МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Навчально-науковий інститут неперервної освіти
Кафедра публічного управління та адміністрування

ДОПУСТИТИ ДО ЗАХИСТУ
В.о.завідувача кафедри
Кожина Алла Василівна

_____

“___” _____ 2024 року

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ “МАГІСТР”
спеціальності 281 “Публічне управління та адміністрування” освітньо-професійної програми «Менеджмент в органах публічного управління»

Тема: “ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІД ЧАС ДІЇ ВОЄННОГО СТАНУ В УКРАЇНІ”

Електронний підпис
КАБАНОВ СЕРГІЙ ОЛЕКСАНДРОВИЧ
ЄДРПОУ/ІПН 2883500752
Підписано у Вчасно

Виконавець: студент групи М-281-23-1-МУ Кабанов Сергій Олександрович

Електронний підпис
ЛЕЛЕЧЕНКО АНЖЕЛА ПАВЛІВНА
Ідентифікаційний код 2544808106
Підписано у Вчасно

Керівник: Д.держ.упр., професор Лелеченко Анжела Павлівна

Нормоконтролер: А.П Лелеченко

Електронний підпис
Кожина Алла Василівна
Ідентифікаційний код 2686200868
Підписано у Вчасно

Київ 2024

ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Навчально-науковий інститут неперервної освіти
Кафедра публічного управління та адміністрування
Спеціальність 281Публічне управління та адміністрування

ЗАТВЕРДЖУЮ:

В.о. завідувача кафедри

_____Алла КОЖИНА

«_____»_____2024 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи (проєкту)

Кабанова Сергія Олександровича

1. Тема кваліфікаційної роботи (проєкту): «ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІД ЧАС ДІЇ ВОЄННОГО СТАНУ В УКРАЇНІ» затверджена наказом ректора від 15.10.2024 року № 2241/ст.

2. Термін виконання роботи (проєкту): з 15.10.2024 р. по 25.11.2024 р.

3. Вихідні дані по роботі (проєкту):

- проаналізувати об'єкти критичної інфраструктури з урахуванням існуючих класифікацій;
- розкрити особливості нормативно-правового забезпечення захисту критичної інфраструктури в умовах воєнного стану;
- узагальнити світовий досвід впровадження інноваційних методів із забезпечення безпеки та стійкості критичної інфраструктури;
- ідентифікувати потенційні загрози та здійснити аналіз ризиків, що впливають на функціонування критичної інфраструктури;

- охарактеризувати сучасний стан захищеності об'єктів критичної інфраструктури в контексті національної безпеки України;
- розробити практичні рекомендації щодо забезпечення стійкості критичної інфраструктури під час дії воєнного стану в Україні.

4. Зміст пояснювальної записки: Оцінка джерел загальної інформації, літератури та інших прийнятних робіт. Проведений точний аналіз сучасних підходів до підвищення стійкості критично важливих об'єктів інфраструктури. Підвищення стійкості критичної інфраструктури від різних типів загроз. Розробка рекомендацій для оптимізації заходів з підвищення стійкості об'єктів критичної інфраструктури.

5. Перелік обов'язкового графічного (ілюстративного) матеріалу.

6. Календарний план-графік:

№ з/п	Графік виконання роботи	Строк виконання	Фактичне виконання
1.	Розроблення детального плану роботи	17.10.2024	17.10.2024
2.	Підготовка Розділу 1	27.10.2024	27.10.2024
3.	Підготовка Розділу 2	10.11.2024	10.11.2024
4.	Підготовка Розділу 3	18.11.2024	18.11.2024
5.	Підготовка Вступу, Висновків та Анотації	24.11.2024	24.11.2024
6.	Надання завершеної роботи науковому керівнику для перевірки	25.11.2024	25.11.2024

7. Дата видачі завдання: «15» жовтня 2024р.

Керівник кваліфікаційної роботи (проєкту): _____ Лелеченко А.П.
(підпис керівника (П.І.Б.)

Завдання прийняв до виконання: _____ Кабанов С. О.
(підпис здобувача вищої освіти) (П.І.Б.)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Особливості забезпечення стійкості критичної інфраструктури під час дії воєнного стану в України»: 86 с., 94 літературних джерела.

Об’єкт дослідження: критична інфраструктура України як система життєво важливих об'єктів і служб.

Мета роботи: обґрунтування теоретичних засад і розробка практичних рекомендацій щодо забезпечення стійкості критичної інфраструктури під час дії воєнного стану в Україні.

Методи дослідження: аналітичний, системно-функціональний, порівняльний аналіз, узагальнення.

Результати магістерської роботи рекомендується використовувати в практичній діяльності фахівців з публічного управління та адміністрування для підвищення ефективності заходів щодо зміцнення стійкості критичної інфраструктури.

СТІЙКІСТЬ, КРИТИЧНА ІНФОРАСТРУКТУРА, ОБ’ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ, БЕЗПЕКА, КРИЗА, ЗАГРОЗА, РИЗИКИ.

ЗМІСТ

ВСТУП

З початком повномасштабного вторгнення Росії на територію України в 2022 році, забезпечення стійкості критичної інфраструктури набуло нового виміру у контексті національної безпеки. Критична інфраструктура, включаючи енергетичні системи, комунікаційні мережі, транспортні та логістичні вузли, медичні установи, стала мішенню для постійних атак ракетами та безпілотниками. Це викликає необхідність адаптації до нових умов ведення війни, де неперервність функціонування цих систем є критичною для підтримки обороноздатності держави та загальної стабільності.

Аналізуючи сучасні загрози для критичної інфраструктури в Україні, виявляється потреба в комплексних заходах захисту. Це охоплює впровадження передових технологій, зміцнення фізичного захисту об'єктів та забезпечення кібербезпеки. Разом з технологічними рішеннями, критичне значення має розробка та впровадження відповідних нормативно-правових актів та стратегій, які дозволять синхронізувати дії різних органів безпеки і управління в умовах кризи.

Вагомий внесок у розвиток методик захисту та ідентифікації вразливих об'єктів зробили відомі зарубіжні вчені, такі як Д. Дуденхофер і П. Педерсен, та українські науковці, серед яких Л. Арсенович, В. Антипенко та С. Кондратов, О. Батюк, Д. Бобро, Д. Бірюкова, Г. Зубко, С. Кондратова, О. Мельничук, С. Кондратов, О. Суходоля, С. Теленик, В. Храпкіна, А. Чорноус. Незважаючи на значну кількість досліджень, спрямованих на антитерористичний захист, аналізу стійкості критичної інфраструктури в умовах воєнного стану досі потребує подальших досліджень для розробки інтегрованих підходів забезпечення національної безпеки.

Мета дослідження – обґрунтування теоретичних засад і розробка практичних рекомендацій щодо забезпечення стійкості критичної інфраструктури під час дії воєнного стану в Україні.

Для досягнення поставленої мети необхідно виконати такі основні завдання:

- проаналізувати об'єкти критичної інфраструктури з урахуванням існуючих класифікацій;
- розкрити особливості нормативно-правового забезпечення захисту критичної інфраструктури в умовах воєнного стану;
- узагальнити світовий досвід впровадження інноваційних методів із забезпечення безпеки та стійкості критичної інфраструктури;
- ідентифікувати потенційні загрози та здійснити аналіз ризиків, що впливають на функціонування критичної інфраструктури;
- охарактеризувати сучасний стан захищеності об'єктів критичної інфраструктури в контексті національної безпеки України;
- розробити практичні рекомендації щодо забезпечення стійкості критичної інфраструктури під час дії воєнного стану в Україні.

Об'єкт дослідження – критична інфраструктура України як система життєво важливих об'єктів і служб.

Предмет дослідження – особливості забезпечення стійкості критичної інфраструктури під час дії воєнного стану в України.

Методи дослідження. У рамках дослідження особливостей забезпечення стійкості критичної інфраструктури під час дії воєнного стану в Україні застосовано комплекс методів, що забезпечують глибокий аналіз і об'єктивність отриманих результатів. Використання філософсько-світоглядних, загальнонаукових та спеціалізованих методів дозволило підійти всебічно до вирішення поставлених завдань. Зокрема, аналітичний метод сприяв ретельному розгляду існуючих механізмів захисту та виявленню потенційних слабких місць критичної інфраструктури, тоді як системно-функціональний аналіз допоміг розкрити особливості взаємодії між її елементами. Порівняльний аналіз дозволив оцінити міжнародний досвід і адаптувати кращі практики для підвищення стійкості української інфраструктури. Використання узагальнення сприяло формулюванню

обґрунтованих висновків і рекомендацій, спрямованих на зміцнення критичних об'єктів у кризовий період.

Наукова новизна дослідження полягає у комплексному аналізі забезпечення стійкості об'єктів критичної інфраструктури України під час дії воєнного стану, з огляду на унікальний контекст повномасштабного вторгнення Росії. Вперше систематизовано зазначені об'єкти згідно з їх вразливістю до сучасних збройних атак, включаючи ракетні удари та дрони, та оцінено аспекти їхньої захищеності відповідно до світового досвіду та сучасних підходів. Визначено прогалини в нормативно-правовому регулюванні, що дозволяє сформулювати рекомендації та ключові заходи для підвищення стійкості критичної інфраструктури, що є актуальним для забезпечення національної безпеки в екстремальних умовах.

Практичне значення отриманих результатів дослідження полягає у визначенні та розробці ефективних стратегій та механізмів для забезпечення стійкості критичної інфраструктури в умовах воєнного стану в Україні. Результати дослідження підкреслюють необхідність розробки комплексних підходів до управління ризиками, які включають як фізичний захист, так і кіберзахист об'єктів критичної інфраструктури.

Зокрема, результати дослідження сприяють формуванню нормативно-правової бази, яка дозволяє зміцнити систему національної безпеки через чітке визначення повноважень та відповідальності між різними органами державного чи публічного управління. Важливим аспектом є розробка та впровадження програм підготовки персоналу, здатного ефективно діяти в умовах кризи, а також створення резервних систем і альтернативних логістичних шляхів для забезпечення неперервності діяльності критичної інфраструктури.

Структура та обсяг роботи. Відповідно до мети, завдання й предмета дослідження наукова робота складається зі вступу, трьох розділів, які об’єднують 8 підрозділів, висновків, списку використаних джерел. Загальний обсяг роботи - 86 сторінок, список використаних джерел – 94 найменування.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Систематизація об'єктів критичної інфраструктури

Історичний аналіз розвитку світових держав та цивілізацій свідчить, що суспільства на всіх етапах своєї еволюції стикаються з різноманітними загрозами, як зовнішніми, так і внутрішніми. Ці загрози є непостійними і змінюють свої форми та цілі, відповідно до ступеня економічного, соціального та технологічного прогресу суспільства. Наслідки таких загроз можуть бути катастрофічними і часто включають людські жертви та значні матеріальні збитки, що негативно впливають на соціально-економічний розвиток, суверенітет, територіальну цілісність та національну безпеку держави.

Ще в давнину, великі цивілізації, такі як китайська та грецька, розуміли важливість певних об'єктів для стабільності суспільства. В історичних трактатах, як-от «Мистецтво війни» Сунь Цзи, датованому VII століттям до нашої ери, вказується на п'ять основних цілей, які ворог намагається знищити під час нападу: людські ресурси, провіант, табори, склади та військові підрозділи [92, с. 70].

У давнину до переліку критично важливих об'єктів часто входили транспортні мережі та системи водопостачання, які були вирішальними для підтримки життєдіяльності населення. Безперервна робота цих об'єктів була критичною для задоволення потреб громадян та вважалася ключовим аспектом управління населенням. Відтак, захист цих об'єктів під час нападів ставав пріоритетним завданням захисників. Контроль або знищення цих об'єктів став стратегічною основою військових доктрин та операцій спеціальних служб в наступні епохи.

Ініціальне використання терміна «інфраструктура» зазвичай асоціюється з давньогрецьким філософом Сократом (V століття до н.е.), який вважав, що для стабільного існування людини суспільство має забезпечити необхідні основи, такі як безпека, соціальний порядок і матеріальні блага, які людина отримує через дотримання соціальних концепцій та виконання обов'язків, особливо у підтримці інфраструктури та надання суспільних послуг [69]. Водночас, термін «інфраструктура» спочатку застосовувався у військовому контексті у Франції для опису «підземних споруд». Згідно з дослідженнями Стефена Левіса, цей термін увійшов у широке вживання у США завдяки французьким інженерам, які працювали над реалізацією проєктів залізниць, тунелів та мостів, сприяючи трансформації його значення на американському континенті [74].

У XX столітті світ став свідком появи так званих «гібридних війн», характеристикою яких є використання агресором різноманітних загроз, що цілеспрямовано направлені на вразливі місця противника. Це включає застосування комбінацій конвенційної зброї, партизанських дій, терористичних актів з метою досягнення політичних цілей. Відомий військовий аналітик Ф. Хофман передбачав, що такий тип війн стане все більш розповсюдженим [72]. Український політолог Є. Магда акцентує на різноманітності тактик, використаних у гібридних війнах, включно з політичними, військовими, економічними, соціальними, інформаційними та підривними діями [21, с. 30-31].

Останні десятиліття позначені значними змінами в методах та засобах ведення війн, що відображає еволюцію цілей агресії. Особливо велике значення в цьому процесі мають стрімкий розвиток інформаційних технологій та їх вплив на інтеграцію, взаємозалежність та взаємопроникнення різних систем. У двадцятому столітті, зокрема під час кризи на Кубі, були зафіксовані значні зміни в стратегіях захисту важливої цивільної інфраструктури, включаючи системи телекомунікацій. Видатним прикладом кібернападів на такі об'єкти є втручання в іранські атомні

установки у 2010 році через шкідливе програмне забезпечення «Stuxnet» [8]. Крім того, інфраструктурні об'єкти України регулярно потерпають від кібернападів. Наприклад, у 2015 році через вірус «BlackEnergy» сталася зупинка електропостачання від компанії «Прикарпаттяобленерго», внаслідок чого приблизно 230 тисяч людей залишились без світла. Згідно з даними, оприлюдненими на засіданні Ради національної безпеки і оборони України, в останні два місяці 2016 року кількість кібератак в Україні досягла 2,5 тисячі [47]. На глобальному рівні, провідні держави активно працюють над забезпеченням захисту критичної інфраструктури, охоплюючи як фізичні, так і кібернетичні компоненти. Наприклад, в Плані захисту критичної інфраструктури США за 2015 рік акцент зроблено на мінімізацію ризиків від потенційних загроз і швидке відновлення функціонування після інцидентів [79]. В Німеччині, крім терористичних загроз і надзвичайних ситуацій викликаних природними катастрофами, також враховуються загрози з боку технічних несправностей і помилок операторів, включно з кіберзагрозами [15]. Необхідно відмітити, що природні катастрофи, такі як повені, посухи, епідемії, землетруси та інші стихійні лиха, розглядаються як окремий вид загроз, які не викликані соціальними факторами. Аналізуючи світові методики, можемо визначити три основні стратегії оборони важливих інфраструктурних об'єктів:

1. Оборона від загроз національній безпеці, що враховує як зовнішні, так і внутрішні ризики, які можуть спричинити фізичне ушкодження або знищення витальних інфраструктур.
2. Захист проти кібератак.
3. Превенція ризиків від різного роду надзвичайних ситуацій.

Критична інфраструктура постійно опиняється під загрозою як потенційна мішень для нападів чи стихійних подій, включаючи природні катастрофи. Ідентифікація та розуміння терміну «критична інфраструктура» зазнали істотних змін, що відбивають еволюцію суспільних умов. В Америці цілеспрямовані заходи зі захисту цієї сфери були започатковані з 1980-х

років, зокрема завдяки дослідженням Національного дослідницького інституту [74]. Важливим чинником, який підштовхнув до розвитку цих досліджень, стали події, такі як терористичні напади 11 вересня 2001 року в США, атаки 11 березня 2004 року в Мадриді та терористичні акти 7 липня 2005 року в Лондоні [55].

Україна також зазначила значний прогрес у цій області з початку 2000-х, особливо після 2015 року. Популяризації та розвитку напряму сприяла публікація дослідження Національного інституту стратегічних досліджень у Зеленій книзі з питань захисту критичної інфраструктури в Україні. В документі вказується, що під критичною інфраструктурою розуміють ключові фізичні та цифрові системи та ресурси, необхідні для життєдіяльності населення, порушення яких може призвести до критичних наслідків для соціально-економічного стану та національної безпеки [16]. Цей документ також визначає основні цілі та завдання національної політики у цій сфері.

Термінологія, що використовується для опису критичної інфраструктури, систематично оновлюється та допрацьовується. У 2002 році на засіданні Євроатлантичної ради НАТО було прийнято визначення, яке включає не тільки фізичні, але і кібернетичні системи, що підтримують ключові функції управління економікою та суспільством, включаючи телекомунікаційні, енергетичні, банківські, фінансові системи, а також водопостачання та аварійні служби [22, с. 32].

Від 2003 року в Європейському Союзі розгорнуто інтенсивні дослідження в галузі безпеки через програми, такі як «European industrial potential in the field of security research» та «European Security Research Programme (ESRP)». Ініціатива «Research for Secure Europe», що стартувала у 2007 році, має на меті підготовку до можливих військових конфліктів та екстрених ситуацій. З 2004 року ЄС разом із Європейською комісією запровадили проект «European Programme for Critical Infrastructure Protection» (EPCIP), у рамках якого особливий акцент робиться на захист від

терористичних акцій. Під критичною інфраструктурою в цей період розуміють обладнання, послуги та інформаційні системи, чиє ушкодження або знищення може мати серйозні наслідки для стабільності суспільства, економіки, охорони здоров’я або державного ладу.

17 листопада 2005 року Європейська Комісія схвалила знаний як «Зелена книга» документ з питань захисту критичної інфраструктури (EPCIP), який закладає основу уніфікованої стратегії і практичних заходів захисту в ЄС. Важливою частиною цієї документації є підсилення кооперації та обміну інформацією серед країн-членів у сфері транснаціональних загроз [22].

Аналіз країн ЄС показує, що критична інфраструктура розглядається як комплексна система мережевих вузлів та компонентів, де пошкодження одного елемента може спровокувати масштабні перебої в роботі цілої системи. Це наголошує на важливості захисту кожного вузла для забезпечення загальної резистентності [22].

