МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЕКОЛОГІЧНОЇ БЕЗПЕКИ, ІНЖЕНЕРІЇ ТА ТЕХНОЛОГІЙ
КАФЕДРА ЦИВІЛЬНОЇ ТА ПРОМИСЛОВОЇ БЕЗПЕКИ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ Б.Д. ХАЛМУРАДОВ
«_____»_____ 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА

СПЕЦІАЛЬНІСТЬ 263 «ЦИВІЛЬНА БЕЗПЕКА»

Тема: **«ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»**

Виконавець: студент групи ЦБ 201Мз КІЧАТА Наталія Миколаївна
(студент, група, прізвище, ім'я, по батькові)

Керівник: д.т.н., професор Третьяков Олег Вальтерович
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

Нормоконтролер: _____ Федина В.П.
(підпис) (П.І.Б)

КИЇВ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Факультет екологічної безпеки, інженерії та технологій
Кафедра цивільної та промислової безпеки
Спеціальність 263 «Цивільна безпека»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____Б.Д. Халмурадов
«____» _____ 2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи
КІЧАТОЇ НАТАЛІЇ МИКОЛАЇВНИ

1. Тема роботи: **«Підвищення ефективності реалізації державної політики у сфері захисту критичної інфраструктури»** затверджено наказом ректора від «10» жовтня 2023 року № 2075/ст.

2. Термін виконання роботи: з 02.10. 2023 р. по 31.12. 2023 року.

3. Вихідні дані до роботи: аналіз нормативно-правової бази у сфері захисту критичної інфраструктури, статистичні данні щодо оцінки ризиків критичній інфраструктури, методи індентифікації основних загроз та небезпек об’єктів критичної інфраструктури.

4. Зміст пояснювальної записки: аналітичний огляд літературних джерел з тематики диплому. Організаційні заходи щодо забезпечення захисту об’єктів критичної інфраструктури. Визначення різних типів загроз і небезпек на сферу критичної інфраструктури. Методи оцінки загроз критичній інфраструктурі Надання рекомендацій щодо підвищення ефективності реалізації державної політики у сфері захисту критичної інфраструктури.

5. Перелік обов'язкового ілюстративного матеріалу: класифікація критичних інфраструктур, таблиці, рисунки.

6. Календарний план–графік

№ з/п	Завдання	Термін виконання	Підпис керівника
1.	Отримання та уточнення завдання	02.10.2023	
2.	Пошук та огляд літературних джерел	03.10.2023 - 16.10.2023	
3.	Аналітичний огляд основних заходів захисту об’єктів критичної інфраструктури	17.10.2023 – 23.10.2023	
4.	Написання тез до конференції	24.10.2023 – 02.11.2023	
5.	Аналізування нормативно-правового регулювання у сфері захисту критичної інфраструктури	03.11.2023 – 11.11.2023	
6.	Дослідження методів оцінки загроз критичній інфраструктурі	12.11.2023 – 22.11.2023	
7.	Обгрунтування напрямків щодо реалізації державної політики у сфері захисту критичної інфраструктури	23.11.2023 – 30.11.2023	
8.	Формування висновків по кваліфікаційній роботі	01.12.2023 – 09.12.2023	
9.	Оформлення пояснювальної записки	10.12.2023 – 14.12.2023	
10.	Попередній захист кваліфікаційної роботи	15.12.2023	

7. Дата видачі завдання: «02» жовтня 2023 р.

Керівник кваліфікаційної роботи: _____ О.В.Третьяков

Завдання прийняв до виконання: _____ Н.М. Кічата

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Підвищення ефективності реалізації державної політики у сфері захисту критичної інфраструктури» містить: **88 с., 5 рис., 5 табл., 68 літературних джерел.**

Об'єкт дослідження – система державного управління безпекою та забезпеченням життєво важливої інфраструктури для населення і територій.

Предмет дослідження – нормативне та адміністративне забезпечення державного управління критичною інфраструктурою.

Мета кваліфікаційної роботи – полягає в обгрунтуванні теоретичних засад та розробці практичних рекомендацій щодо вдосконалення державного управління забезпеченням безпеки критично-важливих об'єктів.

Методи дослідження, застосовані в дипломній роботі: аналіз та синтез – для деталізації об'єкта дослідження; узагальнення та порівняння – для дослідження закономірностей державного управління забезпеченням безпеки критичної інфраструктури в Україні; ідентифікації – для встановлення основних загроз та небезпек; експертний метод з метою оцінки рівня загроз надзвичайних ситуацій на важливих об'єктах України, аналіз взаємозв'язків між складовими системами захисту критичної інфраструктури.

Практичне значення роботи полягає в тому що теоретичні та методичні основи дослідження роботи були перетворені на конкретні рекомендації удосконалення управління у сфері захисту КІ, та пропозиції, які можуть бути застосовані в різних сферах.

Розроблені автором рекомендації можуть бути запропоновані для подальшої розробки концептуальних засад розвитку захисту критичної інфраструктури в Україні.

КРИТИЧНА ІНФРАСТРУКТУРА, ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ, ДЕРЖАВНА ПОЛІТИКА, ЗАГРОЗИ, НЕБЕЗПЕКИ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ

КІ – критична інфраструктура

ЄС – Європейський Союз

РНБО – Рада національної безпеки і оборони України

ДСНС – Державна служба України з надзвичайних ситуацій

СБУ – Служба безпеки України

АТЦ – Антитерористичний центр

ЦЗ – цивільний захист

ВСТУП

Актуальність теми. Світові тенденції, спрямовані на збільшення негативних явищ природного та техногенного характеру, наростання терористичних загроз, і інтенсивні кібератаки, а також вражаючі події нашого часу, виголошують актуальність питань щодо захисту інфраструктури, яка є визначеною як «критична» для життєвого функціонування людства, суспільства і держави.

У сучасних умовах війни, коливань у світовій економіці та нестабільності зовнішнього середовища стало очевидним, що критичні інфраструктури (КІ) виявляють вразливість та обмежену здатність до адаптації на мікрорівні. Ці системи не здатні ефективно протистояти та подолати існуючі труднощі. Забезпечення стійкості та сприяння розвитку є одним із основних завдань будь-якої економіки. Стійкість економічної системи визначається як ключовий фактор для забезпечення росту та нормального функціонування країни та її регіонів, а також для ефективної діяльності галузей економіки на зовнішніх і внутрішніх ринках.

У країнах, які тісно слідкують за своєю національною безпекою, термін «критична інфраструктура» визначає об’єкти та системи, які є настільки важливими для життєдіяльності громадян і функціонування держави, що будь-які порушення їхньої роботи можуть мати катастрофічні наслідки. Особливу загрозу становлять ситуації, коли відмова одного об’єкта критичної інфраструктури може спричинити порушення роботи інших об’єктів через їх взаємозалежність («ефект доміно»). З іншого боку, до критичної інфраструктури відносять особливо небезпечні промислові об’єкти, де навіть невеликі аварії, спричинені будь-якими причинами, можуть мати глобальні наслідки.

Сучасна військова обстановка в Україні несе загрозу не лише самій країні, але й країнам Європейського Союзу (ЄС). Ця ситуація вимагає спільних рішень для створення комплексної системи захисту України. У такому контексті об’єкти критичної інфраструктури стають особливо вразливими перед можливими диверсіями, терористичними актами та несанкціонованими втручаннями. Країна-

агресор використовує життєво важливі об’єкти як інструмент для морально-психологічного тиску на цивільне населення з метою підвищення внутрішньої нестабільності країни. В таких умовах особливо важливі комплексні заходи на державному рівні, які повинні бути узгоджені між органами безпеки та правоохоронними структурами, зокрема для протидії сучасним загрозам гібридного характеру.

Важливість обґрунтування актуальної державної політики у сфері захисту критичної інфраструктури в умовах війни в Україні визначається кількома факторами:

1. По-перше, наслідки ракетних ударів, аварій, катастроф та інших надзвичайних ситуацій стають все більш масштабними та загрожують безпеці населення та стабільному функціонуванню економіки та забезпеченню життєво важливих потреб населення.

2. По-друге, кризові ситуації, що виникли в українському суспільстві під час військової агресії, є надзвичайними для сучасного світу. Ці події підкреслили важливість злагодженої державної політики у сфері захисту критичних інфраструктурних об’єктів та необхідність глобальних перетворень в цій галузі.

3. Третя важлива аспектів стосується організаційної структури, функціонування та майбутнього розвитку системи захисту критичної інфраструктури та визначення ролі держави. Найбільш важливим є розгляд питань, пов’язаних із формуванням державної політики щодо захисту критичних об’єктів у мирний та воєнний період. Однією з ключових справ є створення спеціалізованих органів управління, відповідальних за захист критичної інфраструктури в умовах надзвичайних ситуацій на всіх рівнях державного та місцевого управління, визначення їх завдань і функцій.

Створення системи спеціально уповноважених органів управління у сфері захисту критичної інфраструктури на всіх рівнях державної влади та місцевого самоврядування, визначення їхніх завдань та функцій, слід розглядати як пріоритетну галузь державної політики, яка допомагає забезпечити ефективний засіб КІ в умовах сучасних загроз.

Мета і завдання виконання кваліфікаційної роботи полягає в обгрунтуванні теоретичних засад та розробці практичних рекомендацій щодо вдосконалення державного управління забезпеченням безпеки критично-важливих об'єктів. Заради досягнення поставленої мети потрібно визначити і вирішити такі завдання:

- розкрити сутність державного управління забезпеченням безпеки об'єктів критичної інфраструктури;

- визначити функції та повноваження державної політики у сфері захисту критичної інфраструктури;

- виявити загрози та небезпеки, які впливають на сферу критичної інфраструктури в Україні;

- здійснити оцінку нормативного й адміністративного забезпечення державного управління критичною інфраструктурою;

- запропонувати шляхи вдосконалення державної політики захисту критичної інфраструктури в Україні.

Об'єкт дослідження – система державного управління безпекою та забезпеченням життєво важливої інфраструктури для населення і територій.

Предмет дослідження – нормативне та адміністративне забезпечення державного управління критичною інфраструктурою.

Методи дослідження, застосовані в кваліфікаційній роботі: аналіз та синтез – для деталізації об'єкта дослідження; узагальнення та порівняння – для дослідження закономірностей державного управління забезпеченням безпеки критичної інфраструктури в Україні; ідентифікації – для встановлення основних загроз та небезпек; експертний метод з метою оцінки рівня загроз надзвичайних ситуацій на важливих об'єктах України, аналіз взаємозв'язків між складовими системами захисту критичної інфраструктури.

Наукова новизна отриманих результатів полягає в:

- розкрита сутність, основні завдання і недоліки існуючої системи державного управління забезпеченням безпеки об'єктів критичної інфраструктури;

- запропонуванні стратегії розробки ефективної системи комунікацій між різними рівнями управління та між суб'єктами критичної інфраструктури для оперативного обміну інформацією та координації заходів у разі загроз;
- аналізі нових, раніше невизначених, загроз для об'єктів критичної інфраструктури експертним методом;
- запропонованій необхідності розробки алгоритму дій при появі відповідних загроз для типових об'єктів критичної інфраструктури;
- наданні пропозицій щодо підвищення освіти та кваліфікації керівного складу і фахівців у галузі захисту об'єктів критичної інфраструктури з урахуванням сучасних тенденцій та викликів;

Практичне значення отриманих результатів. Матеріали кваліфікаційної роботи можуть бути використані для оцінки потенційних небезпек на сферу критичних інфраструктур. Теоретичні та методичні основи дослідження роботи були перетворені на конкретні рекомендації удосконалення управління у сфері захисту КІ, та пропозиції, які можуть бути застосовані в різних сферах: у наукових дослідженнях як основа для подальшої розробки концептуальних засад розвитку захисту критичної інфраструктури в Україні; у процесі управління критично важливими об'єктами, як основа для вдосконалення державної політики України зі забезпечення безпеки та підвищення стійкості об'єктів критичної інфраструктури; в межах функціонування органів самоврядування для покращення державної системи захисту критичної інфраструктури; і під час розробки нормативних засад державного управління забезпеченням безпеки критичної інфраструктури, а також для підвищення освіти та кваліфікації керівного складу і фахівців у галузі захисту об'єктів критичної інфраструктури.

Публікації. Основні положення та результати дослідження за темою кваліфікаційної роботи відображено у двох наукових працях.

Кічата Н.М., Третьяков О.В. Підвищення ефективності реалізації державної політики у сфері захисту критичної інфраструктури. Тези доповідей одинадцятої міжнародної науково-технічної конференції «Проблеми інформатизації», Баку – Харків – Бельсько – Бяла, 2023р., с. 73.

Кічата Н.М., Третьяков О.В. Державний механізм забезпечення захисту критичної інфраструктури. *Людина, суспільство, комунікативні технології* : зб. матеріалів 11 міжнар. наук.-техн. конф. 27–28 жовт. 2023 р. Харків : УкрДУЗТ, 2023. С. 214–216.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ СУЧАСНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Побудова сучасної системи захисту критичної інфраструктури базується на ряді теоретичних основ і підходів, які спрямовані на забезпечення стійкості та безпеки важливих об’єктів та послуг, що є життєво важливими для суспільства. Основні теоретичні аспекти цієї побудови включають аналіз самої критичної інфраструктури та її потенційних загроз та ризиків, які можуть вплинути на неї. Система захисту критичної інфраструктури повинна бути спроектована з урахуванням можливості стійкості та можливості швидкого відновлення в разі надзвичайних ситуацій. Це включає розробку планів для відновлення послуг та інфраструктури. Важливим аспектом забезпечення безпеки критичної інфраструктури є співпраця між різними зацікавленими сторонами, включаючи державні органи, приватні компанії та громадські організації, співпраця між країнами, розроблення відповідної законодавчої та нормативної бази щодо захисту критичної інфраструктури, застосування передових технологій, включаючи системи моніторингу, кіберзахисту, системи виявлення і реагування на загрози.

Побудова сучасної системи захисту критичної інфраструктури – це складний та багатоаспектний процес, який вимагає поєднання технічних, організаційних, правових та міжнародних підходів для забезпечення безпеки та стійкості цих важливих об’єктів.

Пріоритетність у актуалізації непорушності основних принципів і фундаментальних засад забезпечення національної безпеки має надзвичайно важливе значення для будь-якої суверенної держави світу. Нині, в умовах військової агресії, для України це питання номер один у сфері державного управління.

Система захисту критичної інфраструктури в контексті національної безпеки України показує, що ця сфера має значний обсяг теоретичних досліджень українських та закордонних вчених. Автори, які зробили вагомий внесок у цю область: М.Б.

Домарацький, Я. О. Страхніцький, Д. Г. Бобро, Ю. А. Абрамов, С. С. Теленик, В. А. Андронов, Ю.М. Бєлоусов, Б. Е. Братка, П. Б. Волянський, А. Б. Качинський, В. В. Коврегін, В. А. Ліпкан, О. А. Мельниченко, Д. О. Полковниченко, В. О. Пономаренко, А. В. Ромін, В. П. Садковий, В. Ю. Стрельцов, Г. П. Ситник, М. В. Сунгуровський та інших.

У той же час, деяким аспектам цієї важливої проблематики, зокрема питанням розробки ефективних стратегій розвитку державного управління для критично важливих об’єктів, практично приділено не достатньо уваги. Ці проблеми залишаються недостатньо дослідженими, як з практичної, так і з теоретичної точки зору. Особливо сьогодні, в сучасних умовах війни і загроз національній безпеці України, досягнення стабільного соціально-економічного розвитку вимагає забезпечення економічної стійкості кожного регіону та стійкості соціально-економічних систем на більш низьких рівнях, таких як галузі, підприємства та фінансові установи. Наразі, росія використовує критичні об’єкти, необхідні для забезпечення життєвих потреб населення, як інструмент морально-психологічного тиску на мирне населення з метою зростання внутрішньої нестабільності у країні. У такому контексті особливо важливими стають комплексні заходи на рівні держави, що потребують взаємодії між різними безпековими та правоохоронними структурами для ефективного протистояння сучасним загрозам.

Система захисту критичної інфраструктури України має взаємодіяти з Єдиною державною системою цивільного захисту в рамках загальної системи безпеки країни. Співпраця між цими двома системами полягає в обміні інформацією, координації дій та спільному вирішенні питань, пов'язаних з захистом національної безпеки та готовності до надзвичайних ситуацій.

Ключовим аспектом співпраці між системою захисту критичної інфраструктури та Єдиною державною системою цивільного захисту в Україні є координація заходів під час надзвичайних ситуацій: Обидві системи повинні працювати разом під час надзвичайних подій, таких як природні катастрофи, техногенні аварії, терористичні загрози тощо. Координація дій дозволяє ефективно взаємодіяти та вирішувати ситуації.

Обидві системи повинні обмінюватися інформацією щодо поточного стану об'єктів критичної інфраструктури, можливих загроз і ризиків, а також здійснювати спільний моніторинг ситуації. Проводити спільне планування та тренування, це допомагає обом системам готуватися до надзвичайних ситуацій та реагувати на них швидко та координовано.

Загальна мета співпраці полягає в забезпеченні національної безпеки та готовності до різних небезпек, зокрема враховуючи потенційні загрози критичній інфраструктурі.

Задача кваліфікаційної роботи передбачає аналіз оцінки сучасної системи захисту критичної інфраструктури в Україні, виявлення потенційних загроз та небезпек які можуть вплинути на критичну інфраструктуру та розробку конкретних рекомендацій для поліпшення способів, якими держава захищає та забезпечує стійкість критичних об'єктів інфраструктури.

1.1 Сутність поняття критичної інфраструктури

У країнах, які використовують поняття «критична інфраструктура» для гарантування національної безпеки, під ними розуміють об’єкти і системи, які є настільки важливими для забезпечення життєдіяльності людей і держави, що будь-яке порушення їхньої роботи може призвести до серйозних негативних або навіть катастрофічних наслідків. Особливість небезпеки полягає в тому, що коли робота одного об’єкта критичної інфраструктури порушується, це може вплинути на роботу інших об’єктів і систем через їх взаємозалежність, спричиняючи такий ефект, який іноді називають «ефектом доміно» [1].

Враховуючи досвід Європейського Союзу, Сполучених Штатів, країн-членів НАТО, в Національному інституті стратегічних досліджень була розроблена Зелена книга щодо захисту критичної інфраструктури в Україні у 2015 році [2]. Цей документ узагальнює підходи до визначення «критичної інфраструктури» як «систем та ресурсів, будь то матеріальні або віртуальні, які забезпечують функціонування послуг та функцій, порушення яких може призвести до серйозних негативних наслідків для суспільства, соціально-економічного розвитку та національної безпеки». Документ

також визначає основні групи загроз для критичної інфраструктури, такі як техногенні аварії, природні катастрофи та зловмисні акти, і надає рекомендації стосовно секторів і принципів, на яких має ґрунтуватися подальший розвиток системи захисту критичної інфраструктури в Україні. Основною метою цієї системи є забезпечення можливості критичної інфраструктури функціонувати, а в разі перерви, якнайшвидше відновлювати функції, необхідні для життя людей, суспільства, бізнесу і держави.

