої культури співпраці та довіри між учасниками мережі, яких часто бракує у конкурентному середовищі державних органів [9]. Ринкова модель координації через конкуренцію та контрактні відносини може бути ефективною для окремих функцій, але неприйнятна для стратегічних питань національної безпеки.

Гібридна модель координації, що комбінує елементи ієрархії для критичних рішень та мережевої співпраці для операційної діяльності, видається найбільш адекватною для протидії багатовимірним загрозам, хоча вимагає складного організаційного дизайну [10]. Ключові механізми інституційної координації у протидії гібридним загрозам включають створення координаційних органів вищого рівня, таких як ради національної безпеки чи міжвідомчі комісії з повноваженнями стратегічного планування, формалізацію процедур обміну інформацією через спільні бази даних та системи раннього попередження, розвиток спільного ситуаційного усвідомлення всіма учасниками координації, чіткий розподіл ролей та відповідальності у різних сценаріях загроз, проведення спільних навчань та тренувань для відпрацювання процедур координації, а також оцінку ефективності координації через моніторинг та аналіз результатів спільних дій [18]. Виклики координації, виявлені у дослідженнях

міжвідомчої взаємодії, пов'язані з організаційною культурою різних відомств, різними професійними мовами та підходами, конкуренцією за ресурси та вплив, бюрократичними процедурами, що сповільнюють обмін інформацією, а також проблемами довіри між інституціями [20].

Проаналізуємо моделі інституційної координації (таблиця 1.2).

Таблиця 1.2 – Моделі інституційної координації: порівняльна характеристика

Модель координації	*Механізм узгодження*	*Переваги*	*Недоліки*	*Сфери оптимального застосування*
Ієрархічна	Накази, директиви, вертикаль влади	Швидкість рішень, чіткість виконання	Жорсткість, низька адаптивність	Кризові ситуації, військові операції
Мережева	Добровільна співпраця, консенсус, довіра	Гнучкість, інноваційність	Повільність рішень, залежність від довіри	Стратегічне планування, профілактика
Ринкова	Конкуренція, стимули, контракти	Ефективність через конкуренцію	Фрагментація, дублювання	Закупівлі послуг, аутсорсинг
Гібридна	Комбінація вертикалі та мереж	Баланс швидкості та гнучкості	Складність управління	Протидія гібридним загрозам

Джерело: розробка автора.

Порівняльна характеристика моделей інституційної координації, представлена у таблиці 1.2, виявляє відсутність універсального рішення, придатного для всіх типів завдань та контекстів у сфері національної безпеки.

Ієрархічна модель, домінуюча у традиційних військових та силових структурах, забезпечує швидкість та чіткість виконання команд у критичних ситуаціях, коли час на обговорення та досягнення консенсусу обмежений, проте ця модель може бути контрпродуктивною для завдань, що вимагають креативності, міжсекторальної експертизи та адаптації до швидкозмінних обставин.

Мережева модель координації, що набула популярності у контексті реформ нового публічного управління та whole-of-government підходу,

демонструє значні переваги у залученні різноманітної експертизи, стимулюванні інновацій та забезпеченні легітимності рішень через інклюзивність процесу, але потребує високої організаційної культури довіри та готовності до компромісів [1].

Гібридна модель, що комбінує вертикальну координацію для стратегічних рішень та кризового реагування з горизонтальними мережами для операційної діяльності та міжсекторальної співпраці, на нашу думку, видається найбільш адекватною для протидії багатовимірним гібридним загрозам, хоча вимагає складного організаційного дизайну та постійного балансування між різними логіками координації.

Інституційна архітектура координації у протидії гібридним загрозам на національному рівні типово включає три рівні, що забезпечують вертикальну інтеграцію від стратегічного планування до оперативного виконання.

Стратегічний рівень, представлений радами національної безпеки чи еквівалентними органами при главах держав, відповідає за визначення пріоритетів, затвердження стратегій, прийняття ключових рішень щодо розподілу ресурсів та політичних ініціатив [78]. *Оперативно-тактичний рівень*, реалізований через міжвідомчі комісії, робочі групи чи ситуаційні центри, координує поточну діяльність різних відомств, забезпечує обмін інформацією, вирішує конфлікти повноважень та розробляє оперативні плани відповіді на конкретні загрози. *Виконавчий рівень* включає безпосередню співпрацю між профільними підрозділами різних органів влади у реалізації конкретних заходів протидії загрозам, що вимагає налагодження регулярних комунікацій та розвитку особистих професійних зв’язків між виконавцями.

Особливе значення у координації протидії гібридним загрозам має взаємодія між центральними та місцевими органами влади, оскільки багато гібридних впливів реалізуються на локальному рівні через експлуатацію регіональних особливостей, етнічних та мовних розбіжностей, соціально-економічних проблем, місцевих політичних конфліктів.

Вертикальна координація між центром та регіонами стикається з

викликами різних інституційних спроможностей, обмеженості ресурсів місцевих органів, специфіки регіональних політичних еліт, що можуть мати власні інтереси, не завжди узгоджені з національними пріоритетами [19]. Українські дослідники наголошують на критичній важливості розбудови спроможностей місцевих органів влади у виявленні та протидії гібридним загрозам, особливо в контексті децентралізації та розширення повноважень територіальних громад, що створює нові можливості, але й нові ризики для національної безпеки [46].

Механізми вертикальної координації можуть варіюватися від жорстких централізованих директив до гнучких договірних відносин та мережевої координації через асоціації місцевого самоврядування, кожен з яких має специфічні переваги та обмеження залежно від політичної системи та адміністративно-територіального устрою країни [81].

Узагальнюючи теоретичні підходи до концептуалізації гібридних загроз та інституційної координації діяльності органів публічної влади, можна констатувати складність та багатовимірність цих феноменів, що вимагають міждисциплінарного аналізу та інноваційних організаційних рішень. Гібридні загрози, що поєднують військові, економічні, інформаційні, кібернетичні та дипломатичні інструменти у скоординованих кампаніях, експлуатують вразливості демократичних систем та розмивають традиційні межі між війною та миром, внутрішніми та зовнішніми загрозами [40]. Ефективна протидія таким загрозам вимагає координації зусиль численних державних органів через гібридні моделі, що комбінують ієрархічну вертикаль для стратегічних рішень з мережевою горизонтальною співпрацею для операційної гнучкості.

Особливою проблемою залишається вертикальна координація діяльності між центральними та місцевими органами влади, що потребує балансу між єдністю національної політики та врахуванням локальної специфіки загроз і можливостей [23].

1.2 Міжнародний досвід координації діяльності центральних та місцевих органів влади у протидії гібридним загрозам

Міжнародний досвід координації органів влади у протидії гібридним загрозам, накопичений демократичними країнами протягом останнього десятиліття, представляє цінний матеріал для вивчення різних інституційних моделей, механізмів взаємодії та уроків імплементації. Країни НАТО та Європейського Союзу, зіткнувшись з російською гібридною агресією проти Грузії, України, а також з спробами дестабілізації через дезінформаційні компанії, кібератаки та втручання у виборчі процеси, розробили різноманітні підходи до координації національних зусиль у протидії цим загрозам [41].

Компаративний аналіз національних моделей координації, здійснений провідними аналітичними центрами та науковими інституціями, дозволяє виявити як спільні принципи та найкращі практики, так і специфічні рішення, адаптовані до конкретних національних контекстів, правових традицій та організаційних культур [26]. Особливу увагу у міжнародному досвіді привертають моделі Сполучених Штатів з їхньою потужною президентською координацією, Фінляндії з інноваційним whole-of-society підходом, країн Балтії з їхнім унікальним досвідом протистояння російському впливу.

Європейський Союз розробив інституційну рамку координації протидії гібридним загрозам на наднаціональному рівні, яка доповнює національні зусилля держав-членів та забезпечує обмін інформацією, спільний аналіз загроз та координовані відповіді. Ключовим елементом європейської системи координації є Центр аналізу розвідданих та ситуаційного усвідомлення ЄС, створений у структурі Європейської служби зовнішніх дій, що збирає та аналізує інформацію про загрози від національних розвідслужб та надає щоденні брифінги для керівництва ЄС. Європейський центр досконалості з протидії гібридним загрозам, створений у 2017 році у Гельсінкі за ініціативою Фінляндії, об’єднує понад тридцять країн-учасниць та надає платформу для обміну

кращими практиками, розробки методологій та спільних тренінгів з протидії гібридним впливам [2]. Модель координації ЄС базується на принципі доповнюваності, де наднаціональні інституції координують загальноєвропейські зусилля, але основна відповідальність за протидію гібридним загрозам залишається на національному рівні, відповідно до принципу субсидіарності європейської інтеграції [4].

Система швидкого реагування Rapid Alert System, запроваджена ЄС у 2018 році після виявлення масштабних російських дезінформаційних компаній, забезпечує швидкий обмін інформацією між державами-членами про виявлені дезінформаційні кампанії та координовані кібератаки [3]. East StratCom Task Force, створена у 2015 році після анексії Криму як відповідь на зростаючу загрозу російської пропаганди, координує зусилля ЄС у протидії російській дезінформації у східному напрямку та підтримує незалежні медіа у постраднянських країнах через фінансові програми та технічну допомогу. Вітчизняні дослідники відзначають важливість європейського досвіду для України як країни-кандидата до ЄС, що потребує гармонізації національних підходів з європейськими стандартами координації [43].

Таблиця 1.3 – Інституційні моделі координації протидії гібридним загрозам у країнах-партнерах України

Країна	*Координаційний орган*	*Рівень централізації*	*Ключові механізми*	*Особливості моделі*
США	Рада національної безпеки при Президентові	Високий	Міжвідомчі директиви, ситуаційна кімната, спільні операційні центри	Президентський контроль, сильна вертикаль, розвинута розвідувальна координація
Велика Британія	Комітет національної безпеки Кабінету	Високий	Спільні оцінки загроз, інтегровані команди, COBRA кризові наради	Кабінетна модель, колегіальність з чіткою відповідальністю міністрів

Продовження таблиці 1.3

Країна	*Координаційний орган*	*Рівень централізації*	*Ключові механізми*	*Особливості моделі*
Фінляндія	Рада безпеки при Президентові, whole-of-society підхід	Середній-високий	Комплексна модель безпеки, залучення усіх секторів суспільства	Широка соціальна участь, акцент на стійкості, горизонтальна координація
Естонія	Комісія національної оборони, уряд	Середній	Кіберкоманда, мережа оборони, е-урядування	Цифрова координація, парламентський контроль, залучення ІТ-сектору
Литва	Рада національної безпеки при Президентові	Високий	Департамент стратегічних комунікацій, координація силових відомств	Сильна президентська роль, акцент на стратегічних комунікаціях

Джерело: розробка автора.

Таблиця 1.3 інституційних моделей координації у країнах-партнерах України, складена на основі аналізу офіційних документів та наукових досліджень і демонструє значну варіативність організаційних рішень, адаптованих до специфіки національних політичних систем, історичного досвіду та актуальних загроз [54]. Американська модель з потужною Радою національної безпеки при Президентові, підкріпленою величезним апаратом аналітиків та координаторів, забезпечує високий рівень централізації стратегічних рішень та оперативну реакцію на загрози, проте критикується за надмірну концентрацію влади в руках президентської адміністрації та обмежену прозорість для парламентського контролю.

Британська кабінетна модель з Комітетом національної безпеки, що об’єднує ключових міністрів під головуванням прем’єр-міністра, забезпечує колегіальність прийняття рішень та чітку міністерську відповідальність перед парламентом, створюючи баланс між ефективністю та демократичною підзвітністю.

Фінська модель whole-of-society, що виходить за межі традиційного державоцентричного підходу та залучає приватний сектор, громадянські

організації, медіа, академічні інституції до спільної роботи з протидії гібридним загрозам, демонструє можливість побудови широкої соціальної стійкості через горизонтальну координацію та довіру між різними секторами суспільства [49].

Американська модель координації протидії гібридним загрозам, центром якої є Рада національної безпеки при Президентові, характеризується високим рівнем централізації та президентським контролем над усіма аспектами національної безпеки. Рада національної безпеки, створена ще у 1947 році Актом про національну безпеку, еволюціонувала від консультативного органу до потужного центру координації, що об'єднує міністрів оборони, держави, директора національної розвідки, голову об'єднаного комітету начальників штабів та інших ключових посадовців. Помічник Президента з національної безпеки очолює апарат Ради, що налічує сотні співробітників, організованих у директорати за географічним та функціональним принципом, кожен з яких відповідає за координацію політики у своїй сфері. Координація відбувається через систему міжвідомчих груп на різних рівнях, де Комітет принципалів приймає стратегічні рішення, Комітет депутатів координує оперативну діяльність, а численні робочі групи опрацьовують конкретні теми та готують рекомендації для вищого керівництва.

У сфері протидії гібридним загрозам США створили спеціалізовані координаційні структури, що відображають багатовимірність цих викликів та необхідність міжвідомчої співпраці. Кіберкомандування США, створене у 2009 році та підвищене до статусу об'єднаного бойового командування у 2018 році, координує військові кібероперації та співпрацює з цивільними агентствами у захисті національної кіберінфраструктури.

Агентство з кібербезпеки та інфраструктурної безпеки у складі Департаменту внутрішньої безпеки, створене у 2018 році, відповідає за захист критичної інфраструктури та координацію між федеральним урядом, штатами та приватним сектором. Глобальний центр залучення Державного департаменту координує протидію іноземній пропаганді та дезінформації через співпрацю з союзниками та підтримку незалежних медіа у вразливих країнах. Виклики

американської моделі, виявлені у дослідженнях та парламентських розслідуваннях, пов’язані з міжвідомчою конкуренцією, особливо між різними розвідувальними службами, бюрократичними процедурами узгодження та періодичною політизацією питань національної безпеки залежно від політичних циклів.