У США критична інфраструктура поділена на 16 секторів, тоді як у Європі існує класифікація на кілька рівнів секторів та послуг, від 8 до 10. Первісно, захист критичної інфраструктури в Європі орієнтувався на стабільність національних систем. Сьогодні ж головна мета полягає в забезпеченні всебічного захисту на всій території Європи, з ключовими завданнями у вигляді боротьби з тероризмом та кіберзагрозами.

З урахуванням вищевикладеного, доцільно вбачати в оновленому визначенні вітчизняної критичної інфраструктури як матеріальні, так і нематеріальні компоненти. Визначення цих об'єктів як надзвичайно важливих підтверджується законодавствами США та Німеччини, де вони описуються як системи та засоби, фізичні чи віртуальні, життєво важливі [16]. Тому пропонується розширене національне визначення критичної інфраструктури, що охоплює надзвичайно важливі матеріальні та нематеріальні об'єкти національної інфраструктури. Таке законодавче оформлення сприятиме ефективному протидії тероризму та кіберзагрозам, а також координації

захисних заходів на національному рівні, як це вже практикується у країнах ЄС.

Сучасне визначення критичної інфраструктури наголошує не тільки на фізичних аспектах об'єктів, але й на їхніх функціональних особливостях та наданих послугах, відіграючи ключову роль у задоволенні потреб суспільства, держави та її економіки. Цей методологічний підхід сприяє формуванню критеріїв для визначення пріоритетності захисту елементів критичної інфраструктури [16].

Термін «об'єкт національної інфраструктури» охоплює широкий спектр державних та приватних підприємств, організацій, установ та їх майна, що спільно формують механізм функціонування держави, економіки та суспільства [10, с. 20-27]. Це включення дозволяє об'єктам виходити за межі традиційних визначень українського законодавства.

Об'єкти, які мають критичне значення для забезпечення державної безпеки, визначаються як найважливіші елементи критичної інфраструктури. Цей методологічний підхід дозволяє встановити чіткі критерії для ідентифікації таких компонентів національної інфраструктури, які потребують особливого захисту [11, с. 39].

У європейському законодавстві розрізняють дві основні категорії критичної інфраструктури: національну та європейську. Національна категорія включає засоби, системи та їх компоненти, розташовані в країнах-членах ЄС, визнані невід'ємними для підтримки основних функцій суспільства, включаючи здоров'я, безпеку та соціально-економічні умови населення. Збої або знищення цих компонентів можуть мати серйозні наслідки [91]. Концепція європейської критичної інфраструктури охоплює об'єкти, чия дисфункція може призвести до значних наслідків у мінімум двох країнах ЄС [91].

Професор Йозеф Ржига у своєму аналізі, опублікованому в «Урбанізм і територіальний розвиток», акцентує на критеріях відбору об'єктів для включення до критичної інфраструктури, зазначаючи про важливість

професійного підходу, значимість об'єктів та часові аспекти, що визначають необхідність їхнього захисту [87].

Термін «критична інфраструктура» повинен включати об'єкти, що мають життєве значення для держави, і чиє пошкодження або дисфункція може призвести до значних негативних наслідків для здоров'я та безпеки громадян, а також для соціально-економічного стану країни. Ці об'єкти є основою для забезпечення стабільності національної інфраструктури та економіки в цілому.

Національне розуміння критичної інфраструктури може бути виражене через систему надзвичайно важливих матеріальних та нематеріальних об'єктів, що є вирішальними для стабільного функціонування країни. Пошкодження або знищення цих об'єктів внаслідок різноманітних загроз може мати великі наслідки для людських життів, матеріальних ресурсів та може суттєво вплинути на життєздатність суспільства, соціально-економічний розвиток та національну безпеку [25].

Об'єкти критичної інфраструктури охоплюють ключові підприємства та установи, розташовані у стратегічно важливих галузях, таких як енергетика, хімічна промисловість, транспорт, фінанси, інформаційні технології, телекомунікації, охорона здоров'я та продовольча сфера. Критичне значення цих об'єктів полягає у їх ролі в функціонуванні економіки та безпеки держави, а їх пошкодження або виведення з ладу може спричинити серйозні наслідки для національної безпеки, промисловості, екології та життя громадян.

Законопроект №5219 від 09.03.2021 визначає, що критична інфраструктура включає об'єкти, що оперують у критично важливих секторах, важливих для підтримки ключових функцій і послуг. Наслідки збоїв у їх діяльності можуть мати серйозні негативні впливи на національну безпеку України та на обслуговування населення. Об'єкти критичної інфраструктури розділені на чотири категорії, які залежать від ступеня

їхнього впливу на виконання життєво важливих функцій у відповідних секторах [35].

Закон України “Про основні засади забезпечення кібербезпеки України” уводить поняття критично важливі об'єкти інфраструктури. Це юридичні особи, діяльність яких пов'язана з ключовими технологічними процесами та/або наданням послуг, які є важливими для промисловості, економіки, і безпеки населення. Також, закон визначає об'єкти критичної інформаційної інфраструктури – як технологічні або комунікаційні системи, чиї збої можуть прямо впливати на функціонування критичної інфраструктури [8].

Об'єкти критичної інфраструктури визначаються як вирішальні елементи, розміщені в стратегічно значущих секторах економіки — енергетиці, хімічній промисловості, транспорту, фінансах, IT та телекомунікаціях, охороні здоров'я та продовольчій галузі. Ці елементи мають вирішальне значення для забезпечення неперервності економічної та соціальної діяльності, а їхній збій чи знищення може призвести до серйозних наслідків для національної безпеки, довкілля, а також здоров'я і життя населення.

Статус критичної інфраструктури в Україні визначається відповідно до Постанови Кабінету Міністрів України № 1109, за якою відповідальність за охорону та регуляцію сфер критичної інфраструктури покладається на секторальні органи, такі як Держспецзв'язку, Міністерства внутрішніх справ, економіки, енергетики, інфраструктури, оборони, цифрової трансформації, фінансів, охорони здоров'я, Національний банк, Національну службу здоров'я України та Службу безпеки України.

Згідно з цією Постановою, законодавство України встановлює чітку ієрархію критичності об'єктів критичної інфраструктури, поділяючи їх на чотири категорії за ступенем важливості та можливим впливом на національні або місцеві функції у випадку їх дисфункції чи призупинення. Об'єкти першої категорії відіграють критичну роль для держави, їхня діяльність має значний вплив на інші об'єкти критичної інфраструктури, а

їхня неспроможність може призвести до національної кризи. Об'єкти другої категорії є життєво необхідними для підтримки регіональних функцій, а їхній збій може спричинити регіональні кризи. Третя категорія включає об'єкти, значущі для місцевих спільнот, припинення їхньої діяльності може призвести до місцевих кризових ситуацій. Нарешті, четверта категорія об'єктів необхідна для підтримання місцевого життя, а їхнє порушення може створити локальні проблеми. Ця диференційована класифікація допомагає у вдосконаленні планування заходів зі зміцнення стабільності критично важливих функцій у суспільстві.

1.2. Нормативно-правове регулювання захисту критичної інфраструктури в умовах воєнного стану

Відповідно до Указу Президента України від 12 лютого 2007 року № 105/2007, який втратив чинність, були сформульовані основні внутрішні та зовнішні загрози, що становлять ризик національній безпеці України [40]. Це питання було далі розглянуто Рішенням Ради національної безпеки і оборони України від 6 травня 2015 року, що передбачало розробку Урядом комплексних пропозицій щодо реформування органів сектору безпеки і оборони України [41].

Важливим кроком у зміцненні системи національної безпеки є Розпорядження Кабінету Міністрів України від 6 грудня 2017 року № 1009-р, яке затвердило Концепцію створення державної системи захисту критичної інфраструктури. Згідно з цією Концепцією, одним із пріоритетів реформ в оборонному та безпековому секторах є створення ефективної системи захисту критичної інфраструктури [42].

Однак, Концепція також виявила ряд проблем, які потребують негайного вирішення. Серед них: відсутність уніфікованої системи захисту критичної інфраструктури; недостатність та неузгодженість нормативно-правового регулювання; відсутність спеціалізованого державного органу для

координації захисту критичної інфраструктури; невизначеність повноважень та правового статусу власників критичної інфраструктури; відсутність методології для визначення, паспортизації та категоризації критичної інфраструктури; недостатній розвиток державно-приватного партнерства; неясність джерел фінансування заходів захисту; та недостатній рівень міжнародного співробітництва у цій сфері [42].

У травні 2019 року було ініційовано Проєкт Закону «Про критичну інфраструктуру та її захист», що став логічним наслідком реалізації положень Концепції створення державної системи захисту критичної інфраструктури [34]. Як зазначено у пояснювальній записці до цього законопроєкту, його метою було створити умови для ефективного формування та реалізації державної політики у цій сфері. Наголошувалося, що прийняття Проєкту Закону мотивоване не тільки збройною агресією Російської Федерації, але й потребою захисту від природних чи техногенних загроз, які спостерігалися у східних та південних регіонах України. Проте, зазначений законопроєкт не був прийнятий [34].

Далі, у жовтні 2020 року, Уряд України прийняв Постанову «Деякі питання об’єктів критичної інфраструктури», якою було затверджено Порядок віднесення об’єктів до критичної інфраструктури, а також Перелік секторів і основних послуг критичної інфраструктури держави. Також у постанові визначено Методику категоризації таких об'єктів і встановлено ряд визначень, включаючи захист об’єктів критичної інфраструктури як комплекс заходів (організаційних, нормативно-правових, інженерно-технічних тощо) для забезпечення безпеки [6].

У листопаді 2021 року було прийнято Закон України «Про критичну інфраструктуру», який встановив організаційно-правові засади створення і функціонування національної системи захисту критичної інфраструктури. Цей Закон визначає термін «захист критичної інфраструктури» як всі види діяльності, що включають створення, функціонування, відновлення та реорганізацію об'єктів критичної інфраструктури, спрямовані на виявлення,

запобігання, нейтралізацію загроз та мінімізацію наслідків потенційних інцидентів [35].

У травні 2019 року ініційовано розробку Проєкту Закону «Про критичну інфраструктуру та її захист» [34], який став послідовним кроком у реалізації положень, визначених у Концепції. Згідно з пояснювальною запискою, головною метою цього Проєкту Закону було створення належних умов для втілення державної політики у сфері захисту критичної інфраструктури. Потреба в його адопції була обґрунтована з огляду на збройну агресію Російської Федерації, що уже мала місце на час подання Проєкту. Відтак, розробка ефективної системи захисту об'єктів критичної інфраструктури враховувала не лише природні чи техногенні загрози, а й збройне втручання до її масштабного нарощування та наслідки пошкодження інфраструктурних об’єктів у східних та південних регіонах України. Проєкт Закону, однак, було згодом відкликано.

Далі, у жовтні 2020 року, Уряд ухвалив Постанову «Деякі питання об’єктів критичної інфраструктури» № 1109 [6], яка затверджувала Порядок віднесення об’єктів до категорії критичної інфраструктури, визначала перелік секторів критичних послуг і методику категоризації цих об'єктів. Також було регламентовано визначення захисту об'єктів критичної інфраструктури як сукупність заходів різного спрямування, метою яких є забезпечення безпеки таких об'єктів.

У грудні 2021 року Верховна Рада України ухвалила Закон «Про критичну інфраструктуру», який створив юридичну основу для національної системи захисту важливих об’єктів. Відповідно до цього закону, «захист критичної інфраструктури» є комплексом заходів, що розглядаються на початку, під час та після експлуатації або модифікації інфраструктури, маючи на меті ефективне виявлення, запобігання, ліквідацію наслідків загроз, а також мінімізацію шкоди від можливих інцидентів. .

Цікаво, що поняття «захист критичної інфраструктури» отримало нове тлумачення, яке узгоджується з аналогічними термінами в законодавстві

Європейського Союзу. Це виявляється у більшому обмеженні дійсності через включення фрази, таких як всі види діяльності та нейтралізація загрози, розширюючи тим самим поняття застосування цього закону [59].

Також, Проєкт Закону містив термін «державна система захисту критичної інфраструктури», що означало систему суб'єктів забезпечення формування та реалізації державної політики у цій сфері [34]. Водночас, Закон України «Про критичну інфраструктуру» визначає термін «національна система захисту критичної інфраструктури», що надає більш деталізоване уявлення про учасників і структурні елементи системи захисту, включаючи сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади, органів місцевого самоврядування та операторів критичної інфраструктури [35].

Проте необхідно враховувати і ті пропозиції, які були включені в Проєкт Закону, але не знайшли відображення у чинному законодавстві. Наприклад, у порівняльній таблиці Проєкту Закону було запропоновано доповнити Закон України «Про правовий режим воєнного стану» поняттям "захист критичної інфраструктури" [36]. Ця ініціатива здається особливо важливою, адже стаття 3 Закону «Про критичну інфраструктуру» регулює застосування даного закону в мирний час, тоді як захист критичної інфраструктури в умовах воєнного стану, надзвичайних ситуацій вимагає наявності чітких нормативних регуляцій, які не враховані у чинному визначенні воєнного стану" позбавленому компоненту «захист критичної інфраструктури».

Державна політика України в області захисту критичної інфраструктури, закріплена у статті 5 Закону України «Про критичну інфраструктуру» [35], вимагає забезпечення безпеки об’єктів критичної інфраструктури та включає декілька ключових завдань. Передусім, державна політика спрямована на запобігання несанкціонованому втручанню у функціонування цих об’єктів та на прогнозування та запобігання кризовим

ситуаціям на них. Ці завдання є похідними від основної мети, яка полягає у захисті критичної інфраструктури.

Важливість належного нормативно-правового регулювання та розробки нормативно-технічної бази у цій сфері може бути пояснена через перспективу Ю. В. Желіховської, яка стверджує, що захист є реакцією на порушення, ведучи до відновлення суб'єктивного права [12, с. 20]. З метою реалізації державної політики у сфері захисту критичної інфраструктури, ч. 2 статті 13 Закону України «Про критичну інфраструктуру» передбачає функціонування секторальних та функціональних органів, відповідальних за захист критичної інфраструктури.

Особлива актуальність питань захисту критичної інфраструктури виникла після масштабних ракетних атак, які виконала російська федерація на території України восени 2022 року. У відповідь на це, було прийнято Закон України «Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України» від 18.10.2022 р. [29]. Закон вніс зміни до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» наділяючи Державну службу спеціального зв'язку та захисту інформації України повноваженнями уповноваженого органу у сфері захисту критичної інфраструктури України, що діятимуть під час правового режиму воєнного стану та протягом 12 місяців після його завершення [30].

Згідно з Законом України «Про критичну інфраструктуру» формування та реалізація державної політики у сфері захисту критичної інфраструктури, а також координація діяльності суб'єктів національної системи захисту віднесено до компетенції Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку) [35]. Стаття 14 цього ж Закону окреслює структуру національної системи захисту, включаючи в невичерпний перелік суб'єктів, які відіграють ключові ролі в цьому процесі: Кабінет Міністрів України, Раду національної безпеки і оборони України, Центральну виборчу комісію, Національний банк, різні національні комісії з регулювання

у сферах фінансів, зв’язку, енергетики та комунальних послуг, а також інші центральні органи виконавчої влади [35].

Ці суб'єкти спільно з Держспецзв’язку утворюють мережу, що забезпечує захист критичної інфраструктури, від оперативного реагування до стратегічного планування. Крім того, Закон визначає роль Держспецзв’язку як уповноваженого органу, який відповідає за керування національною системою захисту, координацію дій міністерств та операторів інфраструктури, ведення реєстру об’єктів критичної інфраструктури, оцінку ризиків на національному рівні, створення баз даних загроз та вразливостей, а також формування стратегій національної безпеки та кібербезпеки.

Повноваження Держспецзв’язку, зокрема, посилені в умовах введеного воєнного стану, а також протягом 12 місяців після його припинення чи скасування, що забезпечує постійну готовність та адаптивність системи захисту критичної інфраструктури до поточних загроз та викликів.

Узагальнюючи викладене вище, можна зазначити, що урядом України були вжиті суттєві заходи з метою оптимізації системи захисту критичної інфраструктури. По-перше, було вдосконалено нормативно-правову базу щодо захисту критичних об’єктів, забезпечуючи таким чином підвищення їхньої безпеки. По-друге, повноваження щодо координації діяльності національної системи захисту було делеговано спеціалізованому державному органу. Також, було адаптовано чинні національні законодавчі норми до стандартів Європейського Союзу у цій сфері. Нарешті, на законодавчому рівні було визначено відповідні сектори та здійснено категоризацію об'єктів критичної інфраструктури, що сприяло підвищенню ефективності заходів захисту.

1.3. Світовий досвід забезпечення безпеки та стійкості критичної інфраструктури

Аналіз динаміки розвитку систем реагування на кризові ситуації, згідно з даними попереднього розділу, підкреслює значення безпеки та стійкості

функціонування критичної інфраструктури як інтегральних компонентів національної системи стійкості. В аналітичній доповіді Національного інституту стратегічних досліджень (НІСД) підкреслюється, що безпека та стійкість критичної інфраструктури (КІ) становлять основу для формування загальної національної стійкості [26].

З точки зору системного аналізу, безпека та стійкість КІ зосереджують увагу на організаційно-функціональній структурі відповідної сфери управління, яка переважно існує на фізичному рівні і забезпечує координацію, обмін ресурсами та інформацією. Відповідно, національна система стійкості охоплює більш широкий спектр аспектів функціонування, включаючи якісні характеристики елементів системи, такі як ефективність управлінських функцій, стабільність соціально-економічного розвитку, психологічну стійкість особистості, рівень освіти та охорони здоров'я. Таким чином, система безпеки та стійкості КІ є складовою частиною ширшої системи національної стійкості, а результати її функціонування використовуються у цілісній системі.

В різних країнах можна спостерігати унікальні національні підходи до розвитку системи безпеки та стійкості КІ, обумовлені специфікою владних структур та моделей управління. Сучасні тенденції свідчать про еволюцію цієї системи від простого забезпечення захисту до зміцнення стійкості функціонування, що гарантує безперебійне надання життєво важливих функцій (ЖВФ) навіть у кризових умовах.

