МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЕКОЛОГІЧНОЇ БЕЗПЕКИ, ІНЖЕНЕРІЇ ТА ТЕХНОЛОГІЙ
КАФЕДРА ЦИВІЛЬНОЇ ТА ПРОМИСЛОВОЇ БЕЗПЕКИ
ІМЕНІ ГЕРОЯ УКРАЇНИ ЧУБА ОЛЕКСАНДРА СЕРГІЙОВИЧА

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ Б.Д.Халмурадов
«____» _____ 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА
ЗА СПЕЦІАЛЬНІСТЮ 263 «ЦИВІЛЬНА БЕЗПЕКА»

Тема: « Оцінка вразливості об’єкту критичної інфраструктури в період воєнного стану»

Виконавець: студент групи 413 ЦБ Литвин Владислав Олександрович

Керівник: д.т.н., професор Третьяков Олег Вальтерович

Нормоконтролер: _____ Козлітін О.О.

КИЇВ 2024

КИЇВ 2024

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет екологічної безпеки, інженерії та технологій

Кафедра цивільної та промислової безпеки імені Героя України Чуба Олександра Сергійовича

Спеціальність 263 «Цивільна безпека»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Б.Д.Халмурадов

«___» _____ 2024 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи

Литвина Владислава Олександровича

1. Тема роботи «Оцінка вразливості об’єкту критичної інфраструктури в період воєнного часу» затверджена наказом ректора від «17» квітня 2024 року № 579/ст.
2. Термін виконання роботи з 20.05.2024 по 16.06.2024.
3. Вихідні дані роботи:

- Поняття та класифікація об’єктів критичної інфраструктури.
- Загрози та ризики для об’єктів критичної інфраструктури.
- Сучасні підходи до підвищення стійкості об’єктів критичної інфраструктури.
- Аналіз існуючого стану захищенності об’єктів критичної інфраструктури в Україні.

- Розробка рекомендацій щодо підвищення стійкості об’єктів критичної інфраструктури.
- Оцінка ефективності запропонованих заходів щодо підвищення стійкості об’єктів критичної інфраструктури.

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 пропозицій щодо підвищення стійкості критично важливої інфраструктури.

5. Календарний план-графік:

№ з/п	Завдання	Термін виконання	Підпис керівника
1	2	3	4
1	Аналіз теми кваліфікаційної роботи	20.05.2024-23.05.2024	
2	Збір інформаційних даних та аналіз літературних джерел	23.05.2024-26.05.2024	
4	Робота з написання розділу №1	26.05.2024-29.05.2024	
5	Робота з написання розділу №2	30.05.2024-04.06.2024	
6	Підготовка, оформлення і друк пояснювальної записки	04.06.2024-06.06.2024	
7	Оформлення презентації в Power Point	07.06.2024-08.06.2024	
9	Підготовка до захисту роботи	09.06.2024-11.06.2024	

6. Дата видачі завдання: «20» травня 2024 р.

Керівник кваліфікаційної роботи: _____ _____

Завдання прийняв до виконання: Литвин В.О _____

РЕФЕРАТ

Відповідно до мети, завдання й предмета дослідження наукова робота складається зі вступу, двох розділів, які об’єднують 6 підрозділів, висновків, списку використаних джерел. Загальний обсяг роботи - 70 сторінок, список використаних джерел – 73 найменувань.

Ключові слова: Критична інфраструктура, забезпечення стійкості, безпека.

Об’єкт дослідження – об'єкти критичної інфраструктури.

Предмет дослідження – процеси та методи оцінки вразливості об'єктів критичної інфраструктури в період воєнного стану.

Мета роботи – ідентифікація та аналіз потенційних вразливостей об'єктів критичної інфраструктури в період воєнного стану і розробка рекомендацій для підвищення їхньої стійкості та безпеки.

Методи, застосовані в кваліфікаційній роботі: Для забезпечення об’єктивності, всебічності і повноти дослідження, а також для отримання науково обґрунтованих і достовірних результатів використано сукупність філософськосвітоглядних, загальнонаукових і спеціальних методів наукового пізнання. Також були використані такі методи: аналітичний – для вивчення існуючих систем захисту та виявлення їхніх недоліків, системно-функціональний метод – для аналізу взаємозв'язків та функціонування компонентів критичної інфраструктури. За допомогою порівняльного аналізу вивчено досвід інших країн у цій сфері. Такий комплексний підхід дозволив оцінити стійкість об'єктів критичної інфраструктури та розробити рекомендації для їхнього зміцнення у період воєнних дій. Метод узагальнення використано для формулювання прикінцевих положень проведеного дослідження.

Наукова новизна полягає у розробці комплексної методології, яка інтегрує традиційні підходи до оцінки вразливості з сучасними аналітичними технологіями, такими як машинне навчання та штучний інтелект, для глибокого аналізу потенційних загроз і визначення слабких місць у структурі

і функціонуванні критичних об'єктів. Введення нових моделей сценарного аналізу дозволяє симулювати різні форми загроз і оцінювати потенційний вплив на об'єкти критичної інфраструктури в умовах воєнного стану. Також було запропоновано адаптувати міжнародні стандарти безпеки до умов воєнного стану в Україні, з урахуванням специфіки місцевих загроз та ресурсних обмежень, що забезпечує підвищену адекватність і ефективність рекомендацій зі зміцнення захищеності критичної інфраструктури.

Основні висновки роботи мають на меті запропонувати рекомендації спрямовані на створення умов, що мінімізують вразливість критичних об'єктів до військових дій, терористичних актів, техногенних катастроф і інших загроз. Реалізація цих рекомендацій забезпечить більш високий рівень безпеки та оперативне реагування на надзвичайні ситуації, що є ключовим для збереження життєво важливих соціальних функцій і національної економіки.

Матеріали дипломної роботи можуть бути використані для подальших досліджень в області безпеки критичної інфраструктури, у розробці нових методів оцінки вразливості та стійкості об'єктів у кризових умовах, а також при написанні наукових статей, монографій і методичних матеріалів з цієї тематики.

ЗМІСТ

ВСТУП

В умовах постійної геополітичної напруженості та зростаючої кількості збройних конфліктів по всьому світу, питання забезпечення стійкості та безпеки критичної інфраструктури набуває особливої актуальності. Критична інфраструктура включає такі життєво важливі об'єкти, як енергетичні установки, водопостачання, телекомунікаційні системи та транспортні мережі, які є основою для функціонування суспільства та економіки кожної країни. Період воєнного стану вносить додаткові ризики та виклики для безперебійної роботи цих об'єктів, роблячи їх особливо вразливими перед обличчям військових загроз. Відтак, оцінка вразливості об'єктів критичної інфраструктури під час воєнного стану стає пріоритетним завданням, яке вимагає всебічного дослідження та розробки ефективних методів захисту.

Дослідження критичної інфраструктури набуває особливої актуальності у контексті зростаючого рівня терористичних загроз у світовому масштабі. Значний внесок у розробку методик, засобів і технологій ідентифікації та захисту об'єктів критичної інфраструктури внесли дослідження, проведені провідними зарубіжними вченими, зокрема, Д. Дуденхофером, П. Педерсеном, М. Перманом, М. Манікою, а також Р. Дженкінсом та Б. Хофманом. В Україні цю проблематику досліджують такі науковці, як В. Антипенко, С. Кондратов, В. Крутов, С. Кудінов, І. Рижов та інші.

Попри значну кількість наукових праць, присвячених антитерористичному захисту критичної інфраструктури, на сьогодні залишається малодослідженою методологія для аналізу критичної інфраструктури і оцінки її захищеності, що є важливою для забезпечення національної безпеки та ефективного реагування на збройну агресію у період воєнного стану.

Мета дослідження – ідентифікація та аналіз потенційних вразливостей об'єктів критичної інфраструктури в період воєнного стану і розробка рекомендацій для підвищення їхньої стійкості та безпеки.

Для досягнення поставленої мети необхідно виконати такі основні завдання:

- розглянути поняття та класифікація об'єктів критичної інфраструктури;
- визначити загрози та ризики для об'єктів критичної інфраструктури;
- проаналізувати сучасні підходи до підвищення стійкості об'єктів критичної інфраструктури;
- здійснити аналіз існуючого стану захищеності об'єктів критичної інфраструктури в Україні;
- розробити рекомендацій щодо підвищення стійкості об'єктів критичної інфраструктури;
- реалізувати оцінку ефективності запропонованих заходів щодо підвищення.

