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

СИСТЕМА ЗАБЕЗПЕЧЕННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПРИКОРДОННИХ РЕГІОНІВ: КООРДИНАЦІЯ МІЖ ВІЙСЬКОВИМИ ТА ЦИВІЛЬНИМИ СТРУКТУРАМИ

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

Науковий керівник роботи:
кандидат наук з державного управління, доцент
_____ Наталія ГРИШИНА

Харків – 2025

ЗМІСТ

ВСТУП

Сучасний етап розвитку України характеризується безпрецедентними викликами безпекового, соціально-економічного та інституційного характеру, що безпосередньо впливають на функціонування держави та стійкість її критичної інфраструктури. Повномасштабна військова агресія проти України актуалізувала проблему забезпечення належного рівня захищеності критичної інфраструктури, зокрема в прикордонних регіонах, які є першою лінією зіткнення з військовими загрозами, диверсіями, ракетними ударами, кібератаками та іншими формами гібридного впливу. Знищення об'єктів критичної інфраструктури призводить до суттєвих порушень життєдіяльності населення, зниження обороноздатності, погіршення економічної ситуації, виникнення гуманітарних криз, що робить цю сферу стратегічною для національної безпеки.

В умовах воєнного стану особливого значення набуває ефективна координація між військовими адміністраціями, органами місцевого самоврядування, територіальними громадами, підрозділами Державної служби України з надзвичайних ситуацій, Національною поліцією, Службою безпеки України, операторами критичної інфраструктури та іншими цивільними структурами. Створення скоординованої міжвідомчої системи управління дає змогу не лише забезпечувати оперативне реагування на загрози, а й підвищувати стійкість критичної інфраструктури, моделювати ризики, запроваджувати превентивні заходи та мінімізувати можливі наслідки атак.

Разом із тим, наявні сьогодні моделі управління та взаємодії виявляють низку системних проблем: фрагментарність інформаційних потоків, недостатню узгодженість функцій та повноважень різних органів, відсутність єдиних стандартів оцінювання загроз, а також слабку інтеграцію військових і цивільних елементів у єдину систему кризового реагування. Особливо це стосується прикордонних

регіонів, де рівень ризику є найвищим, а навантаження на органи влади – максимальним.

У науковій літературі питання безпеки, державного управління у сфері критичної інфраструктури, цивільно-військової координації та управління ризиками отримали значний розвиток, однак дослідження саме системи забезпечення критичної інфраструктури прикордонних регіонів України є недостатньо комплексним.

Питанням публічного управління та національної безпеки присвячено праці Б. Бойка, М.Бортнікова, В. Ліпкана, О. Бєлова, Г. Ситника, В. Абрамова, які сформували фундаментальні підходи до побудови системи державної безпеки. Проблеми державного управління на регіональному рівні висвітлені у працях В. Ребкала, Н. Нижник, Т. Мотренка, О. Оболенського, В. Харченка, які розкривають ключові особливості взаємодії органів влади в умовах завдань підвищеної складності.

Питанням критичної інфраструктури присвячені дослідження О.Власюка, О.Суходолі, М. Ткачука, В. Гвоздя, О. Ольховського, а також праці зарубіжних фахівців – Р.Кука, М.Дункана, Т. Ріда, Дж.Левіна, які розглядають концепції resilience, багаторівневої взаємодії та управління ризиками.

Цивільно-військова координація, інтегроване реагування та моделі співпраці аналізуються у працях Л.Гуменюка, А. Колодія, О. Кілієвича, О.Кириленка, В.кучеренка, а також у дослідженнях НАТО та ЄС, присвячених підвищенню готовності держав до комплексних кризових ситуацій.

Попри таку увагу питання координації в умовах прикордонних регіонів України залишається вивченим лише частково. Відсутні цілісні моделі, які б інтегрували військові вимоги, цивільне управління, правові аспекти та реальні потреби громад, а також враховували виклики сучасної війни. У сукупності це доводить необхідність розроблення сучасних підходів до координації військових і цивільних структур, що забезпечить безперебійну роботу критичної

інфраструктури навіть у надзвичайних умовах. Особливо все вищезазначене актуальне для прикордоння України.

Метою кваліфікаційної роботи є обґрунтування підходів та вироблення практичних рекомендацій щодо вдосконалення координації військових і цивільних структур у забезпеченні стійкості критичної інфраструктури прикордонних регіонів України.

Для досягнення мети поставлено такі завдання:

1. Розкрити зміст поняття критичної інфраструктури та підходи до організації захисту й управління цією сферою.

2. Узагальнити нормативно-правове забезпечення захисту критичної інфраструктури в Україні

3. Дослідити особливості функціонування критичної інфраструктури прикордонних регіонів України.

4. Розглянути практики цивільно-військової взаємодії в умовах кризових ситуацій щодо забезпечння стійкості критичної інфраструктури.

5. Виявити ключові проблеми, бар’єри, дисфункції та ризики у сфері взаємодії.

6. Запропонувати практичні рекомендації щодо вдосконалення управління, цифровізації процесів та підвищення стійкості критичної інфрастуктури.

Об’єкт дослідження – система забезпечення критичної інфраструктури в прикордонних регіонах України.

Предмет дослідження – механізми координації військових і цивільних структур у забезпеченні стійкості критичної інфраструктури прикордонних регіонів України.

У роботі застосовано комплекс методів дослідження. Загальнонаукові методи: аналіз, синтез, індукція, дедукція, порівняння, узагальнення – для опрацювання теоретичних положень; системний аналіз – для розгляду критичної

інфраструктури як цілісної багаторівневої системи; структурно-функціональний метод – для визначення ролей та функцій органів влади, що взаємодіють.

Практична значущість отриманих результатів полягає у можливості їх використання органами військових адміністрацій, органами місцевого самоврядування, структурами ДСНС, СБУ, Національної поліції; операторами критичної інфраструктури для покращення взаємодії у забезпеченні стійкості критичної інфраструктури.

Рекомендації можуть бути застосовані при розробці регіональних планів цивільного захисту, створенні центрів координації реагування, вдосконаленні процедур взаємодії, модернізації інформаційних систем управління, підготовки кардів тощо .

Структура роботи

Магістерська робота складається зі вступу, трьох розділів, висновків, списку використаних джерел.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПРИКОРДОННИХ РЕГІОНІВ

1.1. Поняття та особливості критичної інфраструктури в умовах прикордонних територій

У науковому та нормативно-правовому дискурсі термін «критична інфраструктура» (далі – КІ) з'явився наприкінці XX століття як відповідь на ускладнення техногенних, соціальних і безпекових ризиків, що виникають у зв'язку з глобалізацією, технологічною залежністю та підвищенням уразливості державних систем. Первинно концепт виник у США після терактів 1990-х років і був закріплений у Presidential Decision Directive №63 (1998), де критичну інфраструктуру визначено як системи, ресурси та мережі, порушення яких може призвести до значних негативних наслідків для національної безпеки, економіки, охорони здоров'я або громадської безпеки.

У Європейському Союзі унормування поняття було здійснено в Директиві Ради ЄС 2008/114/ЄС щодо ідентифікації та захисту європейської критичної інфраструктури, де під КІ розуміють об'єкти, системи та їхні частини, які є життєво важливими для підтримки необхідних суспільних функцій.

В Україні поняття критичної інфраструктури набуло нормативного закріплення з ухваленням Закону України «Про критичну інфраструктуру» (2021), де визначено, що КІ – це об'єкти, системи та ресурси, які забезпечують функціонування життєво важливих процесів суспільства, економіки та держави, виведення з ладу яких може мати значні негативні наслідки для національної безпеки. Метою державної політики у сфері захисту критичної інфраструктури є забезпечення безпеки об'єктів критичної інфраструктури, запобігання проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури [10].

Науковці підкреслюють, що критична інфраструктура – це сукупність матеріальних і нематеріальних ресурсів, включно з:

- об’єктами транспорту, енергетики, водопостачання;
- цифровими мережами та інформаційними системами;
- системами охорони здоров’я;
- оборонними та безпековими структурами;
- логістичними мережами;
- соціальною інфраструктурою.

У сучасних дослідженнях наголошується, що поняття КІ постійно еволюціонує, набуваючи широкого міждисциплінарного виміру, оскільки поєднує інженерію, управління ризиками, національну безпеку, публічне управління та регіональні студії [32,33,34,37].

Особливої актуальності воно набуває в умовах прикордонних регіонів, де ризики та загрози значно підвищені через географічне розташування, близькість до зон бойових дій, інтенсивність транскордонних потоків, високий рівень контрабанди, нелегальної міграції, диверсійних загроз і можливих гібридних впливів.

Основні підходи до класифікації критичної інфраструктури

У науковій літературі та нормативно-правових актах найбільш поширеними є такі класифікації критичної інфраструктури:

1. За функціональним призначенням

1. Енергетична КІ – електростанції, мережі, підстанції, газопроводи, сховища палива.

2. Транспортна КІ – залізничні вузли, автошляхи міжнародного значення, порти, аеропорти.

3. Водна та комунальна КІ – водозабори, каналізаційні вузли, очисні споруди.

4. Цифрова та телекомунікаційна КІ – дата-центри, мережі зв’язку, інтернет-інфраструктура.

5. Медична та соціальна КІ – лікарні, центри екстреної допомоги.

6. Оборонна та безпекова КІ – військові об’єкти, склади боєприпасів, прикордонні підрозділи.

7. Фінансова КІ – платіжні системи, банки, резервні фінансові сховища.

8. Харчова та аграрна КІ – логістичні центри, елеватори, об’єкти продовольчого забезпечення.

Таблиця 1.1 – Класифікація критичної інфраструктури за функціональним призначенням та її характеристики

Категорія КІ	**Структурні елементи (підсистеми)**	**Основні функції**	**Ключові характеристики**	**Приклади об’єктів**
1. Інфраструктура життєзабезпечення	• Енергетика (електро-, газо-, тепло-) •Водопостачання та водовідведення • Харчова інфраструктура	Забезпечення базових життєвих потреб населення та функціонування всіх інститутів держави	Неперервність роботи Високий рівень уразливості до атак Критичність для виживання населення Можливість каскадних відмов	Електростанції, ТЕС, ГЕС, газогони, водогони, очисні споруди, логістичні харчові центри
2. Інфраструктура безпеки та оборони	• Військові об’єкти • Прикордонна інфраструктура • Цивільний захист	Оборона держави, контроль кордону, реагування на надзвичайні ситуації	Високий рівень секретності Прямий зв’язок з національною безпекою Вимога оперативного реагування	Прикордонні пункти пропуску, укріплення, військові штаби, сховища, системи оповіщення
3. Транспортно-логістична інфраструктура	• Автомобільні дороги • Залізничні шляхи	Забезпечення мобільності населення, переміщення	Висока територіальна протяжність Наявність	Автомагістралі, мости, аеропорти,

Категорія КІ	Структурні елементи (підсистеми)	Основні функції	Ключові характеристики	Приклади об’єктів
	• Аеропорти • Морські порти	товарів, військових та гуманітарних вантажів	критичних вузлів (мости, тунелі) Значний вплив на обороноздатність	залізничні вокзали, порти
4. Економічна інфраструктура	• Банківська система • Фінансові ринки • Промислові підприємства	Підтримання економічної стабільності та стратегічного виробництва	Висока значимість для національної економіки Уразливість до кібер- та фінансових атак	Банки, сховища цінностей, стратегічні заводи, нафтобази
5. Цифрова та комунікаційна інфраструктура	• Телекомунікації • Інтернет-мережі– • Центри обробки даних • Системи кібербезпеки	Забезпечення зв’язку, інформаційного обміну, цифрових сервісів	Невід’ємність від функціонування всіх секторів Критичність для державного управління Високий рівень кіберризиків	Мобільні оператори, серверні центри, дата-центри, оптоволоконні мережі
6. Соціальна інфраструктура	• Охорона здоров’я • Освіта • Соціальний захист	Забезпечення соціальної стабільності, підготовки кадрів та медичної безпеки	Високий соціальний вплив Важливість у кризових ситуаціях Залежність від інших секторів КІ	Лікарні, навчальні заклади, центри соціальної допомоги, мобільні медичні бригади

2. За рівнем критичності

У ЄС застосовують три рівні:

- національна критична інфраструктура,
- регіональна,
- локальна.