Для детальнішого розуміння мети та завдань забезпечення стійкості КІ та ЖВФ слід звернути увагу на позитивний світовий досвід, зокрема підходи, реалізовані у США. На нашу думку, адаптація міжнародного досвіду може сприяти узгодженню методологічних підходів, спрощенню використання термінології та формалізації процесу управлінської діяльності в області планування та реагування на потреби забезпечення стійкості.

Незважаючи на наявність унікальних інституційних систем і організаційних структур у різних країнах для формування та реалізації державної політики в сфері безпеки та стійкості критичної інфраструктури

(КІ), існують деякі універсальні аспекти. Ключовим є розподіл відповідальностей та повноважень між державними інституціями. У кожній країні існує специфічний державний орган, що займається формуванням політики захисту КІ, який зазвичай є частиною міністерства або спеціально створеним підрозділом у структурі уряду. Цей орган, уповноважений урядом, відповідає за розробку стратегічних документів та забезпечення єдності методологічних підходів до захисту КІ на всіх рівнях управління: національному, секторальному, місцевому та об'єктовому.

Секторальні та функціональні органи влади, які також беруть участь у процесі, враховують галузеву специфіку. Вони займаються деталізацією принципів регулювання безпеки та стійкості критичної інфраструктури на рівні окремих секторів. Ці органи, зазвичай у формі міністерств, незалежних департаментів чи агентств, відповідають за забезпечення захисту КІ у своїх секторах, а також за стійкість функціонування відповідних ланцюгів постачання.

Органи місцевої влади та самоврядування, в свою чергу, адаптують загальні підходи до місцевих умов, враховуючи специфіку територій у питаннях забезпечення безпеки КІ. Вони є відповідальними за стійкість критичної інфраструктури місцевого рівня та за загальну стійкість життєдіяльності місцевих громад в рамках чинних систем реагування та національного законодавства. Така структура забезпечує комплексний підхід до питань захисту та стійкості КІ, від специфічних секторальних завдань до загальнонаціональної стратегії.

З методологічної точки зору, завдання забезпечення стійкості функціонування критичної інфраструктури та стійкості надання послуги або функції розглядаються як конгруентні. Це означає, що принципи планування заходів забезпечення стійкості окремих життєво важливих функцій визначення відповідального суб'єкта планування та координації дій залучених учасників, однакові для обох аспектів стійкості.

Основна відмінність полягає у сферах планування та управління, що включає розширене охоплення учасників, залучених до реагування. Наприклад, для забезпечення стійкості надання послуги, що є критичною для функціонування суспільства і держави, необхідно залучати значно ширше коло учасників порівняно з задачами забезпечення стійкості самої КІ. При плануванні стійкості надання послуги можливе повне заміщення втраченої стандартної КІ, відповідальність за стійкість якої несе окремий оператор КІ. Таким чином, завдання забезпечення стійкості ЖВФ не може бути виключно покладене на оператора КІ, оскільки його фокус зосереджений на збереженні своїх функцій (як власника або оперативного менеджера інфраструктурних об’єктів).

Згідно з загальноприйнятим підходом у всіх країнах, завдання забезпечення національної стійкості вимагає участі всіх суб'єктів, які беруть участь у функціонуванні окремих сфер управління. Наприклад, зусилля всієї нації необхідні для забезпечення національної стійкості, тоді як зусилля всіх членів територіальної громади спрямовані на забезпечення стійкості цієї громади. Різні учасники, відповідно до встановленої моделі організації, виконують різні ролі та мають визначені законодавством повноваження та відповідальності.

Слід чітко розмежовувати залучених суб'єктів реагування на тих, хто володіє владними повноваженнями відповідної сфери управління (уряд може визначити для них завдання щодо планування стійкості), та інших учасників, які можуть бути залучені до виконання конкретних завдань забезпечення стійкості (добровільно або на контрактній основі).

Термін «суб’єкт» застосовується до учасників, які мають законодавчо визначені завдання та повноваження, і уповноважені (можуть бути) забезпечувати стійкість надання окремої ЖВФ у відповідній сфері або відповідальні за функціонування визначеної сфери управління. Всі інші учасники, зацікавлені в наданні такої ЖВФ або впливаючі на процес її надання, вважаються «стейкхолдерами». І саме визначений «суб’єкт»

відповідає за планування стійкості окремої ЖВФ або сфери управління та залучення до цього процесу всіх стейкхолдерів.

Відповідальність за розробку планів дій, рекомендацій та вимог щодо забезпечення стійкості функціонування критичної інфраструктури (КІ) та життєво важливих функцій (ЖВФ) покладено на інституції, які мають необхідні повноваження та інструментарій для залучення всіх стейкхолдерів, які діють у відповідних сферах планування.

Згідно із законодавчими положеннями Закону України «Про критичну інфраструктуру», можна виокремити суб'єктів планування стійкості на різних рівнях державного управління:

- Оператор критичної інфраструктури виступає як суб'єкт планування стійкості функціонування об'єктів КІ;
- На загальнодержавному рівні, орган влади, що відповідає за формування політики у певному секторі КІ, визначається як суб'єкт планування стійкості надання послуг;
- На місцевому рівні, орган влади, визначений за життєдіяльність місцевої громади, відповідає за планування стійкості.

Плани стійкості надання ЖВФ слід розглядати як формальні рамкові угоди між усіма залученими сторонами, які визначають та координують дії, спрямовані на забезпечення безперервності надання функцій або послуг кінцевим споживачам в певній сфері управління.

Значна увага в сучасній глобальній практиці приділяється ідентифікації загроз та оцінці ризиків, з методологіями яких ознайомлені у міжнародних стандартах. Ці методології дозволяють аналізувати потенційні прямі та непрямі наслідки впливу загроз на функціонування системи [9].

Методологічні підходи до оцінювання ризиків зараз активно розвиваються і варіюються від країни до країни, що свідчить про відсутність єдиного універсального методу оцінки. Різноманітність методів оцінювання ризиків порушення функціонування КІ є предметом численних досліджень та аналітичних оглядів [82].

Особливо важливою є розробка та застосування THIRA у США, інструменту, який використовується для оцінки ризиків у надзвичайних ситуаціях, а також у контексті CISA для планування заходів забезпечення стійкості КІ. Цей інструмент дозволяє оцінити вплив загроз та небезпек на критичні параметри функціонування сектору чи галузі [81; 83].

У Стратегічній національній оцінці ризику (SNRA) оцінювання наслідків впливу подій здійснюється за допомогою аналізу шести категорій: втрата життя, травми та хвороби, прямі економічні витрати, переміщення населення, психологічний стрес та вплив на навколишнє середовище. В контексті Національного індексу ризику (The National Risk Index, NRI), який оцінює природні небезпеки для місцевих громад, використовуються три критерії: оцінка економічних втрат, вразливість населення та вплив на стійкість громад.

Міністерство енергетики США звертає увагу суб'єктів, які займаються оцінкою ризиків енергозабезпечення на місцевому рівні, враховувати три сценарії, які можуть суттєво вплинути на життєдіяльність громад (Tier 1–3). Критичність впливу сценарію оцінюється з урахуванням спроможності залучених суб'єктів виконати їхні завдання, а не лише на вплив на життєдіяльність громади.

У Великій Британії, на відміну від США, Національний реєстр ризиків (NRR) охоплює загрози як національного, так і природного або зловмисного характеру. Перелік цих загроз формується на основі науково-експертного аналізу, після чого визначається найбільш імовірний гірший сценарій. Наслідки визначеного ризикованого сценарію оцінюються за восьмома параметрами: економічні втрати, смертність, евакуація населення, суспільне сприйняття, екологічні збитки, вплив на основні послуги, електрозабезпечення та міжнародні відносини [93].

Досвід інших країн у сфері планування стійкості критичної інфраструктури та надання життєво важливих функцій, що необхідні для підтримання життєдіяльності громад, вказує на наявність значних викликів та

проблем, які постають перед суб'єктами планування. Науковці Національного інституту стратегічних досліджень визначають комплекс законодавчих та організаційних перешкод, які ускладнюють забезпечення стійкості на місцевому рівні [27]. Зокрема, заходи із забезпечення стійкості регіонів та територіальних громад в Україні характеризуються як фрагментарні та неупорядковані, що свідчить про відсутність у державі єдиного розуміння механізму забезпечення національної стійкості.

Експерти Національного інституту стратегічних досліджень акцентують увагу на важливості розробки універсального координаційного механізму, який охоплює весь процес забезпечення національної стійкості, включно з аналізом ризиків, ідентифікацією вразливостей, розробкою планів реагування на кризу та відновлення після неї. Проблема взаємодії різних систем реагування на кризові ситуації заслуговує особливої уваги, оскільки існуючі формати міжвідомчої взаємодії часто орієнтовані лише на певні види загроз, такі як терористичні чи воєнні загрози, що не відповідає потребам комплексного реагування на різноманітні надзвичайні ситуації.

Проблематика кризового реагування була досліджена в монографії фахівців НІСД, присвяченій питанням розвитку системи захисту критичної інфраструктури, де було визначено необхідність створення міжвідомчого кризового центру при секторальному органі державної влади, зокрема в енергетичному секторі [63]. Згідно з рішенням Кабінету Міністрів України, такий Антикризовий енергетичний штаб було утворено у 2020 році [43], який з часу широкомасштабної збройної агресії РФ проти України забезпечує координаційну функцію, фактично вирішуючи проблеми, що виникають під час реагування на порушення функціонування критичної енергетичної інфраструктури [48].

У світлі масштабності викликів стійкості надання функції енергозабезпечення під час війни, антикризові штаби також були створені на рівні місцевих органів влади, при обласних державних адміністраціях та

органах місцевого самоврядування, забезпечуючи ефективне управління та координацію відповіді на місцевому рівні.

Досвід енергетичної галузі у створенні механізмів координації діяльності для реагування на кризові ситуації було розширено на інші важливі аспекти підтримання нормальних умов життєдіяльності громад. У 2023 році Кабінет Міністрів України ініціював створення загальнодержавного Координаційного штабу оперативного реагування. Цей штаб має на меті сприяти координації діяльності центральних і місцевих органів виконавчої влади, а також інших державних структур, органів місцевого самоврядування та суб'єктів господарювання у питаннях оперативного реагування та створення умов для забезпечення нормального життя населення під час перебоїв у постачанні електричної енергії [45]. Місцевим органам виконавчої влади також було доручено створити аналогічні штаби на місцевому рівні.

Прогрес у створенні таких механізмів координації, безсумнівно, є позитивним, однак важливо також звертати увагу на необхідність узгодження пріоритетів стійкості критичної інфраструктури та надання життєво важливих функцій з більш широким спектром завдань стратегічного планування розвитку громад та забезпечення національної безпеки.

Завдання, пов'язані із координацією, обміном інформацією та взаємодією різних суб'єктів у кризовій ситуації, є складними і вимагають значних ресурсів не тільки для реагування на кризи, але й для запобігання та відновлення після криз. Ці заходи є капіталоємними та потребують планування та інвестицій на довгострокову перспективу. Також важливо заздалегідь визначити необхідні рівні безпеки критичної інфраструктури та процедури для кризового реагування.

Планування стійкості повинно бути інтегроване з соціально-економічним розвитком громад, забезпечуючи участь усіх стейкхолдерів у процесі планування та виконання підготовлених планів [57]. Водночас, ініціативи з забезпечення стійкості громад і функціонування критичної інфраструктури мають бути узгоджені з більш широкими задачами

управління, наприклад, у контексті енергетичної інфраструктури, плани стійкості енергозабезпечення повинні стати частиною загального плану енергетичної стійкості України.

Висновки до розділу 1

1. Розгляд історичного розвитку об'єктів критичної інфраструктури свідчить про їх незаперечну роль у стабільності та безпеці держави на всіх етапах цивілізаційного розвитку. Визначення та систематизація таких об'єктів здійснювалася з давніх часів, коли ключовими об'єктами вважалися транспортні мережі та системи водопостачання, і продовжується у сучасних умовах, коли до переліку включені технологічні та інформаційні системи.

Сучасні виклики, зокрема гібридні війни та кібератаки, змушують розширювати поняття критичної інфраструктури та впроваджувати комплексні стратегії її захисту. Важливість таких систем відзначається не лише у фізичному захисті об'єктів від традиційних загроз, але й у забезпеченні кібербезпеки і резилієнтності перед обличчям інформаційних та технологічних викликів. Це підкреслюється різноманітними національними та міжнародними ініціативами, що відображають зростаючу глобалізацію і взаємозалежність держав у питаннях критичної інфраструктури.

Важливою є роль національних і міжнародних норм та законодавства, які формують підходи до ідентифікації, захисту і управління критично важливими інфраструктурними об'єктами, що сприяє не тільки відновленню після інцидентів, але й прогнозуванню та запобіганню майбутніх загроз. Підхід, що був розроблений і систематизований на основі досвіду, що накопичувався століттями, сьогодні є ключовим для забезпечення стійкості державних систем у боротьбі з мінливими викликами сучасності.

2. Нормативно-правове регулювання захисту критичної інфраструктури в Україні в умовах воєнного стану постійно вдосконалюється через запровадження нових законів та постанов. Створення ефективної системи

захисту стало пріоритетом для України, особливо з огляду на поточні безпекові виклики та збройну агресію. На основі Концепції створення державної системи було розроблено законодавчі ініціативи, що включають детальні методики категоризації об’єктів і визначення заходів їхнього захисту. Незважаючи на відсутність деяких норм у законопроектах, активно формується правова база, що забезпечує комплексний підхід до захисту критичної інфраструктури від різноманітних загроз.

3. Світовий досвід у забезпеченні безпеки та стійкості критичної інфраструктури вказує на важливість комплексного підходу, що включає організаційно-функціональну структуру управління, розподіл відповідальностей та ефективну координацію ресурсів і інформації. Різні країни реалізують унікальні підходи з огляду на місцеві умови та специфіку управління, але основні напрями включають зміцнення стійкості функціонування через планування та реагування на кризи. Співпраця між секторальними органами влади та місцевим самоврядуванням дозволяє ефективно адаптувати національні стратегії до місцевих умов, гарантуючи стійкість критичної інфраструктури на всіх рівнях. Важливим є також використання позитивного міжнародного досвіду для вдосконалення національних систем, особливо у сферах планування та координації дій.

РОЗДІЛ 2
АНАЛІЗ ОСОБЛИВОСТЕЙ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІД ЧАС ДІЇ ВОЄННОГО СТАНУ В УКРАЇНІ

2.1. Аналіз загроз та оцінка ризиків для об'єктів критичної інфраструктури

Присутність об'єктів критичної інфраструктури в кожній державі підкреслює необхідність забезпечення їхньої захищеності, безпеки та витривалості у відповідь на численні загрози та ризики, що набувають міжнародного характеру. Ці об'єкти відіграють фундаментальну роль у забезпеченні ключових функцій і послуг, які є критично важливими для стабільності та розвитку населення і держави [16]. У контексті глобального зростання екстремізму, тероризму та злочинності, значимість цих об'єктів лише посилюється.

Основною проблемою для стійкості критичної інфраструктури є високий рівень зношеності основних фондів на промислових об'єктах, середній показник якого становить 60,3%. Це створює серйозні загрози безпеки, оскільки збільшує ризик техногенних аварій, особливо на територіях, що використовують значні обсяги небезпечних хімічних речовин. Подібні аварії можуть призвести до катастрофічних наслідків, що впливають на цілі держави або регіони.

Проблематика житлово-комунального сектора в Україні загострюється через застарілі та аварійні водопровідні та теплові мережі. За оцінками, близько 34% водопровідних систем і понад 18% тепломереж зазнають зносу, що спричиняє істотні втрати ресурсів під час транспортування, що, у свою чергу, призводить до підвищення тарифів і соціальної напруги [без змін]. Це створює критичні умови для національної безпеки країни, оскільки збої в роботі критичної інфраструктури мають потенційні ризики. Наприклад,

перехоплення контролю над енергетичними об'єктами, як сталося в Криму, може не впливати на функціональність, але змінює права власності. Кримінальні дії, такі як продаж обладнання як металобрухт на окупованих територіях Донбасу, також підкреслюють цю проблему.

Руйнування інфраструктурних об'єктів цілеспрямовано може спричинити значні економічні витрати на їх відновлення та створювати перешкоди для забезпечення ресурсів. Припинення реконструкції енергетичної інфраструктури може викликати соціально-політичне невдоволення, як це сталося при використанні транспортної інфраструктури для провокацій, наприклад, під час трагедії з рейсом MH17 або блокування транзиту через державні кордони [52, с. 62-76].

Втручання у роботу не лише енергетичної, але і інформаційно-комунікаційної та комунальної інфраструктури підкреслює їхню вразливість перед зовнішніми та внутрішніми загрозами, що вимагає комплексного підходу до їх захисту і підвищення стійкості.

Наслідком природних загроз, таких як снігопади, ожеледиця, буревії, зливи, морози, спека, урагани, шквали, та гідрологічні явища, включаючи повені, селі, паводки, підтоплення та цунамі, є серйозні виклики для критичної інфраструктури. Відзначається зростання частоти цих загроз в Україні, особливо гідрологічні загрози, що є найбільш руйнівними [13].

Значимість ідентифікації, оцінки ризиків та прогнозування катастроф, які можуть пошкодити критичну інфраструктуру, посилюється. Захист суспільних інтересів від потенційних загроз національній безпеці вимагає цих дій. О.С. Бодрук визначає загрозу як реальну, але не неминучу можливість завдання шкоди, яка може мати матеріальні, фізичні чи моральні (духовні) наслідки для індивіда, суспільства чи держави [24, с. 8]. Стратегічне планування та профілактичні заходи є вирішальними для зменшення можливих втрат від цих загроз.