Об'єкт дослідження – об'єкти критичної інфраструктури.

Предмет дослідження – процеси та методи оцінки вразливості об'єктів критичної інфраструктури в період воєнного стану.

Методи дослідження. Для забезпечення об’єктивності, всебічності і повноти дослідження, а також для отримання науково обґрунтованих і достовірних результатів у дисертаційній роботі використано сукупність філософськосвітоглядних, загальнонаукових і спеціальних методів наукового пізнання. Також були використані такі методи: аналітичний – для вивчення існуючих систем захисту та виявлення їхніх недоліків, системно-функціональний метод – для аналізу взаємозв'язків та функціонування компонентів критичної інфраструктури. За допомогою порівняльного аналізу вивчено досвід інших країн у цій сфері. Такий комплексний підхід дозволив оцінити стійкість об'єктів критичної інфраструктури та розробити рекомендації для їхнього зміцнення у період воєнних дій. Метод узагальнення використано для формулювання прикінцевих положень проведеного дослідження.

Наукова новизна дослідження полягає у розробці комплексної методології, яка інтегрує традиційні підходи до оцінки вразливості з

сучасними аналітичними технологіями, такими як машинне навчання та штучний інтелект, для глибокого аналізу потенційних загроз і визначення слабких місць у структурі і функціонуванні критичних об'єктів. Введення нових моделей сценарного аналізу дозволяє симулювати різні форми загроз і оцінювати потенційний вплив на об'єкти критичної інфраструктури в умовах воєнного стану. Також було запропоновано адаптувати міжнародні стандарти безпеки до умов воєнного стану в Україні, з урахуванням специфіки місцевих загроз та ресурсних обмежень, що забезпечує підвищену адекватність і ефективність рекомендацій зі зміцнення захищеності критичної інфраструктури.

Практичне значення одержаних результатів дослідження виявляється у кількох ключових аспектах:

У науково-дослідній сфері – результати можуть бути використані для подальших досліджень в області безпеки критичної інфраструктури, у розробці нових методів оцінки вразливості та стійкості об'єктів у кризових умовах, а також при написанні наукових статей, монографій і методичних матеріалів з цієї тематики.

У навчальному процесі – матеріали дослідження можуть бути інтегровані в навчальні курси з безпеки, управління ризиками та цивільної оборони, сприяючи підготовці кваліфікованих фахівців у цих галузях.

У розробці політики і стратегій – результати дослідження можуть бути використані урядовими та некомерційними організаціями для формування стратегій зміцнення національної безпеки через вдосконалення законодавчої та нормативної бази щодо захисту критичної інфраструктури.

У оперативному управлінні та реагуванні на кризи – використання рекомендацій та методів дослідження може підвищити ефективність планування заходів цивільного захисту та швидкість реагування на надзвичайні ситуації в умовах воєнного стану.

У правозастосуванні – результати можуть слугувати підставою для розробки та удосконалення оперативних процедур і стандартів безпеки для

працівників та управлінців об'єктів критичної інфраструктури, забезпечуючи кращу підготовку до відповіді на воєнні загрози.

Структура та обсяг роботи. Відповідно до мети, завдання й предмета дослідження наукова робота складається зі вступу, двох розділів, які об’єднують 6 підрозділів, висновків, списку використаних джерел. Загальний обсяг роботи - 70 сторінок, список використаних джерел – 73 найменувань.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Поняття та класифікація об'єктів критичної інфраструктури

Історичний аналіз розвитку світових держав та цивілізацій підтверджує, що загрози, як зовнішні, так і внутрішні, час від часу виникають у кожному суспільстві. З плином часу форми цих загроз та цілі, що можуть бути атаковані, змінюються в залежності від рівня економічного, соціального та технологічного розвитку, причому наслідки можуть бути катастрофічними, включаючи людські жертви та великі матеріальні збитки, що негативно впливають на діяльність суспільства, його соціально-економічний розвиток, суверенітет, територіальну цілісність та національну безпеку держави. Ще давні китайці та греки знали про існування об'єктів, важливих для стабільної роботи суспільства.

На ранніх етапах розвитку цивілізацій однією з основних загроз соціальному ладу вважалася можливість іноземного військового вторгнення. Наприклад, великий китайський мислитель Сунь Цзи у VII столітті до нашої ери у своєму трактаті «Мистецтво війни» описав п'ять основних цілей, які зазвичай прагне знищити ворог: людей, провіант, табори, склади та військові підрозділи [72, с. 70].

У давнину до критично важливих об'єктів зазвичай входили транспортні мережі та водопостачання, які були надзвичайно важливими для підтримки життєдіяльності держав. Їхнє безперебійне функціонування гарантувало задоволення потреб громадян і становило ключовий елемент управління населенням. Тому, під час нападів, основним завданням оборонців було захистити ці життєво важливі об'єкти від руйнувань. Контроль або знищення таких об'єктів згодом стали стратегічною основою військових доктрин і діяльності спеціальних служб.

Перше відоме вживання терміна «інфраструктура» приписується Сократу (5 століття до н.е.), який стверджував: «Для існування людини необхідні основи, які забезпечує суспільство: безпеку, соціальний порядок та матеріальні блага. Людина може їх отримати, дотримуючись соціальних концепцій та виконуючи свої обов'язки, особливо забезпечуючи інфраструктуру та послуги, надані суспільством» [53]. Поняття «інфраструктура» (французьке «infra-structure») спершу застосовувалось у військовій сфері у Франції, що означало «підземні споруди». За даними деяких дослідників, зокрема Стефена Левіса, поширення цього терміна в США відбулось через французьких інженерів, які працювали над залізницями, тунелями та мостами, що в подальшому сприяло зміні його значення на американському континенті [58].

Сучасний розвиток цивілізації значно вплинув на методи ведення воєнних конфліктів. Однією з характерних особливостей XX століття стало появлення так званих «гібридних» війн, які часто не оголошуються офіційно [19, с. 21]. За словами військового консультанта Ф. Хофмана, в гібридних війнах агресор використовує різноманітні загрози, спрямовані на слабкі місця противника, включаючи комбінації конвенційної зброї, партизанські дії, терористичні акти з метою досягнення своїх політичних амбіцій. Хофман прогнозує, що такий вид війн стане все більш поширеним [56]. Український політолог Є. Магда вказує на різні методи впливу у таких війнах, включаючи політичні, військові, економічні, соціальні, інформаційні та підривні дії [19, с. 30-31].

Ці змінені засоби ведення війни мають ту саму ціль — вигоду в різних формах, як-от матеріальну, фінансову чи політичну [35]. Вони спрямовані на стратегічно важливі (критичні) об'єкти держави, яка зазнає агресії.

Еволюція засобів і методів ведення війн тісно пов'язана з розвитком цілей агресії, які також зазнають значних змін. Останні декілька десятиліть відзначилися стрімким розвитком технологій, особливо у сфері інформаційних технологій, що спричинило глибокі зміни в інтеграції, взаємозалежності та

взаємопроникненні різних мереж та систем. Ці зміни охопили виробничі, фінансові, комерційні та інші процеси в багатьох країнах світу. XX століття, особливо під час карибської кризи, стало переломним моментом у підході до захисту критичної «невійськової» інфраструктури, зокрема телекомунікаційних мереж. Одним з найвідоміших прикладів кібератак на критичну інфраструктуру є атака на іранські ядерні об'єкти в 2010 році за допомогою вірусу «Stuxnet» [8]. Українські об'єкти також неодноразово ставали мішенями кібератак. Наприклад, в 2015 році в результаті атаки вірусом «BlackEnergy» було знеструмлено енергосистему «Прикарпаттяобленерго», внаслідок чого майже 230 тисяч осіб залишились без електрики. Загальна кількість кібератак в Україні за останні два місяці 2016 року, згідно з відкритими даними, склала 2,5 тисячі, як було зазначено на засіданні РНБО України [35].