Фінська модель координації протидії гібридним загрозам, відома як комплексна безпека або whole-of-society підхід, є однією з найбільш інноваційних та широко цитованих у міжнародній літературі з публічного управління та національної безпеки. Ця модель, розроблена на основі історичного досвіду фінляндизації під час холодної війни та необхідності збереження незалежності у складних геополітичних умовах, базується на принципі залучення всього суспільства до забезпечення національної безпеки, а не лише державних органів [49]. Координацію на стратегічному рівні здійснює Рада безпеки при Президентові Фінляндії, що включає представників усіх ключових міністерств, а також бізнесу, профспілок, медіа, створюючи унікальну мультистейкхолдерську платформу для обговорення питань національної безпеки [12]. Модель виділяє вісім життєво важливих функцій суспільства, включаючи керівництво, міжнародну та оборонну здатність, внутрішню безпеку, економічну безпеку, інфраструктуру та постачання, психологічну стійкість, які мають підтримуватися навіть у кризових ситуаціях через скоординовані зусилля різних секторів.

Ключовим елементом фінського підходу є систематична робота з розвитку стійкості на всіх рівнях суспільства через освіту, комунікацію, тренування, що створює широку соціальну базу для протидії гібридним загрозам. Національна програма медіаграмотності, інтегрована в освітню систему від початкової школи до університету, формує у громадян навички критичного сприйняття інформації та розпізнавання маніпулятивних технік. Регулярні національні навчання з різних сценаріїв кризи, що проводяться щороку та залучають не лише державні органи, але й приватні компанії, громадянські організації, медіа, тестують процедури координації та виявляють слабкі місця у системі реагування.

Координація між центральними та місцевими органами влади здійснюється через регіональні адміністрації та систему муніципальної готовності до надзвичайних ситуацій, що забезпечує вертикальну інтеграцію від національного до локального рівня. Виклики фінської моделі, обговорювані у науковій літературі, пов'язані з часозатратністю процесів консенсусу, можливими проблемами конфіденційності при широкому залученні недержавних акторів, складністю масштабування підходу на великі країни з більш складною інституційною структурою. Спробуємо охарактеризувати механізми вертикальної координації між центральними та місцевими органами влади (таблиця 1.4).

Таблиця 1.4 – Механізми вертикальної координації між центральними та місцевими органами влади

Механізм координації	*Характеристика*	*Переваги*	*Ризики*	*Приклади застосування*
Централізовані директиви	Накази центральної влади для регіонів	Єдність політики, швидкість впровадження	Ігнорування локальної специфіки	Військове управління у воєнний час
Рамкове законодавство	Закони встановлюють цілі, регіони обирають засоби	Баланс єдності та гнучкості	Неоднорідність реалізації	ЄС директиви, федеральні закони США
Договірні відносини	Угоди між центром та регіонами про співпрацю	Добровільність, партнерство	Нерівність потенціалів	Французькі контракти держави-регіони
Фінансові стимули	Гранти, субвенції за виконання пріоритетів	Мотивація до якості	Залежність від центру	Конкурсні гранти на безпекові проєкти
Мережева координація	Платформи обміну практиками між регіонами	Горизонтальне навчання	Залежність від активності	Асоціації місцевого самоврядування

Джерело: розробка автора.

Таблиця 1.4 механізмів вертикальної координації між центральними та місцевими органами влади у протидії гібридним загрозам, систематизована на

основі міжнародного досвіду і розкриває складність взаємодії різних рівнів влади у федеративних та унітарних державах [35]. Централізовані директиви, характерні для унітарних держав з сильною вертикаллю виконавчої влади, забезпечують єдність національної політики та швидкість мобілізації ресурсів у кризових ситуаціях, проте ризикують ігнорувати локальну специфіку загроз та можливостей, що може призвести до неефективності заходів та демотивації місцевих органів влади [17].

Рамкове законодавство, популярне у європейських країнах та особливо у Європейському Союзі через систему директив, пропонує баланс між єдністю цілей та гнучкістю засобів, дозволяючи регіонам адаптувати загальні вимоги до своїх умов, але створює ризики неоднорідності реалізації та можливого відставання деяких регіонів від необхідних стандартів [21].

Мережева координація через асоціації місцевого самоврядування та міжмуніципальні платформи обміну практиками сприяє горизонтальному навчанню та поширенню інновацій без примусу з боку центру, але залежить від активності та ресурсів учасників мережі, що може бути нерівномірною між багатшими та біднішими регіонами.

Країни Балтії, що мають унікальний історичний досвід радянської окупації та сучасний досвід протистояння російському впливу, розробили специфічні моделі координації протидії гібридним загрозам, що поєднують цифрові інновації, територіальну оборону та стратегічні комунікації. Естонська модель акцентує на цифровій координації та залученні приватного IT-сектору до розробки рішень у кібербезпеці, використовуючи конкурентні переваги країни як одного з найбільш цифровізованих суспільств світу. Після масштабних кібератак 2007 року, що паралізували цифрову інфраструктуру країни та стали першим прикладом масованої кібератаки на державу, Естонія створила потужну систему кіберзахисту з координацією між Кіберкомандуванням оборонних сил, Інформаційною системою служби безпеки та приватним сектором.

Центр досконалості кооперативного кіберзахисту НАТО у Талліні став міжнародним хабом експертизи з кіберзахисту та розробив визнані міжнародні

стандарти, включаючи Таллінські посібники з міжнародного права у кіберпросторі [7]. Естонська модель е-урядування з цифровою ідентифікацією, електронними послугами та блокчейн-технологіями створює стійку до маніпуляцій систему державних послуг та громадянської участі.

Литовська модель координації характеризується сильною роллю Президента у питаннях національної безпеки, закріпленою конституційно, та акцентом на стратегічних комунікаціях як ключовому інструменті протидії інформаційним загрозам. Департамент стратегічних комунікацій при Міністерстві оборони Литви, створений у 2014 році, координує протидію дезінформації через співпрацю з медіа, громадянськими організаціями, освітніми інституціями та міжнародними партнерами. Литва також активно розвиває територіальну оборону з залученням добровольців-резервістів, організованих на локальному рівні, що створює мережу «перших відповідачів» на гібридні загрози у громадах та посилює зв'язок між армією та суспільством.

Латвія зосереджується на роботі з російськомовними громадами, що становлять значну частину населення та історично були вразливими до російської пропаганди, через програми інтеграції, підтримку латвійськомовних медіа, освітні ініціативи для зменшення соціальної фрагментації та зміцнення національної ідентичності [61].

Досвід балтійських країн демонструє можливості малих держав компенсувати обмеженість ресурсів через інноваційні підходи, технологічну досконалість, міжнародну співпрацю та мобілізацію суспільства. Проаналізуємо кращі міжнародні практики координації протидії гібридним загрозам (таблиця 1.5).

Таблиця 1.5 – Кращі практики координації протидії гібридним загрозам: міжнародний досвід

Практика	*Країна-ініціатор*	*Суть практики*	*Результати*	*Застосовність для України*
Whole-of-society підхід	Фінляндія	Залучення усіх секторів суспільства до національної безпеки	Висока соціальна стійкість	Висока - відповідає демократичним цінностям

Продовження таблиці 1.5

Практика	*Країна-ініціатор*	*Суть практики*	*Результати*	*Застосовність для України*
Rapid Alert System	ЄС	Швидкий обмін інформацією про дезінформацію між країнами	Координовані відповіді	Висока - Україна є кандидатом до ЄС
Hybrid CoE	Фінляндія + ЄС	Міжнародний центр обміну практиками протидії	База знань, тренінги	Висока - Україна є партнером
Кіберволонтери	Естонія	Мережа ІТ-фахівців-добровольців для кіберзахисту	Швидка мобілізація експертизи	Середня-висока - потужний ІТ-сектор України
Стратегічні комунікації	Литва	Проактивні наративи замість реактивних спростувань	Формування альтернативи пропаганді	Висока - потребує інституціоналізації

Джерело: розробка автора.

Таблиця 1.5 кращих практик координації протидії гібридним загрозам з міжнародного досвіду, складена на основі аналізу успішних кейсів та експертних оцінок, систематизує найбільш інноваційні підходи, що довели свою ефективність у різних національних контекстах та можуть бути адаптовані для українських умов [26].

Фінський whole-of-society підхід, що виходить за межі традиційного державоцентричного розуміння національної безпеки та залучає бізнес, громадянське суспільство, медіа, академічні інституції до спільної роботи з побудови стійкості, демонструє можливість створення широкої соціальної основи для протидії гібридним загрозам та має високу застосовність для України з її розвиненим громадянським суспільством, хоча потребує адаптації до специфіки українського політичного контексту [85]. Європейська система швидкого реагування як механізм обміну інформацією про виявлені дезінформаційні кампанії між країнами-членами ЄС створює мережевий ефект раннього попередження та координованих відповідей, що критично важливо для України як країни-кандидата до ЄС [43].

Центр досконалості з протидії гібридним загрозам у Гельсінкі як міжнародна платформа обміну кращими практиками об'єднує понад тридцять

країн-учасниць та надає унікальну можливість для України як партнера активно долучатися до розробки міжнародних стандартів, трансформуючи власний досвід протистояння повномасштабній гібридній агресії у глобальний експертний ресурс [2].

Критичний аналіз міжнародного досвіду координації протидії гібридним загрозам виявляє як універсальні принципи, релевантні для різних національних контекстів, так і контекстуально-специфічні рішення, що потребують обережної адаптації з урахуванням місцевих умов. Універсальні принципи ефективної координації включають необхідність стратегічної координації на найвищому політичному рівні, формалізацію механізмів міжвідомчої взаємодії через створення постійних координаційних органів та процедур, інвестиції у спільне ситуаційне усвідомлення через обмін інформацією та спільний аналіз загроз, розвиток спроможностей місцевих органів влади через навчання та ресурсну підтримку, залучення громадянського суспільства та приватного сектору до національних зусиль з безпеки.

Водночас, конкретні організаційні форми координації, чи то президентська Рада національної безпеки за американською моделлю, чи урядовий Комітет за британською, чи мультистейкхолдерська платформа за фінською, мають визначатися специфікою національної політичної системи, конституційного розподілу повноважень, організаційної культури державних інституцій та історичного досвіду країни.

Для України, з її специфікою напівпрезидентської республіки, де і Президент, і Прем’єр-міністр мають значні повноваження у сфері національної безпеки відповідно до Конституції, критично важливим є чітке розмежування ролей та налагодження процедур узгодження між різними центрами влади для уникнення конфліктів повноважень та забезпечення ефективної координації [48]. Досвід координації у воєнний час, коли Рада національної безпеки і оборони при Президентові стала де-факто основним координаційним центром з широкими повноваженнями, потребує інституціоналізації та адаптації для умов майбутнього мирного часу з збереженням ефективності та одночасним

посиленням демократичної підзвітності через парламентський контроль.

Міжнародний досвід показує, що найефективніші моделі координації поєднують централізацію стратегічних рішень для забезпечення єдності національної політики з децентралізацією операційної діяльності для забезпечення гнучкості та адаптації до локальної специфіки загроз, створюючи гібридну модель координації.

Узагальнюючи міжнародний досвід координації протидії гібридним загрозам, можна виділити ключові уроки для України щодо побудови ефективної системи координації, що поєднувала б кращі практики демократичних країн з урахуванням національної специфіки. По-перше, необхідність створення потужного координаційного органу на найвищому політичному рівні з чітко визначеними повноваженнями та ресурсами для забезпечення стратегічного планування та міжвідомчої узгодженості у протидії багатовимірним загрозам [80].

По-друге, важливість формалізації процедур обміну інформацією та спільного ситуаційного усвідомлення через створення інтегрованих систем моніторингу та аналізу загроз, що об’єднують дані від різних відомств та створюють цілісну картину ситуації.

По-третє, критична роль розвитку спроможностей місцевих органів влади як «перших відповідачів» на локальні прояви гібридних загроз через навчання, методологічну підтримку та ресурсне забезпечення з центрального рівня [55].

По-четверте, необхідність широкого залучення недержавних акторів, включаючи бізнес, громадянське суспільство, медіа, академічні інституції, до спільної роботи з побудови національної стійкості, що відповідає принципам whole-of-society підходу та демократичним цінностям України [53].

РОЗДІЛ 2
ІНСТИТУЦІЙНИЙ АНАЛІЗ МЕХАНІЗМІВ КООРДИНАЦІЇ ДІЯЛЬНОСТІ ЦЕНТРАЛЬНИХ ТА МІСЦЕВИХ ОРГАНІВ ВЛАДИ У ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ В УКРАЇНІ

2.1 Нормативно-правові та організаційні засади координації діяльності органів влади у сфері національної безпеки

Координація діяльності центральних та місцевих органів влади у сфері національної безпеки України становить складну багаторівневу систему, яка базується на чіткому нормативно-правовому фундаменті та розгалужених організаційних структурах. Конституційні засади цієї системи закладені у статті 118 Основного Закону, яка визначає розподіл виконавчої влади між центральними органами та місцевими державними адміністраціями [44].

Подальша конкретизація координаційних механізмів відбувається через систему спеціалізованих законів, указів Президента України та постанов Кабінету Міністрів. Особливо важливу роль у цьому контексті відіграє Закон України «Про національну безпеку України» від 21 червня 2018 року, який закріпив сучасну систему суб'єктів забезпечення національної безпеки та визначив координаційні функції Ради національної безпеки і оборони України [67].