Один з найбільш актуальних документів для впровадження заходів з захисту європейської критичної інфраструктури – це директива Ради ЄС 2008 року щодо «ідентифікації та позначення європейської критичної інфраструктури та оцінки потреби в її підвищенні захисту» [3]. Ця директива представляє собою перший крок у визначенні європейської критичної інфраструктури та в оцінці необхідності підвищення її рівня захисту, проте вона обмежується двома конкретними секторами (енергетика та транспорт), залишаючи питання включення інших секторів, таких як інформаційні та комунікаційні технології, на майбутнє.

У 2017 році Європейська комісія розпочала оцінку впровадження Директиви 2008 року та акцентувала увагу на її актуальності, ефективності, доданій вартості та стійкості для ЄС. Цей процес оцінки був завершений у 2019 році, що вказує на необхідність перегляду самої Директиви, включаючи інші сектори, крім енергетичного та транспортного, і враховуючи взаємозалежність між ними.

Варто зауважити, що відповідальність за захист критичної інфраструктури залишається національним органам влади, як детально викладено у роботі О. Мельничука [4].

Вперше на небезпеці знищення або пошкодження об’єктів критичної інфраструктури було відзначено у рішенні Ради національної безпеки і оборони України від 1 березня 2014 року під назвою «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» [5]. Важливість захисту критичної інфраструктури для забезпечення національної безпеки була підкреслена у Стратегії національної безпеки України і рішеннях РНБО України, прийнятих у 2016-2017 роках.

Критична інфраструктура України – це системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких може призвести до значних негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки [2].

Сутність цього поняття полягає в тому, що це інфраструктура, яка має високий рівень важливості і може бути об'єктом потенційних загроз, таких як природні катастрофи, кібератаки, терористичні акти, техногенні аварії тощо. Оскільки функціонування цих систем є критичним для забезпечення безпеки, здоров'я та економічного добробуту суспільності, їх захист і стійкість мають велике значення.

Прикладами критичної інфраструктури можуть бути: енергетична інфраструктура (електростанції, газопроводи, нафтопроводи, електричні мережі), транспортна інфраструктура (аеропорти, мости, тунелі, залізничні системи, морські та річкові порти), інформаційно-комунікаційна інфраструктура (мережі зв'язку, інтернет-інфраструктуру, дата-центри), водопостачання і каналізація, системи охорони здоров'я (лікарні, аптечні склади, системи телемедицини), фінансова і банківська інфраструктура, харчова інфраструктура (сховища продуктів, продуктові мережі) та інші сектори, що можуть бути важливими для національної безпеки та економіки, такі як оборона, вугільна промисловість тощо.

Сектор критичної інфраструктури охоплює всі об'єкти, що відносяться до певної галузі економіки або мають спільну функціональну спрямованість в межах цього сектору. У Постанові Кабінету Міністрів України від 16 грудня 2022 р, № 1384 наведено перелік секторів критичної інфраструктури [27].

Відповідно до Постанови, уповноважені органи визначають об'єкти критичної інфраструктури в своїх секторах (підсекторах) критичної інфраструктури, використовуючи перелік секторів (підсекторів) і основних послуг цієї інфраструктури.

Секторальні органи вказують на різні галузеві міністерства та відомства, які відповідають за різні аспекти управління та регулювання в сфері захисту КІ. Секторальних органів в переліку багато, на сьогодні найважливіші з них, це:

Міністерство енергетики, Міністерство регіонального розвитку, Міністерство інфраструктури, Міністерство стратегічного розвитку.

Наприклад, до Міністерства енергетики належить паливно-енергетичний сектор та такі підсектори, як електроенергетика, вугільно-промисловий комплекс, торфодобування, нафтова та газова промисловості, ядерна енергетика (табл.1.1, рис.1.1).

Таблиця 1.1 – **Відповідальність Міністерства енергетики за регулювання в сфері захисту критичної інфраструктури**

Секторальний орган	**Сектор**	**Підсектор**	**Тип послуги**
Міністерство енергетики	Паливно-енергетичний сектор	Електроенергетика	1.Виробництво та розподіл електроенергії. 2.Ззабезпечення функціонування ринку електроенергії. 3.Управління системами передачі та енергопостачання.
		Вугільно-промисловий комплекс	1.Видобуток вугілля для генерації електроенергії. 2.Зберігання та постачання вугілля.
		Торфодобування	1.Розробка родовищ торфу. 2.Видобування корисних копалин.
		Нафтова промисловість	1.Видобуток, зберігання та постачання нафти та нафтопродуктів. 2.Очищення, переробка та обробка нафти.

Продовження таблиці 1.1

	Газова промисловість	1.Видобуток, переробка та очищення газу. 2.Передача, розподіл газу. 3.Експлуатація газотранспортної системи. 4.Зберігання природного газу.
	Ядерна енергетика	1.Виробництво ядерного палива. 2.Експлуатація ядерних реакторів. 3.Експлуатація атомних електростанцій, підприємств і установок по збагаченню та переробці палива, а також сховищ відпрацьованого палива.

Рис.1.1 – Енергетичні мережі

Міністерство регіонального розвитку відповідає за сектор системи життєзабезпечення (табл.1.2, рис.1.2).

Таблиця 1.2 – **Відповідальність Міністерства регіонального розвитку за регулювання в сфері захисту КІ**

Секторальний орган	**Сектор**	**Підсектор**	**Тип послуги**
Міністерство регіонального розвитку	Системи життєзабезпечення	Комунальні послуги	1.Постачання теплової енергії. 2.Постачання гарячої води. 3.Централізоване питне водопостачання. 4.Централізоване водовідведення. 5.Поводження з побутовими відходами.

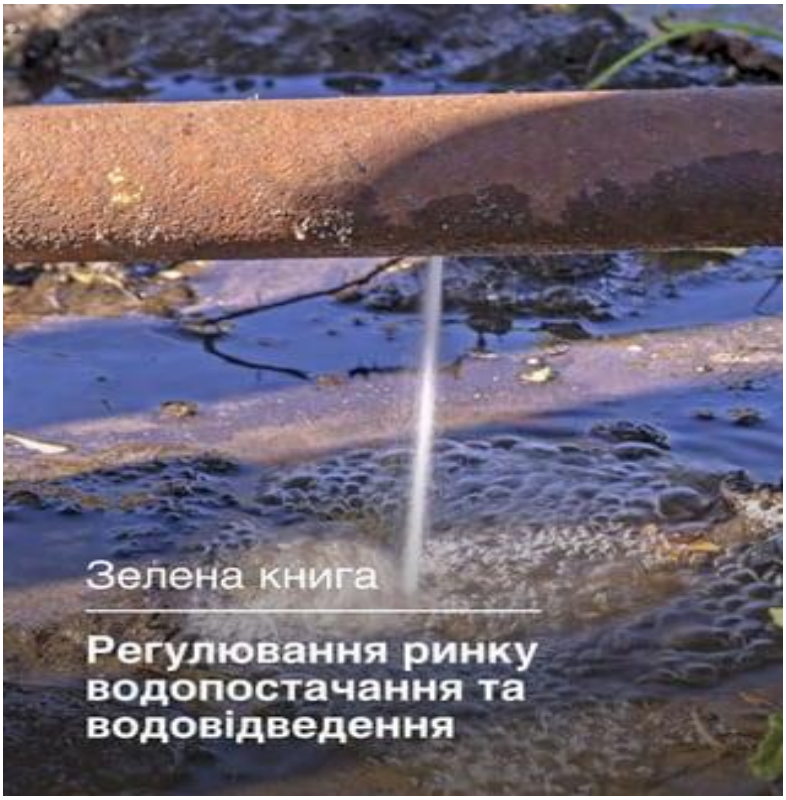

Рис.1.2 – Водопровідно-каналізаційна галузь

Міністерство інфраструктури відвовідає за сектор транспорт і пошта (табл.1.3, рис.1.3).

Таблиця 1.3 – **Відповідальність Міністерства інфраструктури за регулювання в сфері захисту КІ**

Секторальний орган	**Сектор**	**Підсектор**	**Тип послуги**
Міністерство інфраструктури	Транспорт і пошта	Авіаційний транспорт	1.Управління повітряним рухом, авіаперевезення. 2.Забезпечення роботи аеропортів та обладнання в аеропортах.
		Автомобільний та міський електротранспорт, у тому числі метрополітен	1.Автобусні перевезення (міжміські, міжнародні), міські перевезення. 2.Технічне обслуговування транспортної інфраструктури (доріг, мостів, тунелів, шляхопроводів). 3.Управління рухом, мобільністю, взаємодія з іншими видами транспорту.
		Залізничий транспорт	1.Пасажирські, вантажні залізничні перевезення. 2.Експлуатація та технічне обслуговування залізниці. 3.Забезпечення роботи вокзалів та вузлових станцій.
		Морський та річковий транспорт	1.Контроль і управління судноплавством, регулювання руху суден. 2. Операції на транспорті.

Продовження таблиці 1.3

			3.Функціонування керуючих органів портів (суб'єктів) експлуатації портового обладнання. 4.Експлуатація та обслуговування інфраструктури (каналів, дамб, фарватерів тощо).
		Поштовий зв'язок	1.Надання послуг поштового зв'язку.

Рис.1.3 – Транспортна інфраструктура

Сектор промисловості грає ключову роль у сфері захисту критичної інфраструктури. Міністерство стратегічного розвитку відіграє важливу роль у координації заходів щодо захисту критичної інфраструктури в промисловому секторі. Це може включати розробку стратегій та політик безпеки, визначення ризиків, встановлення стандартів захисту, а також співпрацю з іншими секторами та владними органами для вирішення загальних завдань забезпечення безпеки (табл. 1.4, рис.1.4).

Таблиця 1.4 – **Відповідальність Міністерства стратегічного розвитку за регулювання в сфері захисту КІ**

Секторальний орган	**Сектор**	**Підсектор**	**Тип послуги**
Міністерство стратегічного розвитку	Промисловість	Хімічна промисловість	1. Виробництво промислового газу. 2. Виробництво добрив, пестицидів та інших агрохімічних сполук. 3.Виробництво вибухових речовин та органічних та неорганічних речовин.
		Металургійна промисловість	1.Металургійне виробництво та добування залізних руд. 2.Виробництво коксу та коксопродуктів.
		Оборонна промисловість	1.Розробка, виробництво, модернізація та утилізація продукції військового призначення (оборонно-промисловий комплекс)
		Космічна промисловість	1.Виробництво та постачання космічної техніки. 2.Космічна діяльність, космічні технології та послуги.
		Авіаційна промисловість	1.Виробництво та постачання продукції авіаційної промисловості.
		Суднобудівна промисловість	1.Суднобудування та постачання продукції суднобудування.

Рис.1.4 – Авіаційна промисловість

Критично важливим для забезпечення ефективного функціонування та захисту національної інфраструктури України є взаємодія між всіма секторами об’єктів критичної інфраструктури по регіонах.

Одні сектори можуть бути взаємозалежними, і порушення в одному секторі може мати наслідки для інших. Така взаємодія може включати обмін інформацією, розробку спільних стратегій захисту, планування екстрених ситуацій, а також координацію дій у разі кризових подій.

Забезпечення ефективної взаємодії між секторами в регіонах допомагає зменшити ризики та підвищити стійкість перед потенційними загрозами, такими як військові дії, техногенні аварії, кібератаки та інші небезпеки. У цьому контексті розвиток механізмів співпраці та обміну інформацією між різними секторами та регіональними органами стає ключовим елементом забезпечення стійкості та безпеки національної критичної інфраструктури України.

Національна безпека визначається станом захищеності та збереженням суверенітету, територіальної цілісності, політичної стабільності та економічного розвитку країни. Однак ці аспекти національної безпеки можуть залежати від впливу регіональних факторів і подій.

Регіональна безпека в сфері захисту КІ включає в себе забезпечення стабільності та безпеки критичних об’єктів в конкретному регіоні. У випадку України регіональна безпека важлива через наявність різних геополітичних, економічних та соціокультурних викликів у сусідніх регіонах. Наприклад, військові дії на території

України та напруженість у відносинах з окремими сусідніми країнами можуть впливати на національну безпеку країни.

На рис.1.5 можна побачити динаміку по Україні в сфері захисту КІ паливно-енергетичного сектору в 2022-2023 роках [1]. Слід зазначити, що порушення чи припинення функціонування паливно-енергетичного сектору може призвести до втрати управління економікою України, її регіонів, а також до значного зниження безпеки життєдіяльності населення, яке проживає в цих районах протягом тривалого часу.

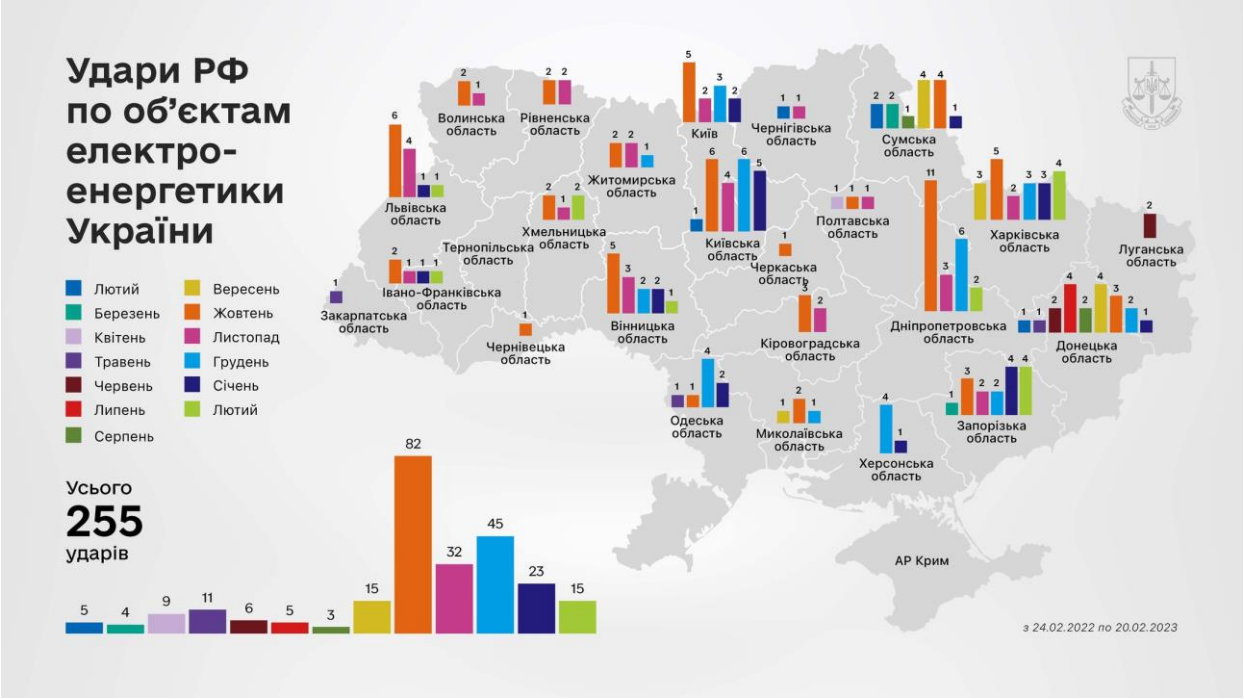

Рис.1.5 – Динаміка дестабілізації енергетичного сектору по регіонам України

Отже, забезпечення національної безпеки України вимагає уважного врахування регіональних контекстів та спрямованих на співпрацю заходів для вирішення спільних проблем і забезпечення стабільності в регіоні.

З метою визначення ступеня вимог щодо захисту об'єктів критичної інфраструктури відповідно до їхнього рівня важливості для забезпечення окремих життєвоважливих функцій в межах секторів критичної інфраструктури, застосовано категоризацію об'єктів критичної інфраструктури за різними рівнями критичності [6]. Ця категоризація включає наступні рівні:

І категорія критичності: особливо важливі об’єкти, які мають загальнодержавне значення, значно впливають на інші об’єкти критичної інфраструктури, і порушення їхнього функціонування може викликати кризову ситуацію державного значення.

ІІ категорія критичності: життєвоважливі об’єкти, порушення функціонування яких може викликати кризову ситуацію регіонального значення.

ІІІ категорія критичності: важливі об’єкти, порушення функціонування яких може викликати кризову ситуацію місцевого значення.

ІV категорія критичності: необхідні об’єкти, порушення функціонування яких може викликати кризову ситуацію локального значення.

Визначення категорій критично важливих об’єктів критичної інфраструктури в Україні ґрунтується на спеціалізованих підходах, зокрема врахуванні секторальних особливостей. Цей підхід базується на розгляді критеріїв, пов’язаних із забезпеченням безпеки в різних аспектах національної безпеки, таких як економічна, політична, державна, енергетична, екологічна та інші. Це призвело до розроблення різних визначень для об’єктів КІ. Наприклад, підприємства, що є стратегічно важливими для економіки та безпеки держави, або значущі державні об’єкти, або об’єкти, які підлягають захисту та обороні в умовах надзвичайних ситуацій та в особливий період, або потенційно небезпечні та об’єкти підвищеної небезпеки, або особливо важливі об’єкти у сфері електроенергетики та нафтогазової промисловості.

Термін «критично-важливі об’єкти» використовується у законодавстві багатьох країн, і хоча його термінологія може трохи відрізнятися, ці різниці не мають значущого впливу. У Законі України «Про критичну інфраструктуру» [6], категорія критичності об’єкта критичної інфраструктури визначається як ступінь або рівень важливості об’єкта, і вона класифікується залежно від впливу цього об’єкта на здійснення життєво важливих функцій або надання необхідних життєвих послуг.

Забезпечення безпеки і захисту критичної інфраструктури є однією з ключових функцій держави, оскільки недостатність або втрата функціонування таких систем може призвести до серйозних наслідків для економіки, суспільства та національної безпеки. В таблиця 1.5 відображені сучасні промислові об’єкти КІ України різних секторів станом на сьогодні [7].