Концептуалізація терміну «загроза» у контексті національної безпеки виправдана кількома ключовими аспектами. По-перше, актуальність

диверсифікаційного підходу у вивченні категорій національної безпеки спонукає до глибокого аналізу і систематизації цього поняття. По-друге, необхідність виділити термін «загроза» через його недостатню розробку та важкість відрізнення від суміжних понять, таких як «небезпека», «виклик», «ризик», «фактор». Третє, відсутність цілісного підходу до розробки категорійно-понятійного апарату в цій галузі, де категорійний ланцюг «моніторинг - загроза - небезпека - управління - система національної безпеки - національна безпека» має ключове значення [17, с. 266]. Четвертий аспект полягає у можливості розробки на базі теоретичних висновків ефективної системи моніторингу та управління загрозами.

У контексті загроз безпеці критичної інфраструктури можна виділити дві основні категорії: природні та антропогенні. Природні загрози включають такі явища як повені, екстремальні погодні умови, лісові пожежі, землетруси, а також епідемії та пандемії. Антропогенні загрози поділяються на ненавмисні, такі як промислові аварії, радіологічні чи ядерні катастрофи та аварії на транспорті, та на умисні дії, що включають кібератаки, терористичні акти та втрату елементів критично важливої інфраструктури. Кожна з цих загроз потребує особливої уваги та специфічних методів управління ризиками для мінімізації потенційних втрат та забезпечення стабільності критичних систем.

Об'єкти, що входять до складу критичної інфраструктури, є фундаментальними для забезпечення стабільності економічних та соціальних процесів у світовому масштабі. Протягом останніх двадцяти років до переліку найбільш значущих сегментів критичної інфраструктури увійшли такі галузі, як електроенергетика, транспорт, водопостачання, харчова промисловість, сільське господарство та ключові виробничі комплекси. Новітній розвиток додав до цього списку інформаційні та телекомунікаційні технології, медіа, фінансові служби, а також сектори, що стосуються екології.

Національні уряди формують системи критичної інфраструктури, враховуючи внутрішні політичні директиви, і при цьому європейські

стандарти вносять свої корективи. Але право визначити критично важливі об'єкти залишається за державами. Зазвичай до таких об'єктів належать енергетичні установки, системи постачання енергії, а також засоби виробництва, транспортування та зберігання небезпечних матеріалів, транспортні та інформаційно-комунікаційні мережі.

Загрози безпеці цих об'єктів класифікуються на фізичні та цифрові (кібернетичні). Фізичні загрози часто асоціюються з інфраструктурою, такою як трубопроводи, електропідстанції, складські приміщення та системи комунікацій, а також з промисловими об'єктами. Цифрові загрози включають ризики для систем моніторингу, баз даних, програмного забезпечення та автоматизованих систем виробництва.

Кожен сектор критичної інфраструктури має свої специфічні вразливості. Наприклад, енергетичний сектор особливо чутливий через складність своїх генеруючих та розподільчих систем. В галузі з небезпечними речовинами ключові ризики асоціюються з логістикою та зберіганням цих матеріалів. Транспортні вузли, такі як аеропорти, мости та тунелі, є основними точками вразливості в транспортному секторі.

Забезпечення безпеки критичної інфраструктури в сучасних умовах вимагає посиленої уваги до загроз, які вона зазнає. Серед ключових проблем

Науковий дискурс акцентує занепокоєння, пов'язане з недостатністю кваліфікованих фахівців у секторі безпеки та оборони, зокрема для реагування на кіберзагрози, такі як кібершпигунство, кібертероризм і кіберзлочинність. Ці загрози ставлять під ризик стабільність функціонування критичної інфраструктури, порушуючи її роботу та створюючи додаткові загрози для державної безпеки.

Значущість звертання уваги на затримки та неефективність державних органів у реагуванні на інциденти, пов’язані з критичною інфраструктурою, не може бути переоцінена. Часто зустрічається неналежне та затягнуте відновлення після інцидентів, що може значно посилити негативний вплив загроз на національну безпеку.

У цьому контексті, систематичний підхід до посилення захисту критичної інфраструктури виступає як ключовий компонент стратегії національної безпеки, вимагаючи впровадження технічних, організаційних та управлінських інновацій на всіх рівнях управління. Сучасні умови акцентують на критичній необхідності охорони об'єктів критичної інфраструктури. Забезпечення їх безпеки, що включає ідентифікацію, аналіз ризиків і розробку ефективних управлінських механізмів, є пріоритетним завданням держави.

З часом може виникати потреба у перекласифікації деяких об'єктів як критично важливих у відповідь на нові ризики та складнощі існуючих загроз. Часто акції проти критичної інфраструктури залишаються без винуватців, особливо у випадку високотехнологічних кібератак, де визначення винуватців може бути вкрай складним завданням.

Обставини, що виникають у сфері критичної інфраструктури, вимагають безперервної уваги з боку державних органів до ідентифікації та мінімізації ризиків. Імперативом стає розробка та вдосконалення систем, котрі вбудовують новітні технології та методології для локалізації та нейтралізації потенційних загроз, що сприяє забезпеченню стійкості та безпеки цих життєво важливих об'єктів.

За міжнародним стандартом ISO 31000:2018 ризик описується як ефект невизначеності на досягнення цілей, з потенційними позитивними чи негативними наслідками, які реалізуються через потенційні події, їх впливи та ймовірність виникнення. Специфічні ризики для критичної інфраструктури включають загрози безпеці населення, майна, навколишнього середовища, інформаційної безпеки та соціальних відносин [67].

Управління цими ризиками потребує інтегрованого підходу, що охоплює:

1. Розробку нормативно-правових актів, що спрямовані на визначення та регулювання ризиків, з метою їх систематичного управління.

2. Встановлення організаційних структур, відповідальних за безпеку критичної інфраструктури, та забезпечення їх взаємодії для досягнення цілей безпеки.
3. Застосування технічних та програмних рішень для створення умов, які знижують ризики або амортизують негативний вплив.
4. Формування фінансових резервів для забезпечення адекватного фінансування ініціатив у сфері управління ризиками.

Наукові дослідження сприяють розробці принципів, методів та інструментів управління ризиками, забезпечуючи їх адекватність та ефективність у відповідь на сучасні виклики. Військово-оборонні заходи, інформаційні стратегії та освітні програми допомагають захистити критичну інфраструктуру від активностей, спрямованих на її ушкодження, тоді як дипломатичні ініціативи важливі для встановлення міжнародних стандартів та мирного вирішення конфліктів.

Окреслені механізми є критичними для створення міцної основи захисту, яка вберігає від існуючих та емерджентних загроз, тим самим підтримуючи стабільність і безпеку критичної інфраструктури на різних рівнях. Однак слід визнати, що дане дослідження не може повністю охопити всі аспекти механізмів управління ризиками для об'єктів критичної інфраструктуриОсоблива увага в ньому приділяється ключовим напрямкам діяльності публічних органів в цій сфері.

Підходи до ОКІ аналізуються через формування правового поля, яке регулює проблематику, пов'язану з цими об'єктами. Термін «критична інфраструктура» був вперше введений в офіційний лексикон в Україні в 2005 році, у зв'язку з парламентськими слуханнями, які стосувалися розвитку інформаційного суспільства. Рекомендовано було розробити заходи для ідентифікації та захисту критичних інформаційних інфраструктур [29]. Стратегія національної безпеки, затверджена у 2007 році указом Президента №105, розширила обсяг захисту критичної інфраструктури, з акцентом на

паливно-енергетичний комплекс та загрози еколого-техногенного характеру, а також підкреслила значення інформаційної безпеки [51].

Оновлена Стратегія національної безпеки України, прийнята в 2020 році за указом Президента №392, акцентує на зміцненні стійкості критичної інфраструктури не тільки шляхом реагування на фізичні та кібернетичні загрози, але й через стратегічне планування, що враховує можливість тривалих конфліктів і часткової окупації території [38]. Роль державно-приватного партнерства в цьому контексті набуває особливого значення, оскільки воно допомагає оптимізувати розподіл відповідальності між зацікавленими сторонами [38].

Стратегічні напрями, такі як стратегії енергетичної, інформаційної та кібербезпеки, мають стати вихідним пунктом для інших стратегічних документів, що визначають подальші дії в рамках забезпечення державної безпеки. Стратегія, затверджена у 2022 році, позиціонує об'єкти критичної інфраструктури як ключовий стовп національної безпеки, поруч із державним суверенітетом, конституційним ладом і територіальною цілісністю України, підкреслюючи їхнє стратегічне значення і високий рівень поточних загроз [39].

Необхідність поліпшення контррозвідувальних дій та засобів протидії агресивним спробам впливу на критичну інфраструктуру є критично важливою [39]. У листопаді 2021 року був прийнятий Закон України «Про критичну інфраструктуру», що вносить розмежування між ненавмисними і умисними загрозами, окреслюючи пов'язані з ними ризики у кризових ситуаціях [35]. Цей закон вводить основоположні принципи управління ризиками на об'єктах великої критичності і сприяє координації відповідальних структур, особливо тих, що належать до сфери діяльності Національного банку України [28].

Також, законодавство акцентує на значенні страхування ризиків, встановлюючи мінімальні стандарти відповідальності для страхування ризиків, що пов'язані з об'єктами критичної інфраструктури, особливо у

фінансовій сфері. При цьому, перелік об'єктів стратегічного значення затверджується Кабінетом Міністрів України, а в умовах воєнного стану ключові функції переходять до Державної служби спеціального зв'язку та захисту інформації [35].

Додатково, закон підкреслює важливість наукових досліджень для аналізу впливу нових технологій на загрози та ризики критичної інфраструктури, підтримуючи розробку ефективних стратегій управління цими ризиками [35]. Важливо, що хоча визначення ризики критичної інфраструктури залишається невизначеним, закон встановлює рамки для їх управління та мінімізації впливу інцидентів безпеки, забезпечуючи стратегії для запобігання несанкціонованому втручанню [35].

У контексті ширшої управлінської практики, в Україні задіяно різні управлінські та виконавчі органи, включно з місцевим самоврядуванням і спеціалізованими адміністраціями. Однак, активність цих органів у питаннях превенції загроз критичній інфраструктурі часто обмежена, а профілактичні заходи реалізуються переважно через залучення іноземних інвестицій, що нагадує практики в інших країнах, як наприклад, в Ізраїлі.

В Ізраїлі Консультативний комітет при Міністерстві фінансів відіграє важливу роль у формулюванні державної політики стосовно іноземних інвестицій, оцінюючи їх вплив на національну безпеку. Цей комітет, до складу якого входять представники високого рівня з ключових міністерств, включно з обороною та національною безпекою, проводить комплексний аналіз інвестиційних ініціатив. Рекомендації комітету, маючи дорадчий статус, все ж мають значний вплив на регуляторні рішення [53].

В Україні пропонується створити подібні консультативні структури, які б аналізували загрози і ризики для критичної інфраструктури на всіх стадіях проекту, від інвестицій до впровадження, з метою підвищення їхньої стійкості та безпеки.

Розвиток технологій надає унікальні можливості для виявлення, запобігання і мінімізації загроз критичній інфраструктурі. Водночас,

цифровізація приносить нові виклики, адже співвідношення користі та проблем, які вона створює, часто є предметом гарячих дискусій. Поширення цифрових технологій збільшує уразливість важливих об'єктів перед кібератаками, що підкреслюється численними інцидентами. Наукове співтовариство активно обговорює ризики, пов'язані з так званою «кібер-зимою», з огляду на зростання кіберзагроз.

Один з відомих прикладів вразливості критичної інфраструктури – атака Stuxnet на іранські ядерні об'єкти. Цей вірус, який цілив системи керування Siemens, викликав серйозні збої в роботі центрифуг, тоді як системи моніторингу показували звичайні показники роботи [56].

У травні 2020 року за допомогою Shodan було виявлено понад 112,000 промислових систем управління з відкритими портами, що свідчить про зростаючі загрози в умовах пандемії та збільшення дистанційної роботи [56].

У розвинених країнах численні промислові системи контролю (ICS) використовують для моніторингу великого діапазону процесів, від простих побутових приладів до складних промислових установок. Ці системи оснащені заходами для підвищення безпеки, включаючи віртуальні буфери та складні мережі для управління трафіком через безпечні сервери, використовуючи протоколи як BACnet, DNP3, EtherNet/IP, IEC 60870-5-104, MELSEC-Q, Modbus, S7 Communication, що демонструє гнучкість та можливості цих систем [90].

Поширення «відкритих зон» в складних технічних системах значно збільшує ризик їхнього порушення та кібернетичних атак, створюючи безпосередню загрозу національній безпеці. У контексті глобального зростання впливу технологій, захист критичної інфраструктури від таких загроз набуває стратегічного значення. Технічні інновації, з одного боку, сприяють оптимізації управління та контролю, з іншого — збільшують вразливість систем до кібернетичних загроз. Катастрофічні наслідки таких атак ілюструє випадок з вірусом Stuxnet, який не тільки вивів з ладу ядерні

центрифуги в Ірані, але й маскував реальний стан систем, симулюючи нормальні показники роботи [56].

Виявлення значного числа підключених до Інтернету промислових систем управління через систему Shodan у 2020 році свідчить про критичну потребу у розробці комплексних заходів безпеки [56]. Сучасні промислові системи контролю (ICS) дозволяють моніторити стан від базових побутових пристроїв до складних промислових установок [90]. Заходи безпеки, такі як віддалений доступ та створення віртуальних буферних зон, допомагають мінімізувати ці вразливості.

Однак, із зростанням технологічних можливостей, збільшується також кількість потенційних «відкритих зон», які можуть стати цілями для кіберзлочинців. Підвищена залежність від технологій збільшує потенційні збитки від дій зловмисників, що потребує від державних структур розробки всеохоплюючої стратегії захисту критичної інфраструктури проти всіх можливих загроз.

2.2. Захищеність об'єктів критичної інфраструктури в сучасних умовах

У контексті забезпечення цивільної безпеки, реалізація заходів захисту об'єктів критичної інфраструктури (КІ) набула особливої актуальності в Україні після початку повномасштабного воєнного конфлікту з Російською Федерацією 24 лютого 2022 року. Трагічні події значно трансформували стратегічний підхід до національної системи захисту КІ, акцентуючи увагу на необхідності усунення існуючих вразливостей і прогалин у захисті.

З самого початку збройних дій, Україна зіткнулася з інтенсивними та організованими нападами на свою інфраструктуру, які охоплювали не тільки фізичні удари по елементах енергетичної, транспортної та комунікаційної систем, але й кібернетичні атаки, метою яких було дестабілізувати внутрішню стабільність та зруйнувати державні структури. Це підкреслило

актуальність розроблення та імплементації ефективних механізмів реагування на надзвичайні ситуації та відновлення після атак.

Перед війною значна увага приділялася модернізації і підвищенню резистентності критично важливих об'єктів, але ці заходи виявилися не однорідними і частково не систематичними, що можна пояснити обмеженими ресурсами та складнощами у координації між різними рівнями управління та приватним сектором.

З початком ескалації конфлікту було вжито низку дій для підвищення захисного потенціалу критичних об'єктів, включаючи впровадження строгіших стандартів безпеки та підвищення готовності до кіберзагроз. Важливим напрямком стала співпраця з міжнародними партнерами для обміну досвідом та ресурсами.

На даний момент Україна активно працює над розробкою системи захисту критичної інфраструктури на основі передових міжнародних практик та директив ЄС, таких як NIS 2 (EU 2022/2555) та RCE (EU 2022/2557). Співпраця з такими організаціями, як Американська агенція з кібербезпеки (CISA), зокрема, підписання меморандуму про співпрацю та проведення тренінгів, стала важливим кроком у цьому напрямку.

У рамках формування правової основи для захисту критичної інфраструктури в Україні активно розробляється необхідний нормативно-правовий арсенал. Вже створені секторальні каталоги об'єктів критичної інфраструктури (ОКІ), і в найближчому майбутньому передбачається прийняття урядового акта, що визначатиме процедуру ведення Реєстру критичної інфраструктури. Даний Реєстр міститиме відомості про ОКІ, включаючи реєстраційні номери, форми власності та основні види діяльності.

Відповідальність за класифікацію об'єктів та подання інформації до Реєстру покладається на секторальні органи управління та операторів ОКІ, які також відповідають за безпосередній захист критичної інфраструктури. Важливу роль у реагуванні на кризові ситуації, такі як ракетні удари,

диверсійні дії та кібератаки, відіграють ключові державні структури, зокрема Збройні сили України, Служба безпеки України та Держспецзв'язку.

Окрему роль у координації зусиль всіх учасників національної системи захисту відіграє уповноважений орган, який займається формулюванням та реалізацією державної політики у сфері захисту критичної інфраструктури, представляючи її інтереси у владних структурах.

Розробка законодавства для паспортизації ОКІ та аналізу національних загроз продовжується, що має на меті забезпечення комплексної та системної відповіді на можливі загрози [54].

Аналіз нормативно-правової бази України, що регламентує забезпечення безпеки та правовий режим функціонування критичної інфраструктури в умовах особливих обставин, зокрема під час воєнного стану, виявив, що ці аспекти врегульовані низкою законодавчих актів. До них відносяться такі закони, як «Про критичну інфраструктуру», «Про внесення змін до деяких законодавчих актів України щодо засад державної регіональної політики та політики відновлення регіонів і територій», «Про правовий режим воєнного стану», та інші, що стосуються різних аспектів державного та регіонального управління.

Зокрема, Закон України «Про критичну інфраструктуру» визначає безпеку критичної інфраструктури як стан захищеності, що гарантує її функціональність, безперервність діяльності, відновлюваність, цілісність та стійкість [35]. Цей закон встановлює основні принципи організації системи захисту критичної інфраструктури, що охоплюють: визначення державної політики у цій галузі; структуру управління системою; категоризацію критичності об'єктів; ведення реєстру критичної інфраструктури; процедури паспортизації об'єктів; суб'єкти системи захисту; режими функціонування; повноваження уповноваженого органу; ролі функціональних та секторальних органів, місцевих виконавчих органів, включаючи військово-цивільні адміністрації; завдання, права та обов'язки операторів; моніторинг безпеки; взаємодію систем у сфері національної безпеки; механізми державно-

приватного партнерства; парламентський контроль, громадський нагляд; відповідальність за порушення законодавства; та міжнародне співробітництво у сфері захисту критичної інфраструктури.