Центральне місце в системі координації займає Рада національної безпеки і оборони України, яка згідно зі статтею 107 Конституції України функціонує як координаційний орган з питань національної безпеки і оборони при Президентові України [69]. Виокремлюючи специфіку її діяльності, варто підкреслити, що РНБО здійснює координацію та контроль за діяльністю органів виконавчої влади як у мирний час, так і в умовах воєнного або надзвичайного стану. До складу РНБО за посадою входять ключові керівники виконавчої влади,

включаючи Прем'єр-міністра, міністрів оборони, внутрішніх справ, закордонних справ, а також Голову Служби безпеки України, що забезпечує міжвідомчий характер координаційної діяльності [70]. Практика роботи РНБО свідчить про те, що її рішення, затверджені указами Президента, стають обов'язковими для виконання всіма органами виконавчої влади, включаючи місцеві державні адміністрації та органи місцевого самоврядування в частині делегованих повноважень.

Важливим нормативним документом, що визначає координаційні механізми протидії гібридним загрозам, є Стратегія національної безпеки України, затверджена Указом Президента №392/2020 від 14 вересня 2020 року [72]. Документ, що охоплює широкий спектр загроз національним інтересам, чітко артикулює необхідність координованої відповіді на гібридну агресію з боку держави-агресора. Стратегія визначає пріоритетні напрями розбудови спроможностей до протидії гібридним загрозам, включаючи інформаційну безпеку, кібербезпеку, захист критичної інфраструктури та протидію розвідувально-підривній діяльності.

Конкретизацію положень Стратегії здійснено через Стратегію протидії загрозам національній безпеці в інформаційній сфері, затверджену Указом Президента №685/2021, яка визначає механізми взаємодії органів державної влади у сфері стратегічних комунікацій та протидії дезінформації [71].

Розглядаючи організаційну структуру координації, неможливо оминути увагою роль міністерств та інших центральних органів виконавчої влади. Закон України «Про центральні органи виконавчої влади» від 17 березня 2011 року встановлює систему взаємовідносин між міністерствами як головними органами у системі центральних органів виконавчої влади та їхніми територіальними підрозділами [76]. Ключова особливість цієї системи полягає в подвійному підпорядкуванні територіальних органів: з одного боку, вони підзвітні відповідним центральним органам з питань реалізації державної політики у визначених сферах, з іншого – координуються місцевими державними адміністраціями при вирішенні питань регіонального розвитку. Така модель,

визначена в Законі України «Про місцеві державні адміністрації», передбачає, що голови місцевих державних адміністрацій здійснюють координацію діяльності територіальних органів міністерств та інших центральних органів виконавчої влади, проводять спільні засідання з керівниками цих органів та вносять подання про відповідальність їхніх керівників у разі неналежного виконання покладених функцій [66].

Особливої уваги потребує аналіз координаційних механізмів на місцевому рівні в контексті реформи децентралізації, розпочатої в Україні у 2014 році. Концепція реформування місцевого самоврядування та територіальної організації влади, затверджена розпорядженням Кабінету Міністрів України від 1 квітня 2014 року, визначила необхідність чіткого розмежування повноважень між органами місцевого самоврядування та місцевими органами виконавчої влади [74]. Важливим кроком у цьому напрямі стало ухвалення Закону України «Про службу в органах місцевого самоврядування» від 2 травня 2023 року, який встановив нові стандарти професійної діяльності посадових осіб місцевого самоврядування та механізми їхньої взаємодії з державними органами [73].

Процес децентралізації, попри об’єктивні складнощі, пов’язані з воєнним станом, продовжує розвиватися, що підтверджується ухваленням у 2024 році комплексу нормативних актів щодо вдосконалення адміністративно-територіального устрою та посилення спроможності громад [30].

Координаційна діяльність у сфері протидії гібридним загрозам здійснюється також через спеціалізовані міжвідомчі органи. Зокрема, при РНБО функціонують Національний координаційний центр кібербезпеки, який координує діяльність суб’єктів сектору безпеки і оборони у сфері кібербезпеки, та Центр протидії дезінформації, створений Указом Президента України №187/2021 для виявлення та протидії дезінформаційним кампаніям [75]. Діяльність цих органів, що базується на принципах оперативної координації та міжвідомчої взаємодії, передбачає регулярний обмін інформацією між центральними та місцевими органами влади, проведення моніторингу загроз та координацію заходів реагування. Практика щорічних командно-штабних

навчань «Національна кіберготовність», які проводяться НКЦК з 2021 року, демонструє зростаючу увагу до відпрацювання механізмів міжвідомчої координації в умовах кризових ситуацій [38].

Нормативно-правова база координації постійно вдосконалюється з урахуванням нових викликів та загроз. Важливим напрямом такого вдосконалення стало запровадження системи захисту критичної інфраструктури відповідно до Закону України «Про критичну інфраструктуру» від 16 листопада 2021 року [65]. Закон визначає координаційну роль Кабінету Міністрів України у формуванні та реалізації державної політики у сфері захисту критичної інфраструктури, а також встановлює обов’язки центральних та місцевих органів виконавчої влади щодо забезпечення захисту об’єктів критичної інфраструктури на відповідних територіях. Серед актуальних проблем реалізації цього Закону дослідники виділяють необхідність створення цілісної системи координації і контролю щодо захисту критичної інфраструктури як для воєнного, так і для мирного часу, а також чіткішого визначення ролі різних державних органів у цьому процесі [91]. Підсумуємо викладене (таблиця 2.1).

Таблиця 2.1 – Основні нормативно-правові акти координації органів влади у протидії гібридним загрозам

Нормативний акт	*Рік прийняття*	*Ключові положення*	*Координаційні механізми*	*Рівень імплементації*
Конституція України (ст. 118)	1996/ред. 2004	Розподіл виконавчої влади між центром та регіонами	Підпорядкування місцевих органів центральним	Конституційний
Закон «Про національну безпеку України»	2018	Визначення системи суб'єктів та координаційних функцій РНБО	Координація та контроль органів виконавчої влади	Базовий
Стратегія національної безпеки України	2020	Пріоритети протидії гібридним загрозам	Міжвідомча координація через РНБО	Стратегічний
Закон «Про критичну інфраструктуру»	2021	Система захисту критичних об'єктів	Розподіл відповідальності між рівнями влади	Секторальний

Продовження таблиці 2.1

Нормативний акт	*Рік прийняття*	*Ключові положення*	*Координаційні механізми*	*Рівень імплементації*
Закон «Про службу в органах місцевого самоврядування»	2023	Професіоналізація муніципальної служби	Стандарти взаємодії з державними органами	Локальний

Джерело: розробка автора.

Аналіз нормативно-правової бази свідчить про поступове формування комплексної системи координації протидії гібридним загрозам, яка охоплює всі рівні публічної влади. Основними координаційними механізмами виступають:

– стратегічне планування через РНБО та затвердження відповідних стратегій і програм; міжвідомча координація через спеціалізовані органи та робочі групи;

– територіальна координація через місцеві державні адміністрації;

– секторальна координація через профільні міністерства та відомства.

Водночас існують певні прогалини та невизначеності, зокрема щодо розмежування повноважень місцевих державних адміністрацій та органів місцевого самоврядування в умовах воєнного стану, механізмів оперативного реагування на кризові ситуації на місцевому рівні, координації діяльності різних силових відомств при протидії гібридним загрозам.

Важливим елементом організаційних основ координації є система інформаційного обміну між різними рівнями влади. Створення інтегрованих інформаційних систем, таких як система моніторингу та раннього попередження про загрози критичній інфраструктурі, електронні системи взаємодії органів влади, дозволяє оперативно виявляти та реагувати на гібридні загрози [32]. Однак виклики, пов’язані з забезпеченням кібербезпеки таких систем, захистом конфіденційної інформації та стандартизацією форматів даних, залишаються актуальними.

Міжнародний досвід країн НАТО та ЄС демонструє, що ефективна координація потребує не лише нормативного закріплення механізмів взаємодії, але й створення культури міжвідомчого співробітництва, регулярних навчань та

відпрацювання процедур реагування на різні сценарії гібридних атак [79].

Розглядаючи питання фінансового забезпечення координаційної діяльності, варто зазначити, що бюджетна децентралізація, здійснена в рамках реформи місцевого самоврядування, суттєво розширила фінансову спроможність територіальних громад. За даними Міністерства фінансів України, доходи місцевих бюджетів зросли з 68,6 млрд грн у 2014 році до понад 600 млрд грн у 2023 році, що створило матеріальну базу для реалізації завдань у сфері забезпечення місцевої безпеки [15]. Водночас, в умовах повномасштабного вторгнення, значна частина фінансових ресурсів громад спрямовується на забезпечення життєдіяльності населення, відновлення зруйнованої інфраструктури та підтримку внутрішньо переміщених осіб, що обмежує можливості фінансування заходів протидії гібридним загрозам. Це актуалізує необхідність цільової державної підтримки місцевих органів влади у виконанні функцій, пов'язаних із забезпеченням національної безпеки.

Роль міжнародного співробітництва у вдосконаленні координаційних механізмів також заслуговує на увагу. Співпраця України з НАТО в рамках Програми підвищеної можливості (ППМ), запровадженої у 2014 році та трансформованої у 2023 році в багаторічну програму допомоги, включає компонент посилення інституційної спроможності до протидії гібридним загрозам [22]. Платформа Україна-НАТО з протидії гібридній війні, створена у 2017 році, надає можливість українським фахівцям обмінюватися досвідом з експертами країн Альянсу, вивчати кращі практики координації різних відомств у відповідь на гібридні виклики. Участь українських представників у роботі Європейського центру передового досвіду з протидії гібридним загрозам у Гельсінкі також сприяє імплементації міжнародних стандартів у національну систему координації [84].

Перспективним напрямом розвитку координаційних механізмів є перехід від реактивної моделі реагування на загрози до проактивної моделі, яка передбачає систематичний моніторинг, раннє виявлення та превентивне нейтралізування потенційних гібридних загроз. Створення в структурі РНБО

Центру протидії дезінформації стало кроком у цьому напрямі, оскільки даний орган зосереджується саме на випередженні дезінформаційних кампаній та координації комунікаційних зусиль різних відомств [57]. Однак для повноцінного функціонування проактивної моделі необхідне подальше зміцнення аналітичних спроможностей як центральних, так і місцевих органів влади, розширення міжвідомчого обміну розвідувальною інформацією, створення спільних оперативних центрів координації на регіональному рівні.

Отже, нормативно-правові та організаційні основи координації діяльності органів влади у сфері національної безпеки України формують складну багаторівневу систему, яка еволюціонує відповідно до нових викликів та загроз. Конституційні норми, спеціалізоване законодавство, стратегічні документи та підзаконні акти створюють правову рамку для координаційної діяльності, визначаючи ролі та повноваження різних суб'єктів.

Організаційна структура координації включає як постійно діючі органи (РНБО, міністерства, місцеві державні адміністрації), так і спеціалізовані міжвідомчі органи (НКЦК, Центр протидії дезінформації). Реформа децентралізації суттєво вплинула на розподіл координаційних функцій, посиливши роль органів місцевого самоврядування у забезпеченні безпеки на місцевому рівні.

Водночас існують певні прогалини та виклики, пов'язані з необхідністю чіткішого розмежування повноважень, вдосконалення механізмів міжвідомчої взаємодії, посилення спроможностей місцевого рівня до протидії гібридним загрозам, що потребує подальшого законодавчого врегулювання та організаційного розвитку.

Резюмуючи зазначимо, що наліз нормативно-правових та організаційних основ координації діяльності органів влади у сфері національної безпеки дозволяє констатувати формування в Україні комплексної системи протидії гібридним загрозам. Ця система базується на конституційних засадах розподілу влади, спеціалізованому законодавстві про національну безпеку та включає як вертикальні (центр-регіони), так і горизонтальні (міжвідомчі) механізми

координації. Ключову роль відіграє РНБО як конституційний координаційний орган, а також спеціалізовані структури (НКЦК, Центр протидії дезінформації), що забезпечують оперативну міжвідомчу взаємодію.

Процес децентралізації суттєво змінив ландшафт координації, посиливши роль місцевого рівня, проте актуалізував необхідність чіткішого розмежування повноважень та вдосконалення механізмів взаємодії між різними рівнями публічної влади в умовах гібридних викликів.

2.2 Практика взаємодії різних рівнів влади у відповідь на гібридні виклики: проблеми та досягнення

Практична реалізація координаційних механізмів у протидії гібридним загрозам в Україні відбувається в умовах повномасштабного російського вторгнення, що розпочалося 24 лютого 2022 року і суттєво трансформувало систему взаємодії органів влади різних рівнів. Воєнний стан, запроваджений в Україні з перших днів агресії, надав додаткові повноваження центральним органам влади та РНБО, водночас актуалізувавши необхідність оперативної координації з місцевим рівнем для забезпечення стійкості державних інституцій та критичної інфраструктури [50].

Попри об’єктивні складнощі, українська система публічного управління продемонструвала високий рівень адаптивності та здатності до швидкого реагування на безпрецедентні виклики, включаючи масовані кібератаки, дезінформаційні кімпанії, диверсійно-розвідувальну діяльність та фізичне знищення критичної інфраструктури.

Одним із ключових досягнень у сфері координації стало створення ефективної системи кіберзахисту, що базується на взаємодії державних органів, приватного сектору та міжнародних партнерів. Державна служба спеціального зв’язку та захисту інформації України (ДССЗЗІ), Служба безпеки України,

Національна поліція та інші суб’єкти забезпечення кібербезпеки під координацією НКЦК забезпечили відбиття тисяч кібератак, спрямованих на критичну інфраструктуру, державні інформаційні системи та електронні послуги [29].

Досвід України у протидії кіберзагрозам визнано міжнародною спільнотою як унікальний та цінний для інших країн, що підтверджується активним залученням українських фахівців до міжнародних платформ обміну досвідом, зокрема в рамках співпраці з країнами ЄС та НАТО [37]. Щорічні командно-штабні навчання «Національна кіберготовність», які у 2024 році відбулися в четверте, стали важливим інструментом відпрацювання механізмів координованого реагування на складні кіберінциденти з залученням усіх ключових суб’єктів забезпечення кібербезпеки.