В Україні з 2023 року введена чотирирівнева система категоризації за ступенем впливу на безпеку.

1) загальнодержавний рівень, управління на якому здійснюється Кабінетом Міністрів України, уповноваженим органом у сфері захисту критичної інфраструктури України, органами державної влади відповідно до розподілу повноважень;

2) регіональний та галузевий рівні, управління на яких здійснюється центральними та місцевими органами виконавчої влади;

3) місцевий рівень, управління на якому здійснюється місцевими органами виконавчої влади (військово-цивільними адміністраціями - у разі створення), органами місцевого самоврядування в межах повноважень;

4) об'єктовий рівень, управління на якому здійснюється оператором критичної інфраструктури на підставі нормативно-правових та регуляторних актів у сфері захисту критичної інфраструктури (Закон.

3. За формою власності

- державна,
- комунальна,
- приватна,
- змішана.

4. За галузевою специфікою

Відповідно до Постанови КМУ №1109 визначено 17 секторів критичної інфраструктури. До життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України, належать, зокрема [11]:

1) урядування та надання найважливіших публічних (адміністративних) послуг;

2) енергозабезпечення (у тому числі постачання теплової енергії);

3) водопостачання та водовідведення;

4) продовольче забезпечення;

5) охорона здоров'я;

6) фармацевтична промисловість;

7) виготовлення вакцин, стале функціонування біолабораторій;

8) інформаційні послуги;

9) електронні комунікації;

10) фінансові послуги;

11) транспортне забезпечення;

12) оборона, державна безпека;

13) правопорядок, здійснення правосуддя, тримання під вартою;

14) цивільний захист населення та територій, служби порятунку;

15) космічна діяльність, космічні технології та послуги;

16) хімічна промисловість;

17) дослідницька діяльність.

Особливості функціонування критичної інфраструктури в умовах прикордонних територій

Прикордонні регіони мають низку специфічних характеристик, що впливають на стан, розвиток і безпеку критичної інфраструктури.

1. Підвищений рівень загроз і небезпек

Науковці наголошують, що прикордонні території частіше стикаються з:

- ризиком військових дій;
- диверсійними атаками;
- перериванням логістичних шляхів;
- спробами втручання іноземних акторів;
- контрабандною діяльністю;
- нелегальною міграцією;
- загрозами кібернетичного характеру [20, 21].

З початком повномасштабної агресії РФ ці ризики для України зросли в рази.

2. Транскордонні потоки як фактор навантаження на інфраструктуру

Прикордонні регіони інтенсивно взаємодіють з інфраструктурою сусідніх держав:

- збільшені транспортні потоки;
- транзит енергоресурсів;
- контроль товарів, людей, вантажів;
- зростання навантаження на транспортні вузли.

Особливо актуальним це стало після переорієнтації логістичних маршруів у 2022–2024 рр.

3. Географічна вразливість

Прикордонні регіони часто мають:

- малу глибину території (легка досяжність для агресора),
- складний рельєф,
- віддалені громади з обмеженим доступом до послуг,
- протяжні та важкодоступні ділянки кордону.

Ці фактори ускладнюють захист об’єктів КІ.

4. Регіональні диспропорції та соціальні чинники

Прикордонні області нерідко характеризуються:

- нижчим рівнем соціально-економічного розвитку,
- відсутністю високотехнологічних підприємств,
- структурною слабкістю місцевого бюджету,
- кадровим дефіцитом фахівців у сфері безпеки.

Це обмежує можливості модернізації КІ.

5. Мережеві та міжнародні аспекти

КІ прикордонних регіонів функціонує не лише в контексті внутрішньої політики, а й у рамках:

- угод транскордонного співробітництва,

- систем міжнародної безпеки,
- логістичних коридорів TEN-T,
- європейського енергетичного ринку,
- стандартів НАТО щодо стійкості (Resilience Baselines).

Таким чином, будь-які зміни стану КІ в прикордонному регіоні впливають на міжнародну безпеку.

Теоретичні підходи до дослідження КІ прикордонних регіонів

Для аналізу критичної інфраструктури в умовах прикордонних територій застосовуються такі підходи:

1. Системний – розглядає КІ як мережу взаємопов'язаних елементів, уразливість одного з яких впливає на всю систему.
2. Ризикологічний – зосереджується на оцінці ризиків, сценаріях загроз, моделюванні впливів.
3. Геополітичний – враховує зовнішні чинники, міжнародну конкуренцію та гібридні впливи.
4. Інституційний – досліджує нормативно-правові механізми захисту та управління КІ.
5. Територіальний та регіональний – враховує просторові особливості, мобільність та транскордонність.
6. Кібернетичний – стосується інформаційних загроз та кіберінфраструктури.
7. Безпековий (security studies**)** – підкреслює оборонну компоненту, стійкість та управління кризами.

Застосування комплексного підходу дає змогу адекватно оцінити стан і вразливість КІ прикордонних регіонів, виявити залежності, міжвідомчі зв'язки, потенційні сценарії розвитку загроз.

Роль критичної інфраструктури у забезпеченні життєдіяльності прикордонних територій

Стан КІ визначає здатність прикордонного регіону:

- забезпечувати безперервне енергопостачання;
- підтримувати транспортну та логістичну доступність;
- гарантувати безпечний рух людей і товарів через кордон;
- протистояти диверсіям та зовнішньому впливу;
- підтримувати управління та комунікацію;
- забезпечувати надання медичної та соціальної допомоги;
- підтримувати оборонний потенціал.

У прикордонних регіонах КІ є також *детермінантою транскордонної взаємодії та міжнародної кооперації*, оскільки забезпечує:

- функціонування пунктів пропуску,
- роботу митної та прикордонної інфраструктури,
- інтеграцію транспортних коридорів,
- енергетичні з'єднання з сусідніми країнами.

Таким чином, КІ прикордонних територій виконує подвійну функцію: внутрішньорегіональну та міжнародну. Критична інфраструктура прикордонних регіонів є складною багаторівневою системою, яка поєднує матеріальні та цифрові об'єкти, соціальні інститути, логістичні мережі та органи влади. Особливості її функціонування визначаються:

- географічним положенням регіону;
- безпековими загрозами;
- інтенсивністю транскордонних потоків;
- міжнародними зобов'язаннями України;
- станом нормативно-правового забезпечення;
- готовністю органів влади до криз реагування.

Умови прикордонності формують специфічні вимоги до управління КІ – від підвищених стандартів безпеки до необхідності міждержавної координації. Це потребує розроблення ефективних моделей захисту, механізмів оцінки ризиків,

сучасної інфраструктурної політики та підготовки фахівців у сфері публічного управління критичною інфраструктурою.

1.2. Загальні засади координації безпекових суб'єктів у прикордонних регіонах

Координація між військовими та цивільними структурами є ключовою умовою забезпечення стійкості критичної інфраструктури, особливо у прикордонних регіонах, які характеризуються підвищеним рівнем ризиків, загроз та невизначеності. Науковці відзначають, що саме ефективний механізм взаємодії між суб'єктами безпеки дозволяє мінімізувати наслідки зовнішніх впливів, забезпечити безперервність надання послуг та убезпечити населення й території.

За А.Шевцовим, координація в системі безпеки – це процес узгодження функцій, повноважень та дій суб'єктів, спрямований на досягнення спільної мети, а саме – зниження ризиків і загроз національній безпеці. Стале функціонування державної комунікаційної системи, що може бути досягнуто шляхом убезпечення комунікаційної інфраструктури, дасть змогу мінімізувати інформаційні інтервенції, сприятиме підвищенню рівня довіри до державних інституцій та належному, своєчасному і проактивному інформуванню громадськості у разі настання криз та їх протидії. Саме тому, на нашу думку, варто актуалізувати питання щодо виокремлення такого об'єкта стратегічної інфраструктури, як комунікаційна, на рівні з інформаційною та іншими [37]. Своєю чергою О.Тищенко наголошує, що без чіткої взаємодії між військовими, місцевим самоврядуванням, службами надзвичайних ситуацій та операторами критичної інфраструктури забезпечення стійкості системи стає неможливим [36].

Особливість координації саме в прикордонних регіонах полягає в тому, що в умовах гібридних загроз військова складова перестає бути ізольованою. Вона інтегрується у сферу цивільного управління, формуючи модель цивільно-

військового партнерства, яке у міжнародних документах НАТО визначається як важливий інструмент підтримання безпеки та функціонування життєво важливих об'єктів [43].

Міжвідомча координація як основа управління критичною інфраструктурою

Міжвідомча координація – це синхронізація дій різних органів влади, служб і організацій у процесі реагування на загрози. У сфері КІ вона передбачає:

1. розподіл відповідальності між секторами;
2. уніфікацію процедур планування та реагування;
3. створення загальних каналів комунікації;
4. спільне управління ризиками;
5. використання єдиних стандартів інформаційного забезпечення.

У науковій літературі виділяють три основні моделі міжвідомчої координації:

1) Ієрархічна модель (централізована)

Характеризується тим, що управління здійснюється через вертикаль влади. Вона ефективна в умовах воєнного стану або надзвичайних ситуацій.

Переваги: швидкість ухвалення рішень; чіткість команд.

Недоліки: можливість перевантаження командного центру; низька гнучкість.

2) Сітьова (мережева) модель

Передбачає горизонтальну взаємодію між суб'єктами безпеки. Її застосовують, коли необхідна гнучкість, швидка обробка інформації та локальні рішення.

Переваги: підвищена адаптивність, наявність кількох каналів інформації. Недоліки: можливі суперечності між інституціями, різний рівень підготовки персоналу [8].

3) Гібридна модель

Поєднує централізоване управління з автономією на місцях. Така модель є базовою у більшості країн НАТО у сфері захисту КІ [44].

Роль військових формувань у системі координації

У прикордонних регіонах до військових структур, що беруть участь у забезпеченні КІ, належать:

– Збройні сили України (ЗСУ);

– Державна прикордонна служба України (ДПСУ);

– Сили територіальної оборони;

– Національна гвардія України;

– військові підрозділи спеціального призначення.

Функції військових структур у забезпеченні КІ включають:

1. охорона об'єктів критичної інфраструктури;
2. супровід і контроль транспортних коридорів;
3. виявлення та нейтралізація диверсійних груп;
4. участь у відновленні пошкоджених об’єктів (інженерні війська);
5. протидія безпілотним апаратам та ракетним загрозам;
6. розробка військово-інженерних рішень щодо укріплення об’єктів КІ.

У сучасних умовах війни проти України важливим став компонент військово-цивільного планування, який передбачає включення військових експертів до процесу оцінки вразливостей КІ.

Роль цивільних структур у механізмах координації

Цивільний компонент включає:

– місцеві державні адміністрації та органи самоврядування;

– операторів критичної інфраструктури (енергетика, транспорт, зв'язок, водопостачання);

– ДСНС;

– Національну поліцію;

– служби цивільного захисту;

– органи охорони здоров’я;

– громадські організації й волонтерські штаби.

Функції цивільних структур:

1. підтримання функціонування інфраструктури;
2. управління ресурсами (паливо, ремонтні бригади, резерви);
3. евакуація населення;
4. комунікація з населенням;
5. регіональне планування розвитку та укріплення КІ;
6. імплементація стандартів ЄС у сфері безпеки КІ.

Зарубіжні підходи до військово-цивільної координації

Найбільш опрацьованими є моделі НАТО, ЄС, США, Ізраїлю та Канади.

Підхід НАТО

Передбачає використання концепції Civil-Military Cooperation (CIMIC). Основні елементи:

– спільні аналітичні центри,

– спільні карти загроз,

– офіцери CIMIC у місцевих адміністраціях,

– тренування за стандартами військово-цивільного реагування .