Таблиця 1.5 – **Найбільші уражені промислові об’єкти (згідно з наявною інформацією за даними Міністерства регіонального розвитку, 2022-2023рр.)**

№	Підприємство	Галузь	Статус
1.	ММК ім. Ілліча	Металургія	Зруйновано
2.	Азовсталь	Металургія	Зруйновано
3.	Мотор Січ	Машинобудування	Пошкоджено
4.	Укртатнафта	Нафтопереробка	Зруйновано
5.	Зоря - Машпроект	Машинобудування	Зруйновано
6.	Українські енергетичні машини	Машинобудування	Пошкоджено
7.	Авдіївський коксохімічний завод	Коксохім	Пошкоджено
8.	Філіп Морріс Україна	Виробництво цигарок	Зруйновано
9.	Антонов	Авіабудування	Пошкоджено
10.	ЛИНІК	Нафтопереробка	Зруйновано
11.	Органік Сістемс	Харчова промисловість	Зруйновано
12.	Новокраматорський машинобудівнийзавод	Машинобудування	Пошкоджено
13.	Рубіжанський картонно-тарний комбінат	Виробництво паперу	Зруйновано
14.	Миколаївський глиноземний завод	Металургія	Пошкоджено
15.	Дніпроспецсталь	Металургія	Пошкоджено
16.	Сандора	Харчова промисловість	Пошкоджено
17.	Енергомашспецсталь	Машинобудування	Пошкоджено
18.	Одеський припортовий завод	Хімічна промисловість	Пошкоджено
19.	Кока-Кола Беверіджіз Україна	Харчова промисловість	Пошкоджено

Продовження таблиці 1.5

20.	Одеський нафтопереробний завод	Нафтопереробка	Пошкоджено
21.	Сєвєродонецьке об’єднання “Азот”	Хімічна промисловість	Пошкоджено
22.	Запорізький залізорудний комбінат	Добування руди	Лише запаси
23.	Шляхове будівництво “Альтком”	Будівництво	Пошкоджено
24.	Фармак (склад продукції)	Фармацевтика	Пошкоджено
25.	Куб-Газ	Добування газу	Зруйновано

Співпраця з іншими відомствами та секторами є важливою, оскільки загрози можуть мати комплексний характер і вимагати взаємодії для ефективного управління та реагування. Забезпечення цілісності, доступності та захищеності промислової інфраструктури стає невід'ємною частиною загального зусилля з узгодженого захисту критичних ресурсів країни.

Сучасна Українська держава стикається з найскладнішим випробуванням з точки зору безпеки за всю свою історію незалежності. Гостра соціально-політична криза, військові дії, посилення екстремізму та тероризму, економічний спад, масштабна гуманітарна криза, руйнування та пошкодження численних підприємств і інфраструктурних об’єктів – це всі нові реалії, з якими сьогодні стикається Україна. В цих умовах головним пріоритетом є забезпечення безпеки громадян, суспільства і державних інституцій.

1.2 Основні завдання захисту критичної інфраструктури

Сучасне суспільство стрімко розвивається, що призводить до різних загроз, які, в основному, виникають через природні катастрофи, технічні аварії, людський фактор, тероризм або злочинну діяльність. У зв’язку з цим виникає потреба в прийнятті заходів для захисту економічних і соціальних компонентів інфраструктури, що є абсолютно необхідними для забезпечення безпеки суспільства та держави.

Особливу увагу в цьому контексті привертають об’єкти критичної інфраструктури, які мають велике значення для держави та суспільства в цілому. Не працездатність таких об’єктів може призвести до змін у повсякденному житті людей, перебоїв у постачанні сировинних ресурсів, серйозних порушень громадської безпеки або інших серйозних негативних наслідків [8].

Підвищення ефективності реалізації державної політики в сфері захисту критичної інфраструктури є критично важливим завданням для забезпечення безпеки та стабільності суспільства.

Один з основних аспектів конкретизації та визначення необхідних заходів для захисту об’єктів критичної інфраструктури – це постійна співпраця між державою і інфраструктурними організаціями. У такій ситуації держава виступає гарантом внутрішньої безпеки та виконує роль посередника в інформаційно-комунікаційних процесах. З іншого боку, інфраструктурні організації, які, як правило, володіють найбільш повною інформацією щодо конкретної кризової ситуації і мають найбільшу компетентність у вирішенні цих проблем (як технічно, так і професійно), здатні вживати ефективні заходи для захисту. З цього погляду, відповідні структури, які керують управлінням кризовими ситуаціями, повинні приймати конкретні заходи для усунення наслідків даної ситуації. Крім того, експерти та науковці підкреслюють необхідність створення системи контролю, такої як «система ризик-менеджменту, яка дозволить вчасно виявляти тенденції і факти, що становлять загрозу для подальшого існування суспільства» [9].

Захист критичної інфраструктури передбачає розробку та впровадження стратегій та заходів з метою забезпечення її стійкості, відновлення та захисту від можливих загроз. Це включає в себе заходи кібербезпеки, плани надзвичайних ситуацій, контингентні плани, технічні засоби захисту та інші заходи, спрямовані на запобігання та реагування на ризики та небезпеки, що можуть вплинути на критичну інфраструктуру.

Головною метою розробки концепції основних заходів для захисту об’єктів критичної інфраструктури є забезпечення безпеки людей шляхом зменшення ризику вразливості критичних компонентів інфраструктури перед військовими атаками,

природними катастрофами, технічними неполадками або помилками людей, а також зниження рівня вразливості до актів тероризму. Ця концепція має включати в себе стандартизовані будівельні, організаційні, кадрові та технічні заходи безпеки, які допоможуть забезпечити захист [2, 10].

В Україні захист об'єктів, які, відповідно до міжнародної практики, вважаються «критичною інфраструктурою» регулюється різними нормативно-правовими актами, які, переважно, стосуються внутрішнього використання. Така ситуація виникла логічно, оскільки кожне окреме відомство було спроможним визначити конкретні загрози для своїх підпорядкованих об'єктів і володіло власним набором інструментів та ресурсів для забезпечення їх безпеки.

Як вказано в Законі України «Про критичну інфраструктуру» [6] серед завдань, пов'язаних із формуванням та впровадженням державної політики захисту критичної інфраструктури України та створення відповідної державної системи, можна виділити такі аспекти: забезпечення безпеки, стійкості та недоторканності критичної інфраструктури України, запобігання кризовим ситуаціям, які можуть призвести до порушень в роботі критичної інфраструктури, утворення та організація державної системи захисту критичної інфраструктури, розроблення нормативно-правової бази по питанням безпеки об'єктів, розроблення та реалізація державних цільових програм, розроблення комплексу заходів, аналіз сучасних викликів та загроз, які можуть вплинути на стійкість критичної інфраструктури, а також оцінка рівня її захищеності.

Мета захисту критичної інфраструктури в Україні випливає з визначення критичних інфраструктурних об'єктів і полягає у гарантуванні надходження населенню, суспільству, бізнесу і державі необхідних та життєво важливих товарів і послуг. Для виконання цієї функції критичної інфраструктури необхідно забезпечувати безперебійну та стабільну роботу об'єктів критичної інфраструктури в установлених режимах, маючи здатність запобігати руйнуванню або непоправній шкоді, припиненню функціонування або втраті контролю над ними внаслідок будь-яких негативних впливів, і забезпечувати швидке відновлення їх функціонування в разі перерви.

Створення системи управління національним процесом захисту критичних об’єктів тісно пов’язане з розробкою основних стратегічних напрямів регіональної політики, яку здійснюють органи місцевого самоврядування в Україні для забезпечення критично важливих об’єктів в надзвичайних ситуаціях та у випадках терористичних актів. Розробка такої регіональної політики включає в себе багаторівневий процес, який повинен враховувати різні природні явища та інші фактори, що можуть мати вплив на загальну систему управління цим процесом. Це підкреслює В. Могильниченко [11] у своїх дослідженнях.

Враховуючи цілі побудови системи захисту критичної інфраструктури, можна сформулювати основні завдання цієї системи таким чином:

1. Забезпечення загальної координації захисту критичної інфраструктури в Україні.
2. Здійснення запобігання кризовим ситуаціям, управління в умовах кризової ситуації, пов’язаних із функціонуванням критичної інфраструктури, і забезпечення відновлення її функціонування.
3. Підтримка прийняття рішень щодо захисту критичної інфраструктури.
4. Застосування механізмів регулювання та контролю за функціонуванням критичної інфраструктури в режимі воєнного стану.

Сучасна критична інфраструктура держави представляє собою складний комплекс різноманітних компонентів, які мають різні характеристики. Вона включає в себе різні організаційні структури, різні моделі управління, функції та системи, які існують як у фізичному, так і в віртуальному просторі. Управління критичною інфраструктурою включає участь державних структур на всіх рівнях з різними областями відповідальності та повноваженнями, а також власників і операторів об’єктів і систем, що входять до критичної інфраструктури. У зв’язку з процесами глобалізації, національна безпека, виробництво, економіка і фінанси кожної країни стають залежними від чинників, що визначають стан безпеки в інших країнах і на глобальному рівні.

Останні роки відзначаються змінами в підходах України до регулювання та управління системою захисту об’єктів критичної інфраструктури. У цьому контексті

було прийнято відповідне законодавство. Основні організаційні завдання, що стосуються цього питання, покладено на Державну службу України з надзвичайних ситуацій (ДСНС). Серед численних функцій ДСНС України важливе місце відводиться реєстрації критично важливих об’єктів, моніторингу їхнього становища та нагляду за діяльністю виконавчих органів влади на рівні державних та місцевих органів [12]. Крім того, ДСНС України регулярно відслідковує так звані «потенційно небезпечні об’єкти», які потребують особливого контролю в плані готовності до запобігання, локалізації та ліквідації надзвичайних ситуацій. Оцінка таких об'єктів проводиться з урахуванням їхнього рівня небезпеки (частота перевірок, методи оцінки та наявність ліцензованих фахівців відповідної категорії).

У сучасний період відбувається формування нової філософії забезпечення безпеки, яка базується на спільних зусиллях громадян, суспільства, бізнесу і держави.

Отже, на першому місці встановлено саме забезпечення захисту об’єктів критичної інфраструктури на території Україні. Варто відзначити, що Закон «Про критичну інфраструктуру» регламентує захист критичної інфраструктури у якості складової частини забезпечення національної безпеки України.

На сьогоднішній день, найбільшою проблемою, що стоїть перед наміром забезпечити стійкий розвиток регіонів нашої держави, є нестабільність зовнішнього оточення внаслідок війни російської федерації проти України. Ця нестабільність призвела до серйозних людських втрат, масового переміщення населення та значного пошкодження інфраструктури.

1.3 Нормативно-правове регулювання у сфері захисту КІ

Нормативно-правове регулювання у сфері захисту критичної інфраструктури включає в себе різноманітні закони, стандарти та положення, які мають на меті забезпечення безпеки та надійності критичних об’єктів. Зазвичай це регулювання орієнтоване на важливі сектори, такі як енергетика, транспорт, інформаційні технології, комунікації та інші, які є важливими для економічного функціонування та безпеки країни.

Загальний еволюційний шлях розвитку українського правового поля в питаннях захисту критичної інфраструктури досить трансформаційний. Вихідною точкою для

захисту критичної інфраструктури є Закон України «Про національну безпеку України» [13], який, відповідно до Конституції України , визначає основи та принципи національної безпеки та оборони. Цей закон встановлює цілі, основні засади державної політики та розмежовує повноваження державних органів у сферах національної безпеки та оборони.

Згідно з цим законом, на Службу безпеки України покладається контррозвідувальний захист об'єктів критичної інфраструктури.

Наступним важливим документом є Стратегія національної безпеки України 2015 року [14]. У цьому стратегічному документі були визначені актуальні загрози національній безпеці України, серед яких особливу увагу приділено саме агресивним діям Росії, спрямованим на виснаження української економіки та підрив суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території. Також визначено інші суттєві загрози, такі як неефективність системи забезпечення національної безпеки та оборони, корупція, неефективна система державного управління, економічна криза, виснаження фінансових ресурсів держави, загрози енергетичній, інформаційній, кібер та екологічній безпеці.

Отже, в рамках Стратегії національної безпеки України були визначені та закріплені в нормативних актах відносини в галузі захисту критичної інфраструктури. У цьому документі вперше в Україні введено поняття «захист критичної інфраструктури» і віднесено його до окремого правового статусу. Це надало змогу законодавцям розробити та узгодити спеціальне нормативно-правове забезпечення, що регулює захист критичної інфраструктури як самостійної та важливої сфери. Важливим аспектом у цій Стратегії є визначення не лише окремої категорії об'єктів критичної інфраструктури, але й конкретних загроз, які можуть становити потенційну небезпеку для цих об'єктів.

Основну роль в забезпеченні правильного функціонування механізму захисту об'єктів критичної інфраструктури в Україні відіграють підзаконні нормативно-правові акти, зокрема укази та розпорядження Президента України. Згідно зі статтею 106 Конституції України [15], Президент має повноваження видавати укази й розпорядження, які є обов'язковими до виконання на території України.

Наприклад, указом Президента України від 23 лютого 2022 року була затверджена Річна національна програма під егідою Комісії Україна – НАТО на 2022 рік [16]. У цьому нормативно-правовому акті визначено питання функціонування системи захисту критичної інфраструктури. Особливий акцент робиться на формуванні принципів цивільного контролю над сектором безпеки й оборони, підвищення рівня професійної компетентності держслужбовців, створення національної системи стійкості та реформування оборонної промисловості. Таке правове регулювання визначає ключові аспекти та завдання для ефективного захисту критичних об'єктів.

Основні аспекти функціонування механізму захисту об'єктів критичної інфраструктури, зокрема в протидії найбільш загрозливим явищам, таким як тероризм, забезпечуються через видачу актів Президента України. Ці акти визначають стратегічні напрямки та механізми боротьби з тероризмом. Наприклад, значимими є такі нормативно-правові акти:

1. Указ Президента України від 4 червня 2021 р. № 251/2021 [17]: Указом затверджено введення в дію рішення Ради національної безпеки і оборони України щодо результатів загальнодержавної системи боротьби з тероризмом.

2.Указ Президента України від 5 березня 2019 р. № 53/2019 [18]: цим Указом затверджено Концепцію боротьби з тероризмом в Україні. Документ визначає стратегічні принципи та заходи для ефективної протидії терористичним загрозам.

3. Указ Президента України від 9 липня 2019 р. № 506/2019 [19]: цим Указом затверджено Порядок проведення огляду загальнодержавної системи боротьби з тероризмом. Документ визначає процедури та вимоги для оцінки ефективності системи боротьби з тероризмом.

4. Указ Президента України «Про деякі питання координації діяльності суб'єктів боротьби з тероризмом» від 25 квітня 2013 р. [20]: Указ регулює питання координації різних суб'єктів, які здійснюють діяльність у сфері боротьби з тероризмом.

Ці акти визначають стратегічні пріоритети, спрямовані на забезпечення ефективної боротьби з тероризмом та мають обов'язковий характер для виконання на території України.

У контексті здійснення правового функціонування механізму захисту об'єктів критичної інфраструктури важливу роль набувають акти Президента України, які введено в дію на підставі рішень Ради національної безпеки і оборони України (РНБО), згідно зі статтею 107 Конституції України. Серед таких актів особливо важливі:

1.Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 7 листопада 2023 р. «Щодо додаткових заходів із посилення стійкості функціонування енергетичної системи» від 7 листопада 2023 р. № 737/2023 [21]: Указ стосується нейтралізації загроз енергетичній безпеці та посилення стійкості функціонування енергетичної системи.

2.Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 17 жовтня 2023 р. «Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій» від 17 жовтня 2023 р. № 695/2023 [22]: Указ стосується посилення обороноздатності і соціально-економічного розвитку держави, захисту об'єктів критичної інфраструктури, забезпечення життєдіяльності населення.

3.Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 р. «Про Стратегію кібербезпеки України» від 15 березня 2016 р. № 96/2016 [23]: Цей Указ стосується стратегічних аспектів кібербезпеки та визначає важливі напрямки дій для захисту інформаційних систем та об'єктів критичної інфраструктури.

4.Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 29 грудня 2016 р. «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» від 16 січня 2017 р. № 8/2017 [24]: Цей Указ визначає заходи для поліпшення захисту об'єктів критичної інфраструктури та підвищення їхньої стійкості.

Ці документи визначають конкретні стратегії та заходи для захисту об'єктів критичної інфраструктури та відіграють ключову роль у забезпеченні безпеки та стійкості системи.

Всі акти Президента України, які визначають правове забезпечення механізму захисту об'єктів КІ, можна класифікувати в три основні групи. Кожна з цих груп має свої особливості та спрямована на вирішення конкретних завдань. Наприклад, до першої групи відносяться нормативно-правові акти Президента, які створюють основу для подальших дій у сфері захисту; вони орієнтовані на визначення стратегії та закріплення основ розвитку механізму захисту об'єктів КІ.

Акти другої групи встановлюють основні напрями та можливі варіанти захисту об'єктів КІ від різноманітних загроз, зокрема тероризму. Ці документи фокусуються на конкретних аспектах захисту та визначають стратегії протидії конкретним небезпекам.

Третя група включає акти, які вводять в дію рішення Ради національної безпеки і оборони України (РНБО) з найважливіших питань функціонування механізму захисту об'єктів критичної інфраструктури. Ці документи надають юридичну силу та обов'язковість рішенням РНБО, що є ключовим для ефективного впровадження заходів з безпеки та захисту критичної інфраструктури.

Також ключовими юридичними документами, які визначають правові аспекти функціонування механізму захисту об'єктів критичної інфраструктури є акти Кабінету Міністрів України. Ці документи мають вирішальне значення у реалізації заходів з безпеки та ефективного захисту стратегічних об'єктів.

Зокрема, акти Кабінету Міністрів України встановлюють конкретні правила, стандарти та процедури, які визначають, як повинен функціонувати механізм захисту. Ці акти можуть охоплювати різні аспекти, такі як планування заходів безпеки, визначення об'єктів критичної інфраструктури, встановлення стандартів безпеки, та інші аспекти, необхідні для ефективного функціонування системи захисту.

Наприклад, розпорядженням Кабінету Міністрів України від 6 грудня 2017 року № 1009-р була ухвалена «Концепція створення державної системи захисту критичної інфраструктури» [25]. Цей правовий документ визначає проблеми, що виникають у

сфері захисту критичної інфраструктури, і вказує на нагальні завдання, які потребують негайного вирішення. Згідно з цією Концепцією, мета створення системи полягає в забезпеченні стійкості критичної інфраструктури до всіх видів загроз, включаючи природні, техногенні, протиправні дії та інші загрози. Одна з ключових проблем, якою займається ця Концепція, полягає у недостатності та неузгодженості нормативно-правового регулювання в цій сфері суспільних відносин.

У зазначеному розпорядженні визначено стратегічний курс щодо вирішення цих проблем, спрямований на створення системи, яка забезпечує ефективний та єдиноцільний захист критичної інфраструктури. Концепція слугує основою для подальших кроків та розвитку нормативно-правового середовища у сфері захисту критичної інфраструктури в Україні.

Отже, акти Кабінету Міністрів України слід розглядати як ключові інструменти у формуванні та реалізації правового середовища для захисту об’єктів КІ в Україні.

Сам Кабінет Міністрів України є визначальним суб’єктом, відповідальним за реалізацію правового забезпечення функціонування механізму захисту об’єктів критичної інфраструктури. Серед всіх документів важливе значення мають рішення Кабінету Міністрів, які встановлюють загальні принципи формування та розвитку механізму захисту об’єктів критичної інфраструктури. Наприклад, Постанова Кабінету Міністрів України від 19 червня 2019 року № 518, якою затверджено загальні вимоги до кіберзахисту об’єктів критичної інфраструктури [26]. Цей документ визначає стандарти та вимоги, які стосуються кібербезпеки, що є важливим аспектом захисту об’єктів критичної інфраструктури.