У сфері протидії дезінформації та інформаційним операціям також напрацьовано практичні механізми координації. Центр протидії дезінформації при РНБО здійснює моніторинг інформаційного простору, виявляє дезінформаційні наративи та координує комунікаційні зусилля різних відомств для їх спростування [58]. Взаємодія Центру з органами місцевого самоврядування, громадськими організаціями та медіа дозволяє оперативно реагувати на локальні дезінформаційні кімпанії, що можуть загрожувати суспільній злагоді та довірі до державних інституцій.

Важливим напрямом роботи є розробка та впровадження національної системи стратегічних комунікацій, яка передбачає координацію інформаційної діяльності всіх органів державної влади з метою формування єдиного наративу та протидії інформаційній агресії [45]. Водночас експерти зазначають, що не створено повною мірою дієвого механізму координації і взаємодії між усіма органами державної влади, залученими до протидії загрозам в інформаційній сфері, що знижує ефективність відповіді на системні інформаційні виклики.

Координація діяльності у сфері захисту критичної інфраструктури стала одним із найбільш складних викликів в умовах тривалих масованих ракетних та дронових ударів по енергетичній системі України. Кабінет Міністрів України,

реалізуючи координаційні функції, визначені Законом «Про критичну інфраструктуру», затвердив перелік об’єктів критичної інфраструктури та встановив вимоги до забезпечення їх безпеки та стійкості [65]. Місцеві державні адміністрації та органи місцевого самоврядування відіграють ключову роль у забезпеченні захисту об’єктів критичної інфраструктури на своїх територіях, координуючи дії енергетичних компаній, правоохоронних органів, аварійно-рятувальних служб. Проте дослідники відзначають, що на сьогодні не існує цілісної та ефективно діючої системи координації і контролю щодо захисту критичної інфраструктури, а покладання значних функцій на ДССЗЗІ без наділення її дієвими інструментами впливу на сили оборони ускладнює вирішення цієї проблеми [91].

Конкретним прикладом ефективної міжвідомчої координації на регіональному рівні може слугувати організація евакуації населення з прифронтових територій Харківської області у травні 2024 року під час активізації бойових дій. Харківська обласна військова адміністрація створила координаційний механізм, який об’єднав зусилля різних суб’єктів забезпечення безпеки та громадських організацій. За даними ГУ ДСНС у Харківській області, протягом травня-червня 2024 року було евакуйовано 25 546 осіб з населених пунктів 16 територіальних громад Богодухівського, Куп’янського, Ізюмського, Чугуївського та Харківського районів [88]. Процес координації передбачав чітке розмежування функцій між учасниками: Харківська ОВА визначала загальну стратегію та пріоритети евакуації, Національна поліція забезпечувала безпеку під час переміщення, ДСНС надавала транспорт та здійснювала безпосереднє супроводження евакуйованих, органи місцевого самоврядування формували списки осіб, які потребували евакуації, а волонтери Українського Червоного Хреста надавали гуманітарну допомогу та психологічну підтримку. Створення Харківського координаційного гуманітарного центру, що працював цілодобово за номером 0800 33 92 91, дозволило централізувати обробку звернень громадян та оперативно координувати дії різних служб.

Другим показовим прикладом є реалізація регіональної цільової програми

розвитку цивільного захисту Харківської області на 2024-2026 роки, затвердженої рішенням обласної ради від 23 грудня 2023 року [77]. Програма передбачає координацію діяльності обласних органів виконавчої влади, територіальних підрозділів центральних органів виконавчої влади та органів місцевого самоврядування у сфері протидії надзвичайним ситуаціям та забезпечення цивільного захисту населення.

Особливістю цієї програми є створення системи регулярних координаційних нарад за участю керівників профільних відомств, що дозволяє оперативно вирішувати питання міжвідомчої взаємодії при реагуванні на надзвичайні ситуації техногенного та природного характеру, а також на наслідки військових дій. Координаційний механізм програми включає щоквартальний моніторинг виконання заходів з обов’язковим звітуванням відповідальних виконавців перед обласною державною адміністрацією.

Ще один приклад стосується організації територіальної оборони Харківської області відповідно до обласної програми на 2022-2025 роки, затвердженої рішенням обласної ради від 16 лютого 2022 року [64]. Програма, фінансування якої за чотири роки становить понад 5,4 млрд гривень, передбачає координацію зусиль військових формувань, правоохоронних органів, органів державної влади та місцевого самоврядування у забезпеченні територіальної оборони регіону.

Механізм координації включає створення обласного та районних органів територіальної оборони, до складу яких входять представники Збройних Сил України, Національної гвардії, СБУ, Національної поліції, обласної та районних військових адміністрацій, органів місцевого самоврядування.

Практична реалізація програми засвідчила важливість регулярних координаційних нарад, спільних навчань підрозділів різної відомчої підпорядкованості, створення єдиних комунікаційних каналів для оперативного обміну інформацією про загрози (таблиця 2.2).

Таблиця 2.2 – Основні напрями практичної взаємодії органів влади у протидії гібридним загрозам

Напрям взаємодії	*Ключові суб'єкти*	*Форми координації*	*Досягнення*	*Проблемні аспекти*
Кібербезпека	ДССЗЗІ, СБУ, НП, НКЦК, приватний сектор	Оперативні штаби, навчання, обмін інформацією	Відбиття масованих кібератак, міжнародне визнання	Недостатня кіберграмотність на місцевому рівні
Протидія дезінформації	Центр протидії дезінформації, МІП, МЗС, ОМС	Моніторинг, спростування, стратегічні комунікації	Виявлення наративів, координація повідомлень	Брак єдиного механізму міжвідомчої координації
Захист критичної інфраструктури	КМУ, профільні міністерства, МДА, ОМС, оператори	Категоризація об'єктів, плани захисту, оперативне реагування	Затвердження переліків ОКІ, локалізація наслідків ударів	Відсутність цілісної системи координації
Територіальна оборона	МО, МВС, НГУ, МДА, ОМС, громадськість	Бригади ТрО, органи територіальної оборони, навчання	Створення системи ТрО, залучення громадян	Нерівномірність розвитку ТрО в регіонах
Управління кризами	РНБО, КМУ, МВС, ДСНС, МДА, ОМС	Ситуаційні центри, оперативні штаби, координаційні ради	Оперативне реагування, координація евакуації	Недосконалість механізмів кризового управління на місцях

Джерело: розробка автора.

У практиці взаємодії місцевих державних адміністрацій з органами місцевого самоврядування спостерігаються як позитивні тенденції, так і певні дисфункції. Децентралізація влади, що відбувалася до 2022 року, значно посилила спроможність територіальних громад самостійно вирішувати питання місцевого значення, включаючи аспекти безпеки громади [31]. В умовах воєнного стану багато громад продемонстрували високу здатність до самоорганізації, оперативного реагування на загрози, забезпечення життєдіяльності населення.

Водночас питання координації дій між МДА та ОМС у надзвичайних ситуаціях, розмежування відповідальності за виконання функцій з забезпечення

громадського порядку, захисту населення залишаються дискусійними. Законопроект №4298 «Про внесення змін до Закону України «Про місцеві державні адміністрації» щодо реформування територіальної організації виконавчої влади в Україні», який передбачає трансформацію МДА в органи префектурного типу з акцентом на наглядових та координаційних функціях, перебуває на розгляді Верховної Ради з 2020 року, що свідчить про складність пошуку оптимального балансу між державним контролем та місцевою автономією [34].

Важливим аспектом практичної взаємодії є фінансова спроможність місцевих органів влади забезпечувати заходи протидії гібридним загрозам. Аналіз виконання місцевих бюджетів за 2023-2024 роки засвідчує значні фінансові виклики, з якими зіткнулися територіальні громади в умовах війни. Так, вилучення військового ПДФО із місцевих бюджетів до спеціального фонду державного бюджету з 1 жовтня 2023 року призвело до різкого скорочення доходів громад, особливо тих, на території яких розташовані військові частини [56]. Зменшення фінансових ресурсів обмежує можливості громад інвестувати в системи відеоспостереження, засоби кіберзахисту, навчання персоналу, розбудову систем оповіщення населення про загрози.

Водночас деякі громади знаходять креативні рішення через залучення міжнародної технічної та фінансової допомоги, співпрацю з приватним сектором, міжмуніципальне співробітництво. Приклади успішної практики включають створення спільних центрів кібербезпеки кількома громадами, реалізацію проектів з підвищення енергонезалежності за підтримки міжнародних донорів, розбудову систем безпеки критичних об’єктів із залученням коштів місцевих бізнесів.

Координація діяльності силових структур на місцевому рівні також демонструє певну специфіку. Підрозділи Національної поліції, Національної гвардії, Служби безпеки України, що діють на територіях, підпорядковані своїм відомствам за вертикаллю, проте повинні координувати діяльність з місцевими органами влади при вирішенні питань забезпечення громадського порядку,

протидії диверсійно-розвідувальній діяльності, охорони критичних об’єктів. Створення обласних та районних координаційних центрів, до складу яких входять представники силових відомств, місцевих державних адміністрацій, органів місцевого самоврядування, сприяє оперативному обміну інформацією та узгодженню дій [11]. Однак брак чітких протоколів взаємодії, дублювання функцій різних відомств, недостатня поінформованість місцевої влади про оперативну обстановку іноді створюють перешкоди для ефективної координації.

До основних форм практичної взаємодії органів влади у протидії гібридним загрозам належать оперативні штаби та ситуаційні центри, які функціонують як постійно діючі або тимчасові органи для забезпечення координації дій у кризових ситуаціях, включаючи представників різних відомств та рівнів влади.

Важливу роль відіграють міжвідомчі координаційні ради та комісії як колегіальні органи для вироблення узгоджених рішень з питань безпеки, захисту критичної інфраструктури та протидії дезінформації. Практичні навички координованого реагування відпрацьовуються через командно-штабні навчання та тренування, призначені для відпрацювання процедур реагування на різні сценарії гібридних атак.

Електронні системи обміну інформацією представлені спеціалізованими платформами для оперативного обміну даними про загрози, інциденти та заходи реагування між різними органами. Для вирішення конкретних завдань створюються спільні оперативні групи як тимчасові міжвідомчі формування, зокрема для розслідування кіберінцидентів або локалізації наслідків диверсій. Регулярні координаційні наради керівників відомств та органів влади забезпечують систематичне обговорення поточної ситуації та узгодження планів дій.

Нарешті, спільні аналітичні центри функціонують як підрозділи для збору, аналізу та поширення інформації про гібридні загрози, включаючи кіберзагрози, дезінформацію та диверсійну діяльність.

Міжнародне співробітництво стало важливим чинником підвищення

ефективності координації протидії гібридним загрозам. Співпраця України з країнами НАТО та ЄС у рамках різноманітних програм та ініціатив дозволяє впроваджувати кращі практики, отримувати технічну допомогу, навчати фахівців. Зокрема, участь українських представників у роботі Європейського центру передового досвіду з протидії гібридним загрозам у Гельсінкі, організованого спільно країнами ЄС та НАТО, надає можливість вивчати досвід інших держав у координації протидії гібридним викликам [33].

Платформа Україна-НАТО з протидії гібридній війні, в рамках якої відбуваються регулярні консультації та обмін досвідом, сприяє вдосконаленню національних механізмів координації з урахуванням стандартів Альянсу [52]. Двостороннє співробітництво з окремими країнами-партнерами, зокрема США, Великою Британією, країнами Балтії, Польщею, також включає компоненти посилення координаційних спроможностей українських органів влади через надання консультативної підтримки, проведення спільних навчань, передачу технічних засобів.

Серед ключових проблем практичної координації варто виділити недостатню стандартизацію процедур, адже відсутність єдиних протоколів взаємодії між різними відомствами та рівнями влади при реагуванні на різні типи гібридних загроз створює неузгодженість у діях. Обмеженість інформаційного обміну проявляється через бар’єри для оперативного обміну розвідувальною та оперативною інформацією між відомствами внаслідок режимів секретності та відомчої закритості. Нерівномірність спроможностей виражається у суттєвих відмінностях у технічному оснащенні, кадровому потенціалі та фінансових ресурсах різних регіонів для протидії гібридним загрозам. Дублювання функцій призводить до паралельного виконання однакових завдань різними відомствами без належної координації, що спричиняє нераціональне використання ресурсів. Нарешті, недостатня інтеграція громадськості виявляється в обмеженому залученні громадських організацій, приватного сектору та експертного середовища до системи координації протидії гібридним загрозам.

Практика взаємодії у сфері територіальної оборони демонструє як успіхи,

так і виклики координації. Створення системи територіальної оборони України відповідно до Закону України «Про основи національного спротиву» від 16 червня 2021 року передбачає залучення широкого кола суб'єктів, включаючи підрозділи Збройних Сил України, Національної гвардії, інших військових формувань, правоохоронних органів, органів місцевого самоврядування, громадських об'єднань [68]. Координація діяльності усіх цих суб'єктів, організація взаємодії між військовими підрозділами територіальної оборони та цивільними органами влади, залучення добровольців вимагають чітких механізмів управління та координації. Створення у кожній області та в м. Києві відповідних органів територіальної оборони, які очолюють командувачі оперативних командувань та включають представників місцевих органів виконавчої влади, сприяє координації зусиль [62]. Проте практика засвідчує нерівномірність розвитку системи територіальної оборони в різних регіонах, залежність від активності місцевої влади та громадськості, що актуалізує необхідність більш директивних механізмів організації ТрО з боку центральних органів (таблиця 2.3).