З введенням воєнного стану на території України спостерігаються значні зміни у законодавчому регулюванні сфери критичної інфраструктури, адаптовані до умов збройного конфлікту. В цей період було оновлено ряд нормативних документів, спрямованих на зміцнення захисту та підвищення стійкості систем життєзабезпечення країни. Серед важливих правових актів:

– Постанова Кабінету Міністрів України встановлює «Порядок формування переліку об'єктів критичної інформаційної інфраструктури» та регламентує процедури внесення даних до державного реєстру таких об'єктів, що забезпечують їх ідентифікацію та захист [6];

– Інша постанова КМУ затверджує «Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури», що включає перелік базових стандартів безпеки, необхідних для забезпечення їх надійної роботи [31];

– Розроблено порядок проведення моніторингу рівня безпеки цих об'єктів, встановлюючи вимоги до акта оцінки стану захищеності [33];

– Концепція створення державної системи захисту критичної інфраструктури, схвалена КМУ, оновлює стратегічний підхід до забезпечення безпеки важливих систем, об'єктів та ресурсів [42];

– Запроваджено процедури ідентифікації та обліку об'єктів підвищеної небезпеки, що включає початок формування відповідного державного електронного реєстру [5];

– Національний банк України встановив положення про організацію кіберзахисту в банківській системі, що визначає критичні об'єкти у фінансовому секторі [32];

– Утворення Державної служби захисту критичної інфраструктури стало значним кроком у формуванні центрального органу виконавчої влади, спрямованого на забезпечення національної стійкості [44];

– Введено рамки для проведення зовнішнього аудиту діяльності уповноваженого органу у сфері захисту критичної інфраструктури, зокрема через складення звітів Рахунковою палатою [7].

З оголошенням воєнного стану в Україні було внесено істотні корективи у законодавчу базу, яка стосується регуляції критичної інфраструктури, що сприяло її адаптації до нових вимог. Ці оновлення є критично важливими для забезпечення стійкості інфраструктури в умовах неперервної військової загрози.

Описані заходи являють собою вираз стратегії державної політики, орієнтованої на забезпечення захисту та оперативне реагування на потенційні загрози, які можуть призвести до ушкодження чи знищення об'єктів критичної інфраструктури. Ефективність цієї стратегії залежить від міжгалузевої координації та консолідації ресурсів. Згідно з чинним законодавством, ряд міністерств несе відповідальність за різні сектори критичної інфраструктури: від енергетики та інформаційних технологій до систем життєзабезпечення та цивільного захисту.

Під час воєнного стану мобілізація ресурсів для захисту критичної інфраструктури здійснюється за допомогою різноманітних органів виконавчої влади, таких як Національна поліція, Міністерство з надзвичайних ситуацій, Служба безпеки України, Національна гвардія, Збройні сили, а також спеціалізовані служби, зокрема Державна служба спеціального зв’язку та захисту інформації, та інші.

Ключові вимоги до захисту критичної інфраструктури включають контррозвідувальну, контртерористичну та контрдиверсійну безпеку, особливо у сферах, таких як енергетика, нафтогазова промисловість, харчова індустрія, ІТ і телекомунікації, системи життєзабезпечення, агропромисловий комплекс, транспорт і пошта, медична сфера, стратегічно важливі галузі національної економіки, а також банківський сектор. Найбільші загрози становлять кібератаки, терористичні акти та диверсії, що можуть призвести

до аварій та надзвичайних ситуацій регіонального, національного або глобального масштабу.

В умовах воєнного стану, який зараз спостерігається в Україні, особлива увага приділяється зміцненню контррозвідувальної, контртерористичної та контрдиверсійної безпеки критичної інфраструктури. Зокрема, це стосується секторів енергетики, включаючи ядерну енергетику, нафтогазової промисловості, харчового виробництва, ІТ та електронних комунікацій, систем життєзабезпечення, агропромислового комплексу, транспорту, пошти, зв'язку, медичної сфери, стратегічно важливих галузей національного господарства, а також банківської сфери. Ключовими загрозами для стабільності та безпеки цих секторів є кібератаки, терористичні акції та диверсії, військові дії, які можуть призвести до серйозних аварій на об'єктах підвищеної небезпеки та, відповідно, викликати надзвичайні ситуації локального, національного чи міжнародного масштабу.

Воєнні дії, здійснювані на території України, особливо торкнулися навіть таких важливих об'єктів, як Запорізька та Південноукраїнська атомні електростанції, створюючи значні ризики не тільки для національної, а й для глобальної безпеки.

Ракетні та артилерійські обстріли мали значний вплив на стан безпеки об'єктів критичної інфраструктури, особливо в енергетичному секторі, що спричинило пошкодження таких об'єктів, як гідроелектростанції Дніпровська, Кременчуцька, Київська, Каховська та ряд теплових електростанцій, включаючи Київську, Трипільську, Харківську, Старобешівську, Слов’янську, Миронівську, Луганську, Курахівську, Зуївську, Зміївську, Запорізьку, Вуглегірську.

Життєво важливі інфраструктурні об'єкти, зокрема електромережі, системи водопостачання, тепло- та газопроводи, телефонні лінії, постійно зазнають обстрілів, особливо в таких регіонах, як Запорізька, Херсонська та Миколаївська області, що охоплюють окуповані території, території, де ведуться активні бойові дії.

Внаслідок військових дій значно постраждали портові інфраструктури, важливі транспортні вузли, мости та переправи, а також промислові об'єкти, нафтогазові мережі, і інші ключові елементи критичної інфраструктури в різних регіонах країни. В умовах воєнних обставин, уряд України ініціював збільшення асигнувань з резервного фонду держбюджету на ремонт та відновлення пошкоджених об'єктів, постраждалих через воєнні дії та акти диверсії, що були спровоковані агресією з боку Російської Федерації. Відповідно до цієї політики, було прийнято низку законодавчих актів, включно з Постановами КМУ щодо регулювання державних закупівель у воєнний час і забезпечення фінансування критичної інфраструктури, а також розпорядження про фінансування місцевих комунальних підприємств. Міжнародне співтовариство також відіграє роль у цьому процесі, застосовуючи фінансові санкції для підтримки заходів.

Додатково, ведеться робота над вдосконаленням законодавчих ініціатив у сфері державної та регіональної політики з метою ефективнішого відновлення критичної інфраструктури. Важливими є законодавчі зміни, які спрямовані на прискорення ремонтних робіт і відновлення регіонів, серед яких закони щодо політики відновлення та регіональної безпеки. Обговорюються також нові норми законодавства щодо введення санкцій за порушення норм безпеки на об'єктах критичної інфраструктури, включаючи застосування дисциплінарних та кримінальних заходів.

Захист цих об'єктів стає основним аспектом забезпечення національної безпеки. Відповідь на виклики, пов'язані з фінансуванням і матеріальним забезпеченням постраждалих об'єктів, зокрема через правові ініціативи, дозволяє створювати умови для їх швидкого і ефективного відновлення.

2.3. Аналіз результативності ініційованих стратегій щодо зміцнення резилієнтності об’єктів критичної інфраструктури

Зміцнення резилієнтності об’єктів критичної інфраструктури є ключовим аспектом сучасних стратегій національної безпеки. В умовах зростаючих загроз,

таких як природні катастрофи, техногенні аварії та воєнні конфлікти, забезпечення стійкості цих об’єктів набуває особливого значення. Цей аналіз має на меті оцінити ефективність заходів, що були ініційовані для підвищення резилієнтності критичної інфраструктури, з огляду на їх здатність мінімізувати ризики та забезпечити неперервність функціонування в кризових умовах.

Резилієнтність інфраструктури визначається як здатність системи витримувати та адаптуватися до зовнішніх впливів, швидко відновлюватися після порушень, забезпечуючи при цьому безперебійність критично важливих функцій. Вивчення резилієнтності охоплює не тільки інженерні та технологічні аспекти, але й соціальні, економічні та управлінські стратегії.

Методологія оцінки ефективності заходів щодо зміцнення резилієнтності критичної інфраструктури обумовлюється використанням комплексу критеріїв, кожен з яких відображає важливий аспект стійкості об’єктів. Перший критерій, стійкість до початкових ударів, фокусується на здатності інфраструктури витримувати безпосередні впливи, такі як природні катастрофи або техногенні аварії, без значних пошкоджень. Цей критерій є визначальним для оцінювання міцності фізичних та технологічних аспектів об’єктів.

Другий критерій, швидкість відновлення, вимірює час, який необхідний інфраструктурі для відновлення до нормального або майже нормального рівня своєї роботи після зазнаної негативної події. Цей показник є критичним для оцінки ефективності планів реагування та відновлення, включаючи якість підготовки персоналу та наявність необхідних ресурсів.

Третій критерій, адаптивність, відноситься до здатності системи змінювати свою структуру та методи функціонування у відповідь на отриманий досвід і змінені умови. Адаптація може включати технологічне оновлення, модифікацію процедур чи впровадження нових підходів у управління безпекою.

Четвертий критерій, соціальна інтеграція, зосереджується на залученні місцевих спільнот та стейкхолдерів до процесів планування, реагування на кризи та відновлення після них. Включення громад у ці процеси не тільки

підвищує обізнаність і готовність до реагування на надзвичайні ситуації, але й сприяє створенню більш резилієнтної соціальної структури.

Ці критерії в сукупності дозволяють всебічно оцінити здатність критичної інфраструктури протистояти різноманітним викликам, швидко адаптуватися та відновлюватися після них, а також ефективно інтегрувати громадськість у процеси підвищення загальної безпеки.

Аналіз впроваджених стратегій щодо зміцнення резилієнтності об’єктів критичної інфраструктури включає оцінку ефективності заходів у кількох ключових аспектах. Одним з основних елементів є технічне укріплення, яке включає модернізацію фізичних конструкцій та систем захисту. Цей підхід має на меті підвищити стійкість об’єктів до фізичних загроз та ударів, зокрема покращення матеріалів та конструкцій, що забезпечують основу об’єктів, та оновлення систем безпеки, що включають засоби активного та пасивного захисту.

Другим важливим аспектом аналізу є розвиток систем кібербезпеки. Цей напрямок зосереджений на захисті інформаційних систем від зовнішніх кібератак. З огляду на збільшення кіберзагроз, особливо в контексті гібридних воєн, значна увага приділяється створенню та впровадженню розширених криптографічних заходів, розробці алгоритмів виявлення вторгнень та забезпеченню цілісності даних.

Третій компонент аналізу стосується навчання персоналу, зокрема розробки та впровадження програм підготовки, які зосереджені на підвищенні готовності персоналу реагувати на кризові ситуації. Ці програми охоплюють не тільки технічні аспекти обслуговування та ремонту, але й підготовку до дій у надзвичайних умовах, включаючи евакуацію, першу допомогу та взаємодію з екстреними службами.

Нарешті, міжнародна співпраця є невід’ємною частиною стратегій зміцнення інфраструктури, де обмін знаннями та технологіями з міжнародними партнерами відіграє ключову роль у розробці передових практик та інноваційних рішень. Ця співпраця включає не лише передачу

технологій, але й спільні дослідження, розвиток стандартів безпеки та розробку спільних проектів, які допомагають підвищити рівень захисту на глобальному рівні.

Такий комплексний підхід до аналізу впроваджених стратегій забезпечує глибоке розуміння ефективності вжитих заходів та сприяє формулюванню рекомендацій для подальшого зміцнення резилієнтності критичної інфраструктури.

Результати проведеного аналізу свідчать про те, що комплексне впровадження стратегій істотно сприяє підвищенню резилієнтності критично важливих інфраструктурних об’єктів. Зокрема, укріплення фізичних структур значно знижує їх вразливість перед лицем початкових ударів, таких як природні катастрофи чи військові атаки, тим самим запобігаючи значним пошкодженням та забезпечуючи стабільність функціонування об’єктів під час кризових ситуацій.

Також було встановлено, що добре розвинуті системи кіберзахисту ефективно мінімізують ризики пов’язані з втратою даних та зупинками в роботі критичних систем, що є особливо важливим в контексті зростаючих кіберзагроз. Завдяки застосуванню сучасних технологічних рішень та впровадженню надійних процедур кібербезпеки можливо значно знизити ймовірність успішних кібератак.

Однак дослідження також підкреслює необхідність постійного оновлення стратегічних планів, що має включати регулярну адаптацію до нових технологічних можливостей та змінених загрозових умов. Цей процес має передбачати не тільки технічне оновлення, але й перегляд управлінських підходів та політик.

Крім того, важливим аспектом є залучення місцевих спільнот у процеси прийняття рішень, що не тільки підвищує прозорість та відповідальність управління критичною інфраструктурою, але й сприяє формуванню спільноти, більш освіченої та здатної адекватно реагувати на потенційні загрози. Ця інтеграція стимулює створення більш міцних та ефективних

систем реагування на надзвичайні ситуації, підвищуючи загальну стійкість інфраструктури.

Отже ефективність стратегій зміцнення резилієнтності критичної інфраструктури є високою, однак потребує неперервної адаптації та інтеграції нових підходів та технологій. Необхідно зосередитися на створенні адаптивних систем управління, що включають різні рівні захисту та відновлення, та забезпечують готовність до викликів майбутнього.

Висновки до розділу 2

1. Аналіз загроз та ризиків, що впливають на критичну інфраструктуру, виявляє серйозні виклики, які ставлять під загрозу функціонування важливих систем у різних секторах. Зношеність обладнання на промислових об'єктах, високий рівень ризику техногенних аварій, особливо на територіях, що використовують небезпечні хімічні речовини, а також застарілі комунальні системи є основними проблемами, що загострюють загрози національній безпеці.

Потенційні ризики, такі як терористичні акти, кібератаки, природні катастрофи, та інші природні та антропогенні загрози, вимагають від урядів і міжнародних організацій впровадження комплексних стратегій для підвищення резилієнтності цих життєво важливих систем. Критична інфраструктура потребує постійного моніторингу, швидкого реагування на інциденти та ефективного управління ризиками, щоб забезпечити стабільність та безперервність їхньої роботи.

Також, забезпечення безпеки критичної інфраструктури вимагає інтеграції між різними урядовими відомствами, приватним сектором та громадськістю для створення ефективних механізмів захисту та відновлення після можливих інцидентів. Науковий підхід до оцінки ризиків та визначення загроз є ключовим для розробки та впровадження адекватних технологічних, організаційних та управлінських заходів, спрямованих на підвищення

стійкості критичної інфраструктури в умовах зростаючих викликів глобалізованого світу.

2. Сучасний стан захисту об’єктів критичної інфраструктури в Україні вимагає відповідного реагування та адаптації до умов повномасштабного воєнного конфлікту. Від початку воєнних дій об’єкти критичної інфраструктури стали мішенями для фізичних та кібернетичних атак, що вимагає підвищення їхньої захищеності. Значна увага в цей період приділяється модернізації інфраструктур та вдосконаленню нормативно-правової бази, включно з міжнародною співпрацею та застосуванням директив ЄС. Розробка і впровадження ефективних механізмів захисту і реагування на надзвичайні ситуації є ключовими для забезпечення функціональності, безперервності та відновлюваності критичної інфраструктури в умовах воєнного стану.

3. На основі проведеного аналізу результативності ініційованих стратегій щодо зміцнення резилієнтності об’єктів критичної інфраструктури можна зробити висновок, що ці заходи значно підвищують стійкість інфраструктури перед обличчям різноманітних загроз. Укріплення фізичних структур ефективно знижує вразливість до початкових ударів, а добре розвинута система кіберзахисту мінімізує ризики, пов’язані з втратою даних і зупинками важливих систем.

Однак, для підтримання високого рівня резилієнтності необхідно постійно оновлювати та адаптувати стратегічні плани з огляду на нові технологічні можливості та зміни в загрозовому середовищі. Крім технічних оновлень, критично важлива також регулярна адаптація управлінських практик та політик.

Важливим є також залучення місцевих спільнот до управління критичною інфраструктурою, що забезпечує не лише збільшення прозорості та відповідальності у прийнятті рішень, але й формує громаду, здатну ефективно реагувати на можливі кризи. Це підсилює загальну стійкість

системи та створює більш міцні механізми реагування на надзвичайні ситуації.

Завдяки комплексному підходу, що охоплює як технічні, так і соціальні аспекти зміцнення резилієнтності, можливо забезпечити високий рівень готовності критичної інфраструктури до майбутніх викликів, що є ключовим для забезпечення стабільності та безпеки на національному рівні.

РОЗДІЛ 3
ПРІОРИТЕТНІ НАПРЯМИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1. Інноваційні методи зміцнення надійності критично важливих інфраструктурних об'єктів в зарубіжних країнах та їх імплементація і Україні

У сучасному глобалізованому світі, де дедалі зростає залежність від складних технологічних систем, ключовим завданням для забезпечення національної безпеки та стабільності держав є зміцнення стійкості об'єктів критичної інфраструктури. Стійкість такої інфраструктури, що включає ключові сектори як енергетику, транспорт, комунікації, фінансові послуги та охорону здоров'я, відіграє вирішальну роль у забезпеченні функціонування національної економіки та підтримці життєво важливих соціальних процесів.

Зміцнення безпеки та стійкості критичних інфраструктур є стратегічним імперативом для державних органів влади в контексті політики Сполучених Штатів, спрямованої на охорону ключових активів. Ця політика передбачає розробку комплексних стратегій профілактики, стримування, мінімізації наслідків та протидії потенційним терористичним атакам або іншим загрозам, які можуть призвести до серйозних ушкоджень чи зловживань з боку критичної інфраструктури. Надзвичайно важливими є також заходи щодо підготовки до надзвичайних ситуацій, оперативного реагування та ефективного відновлення пошкоджених систем [86].

Безпека та стійкість критичних об’єктів інтегровані у ширший контекст політичних завдань, що сприяють сталому розвитку країни. Термін «стійкість» активно вживається у науковій літературі, хоча дефініції цього поняття різняться і знаходять застосування в багатьох дисциплінах, включаючи економіку, екологію та соціологію. В офіційних документах міжнародних організацій, таких як Європейська Комісія, розробляються

власні визначення стійкості, зазвичай наголошуючи на здатності системи швидко відновлюватися після кризових втручань до передбачуваного рівня функціонування [75].