Таким чином, провідні світові держави активно працюють над забезпеченням безпеки не тільки фізичної, але й кібернетичної критичної інфраструктури. Наприклад, у Плані захисту критичної інфраструктури США за 2015 рік особлива увага приділяється мінімізації наслідків від потенційних загроз та підтримці швидкого відновлення систем після інцидентів [62]. В Німеччині, поряд з ризиками від терористичних актів та природних катастроф, виділяють загрози, спричинені технічними збоями та людськими помилками, що включають і кіберзагрози [13].

Також важливо згадати про природні загрози, які не мають соціального походження. Це включає стихійні лиха, такі як паводки, засухи, епідемії, епізоотії, епіфітотії, землетруси, бурі та інші подібні явища. В більшості країн світу такі природні ризики класифікують як окрему категорію загроз.

Розглядаючи світовий досвід, можна виокремити три ключові напрями захисту критичної інфраструктури:

- Захист від загроз національній безпеці, що охоплює як внутрішні так і зовнішні фактори, включаючи можливість фізичного пошкодження або знищення об'єктів критичної інфраструктури;

- Захист від кіберзагроз;

- Захист від різних видів надзвичайних ситуацій.

Критична інфраструктура завжди була в центрі уваги з точки зору захисту і як потенційна ціль агресора або факторів непередбачених ударів, включаючи природні загрози. Осмислення і визначення «критичної інфраструктури» зазнає постійних змін відповідно до розвитку суспільства. Систематичні зусилля з виділення цієї категорії та структурованого захисту на національному рівні розпочалися відносно недавно у світовій історії.

У Сполучених Штатах Америки з 1980-х років відбувається активна робота над проблематикою критичної інфраструктури, зокрема дослідженнями займається Національний дослідний інститут (U.S. National Research Council) [58]. Значний імпульс дослідженню надали такі події, як терористичні акти 11 вересня 2001 року в США, атаки 11 березня 2004 року в Мадриді та вибухи 7 липня 2005 року в Лондоні [42].

Науковий підхід до питання захисту критичної інфраструктури в Україні почав розвиватися на початку 2000-х років, але значний прорив відбувся після 2015 року. Основним каталізатором цього процесу стало дослідження від НІСД, опубліковане у «Зеленій книзі з питань захисту критичної інфраструктури в Україні». У цій публікації під критичною інфраструктурою розуміють системи та ресурси, як фізичні, так і віртуальні, життєво важливі для функціонування суспільства, порушення роботи яких може призвести до серйозних наслідків для соціально-економічного розвитку та національної безпеки [14]. Автори роботи формулювали стратегічні цілі державної політики в цій області, принципи та завдання для системи захисту критичної інфраструктури. В даний час актуальним є подальше розроблення та уточнення моделі функціонування цієї системи, визначення ролей учасників процесу, зокрема, на основі вивчення досвіду європейських країн у цій сфері.

Зміст терміну «критична інфраструктура» постійно оновлюється та вдосконалюється. Так, у 2002 році, на засіданні Євроатлантичної ради НАТО, було ухвалено визначення, за яким критична інфраструктура охоплює фізичні

та кібернетичні системи, необхідні для забезпечення ключових функцій економіки та управління, включаючи телекомунікаційні, енергетичні, банківські, фінансові та водногосподарські системи, а також аварійні служби [20, с. 32].

З 2003 року в рамках програм ЄС, таких як «European industrial potential in the field of security research» та «European Security Research Programme (ESRP)», почались інтенсивні дослідження у галузі безпеки. З 2007 року стартувала ініціатива «Research for Secure Europe», метою якої була підготовка до можливих воєнних дій чи надзвичайних ситуацій. Одночасно з 2004 року ЄС та Європейська комісія розпочали реалізацію проекту «European Programme for Critical Infrastructure Protection» (EPCIP), акцент в якому було зроблено на захист від терористичних загроз. Під критичною інфраструктурою на той час розуміли обладнання, служби та інформаційні системи, відмова або знищення яких могло б послабити суспільство, національне господарство, систему охорони здоров'я або державний устрій.

17 листопада 2005 року Комісія ЄС прийняла «Зелену книгу» з захисту критичної інфраструктури (EPCIP), яка мала на меті сформувати спільну політичну позицію та практичні заходи для захисту критичної інфраструктури в країнах ЄС. Основною темою в документі було підкреслено потребу посилення взаємодії та обміну інформацією між країнами ЄС щодо загроз, які мають транснаціональний характер.

Дослідження підходів країн ЄС до визначення критичної інфраструктури виявляють, що вона сприймається як складна система мереж, включаючи окремі компоненти та зв'язки між ними. Такі точки з'єднання в мережах формують вузли, і пошкодження одного вузла може мати наслідки для всієї системи, спричинюючи порушення її цілісності. Тому захист цих вузлів є критично важливим для забезпечення стійкості критичної інфраструктури [20].

У США розрізняють критичну інфраструктуру та її ключові компоненти, які налічують 16 секторів. В Європі застосовують поділ на «рівні секторів» та

«рівні продуктів і послуг», кількість яких варіюється від 8 до 10. Спочатку захист критичної інфраструктури в Європі був націлений на підтримку стабільності національних систем, але сьогодні основна мета Європейської програми полягає у забезпеченні універсального захисту критичної інфраструктури по всьому європейському простору. Основні завдання програми включають протидію тероризму та кіберзагрозам.

З огляду на зазначене, при формулюванні визначення вітчизняної критичної інфраструктури важливо врахувати доцільність включення до її складу як матеріальних, так і нематеріальних компонентів. Ці об'єкти визначаються як «надзвичайно важливі» і є такими в законодавстві США (Patriot Act, 2001) та Німеччини, де вони описані як «системи та засоби, фізичні чи віртуальні, життєво важливі...» [14].

Тому ми пропонуємо, що вітчизняне визначення критичної інфраструктури повинно охоплювати «сукупність надзвичайно важливих матеріальних та нематеріальних об’єктів національної інфраструктури». Таке визначення на законодавчому рівні дозволить ефективно протидіяти тероризму та кіберзагрозам, забезпечивши координацію заходів захисту на загальнодержавному рівні, подібно до практики в країнах ЄС.

Важливо підкреслити, що сучасне визначення критичної інфраструктури зосереджується не лише на фізичних аспектах об’єктів, але й все більше акцентує на їхніх функціях та наданих послугах. Ці елементи відіграють ключову роль у забезпеченні потреб суспільства, держави та її економіки, що є вирішальним у визначенні критичності цих об’єктів. Цей підхід надає методологічні переваги для встановлення критеріїв відбору елементів критичної інфраструктури та визначення пріоритетності їх захисту [14].

Крім того, критична інфраструктура тісно пов’язана з національною інфраструктурою, яка включає взаємопов'язані системи державного управління та об'єкти, що формують основу для функціонування держави, її економіки та суспільства. Така інтеграція є критично важливою для забезпечення стабільності та безпеки на національному рівні.

Термін «об'єкт національної інфраструктури» охоплює державні та приватні підприємства, організації, установи, а також їх власність і результати діяльності, які становлять єдиний механізм, що забезпечує функціонування держави, її економіки та суспільства [9, с. 20-27]. Використання таких широких категорій, як власність та результати діяльності, дозволяє охопити різноманітні компоненти, що не завжди відповідають традиційним термінам українського законодавства, такі як системи і їх частини, мережі, ресурси, вузли та інше.

Лише об'єкти, що мають надзвичайне значення для забезпечення державної безпеки, класифікуються як елементи критичної інфраструктури. Такий підхід дозволяє встановити чіткі критерії для визначення, які саме компоненти національної інфраструктури потребують особливого захисту з метою забезпечення стабільності та безпеки всієї країни [10, с. 39].

У директиві Ради ЄС критична інфраструктура розглядається у двох основних категоріях: національна критична інфраструктура та європейська критична інфраструктура. Національна критична інфраструктура охоплює засоби, системи та їх частини у державах-членах ЄС, що вважаються невід'ємними для підтримки ключових суспільних функцій, таких як здоров'я, безпека, та забезпечення належних економічних та соціальних умов для населення. Перебої або руйнування таких елементів можуть призвести до серйозних наслідків для держави-члена ЄС [71]. Одночасно, враховуючи транснаціональний вплив деяких елементів, було введено поняття європейської критичної інфраструктури, яке включає об'єкти, розташовані у державах-членах, чиї збої чи руйнація могли б спричинити серйозні наслідки в мінімум двох державах [71].