Підхід Європейського Союзу

ЄС застосовує систему RescEU, кризового менеджменту та механізму захисту КІ згідно з Директивою 2022/2557. Особливість – чітка "секторальна відповідальність" та обов’язкові оцінки ризиків .

Підхід США

США використовують модель Homeland Security Partnership, де операторами критичної інфраструктури є як приватний сектор, так і держава. Основна роль відводиться *спільним інформаційним центрам* та *стандартам NIST* [52].

Українські практики координації між цивільними та військовими структурами

Після 2014 року в Україні сформовано такі механізми:

– РНБО як стратегічний центр;

– обласні та районні військові адміністрації;

– штаби оборони;

– регіональні комісії з питань ТЕБ і НС;

– групи швидкого реагування операторів КІ;

– спільні центри реагування при ДСНС.

З 2022 року посилено:

– обмін розвідувальною інформацією;

– спільне патрулювання та охорона енергетичних об'єктів;

– створення системи енергетичних резервів;

– застосування військових

інженерних рішень для енергетики та транспорту .

Уповноважений орган у сфері захисту критичної інфраструктури України забезпечує формування та реалізує державну політику у сфері захисту критичної інфраструктури, здійснює функціональне управління національною системою захисту критичної інфраструктури, забезпечує координацію діяльності міністерств та операторів критичної інфраструктури з питань забезпечення стійкості та захисту об'єктів критичної інфраструктури.

Діяльність уповноваженого органу у сфері захисту критичної інфраструктури України спрямовує, координує та контролює Кабінет Міністрів України.

Проблемні аспекти:

1. недостатня цифровізація каналів комунікації;
2. нестача спільних протоколів;
3. дублювання функцій;

4. низький рівень підготовки кадрів на місцях;
5. бюрократичні бар’єри між секторами.

Таблиця 1.2 – Моделі координації військових та цивільних структур у прикордонних регіонах

Модель координації	Основні характеристики	Переваги	Недоліки	Приклади країн
Ієрархічна	Централізоване управління; вертикальна підпорядкованість	Швидкість рішень; дисципліна	Низька гнучкість	Україна (воєнний стан), Польща
Мережева	Горизонтальна взаємодія; автономія суб’єктів	Гнучкість; швидкий обмін інформацією	Можливі суперечності	Німеччина, Канада
Гібридна	Поєднання вертикалі та мережевості	Баланс гнучкості та контролю	Потребує високої зрілості інституцій	НАТО, США
Партнерська (CIMIC)	Спільні центри планування; офіцери CIMIC	Висока ефективність реагування	Високі вимоги до персоналу	НАТО

Координація між військовими та цивільними структурами є базовою умовою функціонування критичної інфраструктури прикордонних регіонів. Ефективність взаємодії визначається:

– наявністю єдиних протоколів;

– спільним плануванням;

– інтеграцією інформаційних систем;

– військово-цивільним партнерством;

– готовністю персоналу діяти в умовах криз.

Оптимальною для України є *гібридна модель*, що поєднує централізоване управління у воєнних умовах із мережею локальних центрів взаємодії.

1.3. Нормативно-правове забезпечення захисту критичної інфраструктури в Україні та міжнародні стандарти

Ефективний захист критичної інфраструктури потребує не лише технічних та організаційних заходів, але й надійної нормативно-правової бази, яка визначає повноваження суб'єктів, стандарти безпеки, порядок категоризації, обміну інформацією та контролю за виконанням вимог. У контексті євроінтеграції та з огляду на військові виклики цього завдання набуває особливої значущості Закон України «Про критичну інфраструктуру».

Загальна структура нормативно-правового поля в Україні

В Україні нормативно-правові засади захисту КІ становлять сукупність законів (рамкові норми), постанов Кабінету Міністрів (процедури, методики, вимоги), наказів міністерств і відомств (технічні й галузеві норми), методичних рекомендацій і стандартів для операторів, міжнародних угод і стандартів, що імплементуються на національному рівні. Нормативна база динамічна – вона змінюється відповідно до загроз (кібер-атаки, фізичні удари, гібридні загрози) і практики імплементації.

Нижче подано основні нормативні акти України, які формують правове поле захисту КІ – коротко про зміст та практичні наслідки імплементації.

Таблиця 1.3 – Ключові нормативні акти України щодо КІ

№	Назва документа (посилання)	Рік	Основний зміст / ключові положення	Практичні наслідки
1	Закон України «Про критичну інфраструктуру»	2021	Рамковий закон: визначення понять, підстави для формування Національної системи захисту КІ, база для реєстру, обов'язки операторів, повноваження органів влади.	Створення правової основи для категоризації об'єктів КІ; юридична відповідальність операторів.
2	Постанова КМУ №1109 «Деякі питання об'єктів критичної інфраструктури»	2020	Порядок віднесення об'єктів до КІ, критерії, методики та перелік секторів.	Конкретизація процедури віднесення та первинна класифікація об'єктів.
3	Постанова КМУ №518 «Загальні вимоги до кіберзахисту об'єктів КІ»	2019	Мінімальні обов'язкові вимоги з кіберзахисту для суб'єктів КІ, планування заходів, управління ризиками.	Обов'язковість впровадження базових кіберзаходів для операторів; підґрунтя для аудитів.
4	Постанова КМУ №821 «Порядок проведення моніторингу рівня безпеки об'єктів КІ	2022	Процедури моніторингу, періодичність перевірок, відповідальні органи.	Встановлення режиму регулярного нагляду за станом безпеки.
5	Постанова КМУ №1174 (регламент обміну інформацією між суб'єктами нац. системи захисту КІ)	2022	Регламентація каналів та процедур обміну інформацією про інциденти, рівень доступу, формат повідомлень.	Формування єдиного протоколу інформування та оперативного реагування.
6	Нормативні акти в галузі енергетики, транспорту, фінансів, ЖКГ (накази/стандарти), методики категоризації та методичні рекомендації.	2019–2024	Галузеві вимоги до безпеки і відновлення, методики оцінки ризиків.	Надають деталізацію і технічні вимоги для операторів у різних секторах.

Джерела: офіційні тексти (ВРУ, КМУ, центральні органи виконавчої влади).

Міжнародні стандарти, директиви та кращі практики

Україна активно використовує міжнародні підходи при формуванні політики КІ –особливо рамки ЄС, НАТО та стандарти кібербезпеки (NIST, CISA/DHS).

Нижче – головні міжнародні документи, які мають практичне застосування при реформуванні національного законодавства.

Таблиця 1.4 - Міжнародні стандарти та документи

№	Документ / організація (посилання)	Рік / статус	Короткий опис	Значення для України
1	Council Directive 2008/114/EC (EU)	2008	Про ідентифікацію європейських критичних інфраструктур; методи оцінки впливу та міждержавну координацію.	Основа для ідентифікації ECI; корисно при формуванні процедур транскордонної взаємодії.
2	Directive (EU) 2022/2557 on the resilience of critical entities	2022	Розширює підхід: від ідентифікації до вимог щодо стійкості критичних суб'єктів, управління ризиками, планів відновлення.	Сучасний європейський стандарт; важливий для імплементації національних правил стійкості.
3	NATO guidelines / CIMIC doctrine (CIMIC Handbook, Resilience guidance)	2019–2024	Практики цивільно-військової координації, стандарти обміну інформацією, рекомендації щодо захисту енергетики, транспорту, цифрової інфраструктури.	Корисні для побудови механізмів співпраці військових і цивільних суб'єктів у прикордонних регіонах.
4	NIST Cybersecurity Framework (CSF 1.1, CSF 2.0)	2014; 2018; 2024 (2.0)	Рамка управління кіберризиками для критичної інфраструктури: ідентифікація, захист, виявлення, реагування, відновлення.	Прийнята у світі як «базова» методика для кіберзахисту; застосовується операторами й державами.
5	DHS / CISA guidance and frameworks (US)	2020–2024	Інструменти для національного управління безпекою КІ, рекомендації щодо AI, OT/ICS захисту.	Варто врахувати при розробці національних стандартів кіберзахисту та AI-політик.
6	ISO / IEC стандарти (серія ISO 223xx — resilience, ISO/IEC 27001 — інф. безпека).	різні	Міжнародні стандарти управління безпекою та стійкістю.	Використовуються для сертифікації й підходів до управління ризиками.

Джерела: офіційні тексти ЄС, NIST, NATO, CISA/DHS

Узагальнення нормативної бази дає підстави для таких висновків:

1. Наявність рамкового закону (2021) і підзаконних актів дає Україні юридичну платформу для створення системи захисту КІ, проте імплементація вимагає додаткових процедур і ресурсів (інструменти моніторингу, кадрові ресурси, технічна модернізація).

2. Кіберзахист : Україна встановила загальні вимоги (Постанова №518), але у більшості секторів оператори мають різні рівні готовності.

3. Транскордонна складова: директиви ЄС (2008, 2022) підкреслюють необхідність міждержавної координації та урахування міжсекторних залежностей; для прикордонних регіонів це критично. Україна має узгодити частину практик з сусідніми країнами та адаптувати стандарти стійкості.

4. Оперативний обмін інформацією: національні регламенти (Постанова №1174 та ін.) започатковують протоколи, але на практиці часто бракує автоматизації, єдиних форматів та захищених каналів зв'язку.

5. Цивільно-військова координація: міжнародні практики дають зрозумілий шлях для інтеграції; Україна здійснює кроки у цьому напрямі, але потребує стандартизованих процедур, спільного навчання та обміну даними.

Таблиця 1.5 – Відповідальні суб'єкти та їх ролі

Суб'єкт	**Основні ролі щодо КІ**	**Статус / джерело повноважень**
Кабінет Міністрів / РНБО	Стратегічна політика, координація, постанови	Закон, укази, постанови (№1109, №821)
Міненерго, МІУ, Мінреінтеграції тощо	Галузеві стандарти, плани відновлення	Галузеві нормативи
Оператори КІ (державні/приватні)	Виконання вимог безпеки, впровадження планів кіберзахисту	Закон «Про критичну інфраструктуру», Постанова №518.
ДСНС, Нацполіція, СБУ	Реагування на інциденти, розслідування, підтримка відновлення	Закони про НС, внутрішню безпеку
ДПСУ, ЗСУ, територіальна оборона	Фізична охорона, оборонні заходи у прикордонних регіонах	Відповідні військові положення та директиви

З таблиці 1.5 видно, що першочерговими завданнями в цьому напрямку мають бути такі:

1. Прискорити імплементацію міжнародних практик стійкості: впровадити на національному рівні вимоги до планів забезпечення стійкості для критичних операторів (енергетика, транспорт, телеком).

2. Уніфікувати протоколи обміну інформацією: впровадити машиночитаємі формати інцидентних повідомлень (STIX/TAXII або еквіваленти), захищені канали та єдину платформу оповіщення між військовими та цивільними структурами.

3. Уніфікований підхід до кіберзахисту: рекомендувати операторам прийняти NIST CSF (або сумісний профіль) як базову методику; підвищити обов'язки щодо захисту OT/ICS.

4. Розвинути механізми співпраці у прикордонних ОДА/ВА: офіцери цивільно-військового співробітництва мають бути інтегровані у регіональні центри управління КІ; спільні навчання – регулярні.

5. Створити механізм стимулів та санкцій: поєднати підтримку модернізації (субсидії, гранти, техпідтримка) з відповідальністю за недотримання мінімальних вимог безпеки. Впровадити регулярні аудити та «стрес-тести» інфраструктури (фізичні, кібер), особливо для вузлів, що обслуговують прикордонні коридори.

6. Посилити координацію з партнерами (НАТО, ЄС, CISA/DHS) щодо обмінів розвідданими, практиками відновлення та стандартами.

Україна має базову нормативно-правову платформу для захисту КІ (закон 2021 та підзаконні акти), але головне завдання – швидка і якісна імплементація та стандартизація процедур у секторах. Міжнародні рамки дають чіткі практичні підходи – їх імплементація та адаптація до умов прикордонних регіонів є пріоритетом. Конкретні заходи: уніфікація протоколів, обмін інформацією,

інтеграція кібер- та фізичного захисту, регіональні навчання та регулярні аудити – підвищать стійкість КІ в прикордонних регіонах та зменшать ризики каскадних відмов.