К. Голлінґ визначає стійкість як міру витривалості системи, що дозволяє їй адаптуватися до змін, зберігаючи при цьому стабільність взаємовідносин між її складовими [73]. Й. Гаймс аналізує стійкість у контексті системної інженерії як здатність системи витримувати значні зовнішні впливи, забезпечуючи її відновлення в прийнятні терміни і з мінімальними витратами [71, с. 498–501].

Дослідження, проведені С. Нан, Дж. Сансавіні та іншими вченими, спрямовані на глибокий аналіз стійкості інженерних систем. Вони висвітлюють концепцію стійкості, розглядану як система систем, що базується на здатності систем ефективно протистояти внутрішнім та зовнішнім впливам, здатним раптово або поступово негативно впливати на їх структуру. Ключовим аспектом є можливість системи скорочувати тривалість та інтенсивність падіння продуктивності до рівнів, які можна вважати нормальними [78, с. 35–53].

С. Фолке у своїх наукових роботах, присвячених аналізу вразливості та стійкості соціально-екологічних систем, розглядає стійкість як концепцію, що може стимулювати лідерів та організації до критичного осмислення ключових аспектів переходу суспільства до стійких практик [70, с. 253–267].

Альянс стійкості, створений у Флоридському університеті та Інституті Байєра за участі К. Голлінґа, перетворився на міжнародну дослідницьку платформу, зосереджену на вивченні динаміки соціально-екологічних систем. Організація розглядає стійкість як здатність системи до адаптації та реорганізації, що забезпечує збереження її ідентичності у відповідь на зовнішні виклики та використання досвіду для подальшого відновлення [88].

Концепція «Robustness» описує здатність системи підтримувати свою функціональність попри коливання зовнішніх умов, не зазнаючи суттєвих втрат [50]. У контексті двоїстої природи стійкості виділяють статичну

стійкість, яка визначає базову здатність системи відновлюватися після збоїв до прийнятного рівня, та динамічну стійкість, що акцентує на швидкості та ефективності процесу відновлення. Таке розуміння сприяє кращій оцінці потенціалу інфраструктури до адаптації в умовах змінних обставин, включаючи технічні несправності та екологічні катастрофи, з одночасним забезпеченням швидкого відновлення при мінімальних затратах.

У сучасних розвинених державах концепція «стійкості» втілюється у ключові нормативні та стратегічні документи, які спрямовані на реалізацію державних політик у галузях загальнонаціональної безпеки, захисту життєво важливих об'єктів та сталого розвитку. Спочатку цей термін застосовувався переважно у контексті захисту критичних інфраструктур у рамках Європейської програми, але згодом у офіційних документах з'явилася розширена концепція стійкості, яка підкреслює неможливість забезпечення абсолютного захисту інфраструктур від усіх можливих загроз. Важливість захисту критично важливих об'єктів стала однією з ключових складових таких ініціатив [66].

З початку 2000-х років поняття стійкості активно поширюється в академічних дослідженнях і аналітичних оглядах у сфері публічної політики, продовжуючи традиції, закладені екологами ще у 1970-х роках. Цей науковий інтерес призвів до переосмислення підходів до захисту, з акцентом на більш глибокому розумінні стійкості в контексті дослідження критичних інфраструктур [70; 78].

В Сполучених Штатах Америки зокрема ця тенденція стала помітною в державних політиках. Директива Президента 2013 року визначає стійкість як здатність системи адаптуватися та відновлюватися після різноманітних збоїв, аварій, атак чи природних катастроф, наголошуючи на необхідності швидкого відновлення та протидії загрозам [84].

Документи Європейського Союзу також відображають цю концепцію, особливо у рамках Європейської програми захисту критичної інфраструктури, де з 2012 року стійкість виокремлюється як значущий

елемент, що демонструється в Звіті ЄС 2014 року про оцінку стійкості критичної інфраструктури [67; 85].

На Варшавському саміті НАТО 2016 року були встановлені сім основних вимог до стійкості, що охоплюють забезпечення енергетики, транспортних систем, комунікацій, водопостачання, урядових функцій, контролю за переміщенням людей та надання допомоги при стихійних лихах [68].

Європейський Союз у своїй стратегії «Сильніша Європа» акцентував на стійкості як ключовому пріоритеті, підкреслюючи її значення для демократичного розвитку, безпеки та процвітання, закладаючи основи для розвитку гнучкого суспільства, заснованого на демократії та довірі до інституцій.

Міжнародна стратегія Об'єднаних Націй визначає стійкість як здатність системи, громади або суспільства протистояти небезпекам, абсорбувати втручання та ефективно відновлюватися від їх наслідків, зберігаючи та відновлюючи основні структури та функції. Стійкість охоплює всі аспекти традиційного управління кризами, включаючи профілактику, пом'якшення наслідків, готовність до криз, реагування під час криз та, що найважливіше, відновлення після криз [94].

Стійкість можна поділити на три основні категорії: суспільну, організаційну та технологічну. В аспекті суспільної стійкості важливу роль відіграють державні установи, органи місцевого самоврядування, територіальні громади та індивідуальні учасники, з яких стійкість часто асоціюється з цивільним захистом. У контексті організаційної стійкості ключовими діячами є підприємства та організації, що сприяють важливим взаємодіям у межах критичної інфраструктури. Технологічна стійкість визначається діяльністю операторів критичних об'єктів та зацікавлених сторін, відповідальних за управління матеріальними, інформаційними та фінансовими ресурсами.

У скандинавських країнах концепція стійкості пройшла еволюцію від академічних дебатів до формального політичного документування. Між 2006 та 2010 роками Данське агентство з надзвичайних ситуацій розробило доповіді про національну вразливість, що фокусувалися на вразливості як на протилежності стійкості. В цих документах підкреслюється, що система вважається вразливою, коли не має достатніх засобів для планування, запобігання, реагування або відновлення після реалізації загроз [61; 62]. Національні профілі ризиків за 2013 та 2017 роки в Данії зосереджуються на стійкості, використовуючи стандартний цикл управління кризами, з особливим акцентом на етапи запобігання, готовності та реагування.

У Норвегії, після теракту в Осло у 2011 році, тема стійкості критичної інфраструктури (КІ) почала включатися в офіційні документи, хоча не у вираженій формі. Міністерство юстиції та громадської безпеки опублікувало звіт про громадську безпеку, який згадував КІ, але не описував стійкість як чітко визначену концепцію. Проте, у Королівському указі 2012 року вже зазначено, що відомства повинні аналізувати ризики, вразливість і стійкість своїх секторів, використовуючи національний аналіз ризиків від Норвезької дирекції цивільного захисту [65; 77].

В Великій Британії уряд активно працює над удосконаленням процесів планування та збільшенням інвестицій для прискорення реалізації проектів, спрямованих на поліпшення критичної інфраструктури (КІ). Національний план розвитку інфраструктури демонструє посилену увагу до стійкості та безпеки КІ, з акцентом на виявленні критичних об'єктів для оптимального розподілу ресурсів. Разом з регуляторними органами та промисловістю, уряд прагне забезпечити інвестиції, які беруть до уваги потреби в безпеці та стійкості [80].

В Австралії особлива увага приділяється питанню стійкості критичної інфраструктури в контексті Стратегії стійкості КІ, розробленої урядом країни у 2010 році (AGCIRS). Стратегія орієнтується на взаємозалежності між секторами та мережами КІ, підкреслюючи необхідність координованого

планування, гнучкості та швидкості відновлення після можливих перебоїв або катастроф. Важливість взаємодії між бізнесом і урядом виокремлюється як ключ до ефективного управління стійкістю КІ [58].

Ці приклади ілюструють, як різні країни інтегрують концепцію стійкості в свої стратегії управління критичною інфраструктурою, адаптуючи відповідні підходи до своїх національних умов та потреб.

В Україні актуальним стає розгляд можливості створення органу, який би координував різноманітні заходи управління безпекою критичної інфраструктури (КІ). Такий орган мав би забезпечувати стратегічні рішення щодо стійкості КІ, здійснювати глибокий аналіз та прогнозування загроз, діючи незалежно від інших установ, що сприятиме об'єктивності та ефективності виконання завдань. Цей крок не тільки оновить законодавчу базу, але й підтримає формування продуктивного партнерства між державним та приватним секторами, що є важливим для національної безпеки, економічного процвітання та соціального благополуччя.

В Канаді, Національна стратегія захисту критичної інфраструктури передбачає координацію зусиль державних органів, приватного сектору та громадськості для забезпечення адекватного захисту та відновлення критичних систем, зокрема в перші 72 години після виникнення надзвичайних ситуацій. Це співробітництво покращує загальну ефективність відповідей на загрози. Уряд Канади активно зміцнює взаємодію з операторами та власниками критичної інфраструктури, надаючи їм важливі дані про ризики, загрози та стратегії реагування на кризові ситуації.

У Європейському Союзі, зокрема через Європейський експертний центр з публічно-приватного партнерства (EPEC), активно розвивається залучення приватного сектору до захисту критичної інфраструктури. Це включає підтримку в формуванні інституційного потенціалу та моніторингу публічно-приватних партнерств в різних галузях. Такий підхід дозволяє мінімізувати бюджетні обмеження та залучати приватні інвестиції для виконання публічних функцій та розвитку інфраструктурних проєктів.

Публічно-приватні партнерства в Європі часто передбачають укладення довгострокових контрактів, в рамках яких приватні учасники беруть на себе значну частину ризиків та обов'язків, пов'язаних з проектуванням, фінансуванням, будівництвом, експлуатацією та технічним обслуговуванням інфраструктури, тоді як держава забезпечує регуляцію та виплату за результатами роботи приватного партнера.

Втілення публічно-приватних партнерств сприяє залученню приватних фінансових ресурсів до державних проектів, покриваючи різні сектори від транспорту до соціального житла та охорони здоров'я, і може надати значні переваги для суспільства, незважаючи на високі витрати та потенційні ризики. Такі ініціативи можуть бути структуровані з метою досягнення широкого спектру цілей і внести значний внесок в економічний розвиток та зміцнення національної безпеки.

Європейський Союз нещодавно актуалізував свої стратегічні напрями у сфері захисту критичної інфраструктури та забезпечення життєво важливих послуг. Завдяки співпраці Єврокомісії та держав-членів було розроблено нові політичні лінії та завдання, які були представлені у вигляді Рекомендацій Ради ЄС. Основною метою цих документів є посилення зусиль у фортифікації стійкості критичної інфраструктури, стимулюючи операторів до підвищення захисних мір за допомогою ринкових механізмів та добровільності.

Для втілення цих стратегій Європейський Союз має намір розробити комплекс інструментів, спрямованих на підтримку держав-членів і операторів критичної інфраструктури. Ці інструменти включатимуть методичну підтримку, підвищення кваліфікації персоналу, проведення стрес-тестів, координацію кризових реакцій та фінансування відповідних заходів.

Україна, яка прагне до інтеграції в європейські структури, має звернути увагу на ці нові стратегічні пріоритети ЄС і адаптувати свої внутрішні програми захисту критичної інфраструктури, оновлюючи національні законодавчі та регуляторні рамки згідно з європейськими вимогами.

Відповідно до сучасних загроз та викликів, зокрема військової агресії РФ проти України, Європейський Союз акцентує на необхідності посилити координацію між державами-членами, національними урядами, інституціями ЄС та операторами критичної інфраструктури для забезпечення безперервності важливих послуг.

У грудні 2022 року Рада ЄС ухвалила Рекомендації, маючи на меті забезпечити координований підхід до зміцнення стійкості критичної інфраструктури. Ці рекомендації передбачають розробку інструментів та методик, що дозволяють ефективно взаємодіяти на рівні ЄС, забезпечуючи оперативну готовність та швидку реакцію на інциденти, що можуть вплинути на внутрішній ринок.

Нова Директива щодо стійкості критичних об’єктів (Директива CER), прийнята у тому ж місяці, відкриває нову фазу у політиці безпеки критичної інфраструктури ЄС.

На початку 2023 року було ініційовано зміцнення співпраці між ЄС та НАТО з метою підвищення стійкості критичної інфраструктури. Ці заходи маркують новий етап у політиці ЄС, спрямованій на забезпечення безпеки та зміцнення критичної інфраструктури.

Рекомендації Ради ЄС визначають комплекс стратегій, що сприяють зміцненню стійкості критичної інфраструктури на рівнях Євросоюзу та кожної з держав-членів. Вони включають заходи для покращення здатності виявлення загроз, готовності до реагування на кризові ситуації та підсилення оперативних відповідей на потенційні небезпеки, а також для розширення міжнародної співпраці у цій області.

Виконання цих рекомендацій спрямовано на розширення можливостей ЄС у сфері захисту критичної інфраструктури. Директива CER встановлює конкретні стандарти та інструменти для моніторингу та регуляції, вводить нові зобов’язання для держав-членів та операторів, розширює перелік регульованих секторів. Оновлена Директива NIS2 встановлює комплексні вимоги у сфері кібербезпеки, що охоплюють всі важливі сектори.

Законодавчий акт наділяє Єврокомісію провідною роллю у координації заходів, забезпечуючи відповідні повноваження.

Зміцнення політики ЄС у даному напрямку має на меті гарантувати високий рівень надійності послуг, що є критичними для забезпечення ключових суспільних функцій, економічної активності, громадського здоров'я, безпеки та екологічної сталості.

Особлива увага приділяється зміцненню захисту критичної інфраструктури від антропогенних загроз як пріоритетного напрямку у безпековій стратегії ЄС. Велика вага відводиться транскордонній інфраструктурі, оцінці ризиків, поглибленню співпраці між державами-членами для аналізу загроз та обміну інформацією про виявлені вразливості, а також розробці відповідних стратегій реагування.

Крім того, важливим є посилення міжнародних зусиль для ефективного вирішення ризиків, пов'язаних із експлуатацією критичної інфраструктури, на рівнях ЄС та глобально. Це включає тісну співпрацю між державами-членами, Єврокомісією та Високим представником ЄС із закордонних справ та політики безпеки [49].

3.2. Рекомендації щодо підвищення стійкості об'єктів критичної інфраструктури

Критично важливі інфраструктурні об'єкти (КВІО) становлять основу сталого функціонування держави, особливо під час кризових періодів, таких як воєнний стан. Зміцнення їх резистентності є ключовим елементом національної безпеки України. Важливість цього напряму зумовлена потребою забезпечити неперервність державного управління, економічну стабільність та соціальний захист населення. У цьому контексті розглядаються різні стратегії та методики, спрямовані на підвищення витривалості інфраструктури.

У сучасних умовах ведення воєнних дій значення раннього виявлення загроз та ефективного моніторингу зростає, оскільки ці системи дозволяють не лише фіксувати поточні зміни у безпековому середовищі, а й прогнозувати майбутні загрози, що має вирішальне значення для забезпечення стійкості критично важливих інфраструктурних об’єктів під час воєнного стану. Заходи з раннього виявлення та моніторингу загроз базуються на комплексному підході до аналізу інформації, що включає як традиційні методи збору даних, так і застосування передових технологій.

Інтеграція штучного інтелекту (ШІ) та машинного навчання в системи моніторингу і раннього виявлення дозволяє автоматизувати процеси збору, обробки та аналізу великих обсягів даних. Це, в свою чергу, сприяє підвищенню точності прогнозування та швидкості реагування на потенційні загрози. Штучний інтелект може аналізувати не тільки відомі сценарії загроз, але й ідентифікувати нетипові патерни поведінки або аномалії, що можуть вказувати на розвиток кризових ситуацій.

Крім технічних аспектів, значна увага приділяється і методологічному компоненту систем раннього виявлення. Розробка ефективних алгоритмів обробки даних та їх інтерпретації залежить від якості навчальних даних, наявності компетентних фахівців та постійного оновлення знань бази штучного інтелекту. Такий підхід забезпечує не тільки адаптивність системи до мінливих умов, але й включає механізми самонавчання та самовдосконалення, що є критично важливими для оперативного реагування на непередбачені обставини в умовах воєнного стану.

Таким чином, раннє виявлення загроз та моніторинг за допомогою сучасних технологій стає фундаментальним інструментом у підтримці резистентності критично важливих інфраструктурних об’єктів, забезпечуючи не тільки захист, але й адаптивність виживання інфраструктури в умовах воєнного конфлікту.

Фізичний захист критично важливих інфраструктурних об’єктів є одним із основних аспектів забезпечення їхньої стійкості та безпеки,

особливо у період воєнних дій або політичної нестабільності. До основних заходів фізичного укріплення входить конструктивне зміцнення будівель та споруд, зокрема, використання матеріалів, які здатні витримувати високий рівень механічного впливу, таких як вибухи або обстріли. Це включає застосування залізобетонних конструкцій, спеціальних штукатурок, а також обладнання об’єктів системами пасивного захисту, наприклад, піскосумішевими мішками чи бетонними блоками на вразливих ділянках.

Інший важливий елемент фізичного захисту включає встановлення захисних бар’єрів, які можуть бути як наземними, так і підземними. Ці бар’єри спроектовані для затримки або повного блокування доступу несанкціонованих осіб або транспортних засобів. Броньовані двері та вікна є стандартним рішенням для захисту входів у приміщення від проникнення та збереження цілісності об’єкта під час нападу.

Додатково, важливим компонентом фізичного захисту є системи відеонагляду та сигналізації, які забезпечують контроль за обстановкою на об’єкті та в його околицях. Сучасні системи відеонагляду здатні інтегрувати функції розпізнавання облич або номерних знаків, що забезпечує додатковий рівень безпеки. Також ефективними є системи охоронної сигналізації, які можуть активувати відповідні заходи реагування при спробі несанкціонованого доступу.

Крім того, в контексті збройних конфліктів, кібербезпека критично важливих інфраструктурних об’єктів набуває особливого значення через зростання різноманітності та інтенсивності кібератак. Захист інформаційних систем таких об’єктів вимагає інтеграції комплексних систем кіберзахисту, які мають здатність протистояти не тільки стандартним кіберзагрозам, але й спеціалізованим, які спеціально розроблені для дестабілізації діяльності критичної інфраструктури.

Розробка та імплементація цих систем передбачає впровадження надійних фіреволів, антивірусного захисту, інструментів для виявлення та відповіді на інциденти (SIEM системи), а також рішень для керування

доступом та ідентифікації користувачів. Крім технічних засобів, велике значення має криптографічний захист даних, який забезпечує шифрування інформації, що перешкоджає її несанкціонованому доступу або витоку.