Професор Йозеф Ржига в статті журналу «Урбанізм і територіальний розвиток» висловлює думку, що вибір об'єктів для включення до критичної інфраструктури має базуватися на професійних знаннях, з урахуванням їхньої важливості, обсягу та часового фактору, що визначає терміновість та необхідність їх захисту [67].

Так, аналізуючи концепцію «критична інфраструктура», можна дійти висновку, що вона повинна включати ті об'єкти, які є життєво важливими для держави, і чиє пошкодження або дисфункція можуть спричинити серйозні негативні наслідки для громадян, їх здоров'я, безпеки, а також соціально-економічного стану країни. Від цих об'єктів безпосередньо залежить стабільність національної інфраструктури та економіки загалом.

Отже, вітчизняне визначення критичної інфраструктури могло б виглядати так: критична інфраструктура охоплює систему надзвичайно важливих матеріальних та нематеріальних об’єктів національної інфраструктури, які є ключовими для її стабільного функціонування. Руйнація чи пошкодження цих об’єктів через різні загрози може призвести до значних людських жертв, серйозних матеріальних втрат, та мати глибокі негативні наслідки для життєдіяльності суспільства, соціально-економічного розвитку та національної безпеки країни.

Об'єкти критичної інфраструктури [23] визначаються як ключові підприємства та установи, які здійснюють свою діяльність у таких стратегічно значущих секторах як енергетика, хімічна промисловість, транспорт, фінанси, інформаційні технології та телекомунікації, охорона здоров'я та продовольча галузь. Ці об'єкти є вирішальними для функціонування економіки та безпеки держави, а їхнє ушкодження чи виведення з ладу може спричинити серйозні наслідки для національної безпеки, промисловості, екології або загрожувати життю населення.

Згідно з чинним законодавством, визначення критичної інфраструктури наведено у законопроекті №5219 від 09.03.2021 [28]. Цей законопроект визначає, що до критичної інфраструктури належать об'єкти, діяльність яких відбувається у визначених критичних секторах. Сектори критичної інфраструктури включають галузі, що забезпечують важливі функції чи послуги, відмова яких може мати негативні наслідки для національної безпеки України та впливати на обслуговування населення, такі як управління, енергопостачання, водозабезпечення, продовольство, медичне обслуговування

та інші сектори, зазначені у документі. Об'єкти критичної інфраструктури розподіляються на чотири категорії залежно від їх значення для забезпечення окремих життєво важливих функцій в межах цих секторів.

У законі України «Про основні засади забезпечення кібербезпеки України» [8] вводиться термін «Критично важливі об'єкти інфраструктури», який описує юридичних осіб, чия діяльність пов'язана з важливими технологічними процесами та/або наданням послуг, критичних для промисловості, економіки та безпеки населення. Закон також визначає «об'єкти критичної інформаційної інфраструктури» як технологічні або комунікаційні системи об'єкта критичної інфраструктури, атака на які може безпосередньо вплинути на їх функціонування.

Об'єкти критичної інфраструктури представляють собою ключові підприємства та установи, розташовані в стратегічно важливих секторах, таких як енергетика, хімічна промисловість, транспорт, фінанси, інформаційні технології та телекомунікації, охорона здоров'я та продовольча галузь. Ці елементи є незамінними для забезпечення стабільного функціонування економіки та суспільства, а їх дисфункція чи руйнування може мати серйозні наслідки для державної безпеки, навколишнього середовища, а також здоров'я та життя громадян.

Визначення статусу критичної інфраструктури у законодавстві України регулюється згідно з Постановою Кабінету Міністрів № 1109, де секторальні органи, такі як Держспецзв'язку, МВС, Мінекономіки, Міненерго, Мінінфраструктури, Міноборони, Мінцифри, Мінфін, МОЗ, Національний банк, НСЗУ та СБУ, відповідають за захист і регулювання відповідних секторів критичної інфраструктури.

Відповідно до Постанови № 1109, українське законодавство передбачає чітку ієрархію критичності для об'єктів критичної інфраструктури, розподіляючи їх на чотири категорії залежно від їх важливості та потенційного впливу на загальнодержавні чи локальні функції у разі їхньої дисфункції або зупинки. Перша категорія включає об'єкти, чия діяльність має вирішальне

значення для держави в цілому, здатність яких впливати на інші об'єкти критичної інфраструктури є суттєвою, та їхня недієздатність може спричинити національну кризу. Друга категорія охоплює об'єкти, життєво важливі для регіонів, зупинка яких може викликати регіональні кризи. Третя категорія стосується об'єктів, важливих для місцевих спільнот, чиє припинення діяльності може призвести до місцевих кризових ситуацій. Нарешті, четверта категорія визначає об'єкти, необхідні для підтримки локального життя, порушення в роботі яких може створити локальні проблеми. Ця класифікація сприяє більш ефективному плануванню заходів щодо забезпечення стабільності критично важливих функцій у суспільстві.

1.2 Загрози та ризики для об'єктів критичної інфраструктури

Присутність об'єктів критичної інфраструктури в будь-якій державі посилює необхідність забезпечення їх захисту, безпеки та витривалості перед обличчям многоаспектних загроз і ризиків. Ці об'єкти відіграють ключову роль у підтримці функцій і послуг, які є життєво важливими для безпечного існування та процвітання населення та держави [14]. Зокрема, в умовах глобального посилення екстремізму, тероризму та злочинності, важливість цих об'єктів лише зростає.

Однією з основних викликів для стійкості критичної інфраструктури є високий рівень зносу основних фондів на промислових об'єктах, середній показник якого досягає 60,3%. Це ставить під загрозу безпеку через високий ризик техногенних аварій, особливо на територіях, де розташовані об'єкти, що використовують у своїй діяльності значні кількості небезпечних речовин. Наслідки аварій на таких об'єктах можуть спричинити катастрофічні наслідки на рівні держави або регіону.

Також критичну ситуацію утворюють проблеми в житлово-комунальному секторі, де протяжність ветхих та аварійних водопровідних мереж складає понад 34%, а теплових та парових мереж — понад 18% від їх

загальної довжини по Україні. Такий стан речей призводить до значних втрат води та теплової енергії під час транспортування до споживачів, що, у свою чергу, веде до зростання тарифів і спричиняє соціальну нестабільність.

Наявність критичної інфраструктури у будь-якій країні представляє собою низку викликів для національної безпеки через потенційні ризики, пов'язані з її функціонуванням. Зокрема, порушення умов безпечної роботи цих об'єктів може призвести до серйозних наслідків. Ці порушення охоплюють широкий спектр дій, починаючи від фізичного захоплення об'єктів, як це було з енергетичними активами в Криму, що призвело до збереження їх функціональності, але зміни власності.

Далі, зупинка роботи об'єктів критичної інфраструктури може бути використана як засіб тиску для виконання політичних або економічних вимог, що може включати умови постачання енергоресурсів, викуп активів, або вплив на ринкові ціни. Крім того, розукомплектування обладнання та продаж його як металобрухт, особливо на окупованих територіях, як це відбувалось на Донбасі, є прикладом кримінального заробітку.

Фізичне знищення інфраструктури також може бути спрямоване на завдання критичної шкоди, збільшення витрат на відновлення або навіть неможливість доставки ресурсів. Перешкоджання діяльності з відновлення енергетичної інфраструктури може призвести до формування соціально-політичного невдоволення. Транспортна інфраструктура може бути використана для провокацій, як у випадку з трагедією рейсу MH17, або для блокування транзиту товарів через кордони [39, с. 62-76].

Крім цього, несанкціоновані втручання у роботу не лише енергетичної, а й інформаційно-комунікаційної та комунальної інфраструктури демонструють вразливість сучасних систем до зовнішніх і внутрішніх загроз. Це підкреслює важливість комплексного підходу до захисту і стійкості критичної інфраструктури в умовах зростаючих ризиків.