Таким чином, дослідження засад забезпечення критичної інфраструктури прикордонних регіонів дало змогу сформувати цілісне розуміння сутності, класифікації, специфіки функціонування та нормативно-правового регулювання об'єктів критичної інфраструктури (КІ) в Україні та міжнародному просторі:

По-перше, узагальнено підходи до трактування поняття «критична інфраструктура». Показано, що в сучасних умовах воєнної агресії, технологічної взаємозалежності та високої динаміки ризиків КІ розглядається не лише як сукупність матеріальних об'єктів, але і як **цілісна система**, функціонування якої визначає життєстійкість держави, суспільства та економіки. Визначено основні характеристики КІ: системоутворюючість, незамінність, міжсекторальна взаємозалежність, високий рівень вразливості до гібридних загроз.

По-друге, проведено класифікацію об'єктів критичної інфраструктури залежно від їх функціонального призначення, ступеня критичності та секторальної належності. Особливу увагу приділено специфіці функціонування КІ у прикордонних регіонах, де інфраструктурні об'єкти перебувають під підвищеним ризиком через близькість до державного кордону, можливість диверсій, артилерійських та ракетних ударів, міграційних викликів та транснаціональної злочинності. Встановлено, що прикордонні регіони потребують **підсилених заходів захисту**, зокрема удосконалення координації між військовими, цивільними та спеціальними структурами.

По-третє, проаналізовано основні моделі та підходи до координації взаємодії органів влади, силових структур, військових управлінь та цивільного сектору у сфері забезпечення КІ. З'ясовано, що в умовах сучасних загроз найефективнішими є **мережеві та міжвідомчі моделі**, які забезпечують швидке реагування, обмін інформацією та чіткий розподіл відповідальності. Підкреслено, що сучасні

європейські практики орієнтовані на інтеграцію військових і цивільних механізмів управління безпекою.

По-четверте, виконано системний аналіз нормативно-правового забезпечення захисту КІ в Україні. Встановлено, що українське законодавство активно адаптується до стандартів ЄС та НАТО. Основним документом є Закон України «Про критичну інфраструктуру», який визначає принципи ідентифікації, категоризації, захисту та управління ризиками. Разом із тим, низка процедур – зокрема щодо координації між галузевими органами, обміну інформацією та оцінки стійкості – потребує подальшого вдосконалення.

По-п’яте, узагальнено міжнародні стандарти та директиви, які формують сучасний підхід до забезпечення стійкості та безпеки інфраструктурних об’єктів. До ключових належать: **ISO 31000**, **NIS2 Directive**, стандарти НАТО з планування стійкості, Рамкова міжнародна програма Сендай ООН. Доведено, що впровадження цих стандартів є необхідною умовою для підвищення стійкості КІ України та інтеграції у європейські та євроатлантичні системи безпеки.

Узагальнюючи, слід зазначити, що теоретичні основи забезпечення критичної інфраструктури прикордонних регіонів формують фундамент для подальших прикладних досліджень, пов’язаних із моделюванням ризиків, оптимізацією координації військових і цивільних структур та розробленням практичних заходів щодо підвищення стійкості систем життєзабезпечення. Отримані результати створюють основу для формування системної моделі управління безпекою КІ у прикордонному просторі, що буде висвітлено в наступних розділах роботи.

РОЗДІЛ 2. АНАЛІЗ СИСТЕМИ КООРДИНАЦІЇ ВІЙСЬКОВИХ І ЦИВІЛЬНИХ СТРУКТУР У ПРИКОРДОННИХ РЕГІОНАХ УКРАЇНИ

2.1. Характеристика прикордонних регіонів України та їх критичної інфраструктури

Прикордонні регіони України відіграють стратегічну роль у забезпеченні національної безпеки, економічної стабільності та обороноздатності держави. Їхнє розташування на стику з країнами Європейського Союзу та державами, які становлять потенційну загрозу, визначає підвищені вимоги до координації між військовими та цивільними структурами, ефективного управління ризиками та захисту критичної інфраструктури (КІ).

Охарактеризуємо критичну інфраструктуру та спробуємо оцінити рівень вразливості та для вироблення рекомендацій щодо підвищення стійкості системи управління.

1**. Західні прикордонні регіони**

До західних прикордонних областей відносяться такі: Львівська, Закарпатська, Волинська, Івано-Франківська, Чернівецька.

Географія та стратегічне значення

- Межують із країнами Європейського Союзу (далі – ЄС): Польща, Словаччина, Угорщина, Румунія.
- Мають важливі транспортні коридори, що забезпечують міжнародну торгівлю та гуманітарні перевезення.
- Наявність гірських масивів та річкових систем впливає на логістику та оборонну готовність.

Демографія та економіка

- Населення: 4,5–5,5 млн осіб на регіон.
- Основні галузі: промисловість, транспорт, туризм, аграрний сектор.

- Висока концентрація міст із залізничними вузлами (Львів, Ужгород, Чернівці).

Таблиця 2.1 – Критична інфраструктура західних прикордонних регіонів

Сектор КІ	Основні об’єкти	Значення для безпеки та оборони
Енергетика	ПС 330 кВ Львівська, ТЕЦ Львів, ГРС Ужгород	Живлення військових об’єктів, цивільних потреб
Транспорт	Залізничні станції Львів, Чоп; автодороги Е40	Логістика, евакуація, постачання
Комунікації	Вузли мобільного та інтернет-зв’язку	Координація військових і цивільних структур
Соціально-медична	Центральні лікарні Львів, Ужгород	Надання медичної допомоги під час криз
Оборона	Прикордонні застави, склади ЗСУ	Охорона кордону, стримування агресії

Ризики та рекомендації

- Ризики: диверсії на транспортних вузлах, кібератаки на енергетику, надзвичайні ситуації в гірських районах.
- Рекомендації:

1. Створення резервних маршрутів для транспортних потоків.
2. Дублювання енергетичних мереж для ключових об’єктів.
3. Тісна координація між прикордонною службою, ЗСУ та місцевими адміністраціями.

2. Північні прикордонні регіони

До північних належать такі області: Чернігівська, Сумська, Житомирська.

Географія та стратегічне значення

- Межують з Російською Федерацією та Білоруссю.

- Високий рівень воєнної загрози, потреба в постійній системі спостереження та оборони.
- Основні транспортні шляхи: М-01 Київ–Чернігів–Бориспіль; залізниця Київ–Гомель.

Демографія та економіка

- Населення: 2,5–3,5 млн осіб.
- Основні галузі: сільське господарство, легка промисловість, лісозаготівля.
- Порівняно невелика концентрація великих міст, але висока стратегічна важливість кожного вузла.

Таблиця 2.2 – Критична інфраструктура північних прикордонних регіонів

Сектор КІ	**Основні об’єкти**	**Значення для безпеки та оборони**
Енергетика	ПС Чернігівська, підстанції Сумська	Забезпечення командних пунктів
Транспорт	Залізничні вузли Суми, Чернігів; автошляхи М02	Евакуація, логістика військових підрозділів
Комунікації	Вузли мобільного та інтернет-зв’язку	Оперативне управління силами
Соціально-медична	Лікарні Чернігів, Суми	Медичне забезпечення населення
Оборона	Прикордонні застави, військові склади	Стримування агресії, контроль кордону

Ризики та рекомендації

- Ризики: артилерійські удари, кібератаки, підготовка диверсійних груп.
- Рекомендації:

1. Моніторинг критичних об’єктів за допомогою безпілотних систем.
2. Дублювання каналів зв’язку та резервування енергопостачання.

3. Інтеграція місцевих сил оборони у систему реагування на загрози.

3. Східні прикордонні регіони

До східних прикордонних областей належать такі: Харківська, Луганська, Донецькаі.

Географія та стратегічне значення

- Межують з Російською Федерацією, що визначає високий рівень воєнної загрози.
- Наявність густої мережі транспортних шляхів і промислових центрів.
- Східні регіони є зонами активних бойових дій, що ускладнює управління КІ.

Демографія та економіка

- Населення: близько 4–5 млн осіб.
- Основні галузі: важка промисловість, металургія, машинобудування, транспорт.
- Міста: Харків, Сєвєродонецьк, Краматорськ – важливі логістичні та промислові вузли.

Таблиця 2.3 – Критична інфраструктура східних прикордонних регіонів

Сектор КІ	Основні об’єкти	Значення для безпеки та оборони
Енергетика	ПС Харківська, ТЕЦ Сєвєродонецька, ГРС Лисичанськ	Забезпечення роботи командних пунктів та військових об’єктів
Транспорт	Залізничні вузли Харків, Лисичанськ; автошляхи М03, М04	Логістика, евакуація, постачання
Комунікації	Вузли мобільного та інтернет-зв’язку	Оперативне управління, координація сил оборони
Соціально-медична	Лікарні Харків, Краматорськ	Надання медичної допомоги в кризових умовах
Оборона	Прикордонні застави, склади ЗСУ	Контроль кордону, стримування агресії

Ризики та рекомендації

Ризики: артилерійські та ракетні удари по КІ, диверсії, руйнування мостів і доріг, кібератаки.

- Рекомендації:

1. Встановлення додаткових резервних маршрутів для транспорту.
2. Дублювання енергетичних мереж і резервних джерел живлення.
3. Використання безпілотних систем для моніторингу КІ.
4. Тісна координація між ЗСУ, прикордонною службою та місцевими адміністраціями.

4. Південні прикордонні регіони

До південних областей належать: Одеська, Миколаївська, Херсонська.

Географія та стратегічне значення

- Межують з Молдовою та мають вихід до Чорного моря.
- Південні області є важливими портовими і транспортними вузлами для економіки та оборони.
- Підвищена загроза морських та гібридних атак, блокування портів.

Демографія та економіка

- Населення: 3–4 млн осіб.
- Основні галузі: морська логістика, портова діяльність, промисловість, сільське господарство.
- Важливі міста: Одеса, Херсон, Миколаїв.

Таблиця 2.4 – Критична інфраструктура південних прикордонних регіонів

Сектор КІ	**Основні об’єкти**	**Значення для безпеки та оборони**
Енергетика	ПС Одеса, ТЕЦ Миколаїв, об’єкти ГТС	Забезпечення роботи військових і цивільних систем
Транспорт	Морські порти Одеса, Чорноморськ; залізниця; автошляхи М14	Логістика, постачання, евакуація
Комунікації	Вузли мобільного та інтернет-зв’язку	Координація сил оборони та цивільних служб
Соціально-медична	Лікарні Одеса, Херсон	Медичне забезпечення населення
Оборона	Прикордонні застави, військові склади	Охорона кордону, стримування агресії

Ризики та рекомендації

- Ризики: морські атаки, мінування портів, кібератаки, блокування транспортних коридорів.
- Рекомендації:

1. Моніторинг морських підходів та портової інфраструктури.
2. Створення резервних транспортних маршрутів і складів.
3. Розширення систем відеоспостереження та контролю на ключових об’єктах.
4. Координація дій військових, прикордонників і місцевих адміністрацій.

Узагальнюючи наведене вище, можемо сформулювати такі висновки:

1. Прикордонні регіони України мають високу стратегічну важливість з різними рівнями загроз залежно від географічного положення.
2. Критична інфраструктура охоплює енергетику, транспорт, комунікації, соціально-медичні та оборонні об’єкти.

3. Для забезпечення безпеки необхідна тісна координація між військовими, прикордонними структурами та місцевими адміністраціями.

4. Рекомендації включають: резервування маршрутів, дублювання енергетичних та комунікаційних систем, використання безпілотних засобів моніторингу та інтеграцію міжнародних стандартів захисту КІ.