Окрім технологічних заходів, важливою є підготовка та постійне навчання персоналу методам розпізнавання фішингових атак, соціальної інженерії та інших широко використовуваних хакерами методик. Освітні програми повинні включати тренінги з кібергігієни, з організації безпечної роботи з електронною поштою та з особистими даними, а також з застосування двофакторної аутентифікації та інших засобів захисту доступу.

Інвестиції в кібербезпеку критично важливих інфраструктурних об’єктів є стратегічним вкладенням у національну безпеку, що забезпечує зниження потенційних ризиків від кібератак і підвищення загальної стійкості критичних систем у складних умовах сучасних воєнних та політичних конфліктів.

Розробка детально продуманих планів евакуації та реагування на надзвичайні ситуації є важливим компонентом стратегії забезпечення безпеки критично важливих інфраструктурних об’єктів. Такі плани дозволяють не лише мінімізувати ризики для життя і здоров’я людей, але й забезпечують збереження матеріальних та інформаційних ресурсів. Вони мають бути інтегровані з загальною системою управління безпекою об’єкта та включати чіткі процедури дій у випадку різних типів кризових ситуацій.

Кожен план має містити конкретні алгоритми дій для персоналу, що визначаються залежно від їхніх функціональних обов’язків та розташування в межах інфраструктури. Алгоритми повинні бути розроблені таким чином, щоб кожен співробітник мав чітке розуміння своїх завдань під час евакуації або іншої надзвичайної ситуації. Це включає інструкції з доступу до евакуаційних шляхів, методів забезпечення особистої безпеки та взаємодії з іншими членами команди та рятувальними службами.

Схеми евакуації мають бути візуалізовані та доступні у всіх ключових зонах об’єкта. Вони повинні показувати оптимальні маршрути виходу з

будівель та споруд, місця збору персоналу та розташування засобів первинної медичної допомоги та пожежогасіння. Ці схеми мають регулярно оновлюватися та адаптуватися до змін у внутрішньому устрої чи функціональному призначенні приміщень.

Логістика необхідних ресурсів, таких як медичні засоби, засоби зв'язку, пожежогасіння та евакуаційне обладнання, має бути організована таким чином, щоб гарантувати їх швидку доступність в будь-якій точці об'єкта. Запаси мають регулярно перевірятися на предмет їхньої готовності та справності.

Ефективне впровадження таких планів вимагає регулярних тренувань та навчань для персоналу, проведення яких дозволяє не тільки перевірити актуальність та ефективність планів, але й підвищити рівень підготовки та освітнього рівня співробітників щодо правил поведінки у кризових ситуаціях. Така підготовка є ключем до мінімізації можливих втрат і забезпечення швидкого та організованого реагування на надзвичайні події.

Залучення місцевих спільнот до процесів зміцнення резистентності критично важливих інфраструктурних об'єктів є фундаментальним аспектом сучасних стратегій безпеки, що розглядає не тільки технологічні та організаційні заходи, а й соціальну складову резилиєнтності. Заохочення місцевих спільнот до активної участі у захисті інфраструктури може значно підвищити рівень обізнаності населення про потенційні загрози та розвинути навички адекватної реакції на надзвичайні ситуації.

Розвиток такої взаємодії включає проведення інформаційних кампаній, тренінгів та воркшопів, які націлені на збільшення рівня знань громадян щодо основ безпеки, особливостей функціонування критично важливих об'єктів та засобів персонального захисту. Також це може включати в себе створення місцевих органів реагування, які зможуть оперативно взаємодіяти з керівництвом об'єктів та екстреними службами в умовах кризи.

Міжнародна співпраця в цій галузі відіграє вирішальну роль, оскільки дозволяє обмінюватися досвідом, технологіями та методиками, що були

успішно застосовані в різних країнах. Цей обмін досвідом може охоплювати різні аспекти, від технічних рішень для захисту інфраструктури до методів соціальної інтеграції спільноти в процеси забезпечення безпеки. Міжнародні програми та проекти можуть фінансувати дослідження, підтримувати реалізацію пілотних проектів та стимулювати участь громадськості через освітні та просвітницькі ініціативи.

Таким чином, комплексний підхід, що поєднує місцеву участь та міжнародне співробітництво, є ключовим для підвищення резистентності критично важливих інфраструктурних об’єктів. Це не тільки збільшує ефективність заходів безпеки, а й сприяє розвитку загальної культури готовності та відповідальності перед лицем загроз національній та регіональній безпеці.

Висновки до розділу 3

1. Зміцнення критично важливої інфраструктури через інноваційні методи виявляється необхідністю у відповідь на сучасні загрози національній безпеці та стабільності держав. Інтеграція передових технологій, які охоплюють цифрові рішення, інтелектуальні системи моніторингу та адаптивне управління, є критично важливою для підтримки високого рівня готовності та швидкого реагування на кризи. Стратегічне використання цих технологій може значно покращити здатність інфраструктур адаптуватися та відновлюватися після непередбачуваних подій, мінімізуючи потенційні збитки та забезпечуючи неперервність критичних сервісів.

Важливо також відзначити роль міжнародного співробітництва та публічно-приватних партнерств у посиленні стійкості інфраструктур, що включає обмін знаннями, технологіями та кращими практиками. Це співробітництво дозволяє не тільки оптимізувати використання ресурсів, але й забезпечити гнучке управління відповідно до змінюваних умов і загроз, що,

в свою чергу, сприяє формуванню взаємозалежної та міцної інфраструктурної мережі.

Таким чином, інноваційні методи зміцнення надійності критично важливих інфраструктурних об'єктів стають ключовим фактором у забезпеченні сталого розвитку і безпеки держави, відображаючи необхідність балансу між технологічним прогресом та стійкістю соціально-економічних систем.

2. Стратегічне значення критично важливих об’єктів обумовлює необхідність постійного підвищення їхньої витривалості і захисту, що забезпечується через реалізацію комплексних технічних, технологічних і соціальних заходів.

Важливим аспектом є впровадження сучасних технологій для раннього виявлення загроз і моніторингу, включаючи штучний інтелект та машинне навчання, що дозволяє не тільки реагувати на поточні загрози, а й адекватно прогнозувати потенційні небезпеки. Такі системи значно підвищують швидкість і точність відповідей на кризові ситуації, підтримуючи неперервність критичних функцій інфраструктури.

Фізичний захист об’єктів, включаючи укріплення будівель і встановлення захисних бар’єрів, забезпечує їх стійкість проти фізичних ударів і атак, знижуючи вразливість перед загрозами. В той же час, системи відеонагляду і сигналізації забезпечують додаткові рівні контролю і безпеки.

Значна увага приділяється також кібербезпеці, оскільки зростаюча кількість кібератак вимагає вдосконалення систем захисту інформаційних технологій. Розвиток комплексних систем кіберзахисту і тренування персоналу з методів виявлення та запобігання кіберзагроз стає невід’ємною частиною стратегій захисту.

Міжнародна співпраця та обмін знаннями з метою впровадження найкращих практик і технологій також відіграють важливу роль у посиленні здатності критичної інфраструктури протистояти загрозам. Така співпраця сприяє глобальній стабільності та безпеці.

Отже, комплексний підхід до зміцнення резистентності критично важливих інфраструктурних об’єктів через технічне укріплення, кіберзахист, навчання персоналу, та міжнародну співпрацю є ключовим для забезпечення національної безпеки і сталого розвитку в сучасних умовах.

ВИСНОВКИ

На основі проведеного аналізу потенційних вразливостей об'єктів критичної інфраструктури в період воєнного стану і розробка рекомендацій для підвищення їхньої стійкості та безпеки були сформовані наступні висновки відповідно до завдань дослідження:

1. Проаналізовано об'єкти критичної інфраструктури з урахуванням існуючих класифікацій, що дозволило визначити вирішальну роль критичної інфраструктури для забезпечення стабільності та захисту держави.

З’ясовано, що починаючи від античних часів, де основними об'єктами вважались водопостачання та транспортні шляхи, до сучасності, коли вагомими стають кібернетичні системи та інформаційні мережі, поняття критичної інфраструктури зазнало значних змін. У XX столітті, з розвитком технологій та збільшенням міжнародної інтеграції, критична інфраструктура стала включати ширший спектр об'єктів, що мають стратегічне значення. Визначення та класифікація цих об'єктів розвивались у відповідь на змінювані форми загроз, від традиційних військових вторгнень до сучасних кібератак і терористичних акцій.

У ході дослідження визначено, що сучасні класифікації об'єктів критичної інфраструктури відображають їх різноманіття та комплексність. Вони включають такі категорії як енергетика, водопостачання, телекомунікації, транспорт, охорона здоров'я та фінансові послуги. Кожна з цих категорій має свою власну підструктуру та специфіку ризиків, що вимагає індивідуальних підходів до забезпечення їхньої безпеки. Зокрема, врахування кіберзагроз стало необхідністю у світлі зростання залежності від цифрових технологій.

2. Розглянуто нормативно-правове регулювання захисту критичної інфраструктури в умовах воєнного стану, що має забезпечувати стабільність національної безпеки та відновлення у разі зовнішніх чи внутрішніх загроз. З’ясовано, що національне законодавство, що стосується цього питання,

зазнало кількох важливих змін і доповнень з моменту проголошення Указу Президента України у 2007 році. Згідно з рішенням РНБО від 2015 року, а також Розпорядженням Кабінету Міністрів від 2017 року, було визначено необхідність створення ефективної системи захисту критичної інфраструктури. Проте, ці рішення виявили серію проблем, які потребували негайного вирішення, включаючи відсутність уніфікованої системи захисту, неузгодженість нормативно-правового регулювання, та недостатність міжнародного співробітництва.

Установлено, що проєкт Закону "Про критичну інфраструктуру та її захист" від 2019 року, який не був прийнятий, планував створення умов для реалізації державної політики у цій сфері. Необхідність цього проєкту була підкреслена агресією Росії та потребою захисту від природних та техногенних загроз. Після цього, у 2020 році, було прийнято Постанову, яка визначила процедуру ідентифікації та категоризації об’єктів критичної інфраструктури. У 2021 році закон "Про критичну інфраструктуру" встановив організаційно-правові основи для створення національної системи захисту цієї інфраструктури.

Доведено, що прийняття цього закону сприяло формуванню чітких правил у сфері забезпечення безпеки критичної інфраструктури, визначенню її захисту як комплексу заходів різної спрямованості та розробці методології оцінки загроз. Це дозволило зробити важливий крок до вирішення раніше ідентифікованих проблем та підвищення рівня національної безпеки в сучасних умовах геополітичної нестабільності.

3. У процесі аналізу й узагальнення світового досвіду забезпечення безпеки та стійкості критичної інфраструктури, закцентовано увагу на національних особливостях зарубіжних держав, які визначаються унікальними управлінськими структурами кожної країни. Особливу увагу приділено переходу від базового реагування на кризи до розробки комплексних стратегій зміцнення стійкості, що забезпечують неперервність життєво важливих функцій у кризових умовах. Наприклад, у США та

Європейському Союзі основна увага зосереджена на інтеграції кібербезпеки та фізичного захисту з ширшими управлінськими і міжвідомчими зусиллями, тоді як країни Азії акцентують на технологічних інноваціях для забезпечення стійкості після природних катастроф.

Активне застосування комплексних стратегій, спрямованих на профілактику, стримування ризиків, мінімізацію наслідків та протидію потенційним загрозам, є ключовим аспектом політики багатьох країн, особливо Сполучених Штатів. Стійкість інфраструктури, розуміння якої еволюціонувало від простого відновлення після збоїв до адаптації та реорганізації систем в умовах зовнішніх викликів, зараз включає широкий спектр заходів від надзвичайної підготовки до оперативного реагування.

Цей підхід знайшов відображення в офіційних документах і стратегіях міжнародних організацій, таких як Європейський Союз і НАТО, які підкреслюють необхідність швидкого відновлення системи до прийнятних рівнів функціонування після кризових втручань. Концепції стійкості та вразливості розглядаються через призму суспільної, організаційної та технологічної взаємодії, що сприяє формуванню публічно-приватних партнерств та залученню інвестицій в інфраструктурні проекти.

Національні та міжнародні ініціативи, спрямовані на підвищення стійкості, відображають усвідомлення того, що ефективне управління критичною інфраструктурою в умовах різноманітних загроз є не лише технічним завданням, а й політичним викликом, який вимагає координації на різних рівнях управління. Ці заходи мають на меті не тільки захист і відновлення, але й адаптацію до нових умов, гарантуючи при цьому збереження ключових функцій суспільства, економічну активність та соціальне благополуччя.

4. Ідентифіковано потенційні загрози та аналізи ризиків, що впливають на функціонування критичної інфраструктури. Зазначено, що проблеми в комунальних системах, старіння інфраструктури та кібератаки значно підвищують ризики для стабільності державних функцій та безпеки

громадян. Аналіз виявив, що фізичне старіння об'єктів інфраструктури, таке як ветхі тепло- та водопроводи, сприяє техногенним аваріям, що можуть призвести до катастрофічних наслідків на рівні регіонів чи всієї держави.

Висвітлено, що недостатнє управління та контроль, відсутність належних інвестицій в оновлення та розвиток інфраструктури, а також недоліки у відповідях на кіберзагрози створюють умови для збільшення соціальної нестабільності та загроз національній безпеці.

Критично важливою є потреба у сформульованих і ефективно імплементованих стратегіях управління ризиками, що включають комплексні правові, організаційні, техніко-технологічні, інформаційні, та освітні заходи. Особлива увага повинна бути приділена зміцненню кібербезпеки, модернізації інфраструктури та забезпеченню стійкості до природних та антропогенних загроз. Забезпечення безпеки критичної інфраструктури має стати ключовим аспектом національної безпеки, оскільки її ефективне функціонування є вирішальним для економічного процвітання та стабільності держави.

5. Проаналізовано існуючий стан захищеності об'єктів критичної інфраструктури в контексті національної безпеки України, акцентуючи на викликах, що виникли в результаті військового конфлікту з Росією, починаючи з 24 лютого 2022 року. Виявлено значні недоліки у системі захисту критичної інфраструктури, які включають недостатність фізичних та кібернетичних заходів безпеки. Відзначено, що попри значні зусилля з модернізації і підвищення стійкості до війни, заходи були реалізовані нерівномірно через обмежені ресурси та виклики у координації між урядовими структурами та приватним сектором.

На тлі посилення військового конфлікту, Україна вжила заходів для зміцнення обороноздатності критичних об'єктів, зокрема, шляхом впровадження вдосконалених стандартів безпеки та підвищення готовності до кіберзагроз. Відбувається активна інтеграція міжнародного досвіду та адаптація європейських нормативів, зокрема директив NIS 2 і RCE, що

свідчить про стратегічне орієнтування на європейські стандарти захисту критичної інфраструктури.

За результатами аналізу визначено, що Україна здійснює комплексні зусилля щодо формування ефективної системи захисту критичної інфраструктури, яка включає законодавче урегулювання, розробку міжнародної співпраці та створення відповідної організаційної структури. Впровадження цих заходів має сприяти підвищенню рівня національної безпеки та зменшенню вразливостей у критичній інфраструктурі в умовах збройного конфлікту та інших надзвичайних ситуацій.

6. На підставі врахування основних результатів дослідження, вітчизняного і зарубіжного досвіду, потреб у забезпеченні стійкості критичної інфраструктури та з метою подальшого впровадження в практичну діяльність центральних і місцевих органів виконавчої влади та органів місцевого самоврядування сформульовано практичні рекомендації на таких рівнях:

– Міністерству інфраструктури України спільно з Всеукраїнською асоціацією міст України розглянути можливість створення “Муніципальної он-лайн платформи щодо збереження критичної інфраструктури України: інформування, діалог, здобутки”, яка не тільки сприятиме впровадженню інструментів відкритого врядування і цифрової трансформації громад, систематизації кращих управлінських практик, налагодженню міжмуніципального співробітництва та обміну успішним досвідом збереження критичної інфраструктури, а й дозволить аналізувати динаміку існуючих проблем і розробляти системні заходи для їх вирішення, сприяти розвитку територіальної мобільності, формувати й реалізовувати кар'єрні сценарії для посадових осіб місцевого самоврядування та депутатів місцевих рад, підвищувати якість управління та розширювати можливості участі громадян у вирішенні питань місцевого значення щодо збереження критичної інфраструктури;

– місцевим органам державної влади, органам місцевого самоврядування спільно з громадськістю та суб’єктами господарювання:

включити до Стратегій розвитку територій напрям, який би враховував особливості збереження критичної інфраструктури України та в найближчій перспективі реалізовувався шляхом імплементації інноваційних методів зміцнення надійності та підвищення стійкості критично важливих інфраструктурних об'єктів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Бірюков Д.С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Київ : НІСД, 2012. 96 с.

2. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній 266 інфраструктурі. *Стратегічні пріоритети. Серія: Економіка*. 2015. № 4 (37). С. 83–93. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN= LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21 FM T=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=spe_2015_4_12 (дата звернення: 20.11.2024).

3. Бобро Д.Г., Іванюта С.П., Кондратов С. І., Суходоля О.М. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналіт. доп. Київ: НІСД, 2019. 224 с.

4. Бобро Д. Г. Методологія оцінки рівня критичності об’єктів інфраструктури. *Стратегічні пріоритети*. 2016. № 3 (40). С. 77–86.

5. Деякі питання ідентифікації об’єктів підвищеної небезпеки : Постанова КМУ від 13 вересня 2022 р. № 1030. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/ laws/show/1030-2022-%D0%BF#Text (дата звернення: 20.11.2024).

6. Деякі питання об’єктів критичної інфраструктури : Постанова КМУ від 9 жовтня 2020 р. № 1109. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/ show/1109-2020-%D0%BF#Text (дата звернення: 21.11.2024).

7. Деякі питання проведення зовнішнього аудиту діяльності уповноваженого органу у сфері захисту критичної інфраструктури України : Постанова КМУ від 10 червня 2022 р. № 675. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/ laws/show/675-2022-%D0%BF#Text (дата звернення: 12.11.2024).