У контексті забезпечення національної безпеки та цілісності критичної інфраструктури, природні загрози та явища відіграють значущу роль. Серед

них метеорологічні умови такі як сильні снігопади, ожеледиця, хуртовини, зливи, град, заморозки, посухи, спека, урагани, шквали та смерчі, а також гідрологічні явища, зокрема повені, селі, паводки, підтоплення та цунамі, становлять серйозний виклик. Геологічні процеси, такі як зсуви, просідання ґрунтів та карстові обвали, також входять до цього списку. Частота метеорологічних загроз, зокрема обледеніння, підтоплень та посух, значно зросла в Україні за останні десятиліття. В контексті впливу на критичну інфраструктуру, найбільш руйнівними є гідрологічні загрози, особливо паводки [11].

Актуальність виявлення, оцінки ризиків та прогнозування надзвичайних ситуацій, які можуть завдати шкоди критичній інфраструктурі, стає все більш важливою. Ці заходи необхідні для захисту суспільних інтересів від можливих загроз національній безпеці. О.С. Бодрук висловлює думку, що загроза є реальною, але не фатальною можливістю заподіяння шкоди, яка може мати майнові, фізичні або моральні (духовні) наслідки для особистості, суспільства чи держави [22, с. 8]. Відповідно, стратегічне планування та превентивні заходи є ключовими для мінімізації потенційних збитків від цих загроз.

Необхідність формулювання поняття «загроза» в націобезпекознавстві обумовлена декількома ключовими аспектами. Перш за все, це панування диверсифікаційного підходу в дослідженні категорій національної безпеки, яке спонукає до глибшого аналізу та систематизації цієї категорії. Другий аспект полягає у недостатньо розробленому понятті «загроза» та в проблемі його відмежування від інших споріднених понять, таких як «небезпека», «виклик», «ризик», «фактор». Третє питання пов'язане з відсутністю цілісної проблеми формування категорійно-понятійного апарату в області націобезпекознавства, де категорійний ряд «моніторинг - загроза - небезпека - управління - система національної безпеки - національна безпека» відіграє центральну роль [15, с. 266]. Четверте підґрунтя — можливість створення на базі теоретичних розробок ефективної системи моніторингу та управління загрозами і небезпеками.

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

Об'єкти критичної інфраструктури займають центральне місце в економічному та соціальному житті багатьох країн. Протягом останніх двох десятиліть серед найважливіших галузей світової критичної інфраструктури були електроенергетичні системи, транспорт, водопостачання, харчування, сільське господарство та життєво важливі промислові підприємства. Сучасний розвиток додав до списку критичних секторів інформаційні та телекомунікаційні технології, засоби масової інформації, банківську справу та фінанси, а також навколишнє середовище.

Кожна країна визначає власні критерії для класифікації об'єктів у систему критичної інфраструктури згідно з внутрішньою національною політикою. Незважаючи на існування спільних європейських стандартів, кожен національний уряд має свободу самостійно оцінювати та визначати, які саме інфраструктурні об'єкти є критично важливими для держави. Найчастіше до таких об'єктів належать електроенергетичні системи, об'єкти енергопостачання, виробництво, транспортування та зберігання небезпечних речовин, транспортна та інформаційно-телекомунікаційна інфраструктура.

Загрози безпеці цих об'єктів можна класифікувати на фізичні загрози та кібератаки. Фізичні загрози переважно торкаються об'єктів, таких як трубопроводи, підстанції, склади і комунікаційні системи, а також промислові підприємства. Натомість, кіберзагрози ставлять під небезпеку системи

моніторингу та контролю, бази даних, функціональні системи, програмне забезпечення та автоматизовані виробничі засоби.

Кожен тип критичної інфраструктури має свої специфічні вразливості. Наприклад, енергетичні системи особливо вразливі через генератори та мережі розподілу. У випадку джерел енергії та розподільних мереж це може бути газ і нафтопроводи. У секторі небезпечних речовин вразливість становить транспортування та зберігання, а в транспорті та перевезеннях – критично важливими є аеропорти, мости та тунелі.

Сьогодні, у контексті забезпечення національної безпеки, особливу увагу слід приділити загрозам, які стосуються критичної інфраструктури. Серед основних викликів варто виокремити недостатній розвиток організаційно-технічних заходів, спрямованих на захист таких об'єктів, а також державних електронних інформаційних ресурсів. Це створює умови, при яких об'єкти вразливі перед лицем сучасних загроз.

Також серйозним викликом є брак кваліфікованих спроможностей у секторі безпеки і оборони, що необхідні для ефективного реагування на кіберзагрози, включаючи кібершпигунство, кібертероризм і кіберзлочинність. Ці загрози негативно впливають на стале функціонування критичної інфраструктури, порушуючи її роботу та створюючи додаткові ризики для державної безпеки.

Окрім технічних і спеціалізованих аспектів, важливо звернути увагу на затримки та неефективність дій органів державної влади та силових структур у відповідь на інциденти, пов'язані з пошкодженням критичної інфраструктури. Не завжди своєчасне та адекватне реагування, а також затягування процесу відновлення після інцидентів можуть суттєво погіршити наслідки загроз та збільшити їх вплив на національну безпеку.

З усіх цих причин, системний підхід до зміцнення захисту критичної інфраструктури є ключовим елементом стратегії національної безпеки, який вимагає як технічних, так і організаційних інновацій на всіх рівнях управління.

Сьогодні, коли безпека держави є критично важливою, зростає усвідомлення необхідності захисту об'єктів критичної інфраструктури. Реалізація стратегічного підходу у вирішенні питань, пов'язаних із забезпеченням їх безпеки, стає ключовим завданням для державних структур. Це включає ідентифікацію та аналіз ключових факторів, що спричиняють загрози для об'єктів критичної інфраструктури, а також розроблення та впровадження ефективних механізмів публічного управління, спрямованих на запобігання або мінімізацію негативних наслідків від таких загроз.

З плином часу деякі об'єкти, які раніше не визначались як критично важливі, можуть бути перекваліфіковані відповідно до змін у ризиковому ландшафті, що призводить до появи нових ризиків і ускладнення вже відомих загроз. Зокрема, дії проти критичної інфраструктури часто залишаються без винуватців, особливо коли йдеться про високотехнологічні кібератаки, де ідентифікація замовника або виконавця може бути надзвичайно складною.

Такі умови потребують від органів публічного управління безперервних зусиль у сфері виявлення ризиків та захисту об'єктів критичної інфраструктури. Необхідно створювати і вдосконалювати системи, які включають сучасні інструменти та методи для локалізації і запобігання потенційним загрозам, щоб забезпечити стале та безпечне функціонування цих життєво важливих об'єктів.

У сучасному світі питання захисту об'єктів критичної інфраструктури набуває особливої актуальності. Відповідно до міжнародних стандартів ISO 31000:2018, ризик розуміється як вплив невизначеності на цілі, який може мати як позитивні, так і негативні наслідки, та маніфестується через потенційні події, їх наслідки та ймовірність їх виникнення [51]. Ризики, пов'язані з критичною інфраструктурою, можуть створювати загрози для населення, майна, довкілля, а також загрози інформаційній безпеці та соціальним відносинам.

Управління ризиками вимагає комплексного підходу, який включає різноманітні механізми впливу:

1) Правові механізми включають створення нормативно-правової бази, що дозволяє формувати понятійний апарат і правове врегулювання, необхідне для ідентифікації та управління загрозами.

2) Організаційні механізми передбачають визначення інституцій, відповідальних за безпеку критичної інфраструктури, налагодження їх ефективної взаємодії з іншими організаціями.

3) Техніко-технологічні та програмні механізми спрямовані на створення технічних та програмних умов, які мінімізують ризики або зменшують негативний вплив їх матеріалізації.

4) Фінансові механізми обумовлюють формування фінансових резервів та забезпечення сталого фінансування заходів з управління ризиками.

Наукові підходи включають обґрунтування та вдосконалення принципів, методів та інструментів управління ризиками.

Військово-оборонні та розвідувальні заходи забезпечують протидію зловмисним діям, спрямованим на пошкодження критичної інфраструктури.

Інформаційні стратегії передбачають розробку та поширення інформації про ризики, а також моніторинг інформаційного простору.

Освітні програми спрямовані на підготовку та підвищення кваліфікації фахівців у галузі управління ризиками.