2.2. Стан координації між військовими адміністраціями, органами місцевого самоврядування та Державною службою України з надзвичайних ситуацій

Система координації між військовими адміністраціями (ВА), органами місцевого самоврядування (ОМС) та Державною службою України з надзвичайних ситуацій (ДСНС) у період активної фази збройної агресії Російської Федерації проти України стала ключовою основою забезпечення стійкості територіальних громад, збереження критичної інфраструктури та захисту населення у прикордонних регіонах. В умовах постійної загрози ракетних ударів, артилерійських обстрілів, диверсійно-розвідувальних операцій та комплексних надзвичайних ситуацій (пожежі, аварії, руйнування житлових і промислових об’єктів), ефективність міжвідомчої взаємодії безпосередньо визначає рівень безпеки громад та можливість забезпечення їхнього життєзабезпечення.

У законодавчій площині координація структур базується на Законі України «Про правовий режим воєнного стану», Кодексі цивільного захисту України, Законі «Про місцеве самоврядування» та низці підзаконних актів Кабінету Міністрів і МВС. Відповідно до цих документів:

- *ВА* здійснюють загальне управління регіонами у період воєнного стану, координують оборонні заходи, забезпечують виконання рішень Генерального штабу та військового командування.

- *ОМС* відповідають за функціонування комунальної інфраструктури, забезпечення населення базовими послугами, організацію укриттів, підтримку гуманітарних процесів, розвиток місцевих служб цивільного захисту.
- *ДСНС* виконує функції рятувальної служби: реагування на надзвичайні ситуації, ліквідація пожеж, пошук постраждалих під завалами, хімічний та радіаційний моніторинг, відновлення першочергових безпекових умов на пошкоджених об’єктах.

Попри достатньо чітку законодавчу основу, на практиці координація між цими структурами є неоднорідною, фрагментарною та нерідко обмеженою низкою організаційних, інституційних і ресурсних проблем. Особливо гостро вони проявляються у прикордонних регіонах – Сумській, Чернігівській, Харківській, Одеській, Миколаївській, Херсонській, Закарпатській та Волинській областях, де ризики збройних атак та загроза диверсій є постійними.

Нижче подано аналіз стану координації у цих регіонах, проблемні аспекти та їх вплив на безпекову й гуманітарну ситуацію, а також таблицю ключових проблем взаємодії.

Нормативно-правові засади координації та фактичні механізми взаємодії

Роль військових адміністрацій

Створення військових адміністрацій визначено Законом України «Про правовий режим воєнного стану». У прикордонних та прифронтових областях вони виконують не лише функцію оперативного управління, а й координують:

1. Оборонні заходи на рівні громади та області.

2. Міжвідомчу взаємодію**,** включно з ОМС, ДСНС, Нацполіцією, ДПСУ та Силами територіальної оборони.

3. Розподіл ресурсів між службами в умовах обмеження комунікацій і логістики.

4. Пріоритетність укріплення критичної інфраструктури (енергетика, вода, зв’язок).

ВА фактично виступають центрами управління в кризових умовах та забезпечують єдине оперативне керівництво всіма процесами. Спрямування, координацію та контроль за діяльністю районних військових адміністрацій з питань забезпечення оборони, громадської безпеки і порядку, захисту критичної інфраструктури, здійснення заходів правового режиму воєнного стану здійснює Генеральний штаб Збройних Сил України, обласні військові адміністрації (у разі їх утворення), а з інших питань - Кабінет Міністрів України, обласні державні адміністрації у межах своїх повноважень. (закон про воєнний стан

Роль органів місцевого самоврядування

ОМС залишаються основними адміністраторами ресурсів громади. Саме вони відповідають за:

- утримання житлово-комунальної інфраструктури;
- забезпечення функціонування укриттів;
- ремонт критичної інфраструктури;
- організацію гуманітарної допомоги;
- роботу місцевих служб цивільного захисту;
- відновлювальні роботи після обстрілів.

У прикордонних громадах роль ОМС змінюється: замість розвитку території пріоритетами стають безпекові заходи, термінове усунення наслідків атак та підтримка населення.

Роль ДСНС

ДСНС виконує функції «першої лінії» реагування.

У воєнний час служба:

- проводить рятувальні роботи;
- гасить пожежі після обстрілів;
- здійснює розмінування;
- проводить інженерні роботи;
- забезпечує хімічний, радіаційний і біологічний моніторинг;

- забезпечує розгортання мобільних пунктів обігріву та допомоги.

У прикордонних регіонах навантаження на ДСНС зросло в 4–7 разів, залежно від області (аналітичні зведення ДСНС, 2022–2024).

Аналіз практичної координації між ВА, ОМС та ДСНС у прикордонних регіонах

Узагальнюючи інформацію офіційних джерел, проаналізуємо фактичний стан взаємодії на прикладі різних типів громад: сільських, міських, промислових, густонаселених і малих. Для прикордонних регіонів характерні такі тенденції:

1. Швидкість комунікації та обміну інформацією

У більшості випадків ВА виступає основним комунікаційним вузлом. Однак інколи інформація передається з затримкою, зокрема:

- через відсутність захищених каналів зв'язку;
- недостатню інтеграцію інформаційних систем ДСНС та місцевих служб;
- використання старих паперових протоколів у деяких громадах.

У прикордонних областях, де важлива кожна хвилина, такі затримки можуть збільшувати кількість постраждалих.

2. Ресурсне забезпечення і матеріальна підтримка

Проблеми різняться за регіонами:

- Сумська, Чернігівська, Харківська обл. – найбільше навантаження, нестача техніки ДСНС, велика кількість руйнувань.
- Одеська, Миколаївська – високе навантаження під час масованих ракетних атак, дефіцит мобільних підрозділів ДСНС.
- Закарпатська, Волинська – менша інтенсивність атак, але значні проблеми з матеріальною базою місцевих служб.

Ресурсний дисбаланс погіршує координацію: одні регіони потребують підсилення, інші мають недовикористані ресурси.

3. Узгодженість дій під час ліквідації наслідків обстрілів

У більшості прикордонних громад робота організована таким чином:

1. Першими прибувають підрозділи ДСНС.
2. ВА забезпечує стабілізацію ситуації, перекриття територій.
3. ОМС організовують відновлення комунікацій та соціальну підтримку.

Але на практиці виникають труднощі:

- іноді ВА і ОМС ухвалюють різні рішення щодо аварійного відновлення;
- ДСНС не завжди має доступ до необхідної техніки;
- у деяких громадах відсутні чіткі плани реагування.

4. Розбіжності у пріоритетах між ВА і ОМС

Військові адміністрації орієнтовані на оборонні завдання:

- розміщення підрозділів;
- укріплення території;
- захист стратегічних об’єктів.

ОМС орієнтовані на:

- забезпечення життєдіяльності;
- гуманітарні потреби;
- соціальну підтримку.

Різниця у пріоритетах у деяких регіонах спричиняє конфлікти при розподілі ресурсів, особливо під час критичних ситуацій.

3. Алгоритми взаємодії в умовах загрози та надзвичайних ситуацій

Система реагування у прикордонних регіонах базується на багаторівневому управлінні**,** яке визначене Кодексом цивільного захисту України, Законом «Про правовий режим воєнного стану» та нормативами ДСНС щодо організації евакуації, оповіщення та аварійно-рятувальних робіт. Типова схема координації включає такі етапи:

1) Виявлення загрози

- первинні дані надходять від сил оборони, Нацполіції, ДПСУ та систем радіолокаційного й повітряного контролю;
- військові адміністрації отримують зведення від ОК «Північ», «Схід», «Південь» залежно від регіону;
- місцеве самоврядування інформується після підтвердження рівня загрози.

2) Прийняття рішення

- керівник військової адміністрації або голова ОВА скликає оперативний штаб**;**
- представник ДСНС надає оцінку можливих наслідків (пожежі, руйнування, забруднення, обриви мереж);
- ухвалюється рішення про:
  - запуск системи оповіщення;
  - евакуацію (часткову/повну);
  - посилення охорони об’єктів критичної інфраструктури;
  - залучення підрозділів ДСНС, поліції, Нацгвардії.

3) Реагування

- ДСНС виконує рятувальні роботи, забезпечує пожежогасіння, розбір завалів;
- військові підрозділи здійснюють оборону території та супровід евакуаційних колон;
  - місцева влада організовує: транспорт; пункти збору; розміщення населення; забезпечення продуктами та водою.

4) Відновлення

- місцеве самоврядування відповідає за інфраструктурне відновлення;
- ДСНС проводить технічне обстеження будівель;
- військові адміністрації координують залучення фінансування та міжнародної допомоги;

- у прикордонних регіонах ДПСУ долучається до оцінки безпекових ризиків.

У теорії цей алгоритм є чітким, однак у практиці він залежить від швидкості передачі даних, готовності місцевих структур та доступності ресурсів. Головні проблеми координації представлені в таблиці нижче.

Таблиця 2.5 – Основні проблеми координації між ВА, ОМС та ДСНС у прикордонних регіонах

Категорія проблеми	**Сутність**	**Прояви у регіонах**	**Наслідки**	**Нормативні обмеження / прогалини**
Затримки обміну інформацією	Відсутність уніфікованих каналів даних між військовими, ДСНС та громадами	Чернігівська, Сумська, Харківська ОВА – передача даних залежить від конкретних посадових осіб	Повільне ухвалення рішень, втрати часу при загрозах	Немає єдиного стандарту міжвідомчої інформаційної системи
Обмежений доступ до військової інформації	Частина даних може бути надана лише за погодженням Генштабу	ВА часто не передає ОМС деталізовану інформацію про загрози	Неповне планування евакуацій та запасних маршрутів	Норми Закону «Про держтаємницю» не узгоджені з потребами цивільного захисту
Брак транспорту для евакуації	ОМС не мають достатнього муніципального автопарку	Сумська, Волинська, Чернігівська області	Зрив або затримка евакуації	Потреба в доповненні Кодексу цивільного захисту щодо «мобілізації транспорту»
Недостатня підготовка персоналу	Практичні тренування проводяться нерегулярно	Багато громад у 2022–2023 рр. не мали навчань з ДСНС	Неправильні рішення на місцях, хаос під час ударів	Методичні рекомендації ДСНС застарілі

Категорія проблеми	Сутність	Прояви у регіонах	Наслідки	Нормативні обмеження / прогалини
				(частина створена до 2022 р.)
Проблеми з оповіщенням населення	Сповіщення залежить від електропостачання	Відмова сирен у прикордонних селах через обстріли	Люди не отримують попередження	Механізм резервного оповіщення не визначений
Розірвані логістичні мережі	Руйнування доріг та мостів у прикордонних районах	Харківська, Чернігівська області	Неможливість забезпечити швидку доставку підрозділів	Не розроблено протоколи «евакуації в умовах втрати доріг»
Фрагментація відповідальності	Нечіткий розподіл функцій між ВА та ОМС	Залежить від конкретного регіону	Затримки у забезпеченні людей ресурсами	Не врегульовано механізм подвійного підпорядкування
Недостатня інтеграція медичних служб	ВМС, ДСНС і ОМС мають різні стандарти медичної координації	Відсутність спільних медичних пунктів у прикордонних селах	Перевантаження лікарень	Потреба у створенні стандарту «воєнної медицини громад»

Регіональні відмінності у стані координації

Харківська область

- Найвищий рівень загроз, регулярні обстріли.
- Взаємодія між ОВА, ДСНС та військовими але перевантажена.
- Основна проблема – після масованих ударів.
- Координаційні центри працюють цілодобово, але бракує резервних систем зв’язку.

Сумська область

- Численні ДРГ-рейди, мінометні обстріли.
- ВА активно передає інформацію громадам, проте ДСНС має нестачу техніки для реагування.
- Потребує збільшення кількості мобільних пожежних розрахунків.

Чернігівська область

- Має значну протяжність кордону.
- Координація покращилася після 2023 року, запрацювали спільні центри управління**.**
- Проблема – обмежена кількість евакуаційних маршрутів у північних районах.

Закарпатська, Львівська, Волинська області

- Низький рівень активних обстрілів, але висока стратегічна роль як логістичних хабів.
- Основний виклик – перевантаження населенням через переміщення людей з інших регіонів.
- Координація значно краща, але бракує складів гуманітарного резерву.

Таким чином, ефективність можна оцінити за такими критеріями:

1. Швидкість реагування

У регіонах із постійними обстрілами (Харківська, Сумська) швидкість реагування висока, але залежить від навантаження на ДСНС.