Таблиця 2.3 – Порівняння досвіду координації протидії гібридним загрозам: Україна та країни НАТО

Критерій порівняння	*Україна*	*Країни НАТО (середнє)*	*Основні відмінності*
Нормативна база	Розвинута, але фрагментована	Комплексна, інтегрована	Потреба систематизації українського законодавства
Структура координації	РНБО, міжвідомчі органи	Спеціалізовані центри координації	Менша інституціоналізація в Україні
Роль місцевого рівня	Зростаюча через децентралізацію	Традиційно сильна	Швидка адаптація українських громад
Залучення приватного сектору	Зростаюче, але епізодичне	Систематичне, інституціоналізоване	Необхідність формалізації державно-приватного партнерства
Міжнародна співпраця	Інтенсивна, прагматична	Сталі інституційні механізми	Більша гнучкість та адаптивність українського підходу

Джерело: розробка автора.

Аналіз практики реагування на конкретні гібридні загрози дозволяє виявити як успішні кейси координації, так і прорахунки. Наприклад, координоване реагування на масовані кібератаки у перші дні повномасштабного вторгнення, коли ДССЗЗІ, СБУ, приватні кіберкомпанії, міжнародні партнери спільними зусиллями забезпечили захист критичних державних інформаційних систем, демонструє ефективність координаційних механізмів за умови чіткого розуміння ролей та завдань кожного суб'єкта [6]. Водночас, поодинокі випадки затримок у реагуванні на локальні кризові ситуації через неузгодженість дій різних відомств або нечіткість розподілу повноважень між державними та місцевими органами свідчать про необхідність вдосконалення координаційних процедур. Запровадження практики аналізу після дії (After Action Review) для кожного значного інциденту, пов'язаного з гібридними загрозами, могло б сприяти систематичному виявленню та усуненню дисфункцій у координації.

Роль громадськості та волонтерського руху у протидії гібридним загрозам також заслуговує на окрему увагу. Українське громадянське суспільство продемонструвало високий рівень згуртованості та готовності до співпраці з державними органами у забезпеченні безпеки та оборони держави. Волонтерські організації, громадські об'єднання, окремі активісти суттєво доповнюють зусилля офіційних структур у моніторингу інформаційного простору, виявленні дезінформації, протидії диверсійно-розвідувальній діяльності, забезпеченні кіберзахисту [42]. Водночас питання координації діяльності численних волонтерських ініціатив, інтеграції їх зусиль у загальнодержавну систему протидії гібридним загрозам, забезпечення правової та фінансової підтримки з боку держави залишаються актуальними. Створення формалізованих механізмів державно-громадського партнерства у сфері безпеки, включаючи можливість надання волонтерським організаціям статусу суб'єктів, які сприяють забезпеченню національної безпеки, могло б сприяти більш ефективній координації та використанню потенціалу громадянського суспільства.

Перспективи розвитку практики координації визначаються кількома факторами. По-перше, продовження процесу цифровізації публічного

управління створює нові можливості для координації через запровадження інтегрованих електронних систем, що дозволяють в режимі реального часу обмінюватися інформацією, координувати дії, моніторити виконання завдань.

По-друге, поглиблення співпраці з НАТО та ЄС в контексті євроатлантичної інтеграції України сприяє імплементації міжнародних стандартів координації та розбудові відповідних інституційних спроможностей.

По-третє, досвід, набутий в умовах протидії повномасштабній агресії, формує унікальну практику, яка після ретельного аналізу та інституціоналізації може стати основою для побудови сучасної ефективної системи координації протидії гібридним загрозам.

По-четверте, продовження реформи децентралізації та переформатування місцевих державних адміністрацій в органи префектурного типу потребуватиме перегляду координаційних механізмів з урахуванням нового розподілу повноважень та відповідальності.

Аналіз досвіду Харківської області як прифронтового регіону дозволяє виокремити як позитивні практики координації, так і проблемні аспекти, що потребують вирішення. До позитивних напрацювань можна віднести створення дієвих координаційних центрів з чіткими алгоритмами взаємодії різних відомств, ефективне залучення громадських організацій до виконання державних функцій, оперативність прийняття рішень в умовах швидкозмінної ситуації, високий рівень довіри населення до місцевої влади завдяки прозорості дій. Зокрема, досвід створення Харківського координаційного гуманітарного центру довів ефективність централізованого підходу до обробки звернень громадян та координації дій різних служб. Міжвідомчі координаційні штаби, що включають представників усіх ключових суб’єктів забезпечення безпеки, дозволили уникнути дублювання функцій та оптимізувати використання обмежених ресурсів.

Водночас практика виявила низку проблемних аспектів координації. По-перше, недостатня формалізація механізмів міжвідомчої взаємодії призводить до того, що ефективність координації значною мірою залежить від особистих

контактів та ініціативності окремих керівників, а не від чітко прописаних процедур. По-друге, спостерігається певна неузгодженість у плануванні заходів різними відомствами, коли обласні програми територіальної оборони та цивільного захисту розробляються паралельно без належної координації на етапі планування. По-третє, обмеженість фінансових ресурсів місцевих бюджетів в умовах війни змушує органи місцевого самоврядування конкурувати за державне фінансування замість консолідації зусиль. По-четверте, недостатньо розвинена система оперативного інформаційного обміну між різними рівнями влади, що іноді призводить до затримок у прийнятті рішень або дублювання дій.

Для усунення виявлених недоліків доцільно запровадити кілька інституційних та організаційних новацій. Насамперед, необхідно розробити та затвердити на рівні Кабінету Міністрів України стандартні протоколи міжвідомчої взаємодії при реагуванні на різні типи надзвичайних ситуацій та гібридних загроз, які б визначали чіткі ролі, відповідальність та алгоритми дій кожного суб’єкта. Ці протоколи мають бути адаптовані до специфіки прифронтових регіонів з урахуванням досвіду Харківської, Донецької, Запорізької та інших областей.

По-друге, доцільно запровадити обов’язкове узгодження всіх обласних цільових програм у сфері безпеки та оборони на етапі їх розробки через спеціально створений координаційний орган при обласній військовій адміністрації, що дозволить забезпечити синергію різних програм та уникнути неузгодженості цілей.

По-третє, необхідно створити єдину інформаційну платформу регіонального рівня для оперативного обміну даними між різними відомствами та рівнями влади, забезпечивши при цьому належний рівень кібербезпеки та розмежування доступу до інформації різного ступеня секретності.

По-четверте, варто запровадити практику регулярного аналізу після дії для кожного значного інциденту з обов’язковою участю всіх суб’єктів, залучених до реагування, що дозволить систематично виявляти та усувати дисфункції в координації, а також поширювати кращі практики.

Отже, практика взаємодії різних рівнів влади у відповідь на гібридні виклики в Україні демонструє як значні досягнення, так і проблемні аспекти. До основних досягнень належать: створення ефективної системи кіберзахисту з координацією державних та приватних суб'єктів; розбудова механізмів протидії дезінформації через Центр протидії дезінформації та систему стратегічних комунікацій; високий рівень адаптивності місцевих органів влади до нових викликів; активне міжнародне співробітництво та впровадження кращих практик; залучення громадянського суспільства до протидії гібридним загрозам.

Серед основних проблем виділяються: недостатня стандартизація процедур міжвідомчої та міжрівневої координації; обмеженість інформаційного обміну через відомчі бар'єри; нерівномірність спроможностей різних регіонів; певні прогалини у фінансовому забезпеченні заходів протидії на місцевому рівні; необхідність чіткішого розмежування повноважень між державними та місцевими органами влади.

Подальший розвиток практики координації потребує системної роботи з інституціоналізації успішних механізмів, усунення виявлених дисфункцій, посилення спроможностей усіх рівнів влади до координованої протидії гібридним загрозам.

Підбиваючи підсумок зазначимо, що аналіз практики взаємодії органів влади різних рівнів у протидії гібридним загрозам засвідчує формування в Україні дієвої, хоча й не позбавленої недоліків, системи координації. В умовах повномасштабного вторгнення українські органи влади продемонстрували здатність до швидкої адаптації та ефективної координації при відбитті масованих кібератак, протидії дезінформації, захисті критичної інфраструктури.

Ключовими досягненнями є створення спеціалізованих координаційних органів (НКЦК, Центр протидії дезінформації), налагодження оперативної взаємодії між державними органами та приватним сектором, активне міжнародне співробітництво.

Водночас виявлено низку проблем: недостатня стандартизація координаційних процедур, обмеженість інформаційного обміну, нерівномірність

спроможностей регіонів, неповне використання потенціалу місцевого самоврядування та громадянського суспільства. Усунення цих недоліків потребує подальшого вдосконалення нормативної бази, розбудови інституційних спроможностей, систематизації успішних практик та їх інституціоналізації.

РОЗДІЛ 3
ПЕРСПЕКТИВИ УДОСКОНАЛЕННЯ КООРДИНАЦІЙНОЇ ДІЯЛЬНОСТІ ОРГАНІВ ВЛАДИ У ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

3.1 Оцінка ефективності інституційних механізмів координації та виявлення проблемних зон

Оцінювання ефективності інституційних механізмів координації у протидії гібридним загрозам вимагає комплексного підходу, який враховує як кількісні, так і якісні параметри функціонування системи публічного управління. На мій погляд, фундаментальною проблемою сучасних підходів до оцінки ефективності координації в Україні є відсутність єдиної методології, яка б дозволила системно аналізувати міжвідомчу та міжрівневу взаємодію у сфері національної безпеки.

Постанова Кабінету Міністрів України від 24 січня 2020 року №35 запровадила моніторинг та оцінку ефективності діяльності голів обласних державних адміністрацій [63], проте ці інструменти сфокусовані переважно на соціально-економічних показниках розвитку регіонів, а не на спроможності координувати протидію гібридним загрозам.

Для об’єктивної оцінки ефективності координаційних механізмів доцільно застосовувати декілька взаємопов’язаних критеріїв. По-перше, критерій оперативності реагування, який визначає швидкість прийняття узгоджених рішень різними відомствами та рівнями влади у відповідь на виявлені гібридні загрози. Досвід евакуації населення з Харківської області у травні 2024 року засвідчив, що за наявності чітких алгоритмів взаємодії можливо протягом двох діб евакуювати понад чотири тисячі осіб із зони активних бойових дій [88]. Це свідчить про високу оперативність координації на регіональному рівні, проте такі успішні кейси залишаються радше винятком, аніж правилом.

По-друге, критерій повноти охоплення загроз, який відображає здатність координаційної системи реагувати на весь спектр гібридних викликів - від кібератак до дезінформаційних компаній, від диверсійної діяльності до економічного тиску. Аналіз діяльності Національного координаційного центру кібербезпеки свідчить про досягнення значних результатів у координації протидії кіберзагрозам, що підтверджується успішним відбиттям масованих кібератак на державні інформаційні системи з початку повномасштабного вторгнення [29]. Водночас, як зазначають експерти, в Україні не створено дієвого механізму координації і взаємодії між усіма органами державної влади, залученими до протидії загрозам в інформаційній сфері [71], що обмежує повноту охоплення інформаційних загроз координаційними механізмами.

По-третє, критерій ресурсної ефективності координації, який характеризує співвідношення досягнутих результатів до витрачених ресурсів, включаючи фінансові, людські, часові, інформаційні. Створення Харківського координаційного гуманітарного центру, що працював за єдиним номером гарячої лінії, дозволило оптимізувати використання обмежених ресурсів різних служб та уникнути дублювання функцій [51]. Це яскравий приклад ресурсно-ефективної координації, коли централізація обробки звернень громадян дозволила мінімізувати витрати та максимізувати результат.

По-четверте, критерій стійкості координаційних зв’язків, який визначає здатність системи координації функціонувати в умовах кризових ситуацій, зростаючого навантаження, виходу з ладу окремих елементів. Досвід функціонування Регіональної програми розвитку цивільного захисту Харківської області на 2024-2026 роки демонструє створення достатньо стійкої системи координації, яка забезпечує регулярні координаційні наради та моніторинг виконання заходів навіть в умовах постійних обстрілів прифронтової території [77]. Однак залежність ефективності координації від особистих контактів та ініціативності окремих керівників знижує загальну стійкість системи.

По-п’яте, критерій адаптивності координаційних механізмів, який

характеризує здатність системи швидко пристосовуватися до нових типів загроз та змінюваних умов безпекового середовища. Трансформація координаційних механізмів у відповідь на повномасштабне вторгнення продемонструвала високу адаптивність української системи публічного управління. Зокрема, швидке створення Центру протидії дезінформації при РНБО у 2021 році та його оперативне реагування на масові дезінформаційні кампанії з початку війни засвідчили здатність інституційної системи адаптуватися до нових викликів [75].

Застосовуючи ці критерії до аналізу існуючої системи координації, можна виокремити низку проблемних зон, що потребують невідкладного вирішення. *Першою проблемною зоною є фрагментарність нормативно-правового регулювання координації у сфері протидії гібридним загрозам.* Попри наявність базових законодавчих актів, таких як Закон України «Про національну безпеку України», відсутні спеціалізовані підзаконні акти, які б детально регламентували процедури міжвідомчої взаємодії при реагуванні на конкретні типи гібридних загроз. Кожне відомство діє переважно на основі власних відомчих інструкцій, що призводить до неузгодженості дій та втрати часу на узгодження процедур у критичних ситуаціях.

Другою проблемною зоною є асиметрія інформаційного обміну між різними рівнями влади та відомствами. Обмеження доступу до класифікованої інформації, відомча закритість, відсутність єдиних інформаційних платформ створюють бар’єри для оперативної координації. Аналіз функціонування системи захисту критичної інфраструктури виявив, що місцеві органи влади часто не володіють повною інформацією про загрози об’єктам критичної інфраструктури на своїх територіях, що унеможливлює ефективне планування заходів реагування [91]. Водночас центральні органи влади іноді не отримують своєчасної інформації про інциденти на місцевому рівні через недосконалість каналів звітності.