Постанова «Деякі питання об’єктів критичної інформаційної інфраструктури» Кабінету Міністрів України від 9 жовтня 2020 року № 943 [27] встановлює правові основи для визначення об’єктів критичної інформаційної інфраструктури та встановлює процедуру формування і ведення національного переліку та реєстру таких об’єктів.

Методика, ухвалена цією постановою, надає власникам та управлінцям об’єктів критичної інфраструктури можливість оцінити критичність інформаційних систем,

які забезпечують функціонування цих об’єктів та надання життєво важливих послуг та функцій.

На основі наданих операторами інформації про об’єкти критичної інформаційної інфраструктури державні органи формують секторальні переліки, а Адміністрацією Держспецзв’язку створюється національний перелік та реєстр об’єктів критичної інформаційної інфраструктури.

Об’єкти, які потраплять до національного переліку, підлягатимуть першочерговим заходам з кіберзахисту відповідно до законодавства. Це сприятиме посиленню кіберстійкості критичної інфраструктури України та запобігатиме порушенню режиму сталого функціонування об’єктів критичної інфраструктури.

Постанова «Деякі питання об’єктів критичної інфраструктури» Кабінету Міністрів України від 9 жовтня 2020 року № 1109 [28] визначає юридичні принципи для ідентифікації підприємств, установ та організацій, які вважаються об’єктами критичної інфраструктури. Встановлюються конкретні критерії та порядок віднесення об’єктів до категорії «критична інфраструктура», приділяючи особливу увагу їх важливості для економіки та національної безпеки. Важливим аспектом є те, що порушення функціонування цих об’єктів може завдати значної шкоди національним інтересам.

Процес визначення підприємств, установ та організацій як об’єктів критичної інфраструктури надає власникам та управлінцям цих об’єктів необхідність розпочати заходи з посилення їх кіберзахисту. Це означає, що операторам основних послуг слід вживати заходів, спрямованих на забезпечення кіберстійкості критичної інфраструктури України в цілому, відповідно до вимог законодавства.

Постанова Кабінету Міністрів України від 22 липня 2022 р. №821 «Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури» [29] передбачає виконання заходів, спрямованих на отримання, оброблення та аналіз інформації щодо фактичного стану захисту об’єкта критичної інфраструктури, здійснення контролю за ризиками та постійно вдосконалювати заходи, спрямовані на забезпечення безпеки та стійкості об’єкта КІ.

Постанова Кабінету Міністрів України від 14 жовтня 2022 р. № 1175 «Деякі питання подання інформації у сфері захисту критичної інфраструктури» [30] установлює, що секторальні органи у сфері захисту КІ та оператори КІ щороку подають звіти про виконання повноважень, визначених Законом України «Про критичну інфраструктуру» [6].

Акти Кабінету Міністрів України, які орієнтовані на розвиток і відновлення критичної інфраструктури, можна розглядати як ті, чия дія спрямована на підтримку та укріплення функціонування критичних об'єктів. Прикладами таких правових актів є:

1.Постанова Кабінету Міністрів України від 13 грудня 2017 р. № 1071 [31]: затверджує Державну цільову програму відновлення та розбудови миру в східних регіонах України.

2.Постанова Кабінету Міністрів України від 5 серпня 2020 р. № 695 [32]: затверджує Державну стратегію регіонального розвитку на 2021–2027 рр.

3.Розпорядження Кабінету Міністрів України від 19 вересня 2023 р. № 825-р [33]: затверджує Національний план захисту та забезпечення безпеки та стійкості КІ.

Ці акти спрямовані на створення умов для відновлення та підтримки життєважливих об'єктів і інфраструктури в регіонах, що потребують особливої уваги.

Кабінет Міністрів України виступає важливим учасником, відповідальним за забезпечення правового регулювання ефективної функціональності механізму захисту об'єктів критичної інфраструктури. Цей орган управління вживає заходів у формі видання відповідних правових актів, які охоплюють різні аспекти цієї сфери суспільних відносин.

Наступна категорія нормативно-правових актів, яка забезпечує функціонування механізму захисту об'єктів КІ, включає в себе законодавчі документи, прийняті центральними органами виконавчої влади. Прикладом відомчих нормативно-правових актів, які стосуються правового забезпечення функціонування механізму захисту об'єктів КІ в Україні, є:

1. Наказ Міністерства внутрішніх справ України від 21 травня 2020 року № 406, яким затверджено Положення «Про Директорат стратегічного планування та європейської інтеграції Міністерства внутрішніх справ України» [34] .

2. Наказ Міністерства внутрішніх справ України від 31 січня 2018 року № 70, що затверджує Положення «Про Департамент інформатизації Міністерства внутрішніх справ України» [35].

3. Наказ Міністерства внутрішніх справ України від 27 квітня 2020 року № 357, яким затверджено Інструкцію з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події й оперативного інформування в органах (підрозділах) Національної поліції України [36].

Ці документи визначають організаційно-правові засади захисту критичної інфраструктури, у тому числі механізми збору, обробки та аналізу інформації, виконання вимог законодавства, контроль ризиків та постійне удосконалення заходів для забезпечення безпеки об’єктів критичної інфраструктури в Україні.

Ухвалення та прийняття спеціального закону щодо КІ є вкрай очікуваним кроком, оскільки вже давно було виявлено потребу у подоланні роз’єднаності та відзначено очевидний недолік у нормативно-правовому регулюванні захисту систем і об’єктів критичної інфраструктури. Важливо відзначити, що найскладніші питання, пов’язані з взаємодією держави та представників бізнесу в сфері безпеки та захисту критичної інфраструктури, а також визначення відповідних обов’язків і повноважень, регулюються Законом України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX39 [6]. Цим Законом встановлені основи організаційно-правового структурування та операцій національної системи захисту критичної інфраструктури.

Цільовим завданням цього закону є створення умов для налагодження та результативного впровадження державної стратегії в області захисту критичної інфраструктури. Сформульовано критерії включення об’єктів до категорії критичної інфраструктури. Визначено невідкладні функції, порушення яких може призвести до негативних наслідків для національної безпеки України. Введено механізм створення реєстру об’єктів критичної інфраструктури.

Встановлено інститут регулятора в даній галузі, яким стає Уповноважений орган у сфері захисту об’єктів критичної інфраструктури України (Державна служба захисту критичної інфраструктури та забезпечення національної системи стійкості України). Діяльність Уповноваженого органу буде спрямована на керування, координацію та контроль, які здійснює Міністр Кабінету Міністрів України.

У сфері правового врегулювання захисту критичної інфраструктури в Україні головною складністю є відсутність системного підходу на національному рівні та невизначеність взаємодії між державними органами на законодавчому рівні. Навіть за наявності законів і нормативно-правових актів, що регулюють повноваження державних органів у цій галузі, в Україні відсутній системний підхід до управління такими системами та об’єктами.

Важливо відзначити, що в Україні відсутні також будь-які законодавчі вияви державно-приватного партнерства у сфері захисту критичної інфраструктури, що є пріоритетним напрямком, враховуючи світовий досвід. Така правова прогалина може ускладнити ефективну боротьбу з можливими небезпеками. Зараз в Україні існують три окремі системи захисту, які, хоча пов’язані між собою, призводять до неефективного реагування на комплексні загрози.

Необхідно негайно заповнити цю прогалину, оскільки відсутність чіткої термінології та єдиних підходів у цій сфері створюють ризики для держави.

Отже, впровадження державної системи захисту критичної інфраструктури (яка включає організаційні, нормативно-правові, інженерно-технічні, наукові та інші заходи для забезпечення безпеки та стійкості) потребує розробки нормативно-правового «каркасу», що визначатиме основні принципи її функціонування. Також важливо впровадити єдині підходи до організації управління об’єктами системи на рівнях держави та місцевих громад, а також визначити принципи взаємодії між державними органами та підприємствами, громадськістю і громадянами, які залучені до захисту критичної інфраструктури.

1.4 Функції і повноваження державної політики у сфері захисту критичної інфраструктури

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.

Державна політика України у сфері захисту критичної інфраструктури включає в себе ряд функцій та завдань, спрямованих на забезпечення безпеки та стійкості критичних об'єктів.

Законодавча функція: розробка та прийняття законів, нормативних актів та правил, що регулюють захист критичної інфраструктури. Це включає в себе створення нормативно-правової бази для ідентифікації критичних об'єктів, встановлення вимог до їх захисту, а також регулювання обов'язкових стандартів безпеки. В Україні за законодавчу функцію у сфері захисту критичної інфраструктури відповідає Верховна Рада України, яка має повноваження приймати закони та нормативно-правові акти, що регулюють цю сферу. Верховна Рада України приймає закони, які встановлюють правові засади захисту критичної інфраструктури, обов'язки та відповідальність структурних підрозділів держави, а також інші нормативні акти, які стосуються цього питання.

Координаційна функція: організація співпраці та координація діяльності між різними органами влади, агентствами та структурами, що забезпечують захист критичної інфраструктури. Мета полягає в уніфікації дій та об'єднанні зусиль для забезпечення ефективного захисту. У сфері захисту критичної інфраструктури в Україні координаційну функцію виконує Державна служба з надзвичайних ситуацій України (ДСНС України). ДСНС України є головним координатором та виконавчим органом у справах цивільного захисту та захисту критичної інфраструктури в Україні.

Аналітична функція: збір, аналіз та оцінка інформації про потенційні загрози та ризики для критичної інфраструктури. Ця функція передбачає постійний моніторинг ситуації та розробку прогнозів для виявлення нових загроз. Аналітичну функцію в сфері захисту критичної інфраструктури в Україні зазвичай виконує низка державних

та недержавних організацій та інститутів. До найбільш важливих організацій, які можуть здійснювати аналітичну діяльність у цій сфері, належать: ДСНС України, Міністерство цифрової трансформації України, Державна служба стандартизації, метрології та сертифікації України, громадські організації та експерти.

Фінансова функція: виділення фінансових ресурсів для здійснення заходів захисту критичної інфраструктури. Це включає в себе виділення бюджетних коштів, фінансування проєктів та програм, спрямованих на зміцнення безпеки об'єктів. У сфері захисту критичної інфраструктури в Україні фінансову функцію виконують декілька ключових структур та організацій: державний бюджет України, ДСНС України, Міністерство цифрової трансформації України, донорські організації та міжнародні проекти.

Освітньо-інформаційна функція: інформування громадськості, підприємств та інших зацікавлених сторін про загрози та заходи захисту критичної інфраструктури. Освітні кампанії та інформаційні заходи допомагають підвищити обізнаність та готовність суспільства до дій в надзвичайних ситуаціях. Освітньо-інформаційна функція у сфері захисту критичної інфраструктури в Україні виконується спільними зусиллями державних та цивільних структур: Міністерством цифрової трансформації України, ДСНС України, Міністерством освіти і науки України, Міністерством внутрішніх справ України, Міністерством оборони України, громадськими організаціями.

Технічна функція: забезпечення наявності та доступності сучасних технічних засобів та технологій для захисту критичної інфраструктури. Це включає в себе розробку та впровадження систем контролю, виявлення та реагування на загрози. Технічна функція у сфері захисту критичної інфраструктури в Україні виконується різними структурами та відомствами залежно від конкретного сектору та виду інфраструктури: Міністерство цифрової трансформації України, ДСНС України, Міністерство енергетики та захисту довкілля України, Міністерство внутрішніх справ України, Міністерство оборони України, Міністерство транспорту, Міністерство охорони здоров'я та ін., які забезпечують технічний захист і безпеку відповідних об'єктів.

Кризовий менеджмент: розробка та впровадження планів кризового управління, які передбачають дії у надзвичайних ситуаціях та реагування на аварії чи катастрофи. ДСНС України грає ключову роль у координації та управлінні надзвичайними ситуаціями на об'єктах критичної інфраструктури в державі.

Міжнародна співпраця: співпраця з іншими країнами та міжнародними організаціями у сфері захисту критичної інфраструктури для обміну інформацією, досвідом, навчанням, участю в міжнародних проектах та програмах, а також спільними заходами для підвищення рівня стійкості та захищеності об'єктів критичної інфраструктури від потенційних загроз. Міжнародна співпраця в цій сфері відбувається на різних рівнях, і ДСНС є однією з ключових установ, що забезпечують координацію та реалізацію цієї співпраці в Україні.

Державна політика в сфері захисту критичної інфраструктури має на меті забезпечити стабільність та безпеку суспільства, захист важливих об'єктів і ресурсів, а також готовність до дій в надзвичайних ситуаціях техногенного та природного характеру.

Також уповноваженим органом із питань захисту критичної інфраструктури під час дії воєнного стану, а також протягом 12 місяців після його припинення чи скасування призначили Державну службу спеціального зв'язку та захисту інформації України. Держспецзв'язку має забезпечити формування та наповнення реєстру об'єктів критичної інформаційної інфраструктури, роботу з посилення стійкості таких об'єктів.

На сьогоднішній день основними законодавчими та нормативно-правовими актами, що регулюють захист критичної інфраструктури є:

1. Закон України «Про критичну інфраструктуру» [6];

2. Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 «Деякі питання об'єктів критичної інфраструктури» [37];

3. Постанова Кабінету Міністрів України від 22 липня 2022 р. № 821 «Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури» [38];

4. Постанова Кабінету Міністрів України від 14 жовтня 2022 р. № 1174 «Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури» [39];

5. Постанова Кабінету Міністрів України від 14 жовтня 2022 р. № 1175 «Деякі питання подання інформації у сфері захисту критичної інфраструктури» [40].

Державна політика у сфері захисту критичної інфраструктури базується на наступних принципах: гарантування надійності та стабільності критичної інфраструктури; визначення правових вимог до основних принципів, стратегічних напрямків, підходів до захисту критичної інфраструктури; визначення суб'єктів, які складають національну систему захисту критичної інфраструктури, їхніх повноважень та відповідальності; створення умов і впровадження заходів, спрямованих на ефективне управління та контроль над ризиками безпеки, зниження ризику реалізації можливих загроз, а також на ліквідацію наслідків загроз та інших подій; розроблення системи раннього виявлення загроз критичній інфраструктурі; запровадження механізмів державно-приватного партнерства та співпраці між суб'єктами господарювання та населенням у питаннях забезпечення безпеки та стійкості критичної інфраструктури; підтримка міжнародного співробітництва в галузі захисту критичної інфраструктури; створення умов для швидкого відновлення надання життєво важливих функцій та послуг у випадку реалізації загроз і порушень функціонування критичної інфраструктури [5].

Основні повноваження державної політики включають в себе: розроблення стратегічних напрямків у галузі захисту критичної інфраструктури, законодавчу діяльність, міжнародне співробітництво, організацію системи захисту, створення програм і проектів, визначення стандартів і вимог з питань безпеки об'єктів критичної інфраструктури на всіх етапах їх життєвого циклу та аналіз ризиків і загроз для критичної інфраструктури. Ці повноваження визначаються законами та нормативними актами України і забезпечують розвиток та функціонування системи захисту критичної інфраструктури в країні.

Отже, в Україні дбають про захист важливих об'єктів, систем і ресурсів, які зазвичай відносяться до критичної інфраструктури. У країні існують законодавчі

акти, які визначають особливості забезпечення безпеки цих об’єктів. Проте в Україні ще не створено загальний механізм управління захистом і безпекою таких об’єктів, і часто спостерігаються випадки дублювання функцій і ресурсів, а також відсутність єдиної координації та узгоджених дій у вирішенні проблем національного масштабу. Крім того, загрози для цих об'єктів розглядаються на рівні окремих відомств. У кожної системи існують свої набори загроз та ризиків, якими вона зобов'язана займатися, власні режими функціонування у різних ситуаціях безпеки, і власні плани та процедури реагування. Ця ситуація підкреслює важливість впровадження ряду значущих заходів на рівнях державного, регіонального та галузевого управління, з урахуванням правового та організаційно-методичного забезпечення. Також необхідно забезпечити координацію ресурсів у сфері безпеки, а також спільне використання засобів безпеки, які перебувають під контролем окремих відомств.

РОЗДІЛ 2
ВИЗНАЧЕННЯ ЗАГРОЗ І НЕБЕЗПЕК ТА ЇХ ПОТЕНЦІЙНИЙ ВПЛИВ НА СФЕРУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Загрози для сфери критичної інфраструктури можна визначити як потенційні події, дії або умови, які можуть спричинити негативні наслідки для нормального функціонування та безпеки цих об’єктів.

Визначення загроз є важливим етапом у процесі захисту критичної інфраструктури і включає в себе різні аспекти. Спочатку потрібно визначити всі можливі загрози, які можуть вплинути на критичну інфраструктуру. Ця ідентифікація включає в себе аналіз можливих джерел загроз, таких як природні явища (повені, землетруси, урагани), технічні аварії (поломки обладнання, витоки небезпечних речовин), акти тероризму, кібератаки, людський фактор та інші. Потім обов’язково потрібно проаналізувати вразливості критичної інфраструктури, що можуть бути використані загрозами для спричинення шкоди або перешкоди нормальному функціонуванню. Визначити можливі наслідки або збитки, які можуть виникнути внаслідок реалізації загроз. Всі загрози потрібно згрупувати і класифікувати за різними критеріями, такими як тип загрози (природні, техногенні, терористичні), можливість реалізації загрози, потенційні наслідки тощо. Необхідно визначити та встановити пріоритет для кожної загрози залежно від її важливості та можливості виникнення. Розробити стратегії та плани заходів для запобігання, реагування та відновлення внаслідок загроз. І також здійснювати постійний моніторинг загроз, надавати оцінку їх актуальності та оновлення заходів із захисту відповідно до змін у загрозах або вразливості.

Цей процес є постійним і динамічним, оскільки загрози можуть змінюватися з часом, і заходи із захисту повинні бути адаптовані до нових умов. Визначення загроз є важливою передумовою для розробки ефективної стратегії та планування заходів із захисту критичної інфраструктури.

Небезпека відрізняється від загрози тим, що загроза має спрямований характер і призначена для цільового об’єкта, системи або території, в той час як небезпека є

більш загальним імпульсом, або наслідком реалізації загрози. Багато методів аналізу стійкості регіонів орієнтовані на узагальнену небезпеку або сценарії, які є основою для проведення аналізу (наприклад, дослідження впливу втрати електроенергії на критично важливу галузь проводиться через загрозу втрати електроенергії). Однак аналіз, спрямований на наслідки, зазвичай фокусується на конкретній загрозі (наприклад, кібератака на системи промислового управління об'єктом або систему критичної інфраструктури) або небезпеці (наприклад, ураган, який впливає на порт).

Потенційний вплив загроз і небезпек на сферу критичної інфраструктури може бути різноманітним і включати в себе: матеріальні збитки, загрозу життю та здоров'ю людей, перешкоди в нормальному функціонуванні, економічні втрати, заворушення суспільного порядку, вплив на природне середовище, втрати інформації та даних, загрози для національної безпеки.

Щоб врахувати загрози та небезпеки при аналізі регіональної стійкості, важливо розуміти характер цих загроз та як вони можуть вплинути на відповідну інфраструктуру. Отже, аналіз загроз і небезпеки нерозривно пов'язаний з аналізом вразливості. Існують різні рівні аналізу загроз і небезпек, які можна застосовувати в залежності від обсягу оцінки та бажаного рівня складності.