2. Узгодженість дій

Велике значення має робота координаційних штабів**.** Якщо штаб постійно діє (Чернігівська ОВА), процес є стійкішим.

3. Рівень залучення громад

У деяких громадах створені «центри безпеки» (особливо на Заході), але у прифронтових селах таких центрів бракує.

4. Комунікаційна стійкість

Проблеми виникають через:

- відсутність Starlink у частини сільських адміністрацій;
- вразливість мобільного зв’язку;
- відсутність альтернативних систем оповіщення.

Загальні рекомендації щодо підвищення координації можна сформурмулювати такі: створення єдиної інформаційної системи “Безпека-Прикордоння” (передбачає: інтеграцію даних військових адміністрацій, ДСНС, поліції, ДПСУ, автоматичне оповіщення ОМС, прямий канал для передачі координат ударів); удосконалення правової бази (потрібно: оновити Кодекс цивільного захисту (розділи щодо евакуації під час воєнних дій), унормувати механізми доступу ОМС до військової інформації в межах необхідності); формування регіональних «резервних батальйонів ДСНС» особливо для Харківської та Сумської областей; розвиток мережі “Центрів безпеки” у прикордонних громадах (забезпечення: пожежного поста, медичного пункту, укриттів, пунктів резервного зв’язку); запровадження щоквартальних міжвідомчих навчань (обов’язкова участь: ВА, ОМС, ДСНС, поліції, місцевих підприємств критичної інфраструктури); розвиток системи автономного оповіщення (сирени на: сонячних батареях, автономних радіомодулях, резервних акумуляторах); посилення ролі громад у плануванні евакуації (рекомендації: створення громадських добровольчих груп, залучення місцевих депутатів, популяризація «сімейних планів евакуації» тощо). Більш детально такі рекомендації будуть розкриті в розділі 3.

РОЗДІЛ 3. УДОСКОНАЛЕННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПРИКОРДОННИХ РЕГІОНІВ

3.1. Пропозиції щодо вдосконалення організаційно-правових та управлінських механізмів взаємодії військових і цивільних структур

У сучасних умовах збройної агресії та постійних гібридних загроз прикордонні регіони України функціонують у режимі підвищеної безпекової напруги. Це зумовлює об'єктивну потребу в переосмисленні ролі та форм взаємодії військових і цивільних інституцій у системі публічного управління. Як зазначають вітчизняні науковці, «ефективність управління безпекою територій у кризових умовах залежить від здатності держави забезпечити узгоджені дії всіх суб'єктів влади» [35].

Забезпечення безпеки та захист КІ, тобто всі види діяльності, що виконуються перед або під час створення, функціонування, відновлення і реорганізації об'єктів КІ, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об'єктам КІ, а також мінімізацію та ліквідацію наслідківу разі їх реалізації, також є одним з основних напрямів зовнішньополітичної та внутрішньополітичної діяльності держави для забезпеченняїї національних інтересів і безпеки.

У теорії публічного управління взаємодія військових і цивільних структур розглядається як складний багаторівневий процес, що охоплює правові, організаційні, управлінські та кадрові компоненти [38]. У прикордонних регіонах України ця взаємодія має специфічний характер, зумовлений:

- особливим правовим режимом воєнного стану;
- функціонуванням військових адміністрацій як органів публічної влади;
- високою концентрацією об'єктів критичної інфраструктури;
- постійною загрозою збройного впливу.

На думку Г. Ситника, в умовах воєнних загроз «публічне управління трансформується з адміністративної системи в систему безпекового менеджменту» [35]. Це означає, що традиційні управлінські підходи мають бути доповнені інструментами кризового управління, міжвідомчої координації та стратегічного прогнозування.

Створення ефективної системи захисту КІ, заснованої на чіткому розподілі відповідальності її суб'єктів та державно-приватному партнерстві, є одним з основних напрямів зовнішньополітичної та внутрішньополітичної іяльності держави для забезпечення її національних інтересів і безпеки.

Згідно світового досвіду, окремі об'єкти КІ України можна віднести до об'єктів міжтериторіального та транскордонного значення, наприклад: атомні електричні станції, об'єкти трубопровідного транспорту, об'єкти морського та залізничного транспорту.

Результати аналізу, представлені у розділі 2, свідчать, що чинні організаційно-правові механізми взаємодії військових і цивільних структур у прикордонних регіонах є недостатньо системними. Незважаючи на наявність окремих законів і підзаконних актів, вони не формують цілісної моделі управління.

До основних недоліків належать:

- фрагментарність правового регулювання, коли норми розпорошені між різними актами;
- відсутність спеціалізованих регіональних документів, адаптованих до прикордонної специфіки;
- нечіткий розподіл відповідальності між військовими адміністраціями та органами місцевого самоврядування;
- обмежена інституційна роль громад у процесах управління безпекою.

Науковці і пракики односайні в тому, що наявність нормативної бази сама по собі не гарантує ефективної взаємодії, якщо вона не підкріплена організаційними

механізмами реалізації. Це актуалізує необхідність переходу від декларативного до функціонального правового регулювання.

З урахуванням виявлених проблем пропонуємо низку комплексних змін, спрямованих на формування цілісної організаційно-правової моделі взаємодії військових і цивільних структур.

1. Запровадження типових регіональних актів взаємодії

Доцільним є розроблення та затвердження типового регіонального Положення про взаємодію військових і цивільних структур у сфері безпеки та захисту критичної інфраструктури**.** Такий документ має містити:

- визначення суб'єктів взаємодії;
- порядок спільного планування;
- алгоритми дій у кризових ситуаціях;
- механізми обміну інформацією.

2. Інституціоналізація ролі органів місцевого самоврядування

Пропонується нормативно закріпити:

- участь ОМС у міжвідомчих координаційних органах;
- право ініціювати проведення спільних нарад;
- відповідальність громад за первинний моніторинг стану об'єктів КІ.

3. Удосконалення правового статусу військових адміністрацій

В умовах воєнного стану ВА виконують ключову управлінську роль, однак їхні повноваження у взаємодії з цивільними структурами потребують чіткого нормативного визначення, що зменшить управлінські конфлікти та дублювання функцій.

Організаційно-правові зміни не можуть бути ефективними без трансформації управлінських механізмів, які забезпечують практичну реалізацію норм і рішень. Як зазначається у працях з публічного управління, саме управлінські механізми визначають здатність системи реагувати на динамічні загрози та адаптуватися до кризових умов [38].

У прикордонних регіонах України управлінські механізми взаємодії військових і цивільних структур досі значною мірою зберігають відомчо-ієрархічний характер, що обмежує швидкість і гнучкість ухвалення рішень. Це особливо критично в умовах воєнних дій, коли час реагування є ключовим фактором збереження функціонування критичної інфраструктури.

1. Запровадження інтегрованого управлінського циклу

Пропонується впровадити єдиний управлінський цикл взаємодії, який охоплює такі етапи:

- спільне планування;
- координацію виконання;
- оперативний контроль;
- аналіз результатів і коригування рішень.

Такий цикл відповідає підходам integrated public management, що застосовуються в країнах ЄС та НАТО [22; 19].

2. Перехід до процесно-орієнтованого управління

Процесний підхід передбачає концентрацію не на повноваженнях окремих інституцій, а на ключових управлінських процесах, зокрема:

- реагування на надзвичайні ситуації;
- відновлення об’єктів КІ;
- забезпечення безперервності послуг;
- комунікація з населенням.

На думку Ю. Хомич, процесний підхід дозволяє зменшити управлінську фрагментацію та підвищити прозорість відповідальності [40].

3. Посилення механізмів управлінської відповідальності

Однією з проблем чинної системи є розмитість відповідальності між військовими та цивільними структурами. Пропонується:

- закріпити відповідальність за конкретні управлінські процеси;
- запровадити колегіальні управлінські рішення для кризових ситуацій;
- впровадити обов'язковий аналіз управлінських рішень після кризових подій.

Інституційна слабкість є однією з головних причин неефективної взаємодії в умовах криз. Як підкреслює О. Кириленко, «інституційна спроможність визначає здатність публічної влади діяти не декларативно, а результативно» [38].

1. Міжвідомчі координаційні ради при військових адміністраціях

Доцільним є створення постійно діючих міжвідомчих координаційних рад, до складу яких входять: представники ВА, органів місцевого самоврядування, ДСНС, правоохоронних органів, операторів критичної інфраструктури (за згодою).

Такі ради мають не дорадчий, *а управлінський характер,* із правом ухвалювати обов'язкові для виконання рішення в межах компетенції.

2. Робочі групи з питань критичної інфраструктури

Для вирішення спеціалізованих питань пропонується створення галузевих робочих груп (енергетика, водопостачання, транспорт, зв'язок), які забезпечують:

- оцінку вразливостей;
- планування захисних заходів;
- координацію відновлювальних робіт.

3. Інституційна участь громад

Важливим елементом сучасного публічного управління є участь громад. У прикордонних регіонах доцільно:

- залучати представників громад до дорадчих органів;
- проводити консультації з безпекових питань;
- розвивати механізми партнерства «влада – громада – бізнес».

Це відповідає принципам good governance та підвищує довіру до управлінських рішень [30].

Таблиця 3.1 - Пропозицій щодо вдосконалення організаційно-правових та управлінських механізмів

Сфера	Проблема	Існуючий стан	Запропоновані зміни	Очікуваний ефект
Правове регулювання	Фрагментарність норм	Розрізнені акти	Типові регіональні положення	Чіткість і узгодженість
Управління	Відомчий підхід	Ієрархічні рішення	Процесне управління	Оперативність
Планування	Відсутність інтеграції	Окремі плани	Спільне планування	Зменшення ризиків
Координація	Формальні органи	Дорадчі ради	Реальні повноваження	Ефективність
Відповідальність	Розмита	Перекладання	Колективна відповідальність	Якість рішень
Інституційна спроможність	Низька	Нестабільні структури	Постійні координаційні органи	Стійкість системи

Варто зазначити, що запропоновані у підрозділі 3.1 організаційно-правові та управлінські механізми є передумовою реалізації рішень, детально розглянутих у підрозділі 3.2. Зокрема:

- без правового закріплення неможливе функціонування єдиної інформаційної системи;
- без інституційної координації не працюватиме регіональний координаційний центр;
- без управлінської відповідальності неможлива ефективна міжвідомча взаємодія.

Таким чином, підрозділи 3.1 і 3.2 утворюють єдину логічну концепцію вдосконалення системи забезпечення критичної інфраструктури прикордонних регіонів України.

Підготовка та розвиток кадрів як ключовий елемент удосконалення взаємодії військових і цивільних структур

У сучасній теорії та практиці публічного управління кадровий потенціал розглядається як базовий ресурс забезпечення стійкості державних інституцій у кризових умовах. На думку В. Бакуменка, «ефективність управлінських рішень безпосередньо залежить від професійної підготовки суб'єктів управління та їхньої здатності діяти в умовах невизначеності» [38].

У прикордонних регіонах України проблема кадрового забезпечення взаємодії військових і цивільних структур має особливо гострий характер. Це зумовлено:

- постійною ротацією кадрів;
- перевантаженням управлінців в умовах воєнного стану;
- відсутністю системної міжвідомчої підготовки;
- різницею управлінських культур військових і цивільних інституцій.

Сучасні підходи до розвитку персоналу в публічному управлінні ґрунтуються на компетентнісній моделі, яка передбачає формування не лише професійних знань, а й управлінських, комунікативних та кризових навичок [40].

Для посадових осіб, залучених до взаємодії у прикордонних регіонах, доцільно сформувати базовий перелік ключових компетентностей, зокрема:

- здатність працювати в умовах криз і надзвичайних ситуацій;
- навички міжвідомчої координації;
- розуміння правових режимів воєнного стану;
- стратегічне та ситуаційне мислення;
- управління ризиками та прийняття рішень в умовах обмеженого часу.

Запровадження компетентнісного підходу дозволить уніфікувати вимоги до підготовки кадрів у різних інституціях та підвищити рівень взаєморозуміння між військовими й цивільними структурами.