8. Дрейс Ю.О. Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури держави. *Захист інформації.* НАУ, 2017. Т. 19. С. 12–17.

9. ДСТУ IEC/ISO 31010:2013 «Керування ризиками. Методи загального оцінювання ризиків». Київ. *МІНЕКОНОМРОЗВИТКУ УКРАЇНИ*. 2015. 79 с. URL: https://zakon.isu.net.ua/sites/default/files/normdocs/iso_31010.pdf] (дата звернення: 20.11.2024).

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

11. Єрменчук О.П. Сутність та зміст поняття «інфраструктура» в контексті захисту критичної інфраструктури. *Бюлетень Міністерства юстиції України.* 2017. № 11. С. 35–41.

12. Желіховська Ю. В. Співвідношення та розмежування понять «охорона» та «захист». *Науковий вісник Міжнародного гуманітарного університету.* Сер.: Юриспруденція. 2015. № 13. С. 18–21.

13. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки) (аналітична записка) URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/zagrozi-kritichniy-infrastrukturi-ta-ikh-vpliv-na-stan-nacionalnoi (дата звернення: 20.11.2024).

14. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text. (дата звернення: 20.11.2024).

15. Захист критичної інфраструктури. Концепція основних заходів захисту. Рекомендація для підприємств. *Bundesministerium des Innern,* 2006. URL:https://www.bmi.bund.de. (дата звернення: 20.11.2024).

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

17. Канцір В.С. Терористична діяльність і національна безпека. *Часопис Київського університету права.* 2011. No 1. С. 265–269.

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

19. Кузьменко Ю.В., Бондар В.В. Захист об'єктів критичної інфраструктури: адміністративно-правове забезпечення. *Юридичний бюлетень*. 2021. Вип. 21. С. 67–72.

20. Лядовська В.М. Визначення критичної інформаційної інфраструктури та її захист: аналіз підходів. *Зв'язок*. 2014. № 4. С. 3–7.

21. Магда Є. Гібридна агресія Росії: уроки для Європи Київ: Каламар, 2017. 21 с.

22. Марек Сметана. Захист критичної інфраструктури. *Підходи держав Європейського Союзу щодо визначення елементів критичної інфраструктури.* Острава: ВШБ – Техніч. ун-т Острава, 2014/2015. 60 с.

23. Мельничук О.В. Управління критичною інфраструктурою держави: базові методи та критерії ідентифі-кації об'єктів. *Державне управління та місцеве самоврядування*. 2019. Вип. 3 (42). С. 13–27.

24. Мунтіян В.І. Економічна безпека України. Київ: КИИЦ, 1999. 463 с.

25. Об'єкти критичної інфраструткури. *Wikipedia:* URL: https://uk.wikipedia.org/wiki/%D0%9E%D0%B1%27%D1%94%D0%BA%D1%82
%D0%B8_%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%BD%D
0%BE%D1%97_%D1%96%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%8 2%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B8 (дата звернення: 20.11.2024).

26. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. / Бобро Д. Г., Іванюта С. П.,

Кондратов С. І., Суходоля О. М. / за заг. ред. О. М. Суходолі. Київ : НІСД, 2019. 224 с.

27. Організація системи забезпечення національної стійкості на регіональному і місцевому рівнях : аналіт. доп. / Резнікова О. О., Войтовський К. Є., Лепіхов А. В.; за заг. ред. О.О. Резнікової. Киів : НІСД, 2021. 112 с.

28. Пирожков С. І., Божок Є. В., Хамітов Н. В. Національна стійкість (резильєнтність) країни: стратегія і тактика випередження гібридних загроз. *Вісник Національної академії наук України.* 2021. № 8. С. 74–82.

29. Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України: Закон України від 18.10.2022 р. № 2684-IX. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov. ua/laws/show/2684-20#Text (дата звернення: 20.11.2024).

30. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 р. № 3475-IV. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/3475-15#n329 (дата звернення: 20.11.2024).

31. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова КМУ від 19 червня 2019 р. № 518. *Відомості Кабінету Міністрів України.*. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 19.11.2024).

32. Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України : Постанова Правління НБУ від 12 серпня 2022 № 178. URL: https://zakon.rada.gov.ua/laws/show/ v0178500-22#Text (дата звернення: 13.11.2024).

33. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури : Постанова КМУ від 22 липня 2022 р.

№ 821. *Відомості Кабінету Міністрів України.* URL: https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#Text (дата звернення: 15.11. 2024)

34. Про критичну інфраструктуру та її захист: Проєкт Закону України від 27.05.2019 р. № 10328. *Відомості Верховної Ради України.*URL: http:// w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996 (дата звернення: 20.11.2024).

35. Про критичну інфраструктуру. Закон України від 16.11.2021 №1882-IX. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 15.11. 2024)

36. Про правовий режим воєнного стану: Закон України від 12.05.2015 р. № 389-VIII. *Відомості Верховної Ради України.* URL: https://zakon.rada. gov.ua/laws/show/389-19 (дата звернення: 20.11.2024).

37. Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні. Постанова Верховної Ради України від 01.12.2005 №3175-IV. *Відомості Верховної Ради України.* URL:https://zakon.rada.gov.ua/ laws/show/3175-15#Text

38. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» Указ Президента України від 14.09.2020 р. №392/202. URL: https://zakon.rada.gov.ua/laws/ show/392/2020#Text (дата звернення: 15.11. 2024)

39. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки». Указ Президента України від 16.02.2022 № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/ 2022#Text (дата звернення: 15.11. 2024)

40. Про Стратегію національної безпеки України: Указ Президента України від 12.02.2007 р. № 105/2007 (втратив чинність). URL: https://zakon.rada.gov.ua/laws/show/105/2007#n10 (дата звернення: 20.11.2024).

41. Про Стратегію національної безпеки України: Рішення Ради національної безпеки і оборони України від 06.05.2015 р. URL: https://zakon.rada.gov.ua/laws/show/n0008525-15#Text (дата звернення: 20.11.2024).

42. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : розпорядження КМУ від 6 грудня 2017 р. № 1009-р. *Відомості Кабінету Міністрів України*. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (дата звернення: 10.11. 2024)

43. Про утворення Антикризового енергетичного штабу : Постанова Кабінету Міністрів України від 24.04.2020 № 312. *Відомості Кабінету Міністрів України* URL: https://zakon.rada.gov.ua/laws/show/312-2020- %D0 %BF#Text (дата звернення: 20.11.2024).

44. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України : Постанова КМУ від 12 липня 2022 р. № 787. *Відомості Кабінету Міністрів України* URL: https://zakon.rada.gov.ua/laws/show/787-2022- %D0%BF#Text (дата звернення: 17.11. 2024).

45. Про утворення Координаційного штабу із оперативного реагування та забезпечення створення нормальних умов життєдіяльності населення під час обмеження та/або припинення постачання електричної енергії : Постанова Кабінету Міністрів України від 22.09.2023 № 1033. *Відомості Кабінету Міністрів України.* URL: https://zakon.rada.gov.ua/laws/show/1033-2023- %D0 %BF#Text (дата звернення: 20.11.2024).

46. Ризик. *Вікіпедія.* URL: https://uk.wikipedia.org/wiki/%D0%A0%-D0%B8%D0%B7%D0%B8%D0%BA (дата звернення: 02.11.2019).

47. Світова гібридна війна: український фронт: монографія / за заг. ред. В.П. Горбуліна. К., 2017.

48. Справедливий і рівномірний розподіл електроенергії між споживачами обговорили на засіданні *Антикризового енергетичного штабу.*

2022. URL: https://www.kmu.gov.ua/news/spravedlyvyi-irivnomirnyi-rozpodil-elektroenerhii-mizh-spozhyvachamy-obhovoryly-na-zasidanni-antykryzovoho-enerhetychnohoshtabu (дата звернення: 20.11.2024).

49. Стійкість критичної інфраструктури ЄС: посилення політики та координації. 2023. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/stiykist-krytychnoyi-infrastruktury-yes-posylennya-polityky-ta (дата звернення: 20.11.2024).

50. Стійкість систем. *Матеріал з Вікіпедії – вільної енциклопедії.* URL: https://uk.wikipedia.org/wiki/Стійкість_систем (дата звернення: 19.11.2024).

51. Стратегія національної безпеки України «Україна у світі, що змінюється», затверджена Указом Президента від 12 лютого 2007 року №105 (втратила чинність). URL:https://zakon.rada.gov.ua/ laws/show/105/2007#Text

52. Суходоля О.М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. *Стратегічні пріоритети*. 2016. No 3 (40). С. 62-76.

53. Термін «Управління ризиками». База даних: «Законодавство України». URL: https://zakon.rada.gov.ua/ laws/term/31450 (дата звернення: 02.11.2024).

54. Україна починає будувати систему захисту критичної інфраструктури відповідно до вимог європейського законодавства. 2023. URL:https://biz.ligazakon.net/news/219095_ukrana-pochina-buduvati-sistemu-zakhistu-kritichno-nfrastrukturi-vdpovdno-do-vimog-vropeyskogo-zakonodavstva (дата звернення: 02.11.2024).

55. Цигичко В.М., Смолян Г.Л., Черешкін Д.С. Забезпечення безпеки критичних інфраструктур у США (аналітичний огляд). Праці ІСА РАН. 2006. Т. 27. 17 с.

56. A cyber-attack on an American water plant rattles nerves. The breach shows the dangers of connecting critical infrastructure to the internet. The Economist. Feb 9th 2021. URL: https://www.economist.com/united-

states/2021/02/ 09/a-cyber-attack-on-an-american-water-plantrattles-nerves. (дата звернення: 20.11.2024).

57. APEC Energy Resiliency Principle. URL: https://mddb.apec.org/Documents/2020/EWG/EWG59/20_ewg59_023.pdf (дата звернення: 20.11.2024).

58. Australian Government (2010) Critical infrastructure resilience strategy. ISBN: 978–1– 921725–25–8. URL: http://www.emergency.qld.gov.au/publications/pdf/ Critical_Infrastructure_Resilience_Strategy.pdf (дата звернення: 20.11.2024).

59. Council Directive 2008/114/EC «On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection». URL: https://eur-lex.europa.eu/legal-content/en/ TXT/?uri=CELEX:32008L0114 (дата звернення: 20.11.2024).

60. Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure. Brussels, 9 December 2022 (OR. en) 15623/22. URL: https://data.consilium.europa.eu/doc/document/ST-15623-2022-INIT/en/pdf (дата звернення: 20.11.2024).

61. DEMA, National Risk Profile (NRP), The Danish Emergency Management Agency, Denmark, Birkerød, 2013.

62. DEMA Nationalt Risikobillede, Beredskabsstyrelsen, Denmark, Birkerød, 2017.

63. Developing The Critical Infrastructure Protection System in Ukraine : monograph / S. Kondratov, D. Bobro, V. Horbulin, et al. ; general editor O. Sukhodolia. Kyiv: NISS, 2017. 184 p.

64. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557 (дата звернення: 20.11.2024).

65. DSB, Instruks for departementenes arbeid med samfunnssikkerhet og beredskap, Justis – og beredskapsdepartementets samordningsrolle, tilsynsfunksjon

og sentral krisehåndtering (Royal Decree of 15 June 2012), Norwegian Directorate for KIvil Protection, Norway, Oslo, 2012.

66. EC, Green Paper on a European Programme for Critical Infrastructure Protection, Commission of The European Communities, Brussels, 2005 (17 November 2005, (Com)(2005) 576 Final).

67. European Commission Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPKIP), Brussels, 22 June 2012, SWD(2012) 190 final, 2012.

68. European External Relations Service (EEAS) Building, 9A Rond Point Schuman, 1046 Brussels, Belgium URL: https://eeas.europa.eu/topics/eu–global–strategy_en (дата звернення: 19.11.2024).

69. Evolutions of Infrastructure: 15,000 Years of History by Demeter G. Fertis, Anna Fertis, Published by Vantage Press, 1998.

70. Folke C., Resilience: the emergence of a perspective for soKIal – ecological systems analyses. *Global Environmental Change*. 2006. 16(3). P. 253–267.

71. Haimes Y., On the Definition of Resilience in Systems, *Risk Analysis.* 2009. Vol. 29. №4. Pp. 498–501.

72. Hoffman F. Onnot-so-newwarfare: political war fare vs hybrid threats. URL: http://warontherocks.com. (дата звернення: 19.11.2024).

73. Holling C. Resilience and stability of ecological systems, Annual review of ecology and systematics, pp. 1–23, 1973.

74. Infrastructure for the 21st Century: Framework for a Research Age. Washington: National Academies Press, 1987. ISBN 978-030-9078-146.

75. Keogh M., Cody C. Resilience in Regulated Utilities / research document of the National Association of Regulatory Utility Commissioners, 2013. URL:https://pubs.naruc.org/pub/536F07E4-2354-D714-5153-7A80198A436D (дата звернення: 19.11. 2024).

76. Kohler K. National Risk Assessments of Cross-Border Risks. *Center for Security Studies (CSS). ETH Zürich,* 2023. URL:

https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/centerfor-securities-studies/pdfs/RR-Reports-2023-National-Risk-Assessments-of-Cross-Border-Risks.pdf (дата звернення: 20.11.2024).

77. Ministry of Justice and Public Safety, Samfunnssikkerhet, Report to the Storting 29 (2011–2012), Norway, Oslo, 2012.

78. Nan C., Sansavini G. A quantitative method for assessing resilience of interdependent infrastructures, *Reliability Engineering and System Safety.* Elsevier, 2017. Vol. 157(C). P. 35–53

79. National Critical Infrastructure Security and Resilience Research and Development Plan, 2015. URL: https://www.dhs.gov/publication

80. National Infrastructure Delivery Plan 2016 – 2021. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/5 20086/2904569_nidp_deliveryplan.pdf (дата звернення: 19.11.2024).

81. National Risk and Capability Assessment. URL: https://www.fema.gov/emergency-managers/nationalpreparedness/goal/risk-capability-assessment#thira (дата звернення: 20.11.2024).

82. National Risk Assessments: A Cross Country Perspective. URL: https://www.oecd.org/gov/national-riskassessments-9789264287532-en.htm

83. National Threat and Hazard Identification and Risk Assessment (THIRA). *Overview and Methodology.* URL: https://www.fema.gov/sites/default/files/2020-06/fema_national-thira-overview-methodology_2019_0.pdf (дата звернення: 20.11.2024).

84. Presidential Policy Directive – Critical Infrastructure Security and Resilience. 2013. URL: https://www.dhs.gov/sites/default/files/publications/PPD–21–Critical–Infrastructure– andResilience–508.pdf (дата звернення: 16.11.2024).

85. Pursiainen C., Gattinesi P., Towards Testing Critical Infrastructure Resilience, Publications Office of the European Union, JRC SKIentific and Policy Reports, Luxembourg, 2014.

86. Quadrennial Homeland Security Review, 2010, 2014. URL: https://www.dhs.gov/quadrennial-homeland-security-review (дата звернення: 19.11.2024).

87. Říha, Josef. Urbanismus a územní rozvoj. ročník X. číslo 4/2007. URL: http://www.uur.cz/images/5-publikacni-cinnost-a-knihovna/casopis/2007/2007-04/08_kriticka.pdf. (дата звернення: 19.11.2024).

88. Resilience Analysis and Practice, The Resilience Alliance. Research organization. URL: http://www.resalliance.org/index.php/resilience (дата звернення: 19.11.2024).

89. Resolution B.372 by the Ministerial Committee on National Security Affairs (State Security Cabinet), dated October 30, 2019: Establishment of a Process and Mechanism for Evaluating National Security Aspects of Foreign Investments. URL:https://www.gov.il/en/departments/policies/ foreign-investment-board (an unofficial and unbinding translation to English)

90. Shodan. Сайт. URL:https://www.shodan.io/ explore/category/industrial-control-systems

91. Směrnice Rady 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.

92. The Art of War Sun Tzu, Thomas Cleary. by Harper Press. 273 s.

93. The National Risk Register. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/952959/6.6920_CO__CCS_s_National_Risk_Register_2020_11-1-21-FINAL.pdf] (дата звернення: 20.11.2024).

94. UNISDR (n.d.) Terminology on Disaster Risk Reduction, United Nations International Strategy for Disaster Reduction, Switzerland, Geneva, [Online] Available at URL: http://www.unisdr.org/we/inform/terminology (дата звернення: 23.11. 2024).

Документ підписано у сервісі Вчасно (продовження)
ННІНО_2024_281_Кабанов С.О..pdf

Документ відправлено: 03:08 19.12.2024
Документ отримано: 03:08 19.12.2024

Відправник документу

Отримувач документу

Електронний підпис
03:08 19.12.2024
Ідентифікаційний код: 2686200868
Кожина Алла Василівна
Власник ключа: Кожина Алла Василівна
Час перевірки КЕП/ЕЦП: 03:08 19.12.2024
Статус перевірки сертифікату: Сертифікат діє
Серійний номер: 382367105294AF97040000001AA60D002ED32C03
Тип підпису: кваліфікований

Електронний підпис
15:11 20.12.2024
Ідентифікаційний код: 2544808106
ЛЕЛЕЧЕНКО АНЖЕЛА ПАВЛІВНА
Власник ключа: ЛЕЛЕЧЕНКО АНЖЕЛА ПАВЛІВНА
Час перевірки КЕП/ЕЦП: 15:11 20.12.2024
Статус перевірки сертифікату: Сертифікат діє
Серійний номер: 5E984D526F82F38F040000009A92CA0049DB4905
Тип підпису: удосконалений
Тип сертифікату: кваліфікований

Електронний підпис
16:18 20.12.2024
ЄДРПОУ/ІПН: 2883500752
Юр. назва: ФОП КАБАНОВ СЕРГІЙ ОЛЕКСАНДРОВИЧ
КЕРІВНИК: КАБАНОВ СЕРГІЙ ОЛЕКСАНДРОВИЧ
Час перевірки КЕП/ЕЦП: 16:18 20.12.2024
Статус перевірки сертифікату: Сертифікат діє
Серійний номер: 5E984D526F82F38F040000007B9A4F01A70DE304
Тип підпису: удосконалений
Тип сертифікату: кваліфікований