Третьою проблемною зоною є дисбаланс спроможностей різних регіонів до координованої протидії гібридним загрозам. Прифронтові області, такі як Харківська, Донецька, Запорізька, накопичили значний досвід координації в

умовах активних бойових дій, тоді як віддалені від лінії фронту регіони мають обмежену практику такої координації. Це створює ризики неадекватного реагування у випадку розширення географії гібридних загроз. Відсутність системного поширення кращих практик регіональної координації між областями зменшує загальну спроможність країни до протидії гібридним викликам.

Четвертою проблемною зоною є недостатня інтеграція недержавних акторів у систему координації. Попри значний внесок громадських організацій, волонтерських рухів, приватного сектору у протидію гібридним загрозам, механізми їх формальної інтеграції у систему державної координації залишаються недорозвиненими. Як зазначають дослідники, Україна, на відміну від країн НАТО, не створила систематичних інституціоналізованих механізмів державно-приватного партнерства у сфері кібербезпеки та протидії дезінформації [79]. Епізодичність залучення недержавних акторів знижує ефективність використання їхнього потенціалу.

П'ятою проблемною зоною є обмеженість ресурсного забезпечення координаційної діяльності на місцевому рівні. Вилучення військового ПДФО з місцевих бюджетів з 1 жовтня 2023 року призвело до різкого скорочення доходів територіальних громад, особливо тих, на території яких розташовані військові частини [56]. Це обмежило можливості органів місцевого самоврядування інвестувати в системи моніторингу загроз, технічне оснащення координаційних центрів, навчання персоналу. Недостатність фінансування на місцевому рівні створює диспропорцію між завданнями, покладеними на місцеві органи влади у сфері протидії гібридним загрозам, та їхніми реальними можливостями.

Шостою проблемною зоною є недосконалість механізмів моніторингу та оцінки ефективності координаційної діяльності. Відсутність чітких індикаторів ефективності координації, регулярного збору та аналізу відповідних даних ускладнює виявлення дисфункцій та вжиття коригувальних заходів. Постанова КМУ №35 від 24 січня 2020 року запровадила моніторинг діяльності голів облдержадміністрацій, проте цей інструмент не охоплює оцінку ефективності міжвідомчої координації у протидії гібридним загрозам [90]. Без систематичної

оцінки неможливо об’єктивно визначити, які координаційні практики є успішними та потребують поширення, а які виявилися неефективними.

Конкретним прикладом проблемної зони координації може слугувати ситуація із захистом критичної інфраструктури енергетичного сектору. Незважаючи на прийняття Закону України «Про критичну інфраструктуру» у листопаді 2021 року [65], до початку масованих ракетних ударів по енергетичній системі восени 2022 року не було створено ефективної системи координації між Міністерством енергетики, ДССЗЗІ, силовими відомствами, операторами енергетичної інфраструктури та місцевими органами влади. Як наслідок, реагування на перші масовані атаки характеризувалося певною неузгодженістю дій, хоча надалі координація значно покращилася завдяки створенню оперативних штабів та запровадженню процедур оперативної взаємодії.

Іншим прикладом проблемної координації є протидія дезінформаційним кампаніям на регіональному рівні. Центр протидії дезінформації при РНБО здійснює моніторинг інформаційного простору на національному рівні, проте координація його діяльності з регіональними органами влади, які мають кращі можливості для оперативного спростування локальних дезінформаційних наративів, залишається недостатньою [58]. Відсутність стандартизованих протоколів взаємодії призводить до того, що місцеві органи влади іноді дізнаються про дезінформаційні кампанії, спрямовані проти їхніх регіонів, із затримкою, коли ефективність спростування вже знижена.

Третім прикладом є координація територіальної оборони, де, попри прийняття Закону «Про основи національного спротиву» у червні 2021 року [68] та створення відповідних структур, залишаються питання узгодженості дій між підрозділами Збройних Сил України, Національної гвардії, інших військових формувань та органів місцевого самоврядування. Обласна програма розвитку територіальної оборони Харківської області на 2022-2025 роки передбачає координацію зусиль різних суб’єктів [64], проте практична реалізація виявила потребу у більш чітких механізмах оперативної взаємодії, особливо в ситуаціях швидкозмінної оперативної обстановки.

Аналізуючи виявлені проблемні зони через призму міжнародного досвіду, варто зазначити, що країни НАТО та ЄС також стикалися з подібними викликами координації у протидії гібридним загрозам. Європейський центр передового досвіду з протидії гібридним загрозам у Гельсінкі був створений саме для сприяння координації між країнами ЄС та НАТО у цій сфері [84]. Досвід роботи цього Центру засвідчив, що ключовими елементами успішної координації є регулярний обмін інформацією, спільні навчання, розробка стандартизованих процедур взаємодії та створення спільних аналітичних платформ. Україна, хоча і співпрацює з цим Центром, ще не імплементувала повною мірою напрацьовані ним методології координації.

Оцінка ефективності існуючих координаційних механізмів за сукупністю застосованих критеріїв дозволяє констатувати, що українська система координації у протидії гібридним загрозам демонструє високу оперативність та адаптивність, але водночас характеризується недостатньою стійкістю, неповним охопленням загроз та субоптимальною ресурсною ефективністю.

Виявлені проблемні зони вимагають системної роботи з удосконалення як нормативно-правової бази координації, так і практичних механізмів міжвідомчої та міжрівневої взаємодії. Перехід від реактивної моделі координації, коли механізми взаємодії напрацьовуються у відповідь на вже виявлені дисфункції, до проактивної моделі, яка передбачає систематичне вдосконалення координації на основі аналізу потенційних загроз та кращих практик, є стратегічним завданням для України на шляху до створення ефективної системи протидії гібридним загрозам.

Тож, резюмуючи зазначимо, що оцінка ефективності інституційних механізмів координації у протидії гібридним загрозам на основі комплексного застосування критеріїв оперативності, повноти охоплення, ресурсної ефективності, стійкості та адаптивності виявила низку проблемних зон, що потребують системного вирішення.

До ключових проблем належать фрагментарність нормативного регулювання, асиметрія інформаційного обміну, дисбаланс спроможностей

регіонів, недостатня інтеграція недержавних акторів, обмеженість ресурсного забезпечення місцевого рівня та відсутність систематичного моніторингу ефективності координації. Конкретні приклади з практики захисту критичної інфраструктури, протидії дезінформації та організації територіальної оборони демонструють, що виявлені проблеми не є абстрактними, а мають безпосередній вплив на ефективність протидії гібридним загрозам.

3.2 Рекомендації щодо оптимізації взаємодії центральних та місцевих органів влади в умовах гібридних загроз

Узагальнюючи результати аналізу інституційних механізмів координації та виявлених проблемних зон, вважаємо за доцільне сформулювати комплекс рекомендацій щодо оптимізації взаємодії центральних та місцевих органів влади у протидії гібридним загрозам. Ці рекомендації базуються на критичному осмисленні як вітчизняного досвіду, так і кращих практик країн НАТО та ЄС, адаптованих до специфіки українського контексту.

Фундаментальною основою для вдосконалення координації має стати розробка та затвердження постановою Кабінету Міністрів України Єдиного порядку координації діяльності органів виконавчої влади та органів місцевого самоврядування у протидії гібридним загрозам. Цей документ має визначити чіткі ролі та відповідальність кожного суб'єкта координації, встановити стандартизовані процедури міжвідомчої взаємодії для різних типів гібридних загроз, регламентувати механізми оперативного обміну інформацією, порядок створення та функціонування координаційних штабів на національному, регіональному та місцевому рівнях.

На нашу думку, саме відсутність такого базового документу є основною причиною багатьох координаційних дисфункцій, оскільки кожне відомство інтерпретує свої координаційні функції по-різному. Важливо, щоб Єдиний

порядок передбачав диференційований підхід до координації залежно від типу гібридної загрози, адже координація протидії кібератакам потребує значно вищої оперативності та технічної спеціалізації, ніж координація протидії дезінформаційним компаніям.

Паралельно з нормативним удосконаленням необхідно створити потужну технологічну інфраструктуру координації через запровадження Національної платформи координації протидії гібридним загрозам як інтегрованої інформаційно-аналітичної системи, що об'єднає всіх суб’єктів забезпечення національної безпеки. Ця платформа має функціонувати на базі сучасних хмарних технологій з належним рівнем кібербезпеки та диференційованим доступом до інформації різного ступеня секретності. Платформа повинна забезпечувати оперативний обмін інформацією про виявлені загрози, інциденти, заходи реагування, моніторинг виконання узгоджених рішень, спільний аналіз ситуації та прогнозування розвитку загроз, зберігання та систематизацію кращих практик координації. Створення такої платформи потребуватиме значних фінансових інвестицій, однак економічний ефект від оптимізації координації значно перевищить витрати, що підтверджується досвідом країн Балтії, які після подій 2007-2008 років створили інтегровані системи координації [86].

Ефективність координації значною мірою залежить від людського чинника, тому вважаю необхідним запровадити інститут регіональних координаторів з питань протидії гібридним загрозам при обласних державних адміністраціях. Ці посадові особи мають бути наділені повноваженнями координувати діяльність територіальних підрозділів центральних органів виконавчої влади, органів місцевого самоврядування, правоохоронних органів на території області у сфері протидії гібридним загрозам. Регіональні координатори повинні підпорядковуватися безпосередньо голові обласної державної адміністрації та мати функціональний зв'язок з РНБО України, що забезпечить поєднання вертикальної та горизонтальної координації. Функціями регіональних координаторів мають бути організація регулярних координаційних нарад, моніторинг виконання національних стратегій на регіональному рівні,

координація реагування на гібридні інциденти, аналіз регіональних особливостей загроз та сприяння обміну кращими практиками між територіальними громадами.

Водночас призначення координаторів буде неефективним без належної підготовки фахівців, тому необхідно розбудувати систему безперервної професійної підготовки фахівців з координації у сфері протидії гібридним загрозам. Наразі в Україні відсутні спеціалізовані навчальні програми, які б готували фахівців саме з координаційної діяльності у сфері національної безпеки. Пропоную створити при ННІ «Інститут державного управління» Харківського національного університету імені В.Н. Каразіна спеціалізований навчальний центр, який би здійснював підготовку та підвищення кваліфікації посадових осіб усіх рівнів влади з питань координації протидії гібридним загрозам, а також ветеранів війни, готових прийти на публічні посади відбудовувати країні після війни (в тому числі за кошти державного бюджету). Навчальні програми центру мають включати модулі з теорії та практики координації, міжнародного досвіду, інформаційних технологій, кризового управління, стратегічних комунікацій, з особливою увагою до практичних навчань із застосуванням симуляцій різних сценаріїв гібридних загроз.

Не менш важливим є розширення кола учасників координації через інституціоналізацію механізмів державно-приватного партнерства у сфері протидії гібридним загрозам. Вважаю за доцільне внести зміни до Закону України «Про національну безпеку України», якими передбачити можливість надання статусу учасників системи забезпечення національної безпеки приватним компаніям, які надають критично важливі послуги у сфері кібербезпеки, телекомунікацій, енергетики, транспорту. Такий статус має супроводжуватися як додатковими обов’язками щодо співпраці з державними органами, так і певними преференціями, зокрема пріоритетним доступом до державних контрактів та інформаційної підтримки.

Для координації державно-приватного партнерства доцільно створити при РНБО України Раду з питань державно-приватного партнерства у сфері

національної безпеки, до складу якої увійдуть представники ключових державних органів та провідних приватних компаній. Досвід країн НАТО засвідчує, що ефективна протидія кіберзагрозам неможлива без тісної співпраці держави з приватними ІТ-компаніями [36].

Для постійного вдосконалення координаційних практик необхідно запровадити обов’язкову практику аналізу після дії для всіх значних інцидентів, пов’язаних з гібридними загрозами. Кожен випадок кібератаки на критичну інфраструктуру, масована дезінформаційна кампанія, диверсійна акція повинні супроводжуватися детальним аналізом ефективності координації реагування з обов’язковою участю всіх залучених суб'єктів. Результати такого аналізу мають документуватися у стандартизованій формі та передаватися до РНБО України для узагальнення та розробки рекомендацій щодо вдосконалення координаційних процедур. Систематичний аналіз дозволить виявляти повторювані проблеми координації, накопичувати інституційну пам'ять про успішні та неуспішні практики, формувати доказову базу для коригування нормативних актів та процедур. Міністерство оборони України вже застосовує методологію аналізу після дії у військовій сфері [25], і цей досвід може бути адаптований для сфери протидії гібридним загрозам.

Ефективна координація неможлива без належного фінансового забезпечення, особливо на місцевому рівні, тому пропоную посилити фінансове забезпечення координаційної діяльності через створення спеціальної субвенції з державного бюджету місцевим бюджетам на заходи протидії гібридним загрозам. Обсяг цієї субвенції має визначатися на основі об’єктивних критеріїв, таких як близькість до лінії фронту, наявність об’єктів критичної інфраструктури, рівень виявлених гібридних загроз. Кошти субвенції повинні спрямовуватися на створення та оснащення координаційних центрів, закупівлю технічних засобів моніторингу та захисту, навчання персоналу, фінансування спільних з державними органами заходів.

Для забезпечення цільового використання необхідно запровадити чіткі вимоги до звітності органів місцевого самоврядування про витрачання коштів та

досягнуті результати. РНБО України спільно з Міністерством фінансів мають розробити методику розрахунку обсягів субвенції та критерії оцінки ефективності її використання.