Важливим напрямом удосконалення кадрового забезпечення є створення *постійної системи міжвідомчого навчання*, орієнтованої на спільну діяльність військових адміністрацій, органів місцевого самоврядування, ДСНС та інших суб'єктів безпеки.

До основних форм такої підготовки доцільно віднести:

- спільні навчальні курси з кризового управління;
- міжвідомчі тренінги та симуляційні навчання;
- командно-штабні навчання з елементами цивільного захисту;
- обмін досвідом між регіонами.

На думку експертів у сфері державного управління, «навчання в змішаних групах сприяє формуванню єдиного управлінського простору та довіри між суб'єктами взаємодії» [35].

Окремої уваги потребує спеціалізована *підготовка кадрів, відповідальних за управління та захист критичної інфраструктури.* У прикордонних регіонах ці об'єкти є першочерговими цілями впливу, що потребує високого рівня професійної готовності управлінців [9].

Пропонуємо такі підходи:

- запровадити обов'язкові курси з управління критичною інфраструктурою;
- навчати оцінці ризиків і вразливостей об'єктів;
- формувати навички взаємодії з операторами КІ;
- розвивати компетенції планування відновлення та безперервності функціонування.

З метою забезпечення стабільності управлінських процесів доцільним є формування *кадрового резерву прикордонних регіонів*, який може оперативно залучатися у разі кадрових втрат або розширення управлінських функцій.

Система кадрового резерву має включати:

- відбір осіб за компетентнісними критеріями;

- регулярне навчання та перепідготовку;
- оцінювання готовності до роботи в кризових умовах;
- механізми мотивації та професійного росту.

Безперервний професійний розвиток управлінців є необхідною умовою адаптації системи публічного управління до змін безпекового середовища [38].

Таким чином, увдосконалення організаційно-правових та управлінських механізмів взаємодії військових і цивільних структур у прикордонних регіонах України потребує:

- цілісної організаційно-правової моделі;
- сучасних управлінських механізмів, орієнтованих на процеси та результати;
- інституційної координації на регіональному рівні;
- розвитку кадрового потенціалу як ключового ресурсу системи безпеки.

Запропоновані заходи мають системний характер і створюють передумови для реалізації рішень, спрямованих на практичне вдосконалення координації, що буде детально розкрито у підрозділі 3.2. У сукупності вони формують концептуальну основу модернізації системи забезпечення критичної інфраструктури прикордонних регіонів України в межах сучасної парадигми публічного управління.

3.2. Удосконалення системи координації між військовими адміністраціями, ДСНС та органами місцевого самоврядування

Ефективність реагування на загрози критичній інфраструктурі прикордонних регіонів визначається не лише технічним станом об’єктів, але й якістю міжвідомчої координації. За результатами аналізу, здійсненого у розділі 2, встановлено, що чинна система взаємодії між військовими адміністраціями, органами місцевого самоврядування та Державною службою України з надзвичайних ситуацій

характеризується значною асиметричністю, нерівномірністю комунікаційних зв'язків та відсутністю структурованих, нормативно закріплених алгоритмів. Як зазначено у наукових дослідженнях, «ефективність міжвідомчої взаємодії в умовах кризових ситуацій залежить від стандартизації процесів, інтеграції інформаційних потоків та чіткості повноважень суб'єктів» [1].

Представимо обґрунтовування концептуальних й практичних шляхів реформування системи координації, пропозиції щодо вдосконалення інформаційно-аналітичної діяльності, правового забезпечення та організаційно-функціональної структури управління. Особливу увагу приділяємо створенню єдиної цифрової платформи взаємодії, уніфікованому алгоритму спільних дій та формуванню регіональних координаційних центрів як структурних елементів державної політики безпеки критичної інфраструктури.

Засади вдосконалення координації суб'єктів безпеки прикордонних регіонів

Сучасні підходи до управління безпекою критичної інфраструктури базуються на трьох ключових теоретичних підходах:

1. стійкості (resilience model);
2. багаторівневого врядування (multi-level governance);
3. інтегрованого кризового менеджменту (integrated crisis management).

1. Підхід стійкості критичної інфраструктури. Низка міжнародних дослідників наголошує, що стійкість інфраструктури залежить не лише від технічної готовності, а насамперед від керованості системи реагування та якості міжінституційних зв'язків [2; 3].

Підхід resilience передбачає:

- горизонтальну інтеграцію структур безпеки на місцевому рівні;
- високу адаптивність управлінських процесів;
- мінімізацію часових затримок під час обміну інформацією;
- синхронізацію рішень між різними інституціями.

2. Багаторівневе врядування (multi-level governance). Цей підхід, застосований у ЄС, передбачає взаємодію всіх рівнів влади – від центрального до місцевого – на основі принципів субсидіарності та спільної відповідальності. У прикордонних регіонах України потреба у такій моделі є критичною, оскільки ВА виконують функції місцевої влади, але одночасно залишаються елементами військового командування, що створює подвійність управлінських вертикалей.

3. Інтегрований кризовий менеджмент. Згідно з концепцією НАТО з кризового реагування (NATO Crisis Response System), основою успішної дії є стандартизовані процедури, спільні тренування та інтегровані центри управління [4].

Спираючись на ці теоретичні положення, пропонуємо комплексне реформування механізмів координації у прикордонних регіонах.

Створення єдиної інформаційної системи «Безпека-Прикордоння» як інструменту синхронізації управління

Однією з ключових проблем, виявлених у розділі 2, є відсутність єдиної уніфікованої платформи інформаційного обміну. На думку фахівців у сфері безпеки, фрагментованість даних призводить до зниження швидкості реагування, дублювання дій та помилок у прийнятті рішень [5].

У зв’язку з цим пропонується створення автоматизованої регіональної системи моніторингу та реагування «Безпека-Прикордоння», що виконуватиме функцію єдиного інформаційного простору між ВА, ОМС та ДСНС.

Функціональні характеристики системи:

1. Центральна база даних об’єктів критичної інфраструктури з прив’язкою до геоінформаційної системи (GIS).

2. Модуль оперативного обміну повідомленнями, що уніфікує сигнали різних структур.

3. Аналітичний модуль прогнозування загроз, який використовує наявні дані ДСНС, ВА, розвідки, операторів КІ.

4. Система автоматизованих сповіщень, що дозволяє миттєво передавати інформацію про обстріли, пошкодження, аварії.

5. Модуль кризових комунікацій, який забезпечує узгодженість інформації для населення та ЗМІ.

Як показує світовий досвід (Польща, Литва, Ізраїль), централізовані цифрові системи дозволяють скоротити час реагування на 30–60 % [6].

Алгоритм спільних дій під час кризових подій: стандартизація процедур

Сучасна система реагування у прикордонних регіонах часто базується на неформальних каналах, що суперечить принципам кризового менеджменту. На думку ДСНС, «відсутність алгоритмізації призводить до хаотичності дій та втрати операційного часу» [7].

Пропонується запровадження уніфікованого алгоритму спільних дій, який застосовується для всіх типів кризових ситуацій, зокрема обстрілів, диверсій, аварій на об’єктах КІ, кібератак тощо.

Етапи алгоритму:

1. Сигнал про подію — надходить до регіонального координаційного центру через «Безпека-Прикордоння».

2. Класифікація події – визначення рівня загрози (локальна/регіональна/надзвичайна ситуація).

3. Призначення керівної структури – залежно від характеру події (ВА або ДСНС).

4. Активація оперативного штабу – збір представників усіх суб’єктів.

5. Розгортання аварійно-рятувальних сил, координація комунальних служб, операторів КІ.

6. Комунікація з населенням – запуск єдиної системи оповіщення.

7. Звітність у режимі реального часу – оновлення даних у платформі.

8. Післяопераційний аналіз (After Action Review) – формування висновків та оновлення протоколів.

Цей алгоритм відповідає методології Incident Command System (ICS), широко застосовуваній у США, Канаді та країнах НАТО [8].

досконалення нормативно-правового забезпечення міжвідомчої координації

Виявлені у розділі 2 недоліки нормативно-правового забезпечення показали, що чинні акти не забезпечують достатньої чіткості повноважень суб'єктів безпеки. На думку експертів у сфері адміністративного права, «правова невизначеність у кризових умовах є одним з факторів управлінської дестабілізації» [9].

Пропонуються такі напрями вдосконалення:

1. Ухвалення регіональних "Порядків взаємодії у сфері забезпечення стійкості КІ", де чітко регламентуються функції кожної зі сторін.

2. Встановлення юридично обов'язкових стандартів обміну інформацією між ВА, ОМС та ДСНС.

3. Створення інституту уповноважених з питань КІ у громадах, які проходять спеціальну сертифікацію.

4. Оновлення підзаконних актів щодо кризового реагування, зокрема інструкцій з використання резервних джерел енергозабезпечення та алгоритмів дій при обстрілах.

5. Врегулювання правового статусу регіональних координаційних центрів, включно з їх повноваженнями та підпорядкуванням.

Зазначені кроки сприятимуть підвищенню юридичної чіткості системи й зменшенню управлінських ризиків.

Формування реальних міжвідомчих механізмів взаємодії

У практиці публічного управління часто наголошують, що комісії та робочі групи виконують функції формальних утворень без реального операційного впливу [10]. Для прикордонних регіонів це особливо небезпечно.

Пропонується створення функціональних механізмів взаємодії, що працюють у режимі реальної оперативності:

1. спільні чергування диспетчерів ВА–ДСНС–ОМС;
2. щоквартальні міжвідомчі навчання з моделюванням сценаріїв атак на КІ;
3. формування мобільних кризових груп, які виїжджають на події;
4. постійно діючі аналітичні групи при координаційних центрах;
5. введення механізму “оперативних брифінгів”, де рішення ухвалюються протягом 10–15 хвилин.

Такі механізми відповідають європейським стандартам оперативної готовності (EU Civil Protection Mechanism).

Модель Регіонального координаційного центру забезпечення стійкості критичної інфраструктури (далі – РКЦСКІ)

З огляду на міжнародні стандарти та результати аналітики, пропонується створити РКЦСКІ, який стане ядром управління безпекою критичної інфраструктури.

Структура центру:

1. Аналітичний відділ – оцінка ризиків, аналіз даних, прогнозування.
2. Оперативний штаб реагування – координація сил та засобів.
3. Сектор кризових комунікацій – робота з населенням та ЗМІ.
4. Цифрово-технічний сектор – адміністрування платформи «Безпека-Прикордоння».
5. Відділ взаємодії з операторами КІ.

Основні функції центру:

- управління реагуванням у реальному часі;
- забезпечення міжвідомчої координації;
- збір та аналіз інформації про КІ;
- формування резервних управлінських рішень;
- організація навчань та тренувань.

РКЦСКІ діятиме на принципах єдиного керівництва, інформаційної інтеграції та оперативної сумісності.

Основні пропозиції щодо вдосконалення координації взаємодії різних структур вміщено в таблицю нижче.

Право громадського нагляду у сфері захисту критичної інфраструктури реалізується громадянами України через громадські об'єднання, членами яких вони є, через депутатів місцевих рад, особисто шляхом звернення до Уповноваженого Верховної Ради України з прав людини або до державних органів у порядку, встановленому Конституцією України, Законом України "Про громадські об'єднання" та іншими законами України,

Таблиця 3.2 – Удосколаення координації взаємодії

Стан	Проблема	Пропоноване рішення
Інформація про інциденти передається різними каналами	Розбалансованість даних, затримки	Впровадження «Безпека-Прикордоння», уніфікація форматів повідомлень
Реагування здійснюється окремо кожним суб'єктом	Дублювання функцій, хаотичність	Єдиний алгоритм реагування, спільний штаб
Відсутнє нормативне закріплення алгоритмів	Неузгодженість повноважень	Регіональні Порядки взаємодії
Мобільні групи реагування не скоординовані	Повільність і фрагментованість дій	Створення міжвідомчих мобільних груп
Немає структурованого центру управління	Відсутність єдиного керівництва	Створення РКЦСКІ
Обмін даними не стандартизований	Хаос у комунікаціях	Протоколи ICS, стандартизовані форми
Комунікація з населенням неузгоджена	Можливість паніки, недовіра	Сектор кризових комунікацій РКЦСКІ
Недостатня підготовка кадрів	Низька якість реагування	Регулярні навчання, сертифікація

Таким чином, удосконалення координації між військовими адміністраціями, Державної слубою України з питань надзвичайних ситуацій та оргнами місцевого самоврядування має стратегічне значення для стійкості критичної інфраструктури прикордонних регіонів України. Створення цифрової системи «Безпека-Прикордоння», впровадження уніфікованих алгоритмів, формування координаційних центрів та оновлення нормативної бази забезпечать підвищення ефективності реагування та зменшення ризиків для життєво важливих об’єктів. Така модель відповідає сучасним міжнародним стандартам та принципам публічного управління.