Перший рівень аналізу – це загальна оцінка вразливості інфраструктури щодо можливих загроз або небезпек. Основна мета полягає в тому, щоб з'ясувати, чи існує потенціал для впливу цих загроз на інфраструктурні системи. На цьому етапі не проводиться докладний аналіз конкретного впливу, але досліджується можливість такого впливу. Наприклад, цей рівень аналізу може включати визначення ступеня залежності інфраструктурних систем від підключених до Інтернету систем управління, що свідчить про загальну вразливість до кіберзагроз та можливих перебоїв.

Другий рівень аналізу фокусується на більш детальному розгляді конкретної загрози або небезпеки і вразливості інфраструктури до неї. На цьому рівні проводиться також аналіз потенційних наслідків для інфраструктури і для інших залежних об'єктів. Для цього потрібне більше глибоке технічне розуміння конкретної загрози або небезпеки, а також самої інфраструктури. Наприклад, на цьому рівні може

проводитися аналіз конкретних кіберзагроз і технічної вразливості використовуваних систем або моделювання впливу паводків на об’єкти інфраструктури.

В провідних країнах існує різниця у спектрі загроз для критичної інфраструктури та у визначенні цих загроз. Незважаючи на загальну схожість, кожна країна визначає їх індивідуально, враховуючи власну безпекову ситуацію та пріоритети розвитку, що визначені державною політикою. В більшості країн ці загрози закріплені законодавчо, але деякі з них можуть не мати конкретного переліку загроз.

Наприклад, в Європейському контексті, зокрема в Німеччині, існує чітко визначений перелік видів загроз та підвидів для об’єктів критичної інфраструктури, що включає вичерпний перелік цих загроз. У Сполучених Штатах Америки такого чіткого переліку загроз немає. Крім того, існує різниця у підходах до організації заходів протидії цим загрозам.

Оцінка потенційного впливу загроз і небезпек є важливим кроком у розробці стратегій та планів захисту критичної інфраструктури. Вона дозволяє визначити пріоритети та необхідність заходів для запобігання, реагування та мінімізації наслідків загроз і небезпек.

2.1 Методи оцінки загроз критичній інфраструктурі

Застосування сучасних методів і передових технологій для оцінювання ризиків і загроз, моделювання кризових ситуацій і розробки «сценарних» прогнозів дозволяє підвищити надійність отриманих результатів і створити обширу науково обґрунтовану базу даних для подальшого аналізу.

Існує цілий ряд методологій для оцінки загроз і небезпек та розробки програм управління ризиками. Оцінки допомагають урядовцям, власникам і операторам розуміти потенційні інциденти і те, як вони можуть вплинути на інфраструктуру та громади. Оцінка ризиків дає особам, які приймають рішення, кращу інформацію для визначення того, які заходи з пом’якшення наслідків та управління ризиками є найбільш важливими, а також для розуміння того, де різні типи дій є найбільш прийнятними. Спектр доступних заходів включає: координацію з іншими зацікавленими сторонами; надання додаткового обладнання для ліквідації наслідків

або відновлення; модифікацію дизайну інфраструктури; обмеження на операції; найм і навчання персоналу та інші. Оцінка ризиків також утримує увагу від автоматичного перемикання на рідкісні або найгірші події з екстремальними наслідками, сприяючи розгляду низки більш вірогідних подій, навіть якщо вони мають дещо менші, але все ж таки значні наслідки.

Мета полягає у проведенні точних і всебічних оцінок, які індивідуально або колективно охоплюють загрозу, вразливість і наслідки (також відомі як небезпека, частота і наслідки для ризиків, не пов'язаних із загрозами).Тип оцінки може бути визначений на основі міжнародних стандартів, найкращих практик у відповідній галузі або історичних даних. Оскільки кібербезпека є важливою для забезпечення стійкості критичної інфраструктури, комплексне розуміння безпеки та стійкості передбачає аналіз як фізичних, так і кібернетичних аспектів. Тому для проведення такої оцінки важливо залучати експертів як у фізичній безпеці, так і в кібербезпеці критичної інфраструктури.

Повна оцінка ризиків може бути виправдана для всіх або більшості критично важливих елементів інфраструктури в певних районах, де потенційні наслідки від порушень, руйнування або експлуатації є особливо серйозними. Процес перевірки рекомендується застосовувати до всіх інших складових інфраструктури, щоб зменшити вимоги до тих елементів, які можуть не потребувати повного аналізу ризиків. Наприклад, для більшості об'єктів інфраструктури в сільських районах достатньо провести перевірку, тоді як у великих мегаполісах може знадобитися повний аналіз ризиків для певних компонентів інфраструктури.

Надзвичайні ситуації здійснюють значний вплив на соціальні, економічні, політичні та інші процеси у суспільстві. Тому управління в умовах надзвичайних ситуацій різного характеру є однією з важливіших для об'єктів критичної інфраструктури щодо забезпечення стійкого розвитку та національної безпеки країни. Підвищення ефективності управління у цій сфері є актуальним питанням і його реформування потребує зважених та раціональних рішень з урахуванням позитивного досвіду, що формувався під впливом певних історичних умов. Теперішній стан справ, поява новітніх технологій (зокрема, інформаційних), нових ризиків та загроз (у тому

числі воєнні дії) дозволяють зробити висновок, що в подальшому роль держави та її органів управління у цій сфері зростатиме.

Стратегічна національна оцінка ризиків аналізує різноманітні загрози і небезпеки, які становлять потенційні загрози для національної безпеки, класифікуючи їх у широких категоріях, таких як загрози, спричинені людьми, природні катастрофи та технологічні або випадкові ризики, наприклад:, військові дії, пандемії, кіберзагрози, екстремальні погодні умови, аварії або технічні збої.

Оцінка загроз критичній інфраструктурі може бути проведена за допомогою різних методів та підходів [41, 42].

1.Експертний метод: вимагає участі експертів, які мають глибокі знання у сфері критичної інфраструктури та потенційних загроз. Експерти оцінюють ймовірність та наслідки різних загроз на основі свого досвіду та знань.

2.Аналітичний метод: використовує аналітичні інструменти, такі як статистика, математичні моделі, імітаційне моделювання тощо, для оцінки загроз. Наприклад, можна аналізувати історичні дані щодо інцидентів у сфері критичної інфраструктури та робити прогнози на цій основі.

3.Моделювання загроз: використовується створення математичних моделей, які дозволяють аналізувати можливі наслідки різних загроз. Це може включати моделювання поведінки природних катастроф, кібератак, терористичних актів.

4.SWOT- аналіз: використовує аналіз SWOT (Strengths, Weaknesses, Opportunities, Threats), щоб визначити внутрішні і зовнішні фактори, які впливають на критичну інфраструктуру. Загрози визначаються як зовнішні негативні фактори.

5.Мультикритеріальний аналіз: використовується для визначення вагомості різних загроз і їх впливу на критичну інфраструктуру. Зазвичай використовуються числові показники для оцінки загроз.

6.Оцінка імовірності та наслідків: для кожної загрози визначається ймовірність її виникнення та можливі наслідки для критичної інфраструктури. Ці параметри потім комбінуються для визначення рівня загрози.

7.Аналіз вразливості: визначає, наскільки вразлива критична інфраструктура на різні види загроз. Це включає в себе оцінку заходів, призначених для захисту інфраструктури.

Вибір конкретного методу або комбінації методів залежить від конкретних умов і завдань оцінки загроз для критичної інфраструктури.

Найчастіше використовується експертний метод для кількісної оцінки рівня загрози, виражаючи її потенціал (*П*) числово як функцію комплексу з *n* параметрів a_i загрози:

$$П = f(a_1, a_2, ..., a_n). \quad (2.1)$$

Усі ці показники оцінюються фахівцями за однаковими оцінками по шкалі. Конкретний вид функції *П* може варіюватися, але, при рівній важливості параметрів a_i, потенціал загрози можна представити як середнє арифметичне їх бальних оцінок:

$$П = (a_1 + a_2 + \dots a_n)/n. \quad (2.2)$$

У випадку коли важливість параметрів a_i є різною, використовується їх коефіцієнт значимості k_i:

$$П = (k_1 a_1 + k_2 a_2 + \dots + k_n a_n), \quad (2.3)$$

причому $k_1 + k_2 + \dots + k_n = 1$.

Важливо брати до уваги той факт, що потенціал загрози як явища або події може змінюватися з часом *t*, і, таким чином, узагальнено він буде представляти таку форму:

$$П = f(a_1, a_2, \dots, a_n; t). \quad (2.4)$$

Це відкриває можливість достатньо точного прогнозування зміни потенціалу загрози у часі та оцінювання рівня небезпеки для об’єктів критичної інфраструктури, які можуть підпадати під вплив цієї загрози. Важливо відзначити, що комплексна оцінка потенціалу загрози є ключовим фактором в оцінці ризику для об’єктів критичної інфраструктури від цієї загрози.

На сьогодні зростання загрози стосовно падіння рівня безпеки важливих об’єктів критичної інфраструктури в Україні є результатом надмірної експлуатації споруд, конструкцій, обладнання та інженерних мереж, які вже перебувають на межі свого проектного терміну використання. Ця ситуація створює серйозні ризики виникнення надзвичайних ситуацій, які можуть бути природного або техногенного

походження, і загрожувати безпеці функціонування об’єктів критичної інфраструктури [43].

Серед усіх загроз різного походження для безпеки критичної інфраструктури найбільш важливими визначено такі [44]:

- природні: повені, екстремальні погодні явища, лісові пожежі, землетруси, епідемії та пандемії, епізоотії;

- техногенні: промислові аварії, ядерні/радіологічні аварії, аварії на транспорті, втрата критично важливої інфраструктури, кібератаки, терористичні атаки.

Особливої уваги потребують взаємозв’язки та взаємозалежності між загрозами природного походження, коли виникнення одних небезпечних явищ призводить до формування нових через механізм «каскадних ефектів» [10]. Наприклад, така загроза як небезпечні погодні явища пов’язана з наступними загрозами: повені, зсуви, пожежі, забруднення, втрата критичної інфраструктури, транспортні аварії; забруднення з пандеміями.

Сьогодні по всій Україні спостерігаємо зростання ризиків виникнення надзвичайних ситуацій техногенного походження через руйнування багатьох промислових і житлових споруд внаслідок військових дій. Терористичний характер воєнних дій з боку росії, полягає у спрямованому та навмисному пошкодженні критично важливих громадських інфраструктурних об’єктів держави. Ця стратегія включає в себе руйнування водосховищ, гідроелектростанцій, розподільчих станцій, систем електропостачання, газопостачання, підприємств, будівель, залізничних і дорожніх мереж, засобів зв’язку, об’єктів життєдіяльності населення, а також загрози використання ядерних вибухових пристроїв, хімічних, біологічних, токсичних та інших небезпечних речовин, які становлять серйозну загрозу для населення і довкілля.

Варто відмітити зростання кібернетичних загроз для об’єктів критичної інфраструктури держави, обумовлених хакерськими атаками, що можуть призвести до відмов важливої інформаційної інфраструктури. Хакерські атаки були націлені на об’єкти критичної інформаційної інфраструктури енергогенеруючих і енергопостачальних компаній, об’єктів транспорту, ряду банківських установ,

телекомунікаційних компаній. Повідомлення про ураження інформаційних систем комерційних компаній надходили, зокрема, від мережі Auchan, поштової служби DHL, комерційних банків і телеком-операторів. Зараженими вірусом виявились численні державні ресурси включаючи системи міністерства інфраструктури, Державної фіскальної служби, електророзподільчі мережі компанії Укренерго.

Небезпеки, які впливають на критичну інфраструктуру, є складними і нестабільними; загрози, вразливості та можливі наслідки зазнали змін упродовж останнього десятиліття. Наприклад, критичні інфраструктури, які раніше переважно піддавалися ризикам, пов'язаними із фізичними загрозами та стихійними природними лихами, тепер все більше вразливі до кіберризиків. Це обумовлено зростаючою залежністю критичних систем від інформаційних та комунікаційних технологій, а також активізацією кіберзлочинців, які зосереджуються на використанні цієї слабкості для своїх цілей.

Дослідження у сфері запобігання та протидії загрозам різного походження підтверджують необхідність впровадження ризик-орієнтованого підходу у державну систему захисту населення від надзвичайних ситуацій природного та техногенного характеру. Це необхідно для ефективного передбачення та зменшення ризику виникнення різних катастроф для об'єктів критичної інфраструктури [45].

2.2. Єдиний методологічний підхід до оцінки ризиків критичній інфраструктурі

Забезпечення безпеки та стійкості можливе завдяки ефективному управлінню ризиками. Ризик – це потенційна можливість небажаного результату, спричиненого подією чи інцидентом, який визначається ймовірністю (що залежить від загроз та вразливості) та можливими наслідками [44].

Єдиний методологічний підхід до оцінки ризиків критичній інфраструктурі означає уніфікований набір принципів, методів та критеріїв, які застосовуються для визначення та оцінки ризиків, пов'язаних із критичними інфраструктурними об'єктами. Цей підхід розробляється для забезпечення системності та послідовності

при оцінці ризиків, а також для створення єдиної методології, яку можна застосовувати в усіх галузях та сферах, де існують критичні інфраструктурні об'єкти.

Ця єдина методологія враховує стандартизовані процедури та інструменти, які дозволяють визначати та оцінювати ризики від різних видів загроз для критичних інфраструктур. Вона також включає розробку загальних принципів керівництва для взаємодії та реагування в разі виникнення ризикових ситуацій. Такий єдиний підхід спрощує управління та координацію дій у сфері захисту критичних інфраструктур та сприяє підвищенню рівня безпеки.

Процес оцінки ризиків КІ в Україні включає наступні етапи:

1. Визначення критичних об'єктів інфраструктури: цей етап полягає у визначенні та класифікації об'єктів, які вважаються критичними для національної безпеки та функціонування суспільства. Це може включати енергетичні системи, транспортні мережі, комунікаційні системи, водопостачання, системи охорони здоров'я і багато інших об'єктів.

2. Оцінка загроз: на цьому етапі проводиться ідентифікація можливих загроз, які можуть вплинути на об'єкти критичної інфраструктури. Загрози можуть бути природними (наприклад, стихійні лиха) або штучними (такі як кіберзагрози або терористичні акти).

3. Оцінка вразливості: для кожного критичного об'єкта оцінюються його вразливості до можливих загроз. Це включає в себе аналіз, які частини інфраструктури найбільш уразливі та які заходи можуть бути вжиті для їх захисту.

4. Оцінка наслідків: проводиться оцінка потенційних наслідків, які можуть виникнути внаслідок різних загроз для критичних об'єктів. Це може включати втрати людей, економічні втрати, втрати інфраструктури, втрати важливих послуг тощо.

5. Визначення рівня ризику: ризик оцінюється як результат взаємодії загроз, вразливості та можливих наслідків. Ризик може бути оцінений по різних шкалах, від високого до низького.

6. Розробка заходів зі зменшення ризику: на цьому етапі розробляються та впроваджуються стратегії та заходи для зменшення ризику для критичних об'єктів.

Це включає в себе планування заходів щодо підвищення стійкості та підготовки до можливих надзвичайних ситуацій.

7. Моніторинг та перегляд: процес оцінки ризиків є постійним і вимагає постійного моніторингу та перегляду. Об’єкти КІ повинні систематично оцінювати свої ризики і вносити зміни до своїх заходів зі зменшення ризику відповідно до змінених обставин або нових загроз.

8. Захист і реагування: одночасно із зменшенням ризиків, об’єкти КІ повинні мати в місцях захисту та реагування на можливі надзвичайні ситуації, щоб мінімізувати наслідки і відновити функціонування в якнайкоротший термін після інциденту.

Якщо розглянути поетапно, то на першому етапі визначаються всі можливі ризики надзвичайних ситуацій на національному рівні, розробляються сценарії їх можливого виникнення протягом найближчих п’яти років, оцінюється ймовірність та можливі наслідки цих ситуацій. Ця інформація служить основою для подальших досліджень. Також визначаються пріоритетні ризики, використовуючи критерії оцінювання можливих наслідків для людей, економіки, критичної інфраструктури, соціальних послуг, навколишнього середовища, стабільності у суспільстві, громадської та державної безпеки, міжнародного правопорядку. Окремо розглядаються ризики, для яких немає достатньої доказової бази, але вони можуть стати актуальними у майбутньому.

На другому етапі проводиться класифікація всіх підтверджених ризиків на основі їх спільності та можливості взаємного впливу, і вони групуються в категорії стандартних ризиків. Під час розробки детальних сценаріїв для найгірших можливих проявів стандартних ризиків, враховуються середньозважені оцінки їх імовірності та наслідків, які виникають у результаті моделювання різних варіантів і комбінацій їх взаємодоповнення. Важливо дотримуватися принципу реалістичності під час розробки сценаріїв, іншими словами, приймається, що надзвичайні ситуації, які передбачаються цими сценаріями, можуть і не статися, але за найгірших умов ризики можуть мати найбільш тяжкі наслідки. Оцінка в рамках цих сценаріїв найгірших проявів є загальною. Однак такий підхід дозволяє врахувати можливість каскадного

ефекту виникнення послідовних наслідків через взаємодію різних природних та антропогенних ризиків, а також наслідки від так званих «проникаючих» ризиків, які важко визначити через їх міжгалузевий характер. Цей підхід дозволяє одночасно забезпечити національну стійкість до надзвичайних ситуацій, незалежно від їх масштабу, будь то загальнонаціональні катастрофи чи менші події.

На третьому етапі формується шість різних класів ризиків з багатьма критеріями для ранжування: а) пріоритетом державного реагування; б) ступенем важливості і терміновістю зростання здатностей для підвищення національної стійкості; в) методичними особливостями розробки державної політики щодо реагування на зазначені класи ризиків.

Основними критеріями для формування певних класів різнотипних ризиків є такі: 1) наслідки; 2) імовірність; 3) ступінь невизначеності; 4) масштабність поширення наслідків надзвичайних ситуацій; 5) потенціал стійкості/опірності до ризиків; 6) здатність до відновлення після надзвичайної ситуації; 7) тривалість наслідків; 8) ступінь шкоди правам і свободам громадян, іміджу органів влади; 9) потенціал конфліктності у суспільстві (соціальні хвилювання, психологічні реакції тощо) [46].

З урахуванням отриманої інформації в Україні розробляються секторальні плани стійкості, програми забезпечення стійкості громад та інших об’єктів.

В провідних країнах світу існують різні критерії для визначення того, що вважається об’єктами критичної інфраструктури. Проте, як правило, ці критерії базуються на оцінці ризику негативних наслідків від можливих загроз для цих об’єктів. На підставі оцінки ризику формується список об’єктів критичної інфраструктури. Існує багато різних підходів до того, як розуміти та визначати поняття «ризику».

Основні документи Європейського Союзу, що стосуються боротьби з загрозами для критичної інфраструктури, в основному розглядають ризики втрати, травми або пошкодження об’єкта критичної інфраструктури [47].