Україна не може залишатися ізольованою у протидії гібридним загрозам, тому необхідно активізувати міжнародне співробітництво, зокрема через офіційне приєднання до Європейського центру передового досвіду з протидії гібридним загрозам у Гельсінкі. Наразі Україна співпрацює з цим Центром на основі окремих угод [89], однак повноправне членство надасть доступ до всіх розробок Центру, дозволить брати участь у формуванні порядку денного, залучати українських експертів до роботи над спільними проектами. Членство у Центрі також сприятиме імплементації європейських та натівських стандартів координації у вітчизняну практику.

Крім того, доцільно ініціювати створення регіонального мережевого центру з обміну досвідом протидії гібридним загрозам для країн Східної Європи за участю України, Польщі, країн Балтії, Молдови, Грузії. Такий центр міг би функціонувати на ротаційній основі та зосереджуватися на практичних аспектах координації, організації спільних навчань, обміні персоналом.

Для систематичної оцінки ефективності координації необхідно розробити та запровадити систему ключових індикаторів ефективності координації у протидії гібридним загрозам. РНБО України спільно з профільними міністерствами та відомствами має визначити набір кількісних та якісних індикаторів, які б дозволяли систематично оцінювати ефективність координаційних механізмів на національному, регіональному та місцевому рівнях. Такі індикатори мають включати середній час від виявлення загрози до початку координованих дій реагування, частку інцидентів де координація була визнана ефективною, рівень задоволеності суб'єктів координації якістю взаємодії, обсяг інформації якою обмінялися суб'єкти координації. Збір даних за цими індикаторами має здійснюватися регулярно, щонайменше щоквартально, з подальшим аналізом динаміки та виявленням проблемних аспектів. Результати моніторингу індикаторів повинні розглядатися на засіданнях РНБО України та

враховуватися при плануванні заходів з удосконалення координації.

Нарешті, для забезпечення об'єктивності оцінок та зовнішнього контролю необхідно створити механізм громадського моніторингу та оцінки ефективності координації органів влади у протидії гібридним загрозам через залучення незалежних експертів, представників громадянського суспільства, наукової спільноти до аналізу координаційної діяльності. Пропонуємо запровадити практику щорічної публікації Національного звіту про стан координації у протидії гібридним загрозам, який би готувався незалежною комісією за участю представників державних органів, громадських організацій, експертного середовища. Такий звіт має містити оцінку ефективності координаційних механізмів за минулий рік, аналіз кращих практик та виявлених проблем, конкретні рекомендації щодо вдосконалення координації. Публічність звіту сприятиме підвищенню відповідальності посадових осіб за якість координаційної діяльності, стимулюватиме обмін досвідом, залучатиме суспільну увагу до проблематики протидії гібридним загрозам.

Реалізація цих взаємопов'язаних рекомендацій потребуватиме політичної волі керівництва держави, консолідованих зусиль різних гілок влади, залучення значних ресурсів. Однак альтернативи системному вдосконаленню координації у протидії гібридним загрозам немає, оскільки від ефективності такої координації безпосередньо залежить національна безпека України. Вважаємо, що поетапна імплементація цих рекомендацій протягом 2025-2027 років дозволить створити в Україні одну з найбільш ефективних у Європі систем координації протидії гібридним загрозам, що базуватиметься як на унікальному вітчизняному досвіді протистояння масштабній гібридній агресії, так і на кращих міжнародних практиках.

Комплексний характер запропонованих заходів, що охоплюють нормативно-правові, організаційні, технологічні, кадрові, фінансові та міжнародні аспекти, забезпечить синергетичний ефект від їх реалізації та створить умови для якісного стрибка у розбудові спроможностей України до ефективної координованої протидії гібридним викликам.

Підсумуємо, що запропоновані рекомендації щодо оптимізації взаємодії центральних та місцевих органів влади у протидії гібридним загрозам охоплюють нормативно-правовий, організаційний, технологічний, кадровий, фінансовий та міжнародний аспекти координації.

Ключовими напрямами удосконалення є розробка єдиного порядку координації, створення національної інформаційної платформи, запровадження інституту регіональних координаторів, розбудова системи професійної підготовки фахівців, інституціоналізація державно-приватного партнерства, систематичний аналіз ефективності координації, посилення фінансового забезпечення місцевого рівня, активізація міжнародного співробітництва, запровадження системи індикаторів ефективності та створення механізмів громадського моніторингу. Комплексна реалізація цих рекомендацій дозволить суттєво підвищити ефективність координації та зміцнити спроможність України до протидії гібридним загрозам.

ВИСНОВКИ

За результатами дослідження сформульовано нижченаведені основні висновки та пропозиції:

1. Теоретико-методологічний аналіз координації діяльності органів влади у протидії гібридним загрозам виявляє багатовимірність та складність цього феномену, що вимагає міждисциплінарного підходу та синтезу теорій з різних наукових галузей. Гібридні загрози, що характеризуються одночасним використанням військових, економічних, інформаційних, кібернетичних та дипломатичних інструментів у скоординованій кампанії, вимагають відповідної координації зусиль численних державних органів, що традиційно функціонували у відокремлених секторальних сферах.

Концепція інституційної координації у публічному управлінні пропонує теоретичну рамку для розуміння механізмів узгодження дій різних організацій, проте класичні моделі ієрархічної, мережевої чи ринкової координації виявляються недостатніми для складності гібридних загроз, що вимагає гібридних організаційних рішень.

2. Компаративний аналіз міжнародного досвіду координації у країнах НАТО та ЄС демонструє різноманітність інституційних моделей, від централізованої президентської координації у США до децентралізованого whole-of-society підходу у Фінляндії, кожна з яких має специфічні переваги та обмеження. Ключовими принципами ефективної координації, що виявляються з міжнародного досвіду, є стратегічне керівництво на найвищому політичному рівні, формалізація механізмів міжвідомчої взаємодії, спільне ситуаційне усвідомлення через обмін інформацією, чіткий розподіл ролей та відповідальності, розвиток спроможностей місцевих органів влади, залучення недержавних акторів.

Для України критично важливим є адаптація міжнародних кращих практик до специфіки напівпрезидентської політичної системи, досвіду воєнного часу та

потреб посткризової трансформації з балансуванням між ефективністю координації та демократичною підзвітністю.

3. Комплексний інституційний аналіз механізмів координації центральних та місцевих органів влади у протидії гібридним загрозам в Україні дозволяє констатувати наступне. По-перше, в Україні сформовано базову нормативно-правову та організаційну систему координації, яка включає конституційні норми, спеціалізоване законодавство, стратегічні документи та підзаконні акти, що визначають повноваження та механізми взаємодії різних суб'єктів забезпечення національної безпеки. Ключову роль у цій системі відіграють РНБО як координаційний орган стратегічного рівня, спеціалізовані міжвідомчі структури (НКЦК, Центр протидії дезінформації), міністерства та відомства на центральному рівні, місцеві державні адміністрації та органи місцевого самоврядування на регіональному та локальному рівнях.

По-друге, практична реалізація координаційних механізмів в умовах повномасштабного російського вторгнення продемонструвала як значні досягнення української системи публічного управління у протидії гібридним загрозам, так і певні прогалини та дисфункції, що потребують усунення. До основних досягнень належать ефективна система кіберзахисту, механізми протидії дезінформації, високий рівень адаптивності та залучення міжнародної підтримки.

4. Серед проблем виділяються недостатня стандартизація процедур, обмеженість інформаційного обміну, нерівномірність спроможностей, неповне використання потенціалу децентралізації.

Подальший розвиток системи координації потребує комплексного підходу, що включає вдосконалення законодавства, розбудову інституційних спроможностей, посилення місцевого рівня, систематизацію та інституціоналізацію успішних практик, поглиблення міжнародного співробітництва.

Особливої уваги потребує розробка та впровадження стандартизованих процедур міжвідомчої та міжрівневої координації, створення інтегрованих

інформаційних систем, забезпечення належного фінансування заходів протидії гібридним загрозам на всіх рівнях, формалізація механізмів державно-приватного та державно-громадського партнерства у сфері безпеки. Реалізація цих завдань дозволить створити більш ефективну, стійку та адаптивну систему координації протидії гібридним загрозам, здатну адекватно реагувати на виклики сучасного безпекового середовища.

5. Комплексний аналіз перспектив удосконалення координаційної діяльності у протидії гібридним загрозам дозволяє констатувати наявність як значних досягнень української системи координації, так і низки проблемних зон, що потребують системного вирішення.

Оцінка ефективності інституційних механізмів координації на основі критеріїв оперативності, повноти охоплення, ресурсної ефективності, стійкості та адаптивності виявила шість ключових проблемних зон: фрагментарність нормативного регулювання, асиметрію інформаційного обміну, дисбаланс спроможностей регіонів, недостатню інтеграцію недержавних акторів, обмеженість ресурсного забезпечення та відсутність систематичного моніторингу ефективності.

6. Конкретні приклади проблемної координації у сферах захисту критичної інфраструктури, протидії дезінформації та організації територіальної оборони засвідчили практичний вплив виявлених дисфункцій на національну безпеку. Запропонований комплекс з десяти взаємопов’язаних рекомендацій охоплює всі ключові аспекти оптимізації координації - від нормативно-правового регулювання до міжнародного співробітництва. Особливу увагу приділено створенню інституційної та технологічної інфраструктури координації, розбудові кадрового потенціалу, забезпеченню належного фінансування та запровадженню механізмів систематичної оцінки ефективності.

Реалізація цих рекомендацій протягом найближчих років дозволить Україні побудувати одну з найбільш ефективних у Європі систем координації протидії гібридним загрозам, що базуватиметься на унікальному практичному досвіді та кращих міжнародних стандартах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bouckaert G., Peters B.G., Verhoest K. The Coordination of Public Sector Organizations: Shifting Patterns of Public Management. Basingstoke: Palgrave Macmillan, 2010. 266 p.

2. European Centre of Excellence for Countering Hybrid Threats. Annual Review 2023. Helsinki: Hybrid CoE, 2024. 52 p.

3. European Commission. Action Plan Against Disinformation. Brussels: European Commission, 2018. JOIN(2018) 36 final.

4. European Commission. Joint Framework on Countering Hybrid Threats: A European Union Response. Brussels: European Commission, 2016. JOIN(2016) 18 final.

5. Mintzberg H. Structure in Fives: Designing Effective Organizations. Englewood Cliffs, NJ: Prentice-Hall, 1983. 312 p.

6. National resilience of Ukraine: hybrid threats challenge response and prevention strategy: national report / Інститут політичних і етнонаціональних досліджень ім. І.Ф. Кураса НАН України. Київ, 2022. URL: https://ipiend.gov.ua/en/publication/national-resilience-of-ukraine-hybrid-threats-challenge-response-and-prevention-strategy-national-report/ (дата звернення: 09.10.2025).

7. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd edition. Cambridge: Cambridge University Press, 2017. 638 p.

8. NATO. Countering Hybrid Warfare. Brussels: NATO, 2020. 56 p.

9. Osborne S.P. The New Public Governance? *Public Management Review*. 2006. Vol. 8. No. 3. P. 377-387.

10. Peters B.G. Managing Horizontal Government: The Politics of Co-ordination. *Public Administration*. 1998. Vol. 76. No. 2. P. 295-311.

11. Risk and threat management coordination / UNDP Ukraine. 2020.

URL: https://www.ua.undp.org/content/ukraine/en/home/library/recovery-and-peace building/risk-and-threat-management-coordination.html (Last accessed: 09.10.2025).

12. Security Committee. Finland's Security Strategy. Helsinki: Security Committee, 2017. 87 p.

13. Thompson G., Frances J., Levačić R., Mitchell J. Markets, Hierarchies and Networks: The Coordination of Social Life. London: Sage, 1991. 296 p.

14. Wendt A. Social Theory of International Politics. Cambridge: Cambridge University Press, 1999. 429 p.

15. Аналіз місцевих бюджетів за 9 місяців 2024 року: як війна та бюджетні новації вплинули на місцеве самоврядування / Портал «Децентралізація». 2024. URL: https://decentralization.ua/news/18931 (дата звернення: 09.10.2025).

16. Бакуменко В.Д., Князєв В.М., Сурмін Ю.П. Методологія державного управління: словник-довідник. Київ: НАДУ, 2010. 252 с.

17. Батанов О.В. Муніципальна влада в Україні: проблеми теорії та практики. Київ: Видавництво «Юридична думка», 2010. 656 с.

18. Беглиця В.П., Жарков Я.М. Координація діяльності суб'єктів забезпечення національної безпеки. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2018. № 4. С. 27-33.

19. Білоус А.О. Місцеве самоврядування в Україні: проблеми і перспективи. Київ: Логос, 2010. 252 с.

20. Бодрук О.С. Координація діяльності органів виконавчої влади у сфері національної безпеки. *Вісник Національної академії державного управління при Президентові України*. 2015. № 4. С. 45-52.

21. Бориславська О.М., Заверуха І.Б., Захарченко Е.М. та ін. Децентралізація публічної влади: досвід європейських країн та перспективи України. Київ: Центр політико-правових реформ, 2012. 212 с.

22. Відносини з Україною / НАТО. 2024. URL: https://www.nato.int/ cps/uk/natohq/topics_37750.htm (дата звернення: 09.10.2025).

23. Власюк О.С. Національна безпека України: еволюція проблем

внутрішньої політики. Київ: НІСД, 2016. 528 с.

24. Власюк О.С., Кононенко С.В. Актуальні проблеми зовнішньої політики України. Київ: НІСД, 2010. 232 с.

25. Воєнні аспекти протидії «гібридній» агресії: досвід України : монографія / за заг. ред. А. М. Сиротенка. Київ : НУОУ ім. Івана Черняховського, 2020. 268 с. URL: https://nuou.org.ua/assets/monography/mono_gibr_viin.pdf (дата звернення: 09.10.2025).