ВИСНОВКИ

У магістерській роботі здійснено дослідження теоретичних, нормативно-правових та практичних аспектів системи забезпечення критичної інфраструктури України в умовах воєнних загроз та трансформації системи публічного управління. Увагу зосереджено на аналізі особливостей функціонування критичної інфраструктури прикордонних територій, оцінці стану координації між військовими та цивільними структурами, а також на обґрунтуванні напрямів удосконалення організаційно-правових і управлінських механізмів взаємодії.

Логіка дослідження передбачала послідовний перехід від узагальнення наукових підходів і міжнародного досвіду до аналізу реального стану координації в прикордонних регіонах України та формування практично орієнтованих пропозицій. Це дозволило сформувати цілісне розуміння проблеми та визначити ключові напрями підвищення ефективності системи забезпечення критичної інфраструктури в умовах воєнного стану.

За результатами проведеного дослідження сформульовано такі висновки:

1. Встановлено, що критична інфраструктура прикордонних регіонів України є складною багаторівневою системою об’єктів і сервісів, функціонування яких безпосередньо впливає на національну безпеку, життєзабезпечення населення та стійкість держави в умовах воєнних загроз. Особливості прикордонних територій зумовлюють підвищений рівень вразливості таких об’єктів та потребують спеціальних управлінських підходів до їх захисту.

2. Узагальнення підходів до класифікації критичної інфраструктури дозволило обґрунтувати доцільність її розгляду не лише як сукупності технічних об’єктів, а як соціально-управлінської системи, що функціонує у взаємозв’язку з інституціями публічної влади. У прикордонних регіонах ключову роль відіграють енергетична, транспортна, комунальна та інформаційна інфраструктура, що потребує пріоритетного захисту.

3. Дослідження теоретичних підходів до координації між військовими та цивільними структурами засвідчило, що в умовах воєнного стану традиційні ієрархічні моделі управління є недостатньо ефективними. Найбільш результативними є інтегровані моделі взаємодії, які поєднують елементи публічного управління, кризового менеджменту та міжвідомчої координації.

4. Аналіз нормативно-правового забезпечення захисту критичної інфраструктури в Україні показав, що чинна законодавча база загалом відповідає міжнародним стандартам, однак має фрагментарний характер і недостатньо враховує специфіку прикордонних регіонів. Це зумовлює потребу в удосконаленні правового регулювання шляхом розроблення спеціалізованих регіональних механізмів взаємодії.

5. У межах аналізу прикордонних регіонів України встановлено, що їхня критична інфраструктура функціонує в умовах постійного ризику фізичного ураження, обмеженого ресурсного забезпечення та високого навантаження на органи публічної влади. Наявні відмінності між регіонами зумовлюють необхідність диференційованого підходу до управління та захисту критичної інфраструктури.

6. Оцінка стану координації між військовими адміністраціями, органами місцевого самоврядування та ДСНС виявила низку системних проблем, зокрема дублювання функцій, недостатню формалізацію процедур взаємодії, обмежений обмін інформацією та розмитість управлінської відповідальності. Це негативно впливає на ефективність реагування на надзвичайні та кризові ситуації.

7. За результатами дослідження обґрунтовано доцільність удосконалення організаційно-правових механізмів взаємодії військових і цивільних структур шляхом запровадження типових регіональних актів, чіткого розмежування повноважень суб’єктів управління та інституціоналізації міжвідомчої координації на регіональному рівні.

8. Запропоновані управлінські механізми, орієнтовані на процесний підхід, спільне планування та інтегрований управлінський цикл, створюють умови для підвищення оперативності прийняття рішень і зменшення управлінських ризиків у сфері захисту критичної інфраструктури прикордонних регіонів.

9. Важливим результатом роботи є обґрунтування ролі кадрового забезпечення як ключового чинника ефективної взаємодії військових і цивільних структур. Доведено необхідність запровадження компетентнісного підходу, міжвідомчої підготовки кадрів, системи безперервного професійного розвитку та формування кадрового резерву для органів публічної влади прикордонних регіонів.

10. У цілому результати дослідження підтверджують, що удосконалення системи забезпечення критичної інфраструктури прикордонних регіонів України можливе лише за умови комплексного поєднання правових, організаційних, управлінських і кадрових заходів. Реалізація запропонованих у роботі рекомендацій сприятиме підвищенню стійкості регіонів, ефективності публічного управління та зміцненню національної безпеки України.

Отримані в ході дослідження результати підтверджують актуальність обраної теми та засвідчують, що подальше вдосконалення системи забезпечення критичної інфраструктури прикордонних регіонів України є важливою складовою зміцнення національної безпеки та підвищення ефективності публічного управління. Реалізація запропонованих у роботі теоретичних узагальнень і практичних рекомендацій сприятиме формуванню стійкої, скоординованої та адаптивної системи взаємодії військових і цивільних структур, здатної ефективно функціонувати в умовах сучасних безпекових викликів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України : Закон від 28.06.1996 № 254к/96-ВР (із змінами і доповненнями). URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр

2. Про оборону України : Закон України від 06.12.1991 № 1932-XII (із змінами). URL: https://zakon.rada.gov.ua/laws/show/1932-12

3. Про Збройні Сили України : Закон України від 06.12.1991 № 1934-XII (із змінами). URL: https://zakon.rada.gov.ua/laws/show/1934-12

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

5. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII (із змінами). URL: https://zakon.rada.gov.ua/laws/show/389-19

6. Про національний спротив : Закон України від 16.07.2021 № 1702-IX (із змінами). URL: https://zakon.rada.gov.ua/laws/show/1702-20

7. Про місцеве самоврядування в Україні : Закон України від 21.05.1997 № 280/97-ВР (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/280/97-вр

8. Про військово-цивільні адміністрації : Закон України від 03.02.2015 № 141-VIII (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/141-19

9. Про Державну службу України з надзвичайних ситуацій : Закон України. – URL: https://zakon.rada.gov.ua/laws/show/2006-19

10. Закон України «Про критичну інфраструктуру» №1882-IX від 16.11.2021. Відомості Верховної Ради України, 2022. №7, URL:https://zakon.rada.gov.ua/laws/show/1882-20#

11. Постанова Кабінету Міністрів України №1109 «Про перелік секторів критичної інфраструктури» від 09.10.2020. Урядовий кур'єр, 2020. №200.

12. Постанова Кабінету Міністрів України №518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19.06.2019. [Електронний ресурс] cip.gov.ua

13. Постанова Кабінету Міністрів України №821 «Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури» від 22.07.2022. Відомості Верховної Ради України, 2022. №56.

14. Постанова Кабінету Міністрів України №1174 регламент обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури. [Електронний ресурс] – cip.gov.ua

15. Постанова Кабінету Міністрів України №373 «Про затвердження Положення про територіальні центри комплектування та соціальної підтримки». Відомості Верховної Ради України, 2014. №45.

16. Постанова Кабінету Міністрів України №700 «Про затвердження Порядку планування заходів територіальної оборони» від 2022 р. Відомості Верховної Ради України, 2022. №78.

17. Постанова Кабінету Міністрів України №518 «Про утворення військових адміністрацій». Відомості Верховної Ради України, 2015. №13.

18. Абрамов В. І. Державна політика у сфері захисту критичної інфраструктури України. Київ : НАДУ, 2020. – 256 с.

19. Бакуменко В. Д. Державне управління: теорія і практика. Київ : НАДУ, 2018. 520 с.

20. Бортніков М. М. Міжвідомча координація в умовах надзвичайних ситуацій. Харків, 2022.

21. Бортніков М. М. Організаційно-правові механізми забезпечення національної безпеки України. Харків : Право, 2020. – 340 с.

22. Власюк О. С. Критична інфраструктура в системі економічної та національної безпеки України. Київ : НІСД, 2019. – 112 с.

23. Гуменюк Л. М. Психологічна готовність персоналу критичної інфраструктури до дій у кризових ситуаціях. Київ, 2022.

24. Жаліло Я. А. Забезпечення стійкості критичної інфраструктури в умовах гібридних загроз. –Київ : НІСД, 2021.

25. Іванюта С. П. Управління ризиками критичної інфраструктури в умовах надзвичайних ситуацій. Київ, 2020.

26. Качинський А. Б. Управління ризиками національної безпеки. Київ : НІСД, 2020.

27. Кириленко О. П. Інституційна спроможність органів публічної влади в умовах криз. Київ : Юрінком Інтер, 2021. 312 с.

28. Кириленко О. П. Публічне управління в умовах гібридних загроз. – Київ : Ліра-К, 2021.

29. Ковальчук Т. Т. Національна безпека України: виклики захисту критичної інфраструктури. Київ, 2021.

30. Кучеренко В. М. Цивільний захист в умовах воєнних дій. Київ, 2022.

31. Литвин В. М. Територіальна оборона: управлінський аспект. Київ, 2022.

32. Мельник А. Ф. Публічне управління у сфері забезпечення стійкості критичної інфраструктури. Львів, 2022.

33. Міхненко А. М. Інституційні механізми захисту критичної інфраструктури в Україні. Київ : НАДУ, 2019. – 198 с.

34. Романенко Є. О. Державне управління системами життєзабезпечення та критичною інфраструктурою. Київ, 2020.

35. Ситник Г. П. Державна політика у сфері національної безпеки України. – Київ : НАДУ, 2020. 408 с.

36. Тищенко О. В. Цивільний захист і критична інфраструктура: управлінський аспект. Харків, 2021.

37. Шевцов А. І. Національна стійкість України та захист критичної інфраструктури. Київ : НІСД, 2022.

39. Anderson, P. Border Region Resilience Strategy. Cambridge: Cambridge University Press, 2020.

40. Geneva Centre for Security Sector Governance (DCAF). Civil–Military Cooperation Handbook. Geneva, 2020.

41. INTERPOL. Guidelines for Crisis Information Sharing. Lyon, 2022.

42. ISO / IEC standards (ISO 22301, ISO/IEC 27001). URL:https://www.iso.org

43. NATO. Civil Emergency Planning Committee Report. Brussels, 2020.

44. NATO. Civil-Military Cooperation in Crisis Management. Brussels, 2018.

45. NATO Cooperative Cyber Defence Centre of Excellence. Analytical Reviews on Crisis Coordination. Tallinn, 2019–2024.

46. Smith, J. Cross-Government Coordination in Hybrid Threats. London: Routledge, 2021.

47. UNDP. Digital Governance and Crisis Coordination. New York, 2021.

48. UNDP Ukraine. Strengthening Local Governance Under Crisis Conditions. New York, 2022.

49. UN OCHA. Humanitarian Response Plan for Ukraine. Geneva, 2023.

50. UNICEF. Risk Communication in Emergencies. Copenhagen, 2021.

51. USAID. Strengthening Local Institutions for Crisis Response. Washington, 2020.

52. U.S. Department of Homeland Security. Critical Infrastructure Framework. Washington, 2020.

53. Williams, R. Military–Civil Emergency Response. Oxford, 2019.

54. Analitycal pieces on Ukraine's critical infrastructure resilience (2019–2024). – URL: https://ec.europa.eu

55. UK / Germany legislative examples on critical infrastructure (2024–2025). URL: https://www.reuters.com