В країнах ЄС, ризик для об’єкта критичної інфраструктури зазвичай враховує можливість потенційного ураження об’єкта конкретними видами загроз, особливо

якщо ці об’єкти не мають достатнього захисту. Також враховується потенційна вартість наслідків цього ураження. Ці наслідки можуть включати в себе людські жертви, травми, матеріальні збитки, загрозу державній (національній) безпеці та можливі дестабілізаційні процеси в суспільстві.

Деякі європейські країни вважають масштаби небезпеки також важливим показником ризику для об’єкта критичної інфраструктури. Наприклад, у Німеччині ризик розглядається як можливість серйозної загрози для життя та здоров’я людей, економіки країни, сфери послуг, загрозу навколишньому середовищу та культурним і матеріальним цінностям [48].

Загалом, в Європі багато в чому використовується поняття ризику, яке було позичено з нормативно-правових актів США. В цих актах ризик визначається як потенціал для небажаного результату внаслідок інциденту або події, залежно від його ймовірності та можливих наслідків [49].

З урахуванням міжнародних підходів до розуміння цього поняття, доцільно визначити ризик для об’єкта критичної інфраструктури як ймовірність виникнення найбільш негативних наслідків після впливу загрози на цей об’єкт.

Україна може визначати поняття «ризику» шляхом оцінки поточних або можливих загроз та аналізу, як вони впливають на національну інфраструктуру, враховуючи її характеристики, проектну документацію, технічні правила та інші документи, пов’язані з її функціями та експлуатацією. Ця оцінка має відповідати процедурі, затвердженій відповідними нормативно-правовими актами.

Важливою складовою оцінки ризиків є ідентифікація типових груп загроз та їх можливих наслідків. На основі аналізу цих аспектів потрібно розробляти загальні процедури взаємодії під час реагування на загрози, надзвичайні та кризові ситуації на різних етапах їх виникнення. Тобто створювати алгоритми дій для типових груп загроз для об’єктів конкретної галузі. Впровадження єдиної методології оцінювання ризиків і загроз національній безпеці дозволяє здійснювати порівняння та установлення пріоритетів щодо загроз і їх наслідків в різних галузях на основі спільних принципів та критеріїв.

Комплексна система оцінювання ризиків і загроз також повинна включати оцінку готовності та необхідних ресурсів для ефективного реагування на загрози, надзвичайні та кризові ситуації на різних етапах їх розвитку. Це обумовлено тим, що відсутність або недостатність необхідних ресурсів самі по собі можуть становити загрозу для національної безпеки.

Саме оцінка ризиків допомагає вчасно та ефективно взаємодіяти з типовими загрозами, що можуть виникнути для конкретного об'єкта критичної інфраструктури. Це дозволяє забезпечити стабільну роботу цього об'єкта, використовуючи оптимальні ресурси та заходи. Ризики оцінюються для всіх об'єктів національної інфраструктури, які підлягають визначенню як критичні.

Зниження ризику від можливих загроз безпосередньо пов'язане з підвищенням стійкості, зменшенням уразливості, плануванням надзвичайних ситуацій тощо. Ступінь захисту (C) вважається комплексним показником, що враховує всі ці та інші важливі складові. Важливість об'єкта (B) визначає, наскільки важливий цей об'єкт для надання певних послуг або функцій споживачам. Цей показник відображає значення об'єкта для забезпечення життєвих потреб населення. Він має прямий вплив на можливі негативні наслідки, оскільки оцінює масштаб небезпеки, пов'язаної з порушенням нормальної роботи об'єкта, і аналіз наявності небезпечних речовин на ньому.

Реальна практика провідних держав світу показує, що існують різні методи та підходи до визначення та розрахунку ризику настання негативних наслідків від ураження об'єктів критичної інфраструктури (P). Ризик буде залежати від кількох факторів, таких як ступінь захисту об'єкта від конкретної загрози, з урахуванням раніше згаданого потенціалу загрози ($П$), часу тривалості впливу цієї загрози, очікуваного часу відновлення функціонування об'єкта КІ (T) та важливості цього об'єкта (B) для різних видів суб'єктів (держави, суспільства). У загальному вигляді, ризик визначатиметься наступним чином:

$$P = f(П, B, C, T). \quad (2.5)$$

Кожну з цих складових ризику можна оцінити спеціалістами за певною шкалою з використанням методів експертної оцінки, які були розглянуті раніше. У

найпростішому випадку, з урахуванням вагових коефіцієнтів значимості (b_i), функція Р буде виглядати наступним чином:

$$P = b_1 П + b_2 B + b_3 C + b_4 T, \quad (2.6)$$

де $b_1 + b_2 + b_3 + b_4 = 1$.

У європейській практиці поширена позиція, що ризик можна кількісно оцінити, використовуючи добуток масштабу можливих збитків та ймовірності виникнення цих збитків.

Для якісної оцінки ризику використовують наступну групу показників: ефективність, стабільність, відсутність, рівень, якість, стан. Якісна оцінка цих показників перетворюється в кількісний вимір за допомогою бальної шкали, де визначається, яким чином кожній оцінці присвоюється певна кількісна оцінка. Шкала для якісної оцінки ризику повинна мати рівні, такі як «високий - середній - низький - вкрай низький - відсутній» [50].

З метою аналізу ризиків на об’єкті КІ, необхідно ідентифікувати і детально вивчити всі можливі ризики, враховуючи загрози, визначені у відповідних нормативних актах (зазвичай це робиться державними органами з питань безпеки та правопорядку). Крім цього, важливо враховувати індивідуальні особливості та характер ризиків, які можуть виникати на конкретному об’єкті критичної інфраструктури.

Для запобігання негативним наслідкам ризиків створюється система раннього виявлення та попередження їх. Крім того, внесені зміни до політики підприємства щодо фінансування в сфері безпеки. Для досягнення цієї мети розробляються проєкти, які надають перевагу належному захисту об’єкта критичної інфраструктури в умовах конкуренції.

Визначені підходи до оцінки ризиків для об’єктів критичної інфраструктури також включають в себе прогнозування ризиків. Це означає проведення ймовірної оцінки того, як змінюватиметься ризик з часом та які можливі наслідки очікувати в майбутньому внаслідок можливих загроз для об’єкта КІ. При цьому також враховується оцінка необхідних ресурсів і організаційних заходів. Ці прогнози

розробляються на визначений термін, який визначається відповідними нормативними документами.

Існують різні методи прогнозування, які можна узагальнити в такі основні, як методи екстраполяції, методи експертних оцінок та методи моделювання [51]. Моделювання передбачає створення моделі об'єкта КІ з включенням моделей її складових критичних елементів, систем або комплексів. Такі моделі (фізичні або математичні) повинні відображати основні властивості об'єкта та їх складових частин, опис основних процесів їх функціонування, а також моделі загроз та їх вплив на об'єкт КІ. Крім того, методи моделювання є одним з ефективних інструментів проведення аналізу ризиків, що дозволяє заздалегідь оцінити настання можливих загроз та їх вплив на об'єкт КІ, виявити слабкі місця у системах захисту об'єктів КІ та розробити заходи з їх нейтралізації [52].

Під час аналізу ризиків дуже важливим етапом є вивчення вразливості, пов'язаної з кожним типом потенційних негативних чинників. Це включає в себе дослідження, як об'єкти можуть бути вразливі до різних видів загроз, визначення зон можливого ураження, розрахунок кількості осіб, які можуть потрапити під вплив негативних наслідків, оцінку затрат, необхідних для відновлення функціонування об'єктів, вивчення видів загроз та їх поширення та інтенсивності.

Оцінка вразливості об'єктів КІ в процесі визначення ризиків грає ключову роль. Вразливість, в цьому контексті, визначається як індикатор, що вказує на можливість завдання об'єкту КІ шкоди внаслідок впливу різних загроз, засобів та чинників. Важливо враховувати, що при аналізі загроз, які мають навмисний характер (наприклад, акти тероризму чи кібератаки), велика увага приділяється досягненню максимально можливого рівня негативних наслідків внаслідок цих загроз.

Негативні наслідки, які виникають внаслідок впливу на об'єкт критичної інфраструктури (H), фактично є різного роду збитками. Головною метою визначення цих наслідків є визначення категорії об'єкта КІ, що в свою чергу допомагає встановити необхідний рівень захисту. Визначення цієї категорії базується на розгляді можливих масштабів збитків (M) та таких показників, як розмір людських жертв, економічних збитків, втрат безпеки життєдіяльності, втрат в сфері суспільно-

політичних та культурних цінностей, а також втрат для забезпечення державної безпеки і громадського порядку (B). Однією з простих формул для розрахунку цієї категорії є така:

$$H = M \cdot B \tag{2.7}$$

У цій формулі, чим більше значення (H), тим вищий рівень захисту необхідний для об’єкта КІ. Такий метод обчислення частіше використовується для організації захисту об’єктів від кіберзагроз і терористичних загроз. Зараз ця практика активно вивчається і впроваджується фахівцями Агентства з питань кібербезпеки при Службі безпеки України [53].

Загрози для об’єктів критичної інфраструктури оцінюються за допомогою різних методик та програмного забезпечення, які базуються на загальній методології оцінки ризиків. Це підтверджується дослідженнями Інституту захисту та безпеки громадян, який входить до складу Центру спільних досліджень Європейської Комісії [54]. Отже, можна зробити висновок, що, по-перше, загальний підхід до оцінки ризиків для об’єктів критичної інфраструктури включає в себе наступні кроки: ідентифікацію та класифікацію загроз, визначення вразливостей та оцінку можливих наслідків. По-друге, головною особливістю оцінки ризиків для КІ є врахування багатьох взаємозв’язків і взаємодій. Згідно із підходом, який використовує Європейська Комісія, окремі об’єкти КІ взаємодіють між собою фізично (наприклад, через комп’ютерні мережі, електропостачання, транспорт), а також через різноманітні регуляторні норми [55]. Дослідження, проведені з використанням математичного моделювання і спеціального програмного забезпечення, дозволяють оцінити ці взаємозв'язки [56, 57].

В Україні управління ризиками в сфері критичної інфраструктури вимагає комплексного підходу з метою:

1. Визначення, виявлення, передбачення та готовності до можливих загроз та небезпек для КІ країни.
2. Зменшення вразливості важливих активів, систем і мереж КІ.
3. Зменшення можливих наслідків подій або інцидентів для КІ.

Ефективність цього інтегрованого підходу залежить від широкого спектру ресурсів, знань і досвіду критичної інфраструктури та відповідних зацікавлених сторін. Він передбачає ефективний обмін корисною та актуальною інформацією між учасниками з метою збільшення рівня усвідомленості ситуації та прийняття ефективних рішень з урахуванням ризиків.

В Україні сьогодні різні міністерства і відомства виконують оцінку загроз у своїх відповідних галузях використовуючи власні методи та критерії. Проблемою є відсутність можливості порівняти та об'єднати отримані результати, оскільки вони часто несумісні між собою. Також існує недостатня координація та співпраця між різними відомствами у цій області, і недостатнє врахування результатів наукових досліджень у практичній діяльності.

Наявні методи оцінювання загроз на основі історичного досвіду мають свої недоліки, оскільки вони не враховують нові виклики та ситуації, які раніше не мали аналогів. Це призводить до зниження надійності та точності прогнозів, оскільки вони обмежені попереднім досвідом.

Все важливішою стає необхідність розробки стандартних і універсальних процедур та інструкцій для ефективного реагування на типові загрози. Визначення таких загроз, створення сценаріїв кризових ситуацій та створення відповідних баз даних стають основними завданнями, які передбачає національна система оцінювання ризиків і загроз.

Окресливши специфіку державного управління забезпеченням безпеки критичної інфраструктури в Україні та здійснивши оцінку ризиків критичній інфраструктурі від потенційного впливу загроз і небезпек бачимо, що потребується вдосконалення державних механізмів забезпечення безпеки та підвищення ефективності захисту критичної інфраструктури.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ ЕФЕКТИВНОСТІ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Ефективність реалізації державної політики у сфері захисту критичної інфраструктури є важливим завданням для забезпечення національної безпеки і стійкості суспільства перед потенційними загрозами та кризовими ситуаціями. Для оцінки результативності такої політики, важливо розглянути основні складові.

Першим кроком є чітке визначення та ідентифікація об'єктів та систем, які є критичними для функціонування суспільства, економіки та національної безпеки. Це може включати енергетичні системи, транспорт, комунікації, фінансові інституції та інші сектори.

Наступною важливою частиною ефективної політики захисту КІ є оцінка потенційних загроз і ризиків для критичної інфраструктури. Держава повинна аналізувати потенційні загрози, включаючи кібератаки, природні катастрофи, терористичні акти та інші небезпеки.

Обов'язковою складовою є розроблення алгоритму дій при появі відповідних загроз для типових об'єктів КІ. Наразі в Україні існують або формуються кілька систем, які призначені для нагляду та захисту об'єктів та інфраструктури, пов'язаної з інформацією. Для ефективного розроблення планів взаємодії та координації дій серед цих систем необхідно узгодження та прийняття спільної термінології, визначення взаємозв'язків між різними режимами, рівнями та умовами функціонування систем, а також узгодження принципів управління у складних кризових ситуаціях (зокрема, чіткого розподілу відповідальності між учасниками процесу на кожному етапі кризи). Це необхідно, оскільки комплексна криза виникає внаслідок дії декількох небезпечних факторів одночасно. В Україні відсутня система, яка б була призначена для реагування на всі можливі види фізичних загроз або кіберзагроз, а також на їх можливі комбінації, і як наслідок відсутність відповідальності за проблеми захисту критичної інфраструктури на міжвідомчому

рівні та відсутність детальних стратегій реагування на можливі загрози і кризові ситуації.

Також для підвищення ефективності політики захисту КІ необхідно розробляти конкретні заходи захисту для кожного об’єкта критичної інфраструктури. Це включає в себе заходи щодо кіберзахисту, фізичного забезпечення, резервування та відновлення, а також плани екстреного реагування. Впроваджувати технічні заходи безпеки, наприклад, встановлювати сучасні системи захисту кожного типового об’єкту КІ, шифрувати дані, забезпечувати резервні джерела енергії або альтернативні тощо.

Дуже важливим кроком є співпраця з приватним сектором: багато об’єктів критичної інфраструктури перебувають у приватній власності. Ефективна політика захисту КІ вимагає партнерства і співпраці між державними органами та приватним сектором для спільного забезпечення захисту.

Цільовим заходом є забезпечення організації підготовки кадрів щодо захисту КІ. Для цього потрібно встановити співпрацю з університетами та іншими освітніми установами для впровадження спеціалізованих програм та курсів з безпеки критичної інфраструктури, розробити спеціалізовані навчальні курси та програми, які охопили б усі аспекти безпеки, кібербезпеки, управління кризами та відновлення після них, а також основи захисту інфраструктури. Забезпечити організацію системи постійного навчання керівного складу об’єктів критичної інфраструктури усіх галузей господарства, щодо питань з підвищення стійкості і захисту об’єктів критичної інфораструктури. Організовувати семінари, конференції та курси підвищення кваліфікації для професійного розвитку фахівців у цій області на постійній основі; розробляти рекомендації, правила поведінки для персоналу об’єктів КІ з метою зменшення можливих збитків у разі виникнення загроз, а також організовувати спільну діяльність між уповноваженим персоналом державних органів та спеціальних служб для забезпечення координації та взаємодії; проводити симуляційні вправи та тренування для кадрів з різних галузей, щоб навчити їх реагувати на реальні ситуації, що виникають у сфері захисту критичної інфраструктури.

Для оцінки ефективності політики захисту КІ важливо мати систему моніторингу та аналітики для постійного відстеження потенційних загроз та реагування на них. Наприклад, використовувати систему спостереження для виявлення змін у рівні безпеки, які можуть вказувати на можливі загрози або прогностичну модель для передбачення можливих загроз у геополітичному, екологічному або соціальному контексті, аналізувати вразливості інфраструктури для ідентифікації початку загроз. Також для оцінки можливих небезпек та їх потенційного впливу на критичну інфраструктуру можна застосувати метод моделювання. Моделювання включає процес створення моделі критичної інфраструктури, яка охоплює моделі її ключових складових, систем чи комплексів. Ці моделі повинні точно відтворювати основні характеристики і складові частини інфраструктури, описувати основні процеси їх функціонування, а також уявлення загроз та їх впливу на інфраструктуру. Методи моделювання відносяться до ефективних інструментів для ризик-орієнтованого аналізу, дозволяючи передбачити можливі загрози та їх вплив на критичну інфраструктуру, виявити слабкі місця в системах захисту об’єктів критичної інфраструктури та розробити заходи для їх усунення.

Важливим кроком для підвищення готовності та сприяння ефективному захисту критичної інфраструктури є включення громадськості у процес реалізації політики захисту КІ та публічна освіта щодо цих питань, інформування.

Загальна ефективність політики захисту КІ залежить від інтеграції всіх цих аспектів та постійного вдосконалення стратегій та заходів захисту. Реагування на нові загрози та зміни в інфраструктурному середовищі також є важливою частиною ефективної політики захисту КІ.

3.1. Обґрунтування стратегічних напрямків щодо реалізації державної політики у сфері захисту критичної інфраструктури

Сучасний розвиток демократичного суспільства базується на гармонійному функціонуванні основних секторів, які забезпечують необхідність для нашого життя. Необхідність в енергетиці, транспорті, телекомунікаціях, водопостачанні,

газопостачанні, медицині та інших секторах стає актуальною для забезпечення нашого комфорту та реалізації сучасного способу існування.

В українському законопроекті «Про критичну інфраструктуру та її захист» передбачено, що «метою державної політики у сфері захисту критичної інфраструктури є забезпечення безперебійного та стійкого функціонування об'єктів критичної інфраструктури України, запобігання проявам актів несанкціонованого втручання, прогнозування та запобігання кризовим ситуаціям з негативним впливом на об'єкти критичної інфраструктури, а також підвищення рівня захисту, удосконалення заходів безпеки та стійкості цих об'єктів від існуючих загроз» [58].

Для України, нині, в умовах війни дуже є актуальним створення стратегічних напрямків щодо реалізації державної політики у сфері захисту КІ.

Вчений Домарацький М. Б. відносить до життєво важливих інтересів держави такі аспекти [59]:

1. Забезпечення ефективного захисту населення та критично важливих об'єктів на території України у випадку надзвичайних ситуацій і терористичних актів.

2. Гарантування захисту та виживання населення під час воєнних конфліктів.

3. Збереження об'єктів, які мають велике значення для стійкого функціонування економіки та виживання населення.

4. Підвищення стійкості об'єктів критичної інфраструктури протистоянню надзвичайним ситуаціям і терористичним актам.

Хоча в Законі України «Про критичну інфраструктуру» [6] зазначено перелік життєво важливих функцій об'єктів КІ, все ж існує складність у визначенні того, які саме об'єкти можуть вважатися критичними на національному, регіональному або місцевому рівнях інфраструктури [37]. Тобто потрібні уточнення та удосконалення в методиці ідентифікації об'єктів критичної інфраструктури.