26. Гай-Нижник П., Петров М. Імплементація міжнародного досвіду протидії гібридним загрозам в Україні. *Зовнішні справи*. 2020. № 7. С. 22-28.

27. Гай-Нижник П.П. Росія проти України (1990-2016 рр.): від політики шантажу і примусу до війни на поглинання та спроби знищення. Київ: МП Леся, 2017. 332 с.

28. Горбулін В.П. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. *Стратегічні пріоритети*. 2014. № 4(33). С. 5-12.

29. Демедюк С. Довіра та міжнародна співпраця - основа ефективної протидії кіберзагрозам / Рада національної безпеки і оборони України. 2023. URL: https://www.rnbo.gov.ua/ua/Diialnist/7067.html (дата звернення: 09.10.2025).

30. Децентралізація 2024: підсумки року / Портал «Децентралізація». 2024. URL: https://decentralization.gov.ua/news/19071 (дата звернення: 09.10.2025).

31. Децентралізація публічної влади в Україні: здобутки, проблеми та перспективи : матеріали V Міжнародної науково-практичної конференції (12 травня 2023 р., м. Львів) / за наук. ред. О.В. Батанова, Р.Б. Бедрія. Київ; Львів; Щецин : ЛНУ ім. Івана Франка, 2023. 208 с.

32. Євдокимов С.О. Сучасні системи захисту інформації. Київ : ФОП Гуляєва В.М., 2023. 380 с.

33. Європейський центр з протидії гібридним загрозам / Вікіпедія. URL: https://uk.wikipedia.org/wiki/Європейський_центр_з_протидії_гібридним_загрозам (дата звернення: 09.10.2025).

34. З’явився новий законопроєкт про переформатування місцевих

державних адміністрацій в органи префектурного типу / Портал «Децентралізація». 2025. URL: https://decentralization.gov.ua/news/19385 (дата звернення: 09.10.2025).

35. Зарубіжний досвід координації діяльності органів влади: уроки для України / за ред. В. Б. Авер'янова. Київ: Юрінком Інтер, 2008. 304 с.

36. Кібербезпека № 4/2024 : аналітичний дайджест / Інститут інформації, безпеки і права НАП України. Київ, 2024. 320 с. URL: https://ippi.org.ua/sites/default/files/2024-4.pdf (дата звернення: 09.10.2025).

37. Кібербезпека № 9/2023 : аналітичний дайджест / Інститут інформації, безпеки і права НАП України. Київ, 2023. 351 с. URL: https://ippi.org.ua/sites/default/files/2023-9.pdf (дата звернення: 09.10.2025).

38. Кібероборона, інформаційна стійкість та кібердипломатія: НКЦК провів командно-штабні навчання стратегічного рівня «Національна кіберготовність - 2024» / Рада національної безпеки і оборони України. 2024. URL: https://www.rnbo.gov.ua/ua/Diialnist/7086.html (дата звернення: 09.10.2025).

39. Клименко І.В., Линьов К.О. Проблеми координації у сфері національної безпеки України. *Актуальні проблеми державного управління*. 2016. № 2(50). С. 78-84.

40. Коваленко О.О. Координація органів влади у протидії гібридним загрозам: порівняльно-правовий аналіз. *Право і суспільство*. 2022. № 2. С. 112-119.

41. Комарова К.В. Інституційні механізми протидії гібридним загрозам у Європейському Союзі. *Актуальні проблеми міжнародних відносин*. 2019. Вип. 139. С. 98-110.

42. Конгрес сприяє відкритому врядуванню в Україні / Офіс Ради Європи в Україні. 2024. URL: https://www.coe.int/uk/web/kyiv/-/congress-fosters-open-government-in-ukraine (дата звернення: 09.10.2025).

43. Кондратьєва Н.Ю. Європейський досвід протидії гібридним загрозам: уроки для України. *Стратегічні пріоритети*. 2021. № 3-4(60-61). С. 78-89.

44. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 09.10.2025).

45. Користі О.Є., Свиридюк Н.П., Ковальчук Т.І. Оцінювання гібридних загроз та спроможностей протидії їм при формуванні стратегічних комунікацій. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2023. Вип. 77. Т. 2. С. 69-79. DOI: 10.24144/2307-3322.2023.77.2.11/

46. Куйбіда В.С., Білинська М.М., Петроє О.М. Децентралізація в Україні: законодавство, основні проблеми та шляхи їх розв'язання. Київ: ІКЦ «Легальний статус», 2018. 120 с.

47. Магда Є.В. Гібридна агресія Росії: уроки для Європи. Київ: Каламар, 2017. 268 с.

48. Мартинюк Р.С. Конституційні засади координації органів виконавчої влади в Україні. *Право і безпека*. 2020. № 2(77). С. 98-105.

49. Матвієнко О.В. Фінська модель комплексної безпеки: досвід для України. *Стратегічні пріоритети*. 2018. № 1(46). С. 67-74.

50. Місцеве самоврядування в Україні у 2024 р.: тенденції та перспективи розвитку / Law. State. Technology. 2024. URL: https://journals. politehnica.dp.ua/index.php/lst/article/view/650 (дата звернення: 09.10.2025).

51. На Харківщині триває евакуація людей / Харківська районна державна адміністрація. 2024. URL: https://khrda.gov.ua/news/1716229995/ (дата звернення: 09.10.2025).

52. НАТО збирає разом експертів з Молдови і України для посилення співробітництва у протидії гібридним загрозам / НАТО. 2023. URL: https://www.nato.int/cps/uk/natohq/news_220602.htm?selectedLocale=uk (дата звернення: 09.10.2025).

53. Новак А.В. Залучення громадянського суспільства до забезпечення національної безпеки. *Державне управління та місцеве самоврядування*. 2019. Вип. 3(42). С. 78-85.

54. Норкус Р., Зінченко О. Балтійський досвід протидії гібридним

загрозам для України. *Безпека і оборона*. 2019. № 2. С. 45-53.

55. Онищук Б.В. Децентралізація та регіональний розвиток в Україні: сучасний стан та перспективи. *Регіональна економіка*. 2020. № 1. С. 5-15.

56. Онищук І. Аналіз місцевих бюджетів за 9 місяців 2024 року: як війна та бюджетні новації вплинули на місцеве самоврядування / Портал «Децентралізація». 2024. URL: https://decentralization.ua/news/18931 (дата звернення: 09.10.2025).

57. Органи публічної влади як суб'єкти формування та реалізації політики національної безпеки в інформаційному просторі. *Наукові записки*. Серія: Право. 2024. URL: https://pravo.cusu.edu.ua/index.php/pravo/article/view/544 (дата звернення: 09.10.2025).

58. Офіційний сайт Центру протидії дезінформації при Раді національної безпеки та оборони України. URL: https://cpd.gov.ua (дата звернення: 09.10.2025).

59. Парахонський Б.О., Яворська Г.М. Онтологія війни і миру: безпека, стратегія, смисл. Київ: НІСД, 2019. 560 с.

60. Парубчак І.О., Сливка С.С. Конституційно-правові засади координації у сфері національної безпеки. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2021. Вип. 66. С. 123-129.

61. Петрик В.М. Досвід країн Балтії у протидії гібридним загрозам: імплікації для України. *Інформація і право*. 2019. № 2(29). С. 78-86.

62. Про Євроатлантичну Інтеграцію / Міністерство внутрішніх справ України. URL: https://mvs.gov.ua/ministry/projekti-mvs/jevroatlanticna-integraciya-ukrayini/pro-jevroatlanticnu-integraciyu-1 (дата звернення: 09.10.2025).

63. Про затвердження Порядку проведення моніторингу та оцінки ефективності діяльності голів обласних, Київської та Севастопольської міських державних адміністрацій : Постанова Кабінету Міністрів України від 24 січ. 2020 р. № 35. URL: https://zakon.rada.gov.ua/laws/show/35-2020-п (дата звернення: 09.10.2025).

64. Про затвердження Програми розвитку територіальної оборони

Харківської області на 2022-2025 роки : Рішення Харківської обласної ради від 16 лют. 2022 р. № 365-VIII (зі змінами). URL: https://oblrada-kharkiv.gov.ua/wp-content/uploads/2023/09/365-viii-ter-oborona_kodyfikacziya_stanom-na-09-sichnya.pdf (дата звернення: 09.10.2025).

65. Про критичну інфраструктуру : Закон України від 16 листоп. 2021 р. № 1882-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 09.10.2025).

66. Про місцеві державні адміністрації : Закон України від 9 квіт. 1999 р. № 586-XIV / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/586-14 (дата звернення: 09.10.2025).

67. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 09.10.2025).

68. Про основи національного спротиву : Закон України від 16 черв. 2021 р. № 1702-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1702-20 (дата звернення: 09.10.2025).

69. Про Раду національної безпеки і оборони України : Закон України від 5 берез. 1998 р. № 183/98-ВР / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/183/98-вр (дата звернення: 09.10.2025).

70. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14 верес. 2020 р. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 09.10.2025).

71. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки України» : Указ Президента України від 28 груд. 2021 р. № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 09.10.2025).

72. Про рішення Ради національної безпеки і оборони України від 30

грудня 2021 року «Про Стратегію протидії загрозам національній безпеці в інформаційній сфері» : Указ Президента України від 16 лют. 2022 р. № 56/2022. URL: https://www.president.gov.ua/documents/562022-41377 (дата звернення: 09.10.2025).

73. Про службу в органах місцевого самоврядування : Закон України від 2 трав. 2023 р. № 3077-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3077-20 (дата звернення: 09.10.2025).

74. Про схвалення Концепції реформування місцевого самоврядування та територіальної організації влади в Україні : Розпорядження Кабінету Міністрів України від 1 квіт. 2014 р. № 333-р. URL: https://zakon.rada.gov.ua/laws/show/333-2014-р (дата звернення: 09.10.2025).

75. Про Центр протидії дезінформації : Указ Президента України від 7 трав. 2021 р. № 187/2021. URL: https://zakon.rada.gov.ua/laws/show/187/2021 (дата звернення: 09.10.2025).

76. Про центральні органи виконавчої влади : Закон України від 17 берез. 2011 р. № 3166-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3166-17 (дата звернення: 09.10.2025).

77. Регіональна цільова Програма розвитку цивільного захисту Харківської області на 2024-2026 роки : Рішення Харківської обласної ради від 23 груд. 2023 р. № 729-VIII. URL: https://oblrada-kharkiv.gov.ua/program/regionalna-czilova-programa-rozvytku-czyvilnogo-zahystu-harkivskoyi-oblasti-na-2024-2026-roky/ (дата звернення: 09.10.2025).

78. Резнікова О.О., Цюкало В.Ю., Паливода В.О., Дрьомов С.В., Сьомін С. В. Забезпечення національної безпеки України: пріоритети та системні вразливості. Київ: НІСД, 2021. 92 с.

79. Розширення інструментарію НАТО з протидії гібридним загрозам / НАТО Ревю. 2021. URL: https://www.nato.int/docu/review/uk/articles/2021/03/19/rozshirennya-nstrumentaryu-nato-z-protid-gbridnim-zagrozam/index.html (дата звернення: 09.10.2025).

80. Семенченко А.І. Методологія стратегічного планування у сфері

державного управління забезпеченням національної безпеки України. Київ: НАДУ, 2008. 428 с.

81. Серьогін С.М., Липовська Н.А. Механізми координації органів місцевого самоврядування в умовах децентралізації. *Актуальні проблеми державного управління*. 2021. № 1(79). С. 56-63.

82. Ситник Г.П., Олуйко В.М., Вавринчук М.П. Національна безпека України: теорія і практика. Київ: Кондор, 2022. 616 с.

83. Ситник Г.П. Державне управління національною безпекою України: теорія і практика : монографія. Київ: Вид-во НАДУ, 2004. 408 с.

84. Співпраця заради протидії гібридним загрозам / НАТО Ревю. 2018. URL: https://www.nato.int/docu/review/uk/articles/2018/11/23/spvpratsya-zaradi-protid-gbridnim-zagrozam/index.html (дата звернення: 09.10.2025).

85. Сухоруков О.І. Фінський досвід забезпечення комплексної безпеки: можливості застосування в Україні. *Аналітична записка*. Київ: НІСД, 2018. 12 с.

86. Ткачук Т. Суб'єкти забезпечення інформаційної безпеки держави: функціональний аналіз. *Національний юридичний журнал: теорія і практика*. 2017. №6. Ч.2. С. 42-46.

87. Требін М.П. Гібридна війна як нова українська реальність. *Український соціум*. 2014. № 3(50). С. 113-127.

88. У 2024 році на Харківщині сапери ДСНС ліквідували понад 22 тисячі вибухонебезпечних предметів / Харківська обласна державна адміністрація. 2024. URL: https://kharkivoda.gov.ua/news/129882 (дата звернення: 09.10.2025).

89. Україна зацікавлена співпрацювати з Центром передового досвіду з протидії гібридним загрозам / Кабінет Міністрів України. 2020. URL: https://www.kmu.gov.ua/news/ukrayina-zacikavlena-spivpracyuvati-z-centrom-peredovogo-dosvidu-z-protidiyi-gibridnim-zagrozam-alina-frolova (дата звернення: 09.10.2025).

90. Що таке моніторинг та оцінка ефективності діяльності голів обласних державних адміністрацій / Кабінет Міністрів України. 2020. URL: https://www.kmu.gov.ua/diyalnist/regionalna-politika/monitoring-ta-ocinka-

efektivnosti-diyalnosti-goliv-oblasnih-ta-kiyivskoyi-miskoyi-derzhadministracij (дата звернення: 09.10.2025).

91. Як удосконалити захист об’єктів критичної інфраструктури України. *Оборонно-промисловий кур’єр*. 2023. URL: https://opk.com.ua/як-удосконалити-захист-обєктів-крит (дата звернення: 09.10.2025).