Дипломатичні ініціативи допомагають встановлювати міжнародні норми та вирішувати конфлікти, які можуть погіршити стан критичної інфраструктури.

Ці механізми дозволяють створити міцну основу для захисту від існуючих та потенційних загроз, забезпечуючи стабільність та безпеку критичної інфраструктури на різних рівнях.

Це дослідження не може вичерпно описати всі аспекти механізмів управління ризиками для об'єктів критичної інфраструктури (ОКІ), тому особлива увага приділяється окремим пріоритетним напрямам діяльності публічних органів у цій сфері. Спершу ми розглянемо ключові аспекти

формування правового поля, які стосуються регулювання викликів, пов'язаних з ОКІ.

Термін «критична інфраструктура» був вперше офіційно використаний в Україні у 2005 році у Рекомендаціях парламентських слухань з питань розвитку інформаційного суспільства, де Кабінету Міністрів було запропоновано розробити заходи щодо ідентифікації та захисту критичних інформаційних інфраструктур [29].

Другим значущим документом, що визначає стратегію відносно критичної інфраструктури, є Стратегія національної безпеки України «Україна у світі, що змінюється», затверджена Указом Президента від 12 лютого 2007 року №105. Цей документ визначає захист критичної інфраструктури, особливо у контексті паливно-енергетичного комплексу, та вказує на загрози еколого-техногенного та зловмисного характеру. Відтак, велике значення приділяється інформаційній безпеці, зокрема у контексті управління об'єктами критичної інфраструктури [38].

У 2015 році був прийнятий Указ Президента України, що затверджує рішення Ради національної безпеки і оборони України від 6 травня того ж року про Стратегію національної безпеки України. Згодом, згідно з Указом Президента №392/2020 від 14 вересня 2020 року, ця Стратегія була оновлена. Центральним елементом стратегії є принцип «Безпека людини – безпека країни» [30].

Оновлена версія Стратегії національної безпеки, затверджена у 2020 році, включає конкретні положення про загрози критичній інфраструктурі та визначає стратегічні напрямки дій для їх подолання [30]. Серед основних загроз вказано на погіршення технічного стану критичної інфраструктури, відсутність необхідних інвестицій у її оновлення та розвиток, несанкціоноване втручання у її діяльність, яке може мати фізичний та кібернетичний характер, а також тривалі конфлікти та часткову окупацію території України.

У третьому розділі Стратегії окреслено основні напрями зовнішньої та внутрішньої політики, спрямовані на забезпечення національних інтересів та

безпеки. Серед ключових завдань вказано створення ефективної системи безпеки і стійкості критичної інфраструктури, заснованої на чіткому розподілі відповідальності між її суб'єктами та розбудові державно-приватного партнерства [30].

У заключних положеннях стратегії визначено, що цей документ має стати основою для розробки інших стратегічних документів, таких як стратегія енергетичної безпеки, стратегія інформаційної безпеки та стратегія кібербезпеки [30].

У Стратегії забезпечення державної безпеки, прийнятій 16 лютого 2022 року за номером 56/2022, об'єкти критичної інфраструктури визначені як один із стовпів національної безпеки поряд із державним суверенітетом, конституційним ладом і територіальною цілісністю України, що підкреслює їхнє велике значення [31]. Стратегія визначає, що існує високий рівень загроз для об'єктів критичної інфраструктури, зокрема від розвідувально-підривної діяльності, зношення інфраструктур та відсутності інвестицій у їх оновлення.

Стратегія національної безпеки України також акцентує на необхідності удосконалення контррозвідувальних заходів та протидії спробам ворожого контролю над критичною інфраструктурою [31].

У листопаді 2021 року було прийнято Закон України «Про критичну інфраструктуру», який вводить чітке розмежування між ненавмисними і навмисними загрозами до безпеки таких об'єктів та визначає ризики пов'язані з кризовими ситуаціями [28]. Закон передбачає створення фундаментальних вимог до управління ризиками безпеки на об'єктах високої критичності та забезпечення координації відповідальних органів, зокрема в сферах, які контролює Національний банк України. Це охоплює фінансові послуги, платіжні системи та операторів інфраструктури [28].

Зазначений Закон також наголошує на важливості страхування ризиків, а також встановлює мінімальні ліміти відповідальності для страхування, що стосується об'єктів критичної інфраструктури, зокрема у сфері фінансових послуг. Кабінет Міністрів України затверджує перелік таких об'єктів, що

мають стратегічне значення, а в час воєнного стану основні повноваження переходять до Державної служби спеціального зв'язку та захисту інформації України.

Закон також підкреслює необхідність проведення наукових досліджень для вивчення впливу новітніх технологій на ризики та загрози для критичної інфраструктури, сприяючи таким чином розробці ефективних стратегій управління ними [28].

Хоча у прийнятому Законі України «Про критичну інфраструктуру» дано визначення багатьох ключових понять, таких як безпека критичної інфраструктури та кризова ситуація, саме поняття «ризики критичної інфраструктури» не отримало чіткого визначення. Натомість, закон визначає рамки для управління цими ризиками та інцидентами безпеки, а також розробляє стратегії протидії несанкціонованому втручанню.

Організаційний механізм в Україні залучає широкий спектр управлінських та виконавчих органів, включаючи місцеве самоврядування та спеціалізовані адміністрації. Однак, на практиці далеко не всі з цих органів активно займаються питаннями превенції загроз критичній інфраструктурі. Профілактичні заходи часто реалізуються на етапах залучення іноземних інвестицій, що демонструє підхід, аналогічний практиці в Ізраїлі.

В Ізраїлі консультативний комітет при Міністерстві фінансів відіграє ключову роль у визначенні національних інтересів іноземних інвестицій та їх впливу на національну безпеку. Комітет, складений з високопоставлених представників різних міністерств, включаючи оборону та національну безпеку, здійснює глибокий аналіз залучених інвестицій, і хоча його рекомендації є дорадчими, вони впливають на регуляторні рішення [69].

Слід вважати, що подібні дорадчі структури повинні бути створені і в Україні для аналізу загроз і ризиків критичної інфраструктури на всіх етапах реалізації проектів від інвестицій до розвитку, з метою забезпечення більшої стійкості та безпеки.

Сучасний розвиток технологій пропонує багато інноваційних рішень для ідентифікації, превенції та усунення загроз критичної інфраструктури. Однак процеси цифровізації несуть у собі також значний ряд проблем, співвідношення яких із користю від цифрових технологій часто є суперечливим. Зокрема, розвиток цифровізації зробив об'єкти критичної інфраструктури вразливішими перед лицем кіберзагроз, про що свідчать численні атаки. З огляду на це, у наукових колах вже виникають дискусії про настання так званої «кібер-зими».

Ілюстрацією вразливості критичної інфраструктури перед кібератаками є відома атака Stuxnet, яка була спрямована проти іранських ядерних об'єктів більше десяти років тому. Цей вірус, вразивши системи керування Siemens, змусив іранські центрифуги зазнати критичного збою, в той час як системи моніторингу були обдурені і показували нормальні показники роботи [43].

Також в травні 2020 року, з використанням спеціалізованої пошукової системи Shodan, було виявлено понад 112 000 промислових систем керування з відкритими портами, що свідчить про значне посилення загроз в умовах пандемії та дистанційної роботи [43].

В країнах з високорозвиненою промисловістю функціонує значна кількість промислових систем контролю (ICS), які моніторять стан від простих кондиціонерів до великих турбін [70]. Ці системи забезпечуються додатковими заходами безпеки, такими як віртуальні буфери («jump boxes») та управління трафіком через безпечні сервери. Серед використовуваних протоколів можна згадати BACnet, DNP3, EtherNet/IP, IEC 60870-5-104, MELSEC-Q, Modbus, S7 Communication, що демонструють широкий спектр можливостей для контролю та управління.

Проте, збільшення кількості «відкритих зон» у складних системах збільшує ризики їх порушення та кібернетичних атак, що безпосередньо загрожує національній безпеці.