При огляді сучасного структурно-функціонального опису державної політики у сфері захисту критичної інфраструктури в Україні слід відзначити, що в цьому контексті існують декілька рівноправних систем, які працюють паралельно одна з одною.

Перша система – Єдина державна система цивільного захисту, яка охоплює органи управління на різних рівнях влади, сили та засоби центральних та місцевих виконавчих органів, підприємств, організацій, установ які здійснюють державну політику у сфері цивільного захисту. Безпосереднє керівництво цією державною системою цивільного захисту здійснює Державна служба України з надзвичайних ситуацій (ДСНС). Головним завданням підсистем єдиної державної системи цивільного захисту є захист населення і територій від надзвичайних ситуацій як у мирний час, так і в особливий період.

Друга система – Єдина державна система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків. Важливим компонентом цієї системи є Служба безпеки України. У рамках СБУ діє Антитерористичний центр (АТЦ), саме він відповідає за координацію заходів всіх структур, що беруть участь у боротьбі з тероризмом, включаючи заходи для запобігання терактам, диверсіям на об'єктах критичної інфраструктури. Головними завданнями єдиної державної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків є:

1. Запобігання актам тероризму, включаючи вчасне виявлення та усунення причин і передумов для вчинення терактів.

2. Інформування громадян про рівень загрози щодо можливих терористичних актів.

3. Забезпечення безпеки потенційних об'єктів терористичних атак, до яких відносяться важливі державні споруди, об'єкти під державним захистом, об'єкти підвищеної небезпеки, об'єкти транспортної системи України і системи електроенергетики, закордонні дипломатичні установи, консульські представництва та інші іноземні дипломатичні установи на території України, місця масового перебування людей.

Заради виконання зазначених завдань розробляються стратегічні програми для протидії тероризму та створюються плани для запобігання актам тероризму.

Третя система у сфері захисту критичної інфраструктури – Державна система фізичного захисту. Згідно Закону України фізичний захист визначається як

«діяльність у сфері використання ядерної енергії, спрямована на забезпечення захищеності ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання та на зміцнення режиму нерозповсюдження ядерної зброї» [60]. Завдання державної системи фізичного захисту:

1. Створення та здійснення нормативно-правового регулювання у сфері фізичного захисту.

2. Забезпечення безпеки ядерних установок, ядерних матеріалів, радіоактивних відходів та інших джерел іонізуючого випромінювання, враховуючи потенційні загрози.

3. Створення та забезпечення функціонування єдиної системи захищеного зв'язку між органами державної влади та юридичними особами, які відповідають за облік, контроль, фізичний захист та протидію нападам на ядерні установки та інші джерела іонізуючого випромінювання, транспортні засоби, що перевозять радіоактивні матеріали.

4. Здійснення державного нагляду та контролю за станом фізичного захисту.

5. Організація процесу обміну інформацією щодо стану фізичного захисту та збереження цієї інформації.

Суб'єктами цієї системи є: Служба безпеки України, Національна гвардія України, орган державного регулювання ядерної та радіаційної безпеки та органи виконавчої влади, які здійснюють правоохоронну діяльність.

Четвертою системою державної політики у сфері захисту КІ в Україні є Національна система кібербезпеки. Суб'єкти системи кібербезпеки: Національна поліція України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний координаційний центр кібербезпеки.

Таким чином, основними напрямами державної політики у сфері захисту об'єктів КІ України визначено:

1. Захист і забезпечення безпеки критичних об’єктів, включаючи ядерні установки, електроенергетичні системи, телекомунікаційні мережі, транспортні системи та інші ключові інфраструктурні об’єкти.

2. Розроблення та впровадження нормативних актів і правил, що стосуються захисту критичних об’єктів, включаючи створення відповідних правових рамок та норм щодо фізичного та кібернетичного захисту.

3. Забезпечення співпраці та координації між різними системами, відомствами, органами та суб’єктами, які відповідають за захист критичної інфраструктури.

4. Розроблення та впровадження планів попередження та реагування на різноманітні загрози, включаючи терористичні акти, кібератаки, природні катастрофи та інші надзвичайні ситуації.

5. Сприяння розвитку та впровадженню новітніх технологій та інновацій у сфері захисту критичної інфраструктури.

6. Забезпечення навчання та підготовки фахівців для ефективного реагування на загрози та надзвичайні ситуації в області захисту об’єктів критичної інфраструктури.

7. Участь в міжнародних організаціях для обміну досвідом та координації дій щодо захисту критичної інфраструктури на світовому рівні.

Але зовсім не передбачені заходи щодо підвищення стійкості об’єктів критичної інфраструктури протистоянню надзвичайним ситуаціям і терористичним актам, що потребує внесення змін і доповнень у нормативні акти, що регламентують процеси проєктування та експлуатації об’єктів критичної інфраструктури. Стійкість критичної інфраструктури залежить від різновиду наявних загроз, їх потенціалу та дій, які приймаються владою та операторами, які відповідають за захист критичної інфраструктури, для підвищення рівня захищеності цього об’єкта.

На сьогодні в Україні сучасну модель державної політики у сфері захисту КІ в умовах військового стану не вивчено достатньо глибоко. Для ефективного створення стратегічних напрямків щодо реалізації державної політики у сфері захисту КІ надзвичайно важливо ознайомитись, зрозуміти глибину та складність реальних проблем, що виникають в країні під час активних воєнних дій і терористичних актів,

які впливають на об’єкти критичної інфраструктури в реальному часі. Ці знання необхідно враховувати при розробці майбутньої державної політики щодо захисту об’єктів критичної інфраструктури.

Також уряд держави повинен проаналізувати наступні важливі аспекти сучасної ситуації країни:

1. розглянути спектр поточних і передбачуваних критичних загроз і ризиків;
2. оцінити стан та структуру економіки країни;
3. дослідити аспекти культури нації та суспільно-політичну обстановку в країні;
4. проаналізувати загальну інституційну практику державного управління;
5. переглянути основи конституційного ладу країни.

Оцінюючи стратегії державної політики стосовно захисту КІ під час воєнного конфлікту, можна зауважити, що головним чинником залишається регулювання позицій нормативного правового підходу до інституційних аспектів цього питання.

З метою захисту об’єктів КІ та об’єктів, які забезпечують життєдіяльність населення, військове командування спільно з військовими адміністраціями, може визначати і посилювати заходи з охорони таких об’єктів і встановлювати особливий режим їх функціонування. Це також включає в себе визначення процедур та переліку об’єктів, які підлягають посиленій охороні при введенні воєнного стану.

При розгляді сучасних аспектів стратегії державної політики щодо захисту КІ в умовах сьогодення в Україні, можна відзначити, що забезпечення безпеки критичної інфраструктури базується на складному аналітичному процесі. Цей процес включає в себе визначення секторів, які є критично важливими для інфраструктури, створення реєстру об’єктів КІ, визначення поточних загроз для цих об’єктів, формування структури та суб’єктів, відповідальних за політику захисту КІ, покращення інституційної підтримки політики захисту КІ, створення системи для захисту КІ, вжиття необхідних заходів для усунення наслідків пошкоджень об’єктів КІ. Цей комплексний аналіз допомагає забезпечити надійний захист критичної інфраструктури в умовах військового стану.

Серед одних з найсуттєвіших проблем можна виділити недолік механізмів реагування на кризові ситуації та нормативно-правової бази, яка б уточнювала

відповідальність та повноваження відповідних державних установ у цій області. Треба врахувати, що можливості ухвалення законодавчих рішень були обмежені через відсутність чи недосконаліть потрібних рішень. Відсутність чіткого законодавчого порядку і рішень щодо введення воєнного стану насправді призвела до відсутності чітких та однозначних правил узгодження між державою та суб'єктами підприємницької діяльності, обмеживши можливість залучення ресурсів підприємств для забезпечення стійкості роботи критичної інфраструктури. Також виникли труднощі у координації дій держави та підприємств з метою захисту та оборони важливих об'єктів критичної інфраструктури.

Обґрунтування стратегічних напрямків є важливою складовою політики захисту критичної інфраструктури та сприяє забезпеченню стійкості і безпеки суспільства.

3.2. Пропозиції щодо ефективного управління у сфері захисту критичної інфраструктури

Переваги сучасної цифрової епохи та зростання інформаційних технологій призвели до виникнення нових загроз як національній, так і міжнародній безпеці. Функціонування критичної інфраструктури в кіберпросторі, який є особливим середовищем, пов'язане із підвищеною вразливістю та потенційними небезпеками, що вимагають створення нового інструментарію для забезпечення безпеки.

Останнім часом разом із природними небезпечними подіями, кількість та інтенсивність кібератак, ініційованих окремими країнами, групами або особами, постійно зростає, як ми це бачимо. Ефективне забезпечення інформаційної та кібербезпеки передбачає розуміння того, що країна є нерозривною частиною та взаємодіє з іншими структурами та суб'єктами. Ця взаємодія відображається у різних аспектах, включаючи законодавчі, організаційні та технологічні аспекти. Управління безпекою інформації та кібербезпекою об'єктів критичної інфраструктури базується на знаннях про стан цих об'єктів, умови їх функціонування і впливи, яким вони піддаються [61].

З одного боку, недоречно стверджувати, що Україна недостатньо приділяє уваги заходам забезпечення безпеки життєво важливих систем, мереж та об'єктів. Єдина державна система цивільного захисту, яка складається з функціональних і територіальних підсистем та їх компонентів, була створена з метою втілення державної політики у цивільному захисті.

Згідно з ДСНС, вона є центральним органом виконавчої влади, відповідальним за формування та реалізацію державної політики у сфері цивільного захисту і безпосереднє керівництво діяльністю єдиної державної системи цивільного захисту. Проте саму систему реагування на небезпечні події вважають несамодостатньою через акцент лише на обмеженій спроможності єдиної державної системи цивільного захисту вирішувати реальні завдання цивільного захисту. Це, зокрема, пов'язано з роз'єднаністю практики і суспільних потреб і нечіткістю визначення сфери цивільного захисту.

Головними способами покращення єдиної державної системи цивільного захисту є залучення підрозділів реагування ДСНС України та матеріально-технічне забезпечення цих підрозділів [62]. ДСНС України визначає та реалізує державну стратегію у галузі цивільного захисту та надає безпосереднє керівництво єдиною державною системою цивільного захисту (ЦЗ). Критерієм успішності системи реагування на небезпечні події та захисту населення, який вважається найважливішим, є збереження життя та здоров'я людей, що вимагає оперативних дій працівників системи реагування [63].

Проблема полягає не лише у відсутності списків об'єктів або визначенні терміну «критична інфраструктура», але в недостатньому зв'язку між цими аспектами, у відсутності ефективного обміну інформацією між різними установами, у відсутності загального оцінювання ризиків цих об'єктів на державному рівні та відсутності спільного підходу до захисту від різних видів загроз (незалежно від того, чи це техногенні, природні або соціально-політичні загрози). Також немає загальної бази ресурсів для реагування та запобігання загрозам, яка повинна містити інформацію не лише від Міністерства внутрішніх справ, але і від Міністерства регіонального розвитку, будівництва та житлово-комунального господарства

України, Міністерства охорони здоров'я де збирають інформацію про наявність ліжок у лікарнях малих міст України та рівень забезпечення медичним персоналом [64]. Тому існуючий підхід до захисту критичної інфраструктури потребує перегляду та удосконалення.

В Україні діє низка нормативних актів, які пов'язані з захистом критично важливих систем, об'єктів і ресурсів, проте відсутній єдиний узгоджений механізм забезпечення необхідного рівня стійкості та їх безпеки на сьогодні. У практиці це призводить до невідповідності дій різних учасників, які відповідають за цей захист, і несвоєчасної реакції на потенційні загрози. Для ефективного врегулювання цих загроз необхідна спільна мобілізація ресурсів різних галузей і секторів, а також систематичне та раціональне використання засобів та зусиль.

У Зеленій книзі [2] однією з ключових рекомендацій є визначення за координацію заходів у системі захисту КІ відповідального органу. Окрім цього, цьому органу будуть доручатися функції аналізу та прогнозу майбутніх подій, а також організація підтримки у процесі прийняття стратегічних рішень з питань захисту критичної інфраструктури. Важливо підкреслити, що цей орган не повинен входити в структуру жодного з існуючих відомств, що залучені до вирішення завдань захисту КІ. Враховуючи це, однією з конкретних рекомендацій для створення ефективної державної системи захисту критичної інфраструктури в Україні є створення Центру захисту критичної інфраструктури.

Завдання забезпечення безпеки критичної інфраструктури переключає увагу на передбачення можливих кризових ситуацій, пов'язаних із функціонуванням критичної інфраструктури в Україні. Отже, основним завданням Центру захисту критичної інфраструктури має бути передбачення можливих кризових ситуацій, а це вимагатиме постійного моніторингу та виявлення можливих кризових ситуацій, пов'язаних з функціонуванням критичної інфраструктури. Для виконання цих завдань буде потрібно створити окремий відділ в структурі Центру, який буде функціонувати як ситуаційний центр і забезпечувати оперативну підтримку процесу ухвалення стратегічних рішень щодо захисту КІ. Цей відділ Центру повинен взаємодіяти з іншими відомчими, ситуаційними центрами та іншими аналітичними

структурами. Центр не буде мати прямого управління суб'єктами системи захисту критичної інфраструктури, тобто його рекомендації мають враховуватися через прийняття відповідних нормативно-правових актів держави [65].

Пріоритети забезпечення безпеки критичної інфраструктури включають: систематичне поліпшення правової бази для захисту КІ та створення системи державного управління її безпекою; зміцнення заходів з охорони об'єктів критичної інфраструктури, зокрема в енергетиці і транспорті; розвиток співпраці між суб'єктами, відповідальними за захист КІ, і розширення державно-приватного партнерства у запобіганні надзвичайним ситуаціям та реагуванні на них; розробка та впровадження механізмів обміну інформацією між державними органами, приватним сектором і громадськістю щодо загроз критичній інфраструктурі та захисту конфіденційної інформації в цій галузі; проведення профілактичних заходів для запобігання техногенним аваріям та оперативна реакція на них, мінімізація їх наслідків; розширення міжнародних відносин у цій галузі.

Державна стратегія забезпечення захисту об'єктів критичної інфраструктури відноситься до національної політики України. При розробці національної стратегії щодо об'єктів критичної інфраструктури важливо включити повний перелік всіх національних політик, що займаються цим питанням. Деякі політичні структури мають загальне відношення до інфраструктури, для них необхідно чітко визначити, яку роль і місце вони відводять існуючим нормативним рамкам у загальному контексті захисту об'єктів КІ.

Усвідомлюючи ситуацію сьогодення, дослідження українського правового поля в галузі захисту інформації на об'єктах критичної інфраструктури вказує на недостатність національних та спеціалізованих нормативних вимог стосовно гарантування безпеки інформації об'єктів критичної інфраструктури в Україні.

На нашу думку захист інформаційних та кібернетичних аспектів об'єктів КІ повинні включати в себе: розробку та ухвалення необхідних нормативних документів, що відповідають за кібербезпеку, суб'єктів кіберзахисту та власників об'єктів критичної інформаційної інфраструктури під час уникнення, виявлення та

припинення кібератак; визначення вимог до кіберзахисту об’єктів КІ; призначення підрозділів, які відповідають за забезпечення безпеки.

Результати цієї роботи свідчать про необхідність удосконалення державної політики у сфері захисту критичної інфраструктури. А саме той факт, що в країні війна і потрібно враховувати поточний військовий, політичний, соціальний та економічний контекст.

Пропозиціями щодо ефективного управлінння у сфері захисту КІ є:

1. Використання оптимальних стратегій для забезпечення безпеки КІ через підтримку міжнародних партнерів.

2. Розроблення моделі ефективної взаємодії та координації різних суб’єктів у формуванні та впровадженні державної політики в сфері захисту критичної інфраструктури.

3. Створення нових установ захисту об’єктів критичної інфраструктури і оптимізація вже існуючих організацій у сфері оборони.

4. Підтримка співпраці між державою та громадськістю.

5. Безпека різних регіонів України та забезпечення мирних умов у напрямку інтеграції у міжнародний простір безпеки.

6. Спільно з Організацією з безпеки та співробітництва в Європі (ОБСЄ) вжити заходів з метою усунення або зменшення впливу бойових дій на роботу систем водовідведення та енергетики. Це спрямовано на попередження серйозних порушень у функціонуванні важливих систем, що забезпечують життєво важливі потреби населення.

7. Створення Центру захисту критичної інфраструктури як ефективної державної системи захисту КІ в Україні.

8. Створення ситуаційного відділу (на базі Центру), який буде функціонувати і забезпечувати оперативну підтримку процесу ухвалення стратегічних рішень щодо захисту КІ.

9. Забезпечення проведення необхідних наукових досліджень спрямованих на підвищення стійкості об’єктів критичної інфраструктури протистоянню надзвичайним ситуаціям і терористичним актам.

10. Розробка методичного підходу для створення типових алгоритми дій операторів об’єктів КІ при прояві відповідних загроз.

11. Створення в Україні системи підготовки кадрів для обслуговування системи захисту КІ.

Майбутні дії в сфері захисту об’єктів КІ потрібно спрямовувати на урахування того, що сьогодні «інфраструктурна війна» стає дійсним інструментом впливу.

Термін «інфраструктурна війна» відноситься до конфліктів, в яких сторони використовують кібератаки та інші засоби для атак на інфраструктуру противника. Тому ключовим завданням є забезпечення можливості критичної інфраструктури виконувати свої функції, тобто надавати послуги, навіть у випадку пошкодження окремих об’єктів критичної інфраструктури. Цей підхід відомий як «планування для кризових ситуацій» і використовується як у галузі державного управління, так і в діяльності підприємств різних форм власності по всьому світу [66].

Як висновок, варто зазначити, що для державної політики України на сьогодні, дуже важливою задачею являється формування конкретних заходів реагування у сфері захисту КІ. Перш за все – це ввести штатний режим роботи в цій сфері, тобто проводити аналіз потенційних загроз, планувати умови роботи інформаційних систем та визначати заходи реагування відповідно до визначених загроз та їх впливу на різних рівнях важливості. Застосовувати заходи, які спрямовані на уникнення потенційних загроз або зменшення наслідків від них. Вміти реагувати своєчасно на подію або загрозу з метою відновлення роботи інформаційних систем до попередніх параметрів та надання життєво важливих функцій. Завершальним етапом є відновлення режимів функціонування КІ з урахуванням досвіду для покращення процесу відновлення у майбутньому. Також вважаємо, що однією з ключових перспективних напрямків для покращення державної політики забезпечення безпеки об’єктів критичної інфраструктури в Україні є розвиток процесу підготовки кваліфікованих спеціалістів у цій галузі. Потреба в систематизації правових і адміністративних основ для підготовки та підвищення кваліфікації спеціалістів, які займаються захистом критичної інфраструктури, є актуальною.

ВИСНОВКИ

1. Однією з основних проблем у галузі забезпечення національної стійкості є несистематизований характер заходів відповідного спрямування, що робить їх менш ефективними. Відсутність чіткої термінології та концептуального визначення у плані забезпечення національної стійкості об'єктів КІ, а також відповідного законодавства та недосконаліть співпраці в цій галузі – все це значно гальмує процеси зміцнення національної стійкості та порушує основні принципи її забезпечення.

2. Не розроблені рекомендації для визначення цілей, критеріїв та механізмів у відповідній сфері. Заходи, пов'язані з забезпеченням стійкості об'єктів КІ, здійснюються без системності, що ускладнює ефективне використання обмежених ресурсів держави. Відсутність чіткої інституційної моделі для забезпечення національної стійкості в Україні та нерозробленість питань щодо розподілу повноважень призводять до численних проблем у організації відповідної діяльності.

3. Заходи з аналізу та оцінювання ризиків, виявлення загроз виконуються різними установами, міністерствами та дослідницькими організаціями відповідно до своїх сфер діяльності, існує відсутність систематичного обміну повною та всебічною інформацією про всі можливі загрози та надзвичайні події. Одночасно для цих заходів існують значні проблеми не лише методологічного, але й організаційного характеру. Серед них – відсутність єдиної теоретико-методологічної основи для оцінювання ризиків, пов'язаних із національною безпекою, а також стану відповідних спроможностей для підготовки, ухвалення та впровадження стратегічних рішень.

4. Існує проблема відсутності державного органу, який був би відповідальним за координацію діяльності в цій сфері. Крім того, спостерігаються проблеми у взаємному обміні необхідною інформацією для ухвалення державних рішень та вирішення суттєвих питань.

5. На сьогодні в Україні існує низка проблем у створенні та реалізації державної політики та визначенні завдань, спрямованих на забезпечення національної стійкості. Ці проблеми виявляються у таких сферах, як стратегічне планування, кризове управління та розробка загальних планів дій для надзвичайних ситуацій, які мають

міжсекторальний характер, та інші суміжні аспекти. Не деталізовані функції та задачі окремих ключових суб'єктів захисту КІ.

6. Спостерігається низький рівень розвитку партнерства між державою та приватним сектором у сфері безпеки на рівнях як національному, так і регіональному. Крім того, не встановлено стійких двосторонніх комунікаційних зв'язків з громадськістю. Зазвичай, встановлені загальні норми участі громадськості виконуються формально. Щодо результів обговорень, вони залежать від рівня соціального партнерства та готовності суспільства до взаємодії, а часом – від випадкових обставин. Забезпечення національної стійкості в Україні вимагає не лише окремих заходів у різних сферах, але також комплексного регулювання на основі системного підходу та визначених концептуальних засад.

7. Визначено прояви інституційних недоліків у стратегії захисту критичної інфраструктури в умовах військового конфлікту в Україні. Розбіжності, деяка випадковість та непоєднаність стратегічних ухилень в цій сфері розглядаються як перешкода на шляху формування єдиної стратегії національної безпеки. Також було виявлено низку проблем у сфері державної політики захисту критичної інфраструктури та зроблені окремі пропозиції для їх вирішення.

8. Забезпечення життєво важливих функцій та послуг є одним з ключових пріоритетів національної безпеки. Український досвід у галузі енергозабезпечення в умовах воєнних конфліктів та руйнування критичної інфраструктури визначає різноманітні завдання, які виникають у країні під час кризових ситуацій. Розширення системи для забезпечення стійкості роботи критичної інфраструктури та забезпечення життєво важливих функцій потребує створення комплексу організаційних та юридичних механізмів, які спрямовані на узгодження цілей та координацію зусиль всіх зацікавлених сторін.

9. Планування стійкості роботи критичної інфраструктури та надання життєво важливих послуг повинно враховувати майбутні перспективи розвитку інфраструктурних систем, передбачати умови майбутнього функціонування критичної інфраструктури, а також нові технології та знання. Це підвищить можливість виконання одного з головних завдань, а саме - пристосування критичної

інфраструктури до нових умов роботи та її швидке відновлення на більш високому рівні.

10. Одним з важливих перспективних напрямків поліпшення державної стратегії забезпечення безпеки об’єктів критичної інфраструктури в Україні є процес підготовки кваліфікованих кадрів у цій галузі. Адміністрування освітнього процесу щодо забезпечення кадрами об’єктів критичної інфраструктури на різних рівнях із різними спрямуваннями, включаючи управлінський персонал, перш за все повинно базуватися на чіткому та обґрунтованому науковому підґрунті. Діяльність та наслідки роботи в цій галузі залежать від кваліфікації, знань та вмінь фахівців, які працюють в ній.

11. Виявлено розвиток та зміну управлінської та правової регламентації системи захисту критично важливої інфраструктури в Україні. Обгрунтовано, що розвиток законодавства у сфері національної безпеки і адміністративно - правове регулювання державної системи захисту КІ є взаємозалежними. Визначено та докладно описано завдання, які законодавство вирішує у сфері захисту критичної інфраструктури.

12. Питання забезпечення безпеки об’єктів КІ та стійкості є однією з найсуттєвіших аспектів національної безпеки країни. Отже, у майбутніх дослідженнях необхідно розробити пропозиції для вирішення наукових проблем, які стосуються забезпечення ефективного функціонування та розвитку механізмів реагування на кризові ситуації, що можуть загрожувати національній безпеці України.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1.Бірюков Д.С. Про доцільність та особливості визначення критичної інфраструктури в Україні. Аналітична записка. 02.01.2013р. URL: http://www.niss.gov.ua/articles/1026/ (дата звернення 14.09.2023 р.).

2.Зелена книга з питань захисту критичної інфраструктури в Україні: зб. матер. міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов; за заг. ред. О. М. Суходолі. К.: НІСД, 2016. 176 с.

3. Директива Ради 2008/114/ЄС від 8 грудня 2008 р. про ідентифікацію і визначення Європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту. Офіційний вісник Європейського Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_002-08#Text (дата звернення: 15.09.2023 р.).

4. Мельничук О. Управління критичною інфраструктурою держави: базові методи та критерії ідентифікації об’єктів [Електронний ресурс] / О. Мельничук // Державне управління та місце всамоврядування, 2019, Вип. 3 (42). – С.13-27. URL: http://www.dridu.dp.ua/zbirnik_dums/2019/2019_03(42)/4.pdf.

5. Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України: Рішення Ради національної безпеки і оборони України від 01.03.2014. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/n0001525-14 (дата звернення: 15.09.2023 р.).

6. Про критичну інфраструктуру: Закон України від 16.11.2021р. №1882-IX. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 15.09.2023 р.).

7. Проект плану відновлення України: матеріали робочої групи «Аудиту збитків, понесених внаслідок війни». / Національна рада з відновлення України від наслідків війни, липень, 2022 р. [Електронний ресурс]. URL: https://www.kmu.gov.ua/storage/app/sites/1/recoveryrada/ua/audit-of-war-damage.pdf (дата звернення 14.09.2023 р.).

8. Настюк В. Я. Адміністративно-правові режими у сфері національної безпеки та протидії тероризму: монографія. Київ: НКЦ «Ін-т операт. діяльн. та держ. Безпеки», 2008. 245 с.

9. Кондратов С. І. Про забезпечення координації дій, взаємодії та обміну інформацією при створенні державної системи захисту критичної інфраструктури: аналіт. доп. Київ : НСІД, 2018. 30 с.

10. Мельниченко О. А. Надзвичайні ситуації техногенного характеру: сутність та засоби державного управління. Вісник Національного університету цивільного захисту України. Державне управління. Київ, 2014. №2. С. 149–156.

11. Захист населення і територій від надзвичайних ситуацій. Техногенна та природна небезпека / заг. ред. В. В. Могильниченка. Київ: КІМ, 2007. 636 с.

12. Полєжаєв А. М. До питання обліку системи моніторингу і прогнозування надзвичайних ситуацій техногенного характеру. // Системи озброєння і військова техніка. 2013. № 3. С. 139−142.

13. Про національну безпеку України: Закон України від 21.06.2018р. №2469-19. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 15.09.2023 р.).

14. Про Стратегію національної безпеки України: Указ Президента України від 26.05. 2015 р. №287/2015. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text (дата звернення: 15.09.2023 р.).

15. Конституція України, прийнята на п’ятій сесії Верховної Ради України 28 черв. 1996 р. Відомості Верховної Ради України. 1996. № 30. Ст. 141. URL: https://ips.ligazakon.net/document/T000000?an=2 (дата звернення: 15.09.2023 р.).

16. Про Річну національну програму під егідою Комісії Україна – НАТО на 2022 рік: Указ Президента України від 23.02. 2022 р. №189/2022. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/189/2021#Text (дата звернення: 15.09.2023 р.).

17. Про звіт щодо результатів проведення огляду загальнодержавної системи боротьби з тероризмом: Указ Президента України від 04. 06. 2021 р. № 251/2021. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/251/2021#Text (дата звернення: 15.09.2023 р.).

18. Про Концепцію боротьби з тероризмом в Україні: Указ Президента України від 05. 03. 2019 р. № 53/2019 / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/53/2019#Text (дата звернення: 15.09.2023 р.).

19. Про Порядок проведення огляду загальнодержавної системи боротьби з тероризмом: Указ Президента України від 09. 07. 2019 р. № 506/2019 / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/506/2019#Text (дата звернення: 15.09.2023 р.).

20. Про деякі питання координації діяльності суб'єктів боротьби з тероризмом: Указ Президента України від 25.04.2013 р. № 230/2013. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/230/2013#n9 (дата звернення: 15.09.2023 р.).

21. Щодо додаткових заходів із посилення стійкості функціонування енергетичної системи: Указ Президента України від 07.11. 2023 р. № 737/2023. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/n0041525-23#Text (дата звернення: 15.09.2023 р.).

22. Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій: Указ Президента України від 17.10. 2023 р. № 695/2023. / База даних «Законодавство України» / ВР України. URL: https://ips.ligazakon.net/document/MUS38625 (дата звернення: 15.09.2023 р.).

23. Про Стратегію кібербезпеки України: Указ Президента України від 27 січня 2016 р. від 15 березня 2016 р. № 96/2016. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text (дата звернення: 15.09.2023 р.).

24. Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури: Указ Президента України від 16 .01. 2017 р. № 8/2017. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/n0014525-16#Text (дата звернення: 15.09.2023 р.).

25. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 6. 12. 2017 року №

1009-р. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (дата звернення: 15.09.2023 р.).

26. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06. 2019 р. № 518. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 15.09.2023 р.).

27. Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10. 2020 р. № 1109. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (дата звернення: 15.09.2023 р.).

28. Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 09.10. 2020 р. № 1109 [27] / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (дата звернення: 15.09.2023 р.).

29. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 22.07. 2022 р. №821. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#Text (дата звернення: 15.09.2023 р.).

30. Деякі питання подання інформації у сфері захисту критичної інфраструктури: Постанова Кабінету Міністрів України від 14.10. 2022 р. № 1175 / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1175-2022-%D0%BF#Text (дата звернення: 15.09.2023 р.).

31. Про затвердження Державної цільової програми відновлення та розбудови миру в східних регіонах України: Постанова Кабінету Міністрів України від 13.12. 2017 р. № 1071: / База даних «Законодавство України» / ВР України. URL:

https://zakon.rada.gov.ua/laws/show/1071-2017-%D0%BF#Text (дата звернення: 15.09.2023 р.).

32. Про затвердження Державної стратегії регіонального розвитку на 2021-2027 роки: Постанова Кабінету Міністрів України від 5.08. 2020 р. № 695. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/695-2020-%D0%BF#Text (дата звернення: 15.09.2023 р.).

33. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури: Розпорядження Кабінету Міністрів України від 19.09.2023 р. № 825-р. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#n13 (дата звернення: 15.09.2023 р.).

34. Про Директорат стратегічного планування та європейської інтеграції Міністерства внутрішніх справ України: Наказ Міністерства внутрішніх справ України від 21.05. 2020 року № 406. URL: https://minre.gov.ua/zvit-2022-2023/robota-dyrektoratu-strategichnogo-planuvannya-ta-yevropejskoyi-integracziyi/ (дата звернення: 15.09.2023 р.).

35. Про затвердження положення про Департамент інформатизації Міністерства внутрішніх справ України: Наказ Міністерства внутрішніх справ України від 31.01. 2018 року № 70. URL: https://ips.ligazakon.net/document/MVS819 (дата звернення: 15.09.2023 р.).

36. Про затвердження Інструкції з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України: Наказ Міністерства внутрішніх справ України від 27.04.2020 р. № 357. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/z0443-20#Text (дата звернення: 15.09.2023 р.).

37. Деякі питання об’єктів критичної інфраструктури: Постанова КМУ від 09. 10. 2020 р. № 1109. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1109-2020п#Text (дата звернення: 15.09.2023 р.).

38. Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури: Постанова КМУ від 22.07.2022 р. № 821. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/821/-2022-%D0%BF#Text (дата звернення: 15.09.2023 р.).

39. Про затвердження Регламенту обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури: Постанова КМУ від 14.10. 2022 р. № 1174. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1174-2022-%D0%BF#Text (дата звернення: 15.09.2023 р.).

40. Деякі питання подання інформації у сфері захисту критичної інфраструктури: Постанова КМУ від 14.10.2022 р. № 1175. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1175-2022-%D0%BF#n13 (дата звернення: 15.09.2023 р.).

41. Корченко А.О. Метод оцінки рівня критичності для систем управління кризовими ситуаціями / А.О. Корченко, В.А. Козачок, А.І. Гізун // Захист інформації. – 2015. – Т. 17, № 1. – С. 86-98. URL: http://nbuv.gov.ua/UJRN/Zi_2015_17_1_14 (дата звернення: 15.09.2023 р.).

42. Risk assessment methodologies for critical infrastructure protection. Part I: a state of theart / G. Giannopoulos, R. Filippini, M. Schimmer. – Luxembourg: Joint Research Centre of Institute for the Protection and Security of the Citizen, 2012. 70 p.

43. Асиміляційний потенціал геологічного середовища України та його оцінка / С. О. Довгий, В. В. Іванченко та ін.; НАН України, Інститут телекомунікацій і глобального інформаційного простору. Київ: Ніка-Центр, 2016. 176 с.

44. Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. – Luxembourg: Joint Research Centre of Institute for the Protection and Security of the Citizen, 2015. 28 p.

45. Іванюта С. П., Качинський А. Б. Екологічна та природно-техногенна безпека України: регіональний вимір загроз і ризиків: монографія / Нац. ін-т стратегічних досліджень. Київ: НІСД, 2012. 308 с.

46. Бобро Д.Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі // Стратегічні пріоритети. Серія: Економіка. 2015. № 4. С. 83-93.

47. Запобігання, готовність та реагування на терористичні напади: повідомлення Комісії Ради та Європейському Парламенту від 20 жовтня 2004 року /COM (2004) 698 final – Official Journal від 20.01.2005. URL: http://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex:52004DC0702 (дата звернення: 15.09.2023 р.).

48. Защита критической инфраструктуры. Концепция основных мер защиты. Рекомендация для предприятий / Bundesministerium des Innern, 2006. URL: https://www.bmi.bund.de (дата звернення: 19.09.2023 р.).

49. National Critical Infrastructure Security and Resilience Research and Development Plan, 2015. URL: https://www.dhs.gov/publication (дата звернення: 19.09.2023 р.).

50. Єрменчук О.П. Побудова системи захисту критичної інфраструктури в Україні з використанням досвіду сектору безпеки іноземних держав // Актуальні проблеми вдосконалення чинного законодавства України. Івано-Франківськ, 2017. № XLIV. С. 224-235.

51. Сиденко В.М., Грошко И.М. Основы научных исследований. Харьков: Вища школа, 1970. 200 с.

52. Марек Сметана. Защита критической инфраструктуры. Подходы государств Европейского Союза к определению элементов критической инфраструктуры. Острава: ВШБ Технический университет Острава, 2014/2015. 60 с.

53. Національні **с**истеми оцінювання ризиків і загроз: кращі світові практики, нові можливості для України : аналіт. доп. / [Резнікова О. О., Войтовський К. Є. Лепіхов А. В.]; за заг. ред. О. О. Резнікової. Київ : НІСД, 2020. 84 с.

54. Єрменчук О.П. Нормативно-правове регулювання діяльності у сфері захисту національної критичної інфраструктури: аналіз та узагальнення нормотворчої практики США // Науковий вісник ДДУВС. Дніпро. 2017. № 3. С. 135-140.

55. Lewis T.G. Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons, Inc., 2006. – 474 p.

56. Quantification of dependencies between electrical and information infrastructures / Beccutia M., Chiaradonnac S., Di Giandomenicoc F., Donatellia S., Dondossolad G., Franceschinisb G. // Int. J. Critical Infrastructure Protection. 2012. Vol.5. P. 14 – 27.

57. Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research // P.Pederson, D.Dudenhoeffer, S.Hartley, M.Permann. Idaho National Laboratory. U.S. Department of Energy, 2006. 116 p.

58. Про критичну інфраструктуру та її захист: проєкт Закону України від 27.05.2019р. № 10328. / База даних «Законодавство України» / ВР України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996 (дата звернення: 19.09.2023 р.).

59. Домарацький М. Б. Забезпечення безпеки та підвищення ефективності захисту критично важливих об'єктів на державному рівні. Публічне управління і адміністрування в Україні. 2019. Вип. 14. С. 82–85.

60. Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання: Закон України від 19.10.2000 № 2064-III. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2064-14#Text (дата звернення: 20.09.2023 р.).

61. Суходоля О. М. Захист критичної інфраструктури: сучасні виклики та пріоритетні завдання сектору безпеки. Науковий часопис, 2017. Вип. 1-2 (13-14). С. 50-80.

62. Про деякі заходи з оптимізації системи центральних органів виконавчої влади: Указ Президента України від 24.12.2012р № 726/2012. / База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/726/2012#Text (дата звернення: 20.09.2023 р.).

63. Теленик С. С. Досвід правового регулювання системи захисту критичної інфраструктури в США. Науковий вісник НАВС. 2018. № 2 (107). С. 358–370.

64. Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М. Організаційні та правові аспекти забезпечення безпеки і стій кості критичної інфраструктури України. К.: НІСД, 2019. 224 с.

65. Єрменчук О. П. Складові національної інфраструктури. Науковий вісник ДДУВС. 2017. № 4. С. 109–115.

66. Теленик С.С. Державна система захисту критичної інфраструктури України: концептуальні засади адміністративно-правового регулювання / С. Теленик // Херсон: Видавничий дім "Гельветика", 2020. 602 с.

67. Методика побудови системи управління інформаційною безпекою на об’єктах критичної інфраструктури / М. Ю. Комаров, С. Ф. Гончар // Моделювання та інформаційні технології. 2017. Вип. 81. С. 12-19.

68. Цюрупа М. Зміна парадигм воєнно-політичного мислення у доктринах та стратегіях воєнної безпеки України XX–XXI ст. Українознавчий альманах. 2021. Вип. 28. С. 120–126.