В сучасному світі, де постійно зростає роль технологій, захист критичної інфраструктури від загроз стає все більш актуальним. З одного боку, техніко-

технологічні нововведення сприяють більш ефективному управлінню та контролю, з іншого – цифровізація підвищує вразливість до кібератак. Наслідки таких атак можуть бути катастрофічними, як показав приклад з вірусом Stuxnet, який зумів знешкодити іранські ядерні центрифуги, водночас обманюючи системи моніторингу про нормальний стан роботи [43].

З огляду на значний ріст кількості підключених до Інтернету промислових систем управління, які були виявлені за допомогою системи Shodan у 2020 році, стає зрозумілою критична необхідність розробки ефективних заходів безпеки [43]. В світі створено велику кількість промислових систем контролю (ICS), що дозволяють відслідковувати стан різноманітних об'єктів, від простих побутових приладів до великих промислових установок [70]. Заходи безпеки, такі як віддалений доступ і створення віртуальних буферних зон, сприяють зменшенню вразливостей.

Однак, важливо відзначити, що кількість «відкритих зон», які можуть стати мішенями для кібератак, збільшується разом із розширенням технологічних можливостей. Зростаюча залежність від технологій підсилює потенціал шкоди, яку можуть завдати зловмисники, що ставить перед державою важливі завдання розроблення всеохоплюючої стратегії захисту критичної інфраструктури від всіх можливих видів загроз.

1.3 Сучасні підходи до підвищення стійкості об'єктів критичної інфраструктури

У сучасному світі, де зростає залежність від складних технологій, підвищення стійкості об'єктів критичної інфраструктури стає пріоритетним завданням для забезпечення національної безпеки та стабільності держав. Стійкість критичної інфраструктури, що охоплює енергетичні системи, транспорт, комунікації, фінансові послуги, охорону здоров’я та багато інших секторів, є ключем до виживання національної економіки та збереження життєво важливих соціальних функцій.

Зміцнення безпеки та стійкості критичних інфраструктур є вирішальним завданням для органів влади, згідно з політикою США в області захисту важливих активів. В рамках цього плану акцент робиться на низці стратегій: профілактика, стримування, мінімізація та протидія можливим терористичним атакам або іншим загрозам, які можуть призвести до серйозних пошкоджень або зловживань критичною інфраструктурою. Також важливими є підготовка до надзвичайних ситуацій, оперативне реагування та швидке відновлення систем в разі їх пошкодження [66].

Так, безпека та стійкість критичних об’єктів тісно пов'язані з політичними завданнями, що сприяють сталому розвитку країни.

Термін «стійкість» часто зустрічається у науковій літературі, хоча його точне визначення залишається предметом наукових дебатів. Він використовується у багатьох дисциплінах, включаючи економіку, екологію та соціологію, та визначається у офіційних документах міжнародних організацій, таких як Європейська Комісія.

Попри різні підходи до інтерпретації стійкості, вона загалом вказує на здатність системи швидко відновлюватися після катастроф до передбачуваного рівня функціонування [59].

C. Holling визначив стійкість як міру витривалості системи, яка дозволяє їй адаптуватися до змін, зберігаючи стабільні взаємовідносини між складовими [57].

Y. Haimes розглядає стійкість у контексті системної інженерії як здатність системи витримувати значні порушення без критичних втрат, відновлюючись протягом прийнятного часу і з мінімальними витратами [55, с. 498–501].

Дослідження C. Nan, G. Sansavini та інших націлені на аналіз стійкості інженерних інфраструктур, підкреслюють, що стійкість як «система систем» базується на здатності внутрішніх та зовнішніх сил ефективно опиратися будь-яким впливам, що можуть раптово чи поступово руйнувати систему.

Важливою є здатність зменшити і тривалість, і величину зниження продуктивності системи до стану, який може бути нормалізований [61, с. 35–53].

C. Folke у своїх дослідженнях системної вразливості і стійкості у соціально-екологічних системах вказує на стійкість як на мислення, що може орієнтувати лідерів та організації до розуміння важливих аспектів переходу суспільства до стійкого розвитку [54, с. 253–267].

Альянс стійкості, заснований у Флоридському університеті та Інституті Байєра за участю C. Holling, перетворився на міжнародну дослідницьку платформу, зосереджену на соціально-екологічних динаміках. Організація вивчає стійкість як можливість системи адаптуватися, переорганізуватися, зберігаючи при цьому свою ідентичність після порушень, а також вчитися з досвіду для подальшого відновлення [68].

Окремо варто згадати поняття «Robustness», яке описує здатність системи витримувати варіативність зовнішніх умов без серйозних втрат функціональності [37].

В контексті двоїстої природи стійкості, виділяють статичну стійкість — це базова здатність системи відновитися до прийнятного рівня після збоїв, та динамічну стійкість — це швидкість і ефективність процесу відновлення. Таке бачення допомагає краще зрозуміти, як інфраструктура може адаптуватися до змінних умов, включаючи технічні несправності та екологічні катастрофи, забезпечуючи при цьому швидке відновлення з мінімальними витратами.

В розвинених країнах термін «стійкість» часто застосовується у важливих нормативних та стратегічних документах, що мають на меті впровадження публічної політики у сферах безпеки, захисту та стійкого розвитку. Ініціатива спочатку зосереджувалась на захисті критичних інфраструктур, як це було встановлено в Європейській програмі. Проте, в офіційних документах поступово почала з'являтись концепція стійкості, підкреслюючи, що не всі інфраструктури можуть бути повністю захищені від

усіх видів загроз. Визначення пріоритетних напрямків захисту та фокусування на критичних об'єктах було ключовим елементом таких програм [50].

З 2000-х років стійкість стала популярною темою наукових досліджень та аналізів у сфері публічної політики, раніше вона була використана екологами з 1970-х. Це призвело до заміни акценту з чистого захисту на ширше розуміння стійкості в дослідженнях критичної інфраструктури [54; 61].

Ця тенденція була особливо помітна в урядових політиках США. Директива президента 2013 року чітко визначає стійкість як здатність адаптуватися та відновлюватися від збоїв, аварій, нападів та природних катастроф, підкреслюючи здатність протистояти цим загрозам і швидко відновлюватись [64].

Також, офіційні документи ЄС згадують про стійкість, особливо у контексті Європейської програми захисту критичної інфраструктури. Від 2012 року стійкість почала відігравати значущу роль, що було визнано у Звіті ЄС 2014 року про результати тестування стійкості КІ [51; 65].

У 2016 році на Варшавському саміті НАТО було встановлено **сім** основних вимог до стійкості, які включають забезпечення енергії, транспортних систем, комунікацій, водопостачання, урядової діяльності, контролю за переміщенням людей та допомоги в разі стихійних бід [52].

Європейський Союз визначив стійкість як пріоритет у своїй стратегії «Сильніша Європа», підкреслюючи важливість стійкості для демократичного розвитку, безпеки та процвітання, закладаючи основу для гнучкого суспільства, заснованого на демократії і довірі до інститутів.

Міжнародна стратегія Об’єднаних Націй визначає «стійкість» як здатність системи, громади або суспільства опиратися небезпекам, абсорбувати втручання та ефективно відновлюватися від їх наслідків, зберігаючи та відновлюючи основні структури та функції (UNISDR) [73]. Це означає, що стійкість включає в себе заходи захисту та охоплює всі аспекти традиційного управління кризами, включно з профілактикою, пом’якшенням,

готовністю до кризи, реагуванням під час кризи, а найважливіше — відновленням після кризи.

Стійкість можна розділити на три сфери діяльності: суспільну, організаційну та технологічну. У суспільній стійкості ключові ролі відіграють органи влади, місцеве самоврядування, територіальні громади, а також окремі особи, де стійкість часто асоціюється з цивільним захистом. В організаційній стійкості головними суб'єктами є підприємства та організації, що відіграють важливу роль у забезпеченні взаємозв’язків між різними елементами критичної інфраструктури. В технологічній стійкості суб'єктами є оператори об'єктів критичної інфраструктури та зацікавлені сторони, відповідальні за управління матеріальними, інформаційними та фінансовими потоками і безпекою.

У Скандинавських країнах стійкість також перейшла від академічного обговорення до офіційної політичної документації. Данське агентство з надзвичайних ситуацій між 2006 та 2010 роками розробило доповіді про національну вразливість, які фокусувалися на аналізі вразливості як зворотного поняття до стійкості. Ці доповіді підкреслюють, що система є вразливою, коли вона не має достатньої здатності планувати, запобігати, реагувати або відновлюватися після реалізованих загроз. Національний профіль ризику 2013 та 2017 років зосереджується на стійкості, використовуючи модель типового циклу управління кризами і акцентуючи на етапах запобігання, готовності та реагування. Ризики розподіляються за типами подій та охоплюють такі аспекти, як здоров’язабезпечення, погодні умови та політична безпека [46; 47].

У Королівстві Норвегія, поняття стійкості критичної інфраструктури (КІ) почало з'являтися в офіційних документах, хоча й не в явній формі, і особливо після теракту в Осло у 2011 році. Міністерство юстиції та громадської безпеки оприлюднило звіт про громадську безпеку, який включав згадку про КІ, але не обговорював стійкість як виразну концепцію. Однак, у Королівському указі 2012 року вже було зазначено, що відомства повинні

аналізувати ризики, вразливість і стійкість своїх секторів, використовуючи національний аналіз ризиків від Норвезької дирекції цивільного захисту [49; 60]. Цей підхід вказує на зростаючу увагу до питань стійкості, навіть якщо термін «стійкість» явно не використовувався.

У Великій Британії, уряд прагне покращувати планування і збільшувати інвестиції для прискорення втілення проєктів, які сприяють підвищенню інфраструктури. Впровадження Національного плану розвитку інфраструктури засвідчує зосередження уваги на стійкості та безпеці КІ, де ідентифікація критичних об'єктів розглядається як ключ до оптимального розподілу ресурсів. Уряд разом із регуляторами і промисловістю має на меті забезпечити інвестиції, що враховують потреби в безпеці та стійкості [63].

Тим часом, Австралія звернула особливу увагу на стійкість КІ, основуючись на Стратегії стійкості КІ уряду Австралії (AGCIRS) 2010 року. Стратегія розробляється з огляду на взаємозалежності між секторами та мережами КІ, акцентуючи на необхідності координованого планування, гнучкості та своєчасного відновлення після перебоїв чи катастроф. Важливість співпраці між бізнесом та урядом підкреслюється як засіб ефективного управління стійкістю КІ [44].

Ці приклади показують, як різні країни включають поняття стійкості у свої стратегії управління критичною інфраструктурою, кожна з яких адаптує підходи відповідно до своїх національних потреб та контекстів.

У контексті України, необхідність модернізації підходів до управління захистом критичної інфраструктури (КІ) є особливо актуальною. Це пов'язано з недостатністю існуючих нормативних, організаційних та технологічних інструментів, що підтримують безпеку та стійкість КІ. Зарубіжний досвід вказує на ефективність інтегрованого управління через єдиний державний орган, який спрощує координацію та підвищує рівень відповідальності та підзвітності. Наприклад, у США функції координації захисту КІ покладені на Міністерство внутрішньої безпеки, у Великій Британії — на Центр захисту національної інфраструктури, в Іспанії — на Національний Центр з захисту КІ,

а в Польщі та Норвегії існують відповідні урядові центри безпеки та цивільного захисту.

У зв'язку з цим, Україні слід розглянути можливість створення аналогічної установи, що забезпечувала б координацію дій різних відомств у ситуаціях, що стосуються безпеки КІ. Такий орган міг би впроваджувати стратегічні рішення щодо стійкості КІ та здійснювати комплексний аналіз та прогнозування загроз. Незалежність такої установи від інших відомств дозволила б виконувати її функції об'єктивно та ефективно, не втручаючись в організаційну структуру тих, хто вже залучений до захисту КІ.

Цей підхід не лише оновить законодавчу базу, а й дозволить створити ефективне партнерство між державним та приватним секторами, враховуючи, що значна частина КІ в Україні належить приватним компаніям. Така модель співпраці сприятиме розробці стандартизованих методів оцінювання ризиків та загроз, що є критично важливим для національної безпеки, економічного процвітання та соціального благополуччя країни.

У Канаді Національна стратегія захисту критичної інфраструктури вимагає спільних зусиль від державних органів, приватного сектору та громадян, щоб забезпечити належний захист і стійкість у відповідь на надзвичайні ситуації, особливо у перші 72 години після їх настання. Така інтеграція сприяє координації зусиль і підвищує ефективність реагування на загрози. Уряд Канади розвиває партнерство з операторами і власниками об’єктів критичної інфраструктури, забезпечуючи їх важливою інформацією про ризики і загрози та плани дій на випадок надзвичайних ситуацій.

У Європейському Союзі, зокрема через Європейський експертний центр з питань публічно-приватного партнерства (EPEC), підтримується залучення приватного сектору до захисту критичної інфраструктури. Це включає підтримку в розбудові інституційного потенціалу та контроль за розвитком публічно-приватних партнерств у різних секторах. Подібні підходи дозволяють мінімізувати бюджетні обмеження і залучати приватні інвестиції для надання публічних послуг та розвитку інфраструктури.

Проєкти публічно-приватного партнерства в Європі часто включають довгострокові контракти, де приватні партнери несуть значну частину ризиків і відповідальності за проектування, фінансування, будівництво, експлуатацію та обслуговування інфраструктури. Водночас, держава бере на себе регуляторні та політичні ризики, забезпечуючи оплату на основі ефективності приватного партнера.

Впровадження публічно-приватних партнерств дозволяє залучати приватні фінанси для виконання державних проєктів, що можуть включати різні сектори, від транспорту до соціального житла та охорони здоров'я. Ці проєкти можуть бути структуровані для досягнення широкого спектра цілей і забезпечити значні переваги для суспільства, навіть враховуючи високі витрати та потенційні ризики.

Отже, досвід Канади та ЄС показує, що впровадження комплексних програм захисту критичної інфраструктури через державно-приватне партнерство може забезпечити не тільки захист, але й стійкість управління критичною інфраструктурою, а також сприяти розвитку економіки та підвищенню безпеки суспільства в цілому.

Європейський Союз оновив свої стратегічні напрямки у сфері забезпечення діяльності критичної інфраструктури (КІ) і виконання життєво важливих послуг. Нові політичні орієнтири та завдання, розроблені Єврокомісією та державами-членами, були представлені у вигляді Рекомендацій Ради ЄС, які покликані підсилити зусилля ЄС у зміцненні стійкості КІ. Нові стратегії відображають прагнення ЄС до розвитку механізмів, що базуються на ринкових принципах і стимулюють операторів КІ до добровільного посилення захисту своїх об'єктів.

Для підтримки цих ініціатив планується створення комплексу інструментів, спрямованих на допомогу державам-членам ЄС та операторам КІ. Ці інструменти включають методичну та консультативну підтримку, підвищення кваліфікації персоналу, проведення стрес-тестів, а також

координацію дій у разі кризових ситуацій та фінансову підтримку відповідних ініціатив.

Для України, яка прагне інтеграції у європейські структури, важливо врахувати ці нові політичні пріоритети ЄС у своїх стратегіях забезпечення безпеки критичної інфраструктури, адаптувавши національні законодавчі та регуляторні рамки згідно з європейськими вимогами.

Відповідно до нових загроз та викликів, зокрема через військову агресію РФ проти України, Європейський Союз акцентував на необхідності зміцнення координації між державами-членами, національними урядовими органами, інституціями ЄС та операторами критичної інфраструктури для забезпечення безперебійного надання життєво важливих послуг.

У грудні 2022 року Рада ЄС впровадила Рекомендації, які покликані сприяти скоординованому підходу до підвищення стійкості критичної інфраструктури. Ці рекомендації включають розробку інструментів і методик для ефективної взаємодії на рівні ЄС з метою підвищення готовності та швидкого реагування на інциденти, які можуть перешкоджати наданню основних послуг на внутрішньому ринку.

Водночас, у тому ж місяці Рада ЄС прийняла нову Директиву щодо стійкості критичних об’єктів (Директива CER), що відкрила нову фазу у політиці безпеки критичної інфраструктури ЄС. На початку 2023 року було оголошено про координацію зусиль між ЄС і НАТО для додаткового зміцнення стійкості цієї інфраструктури.

Ці рішення відображають новий крок у розвитку політики ЄС у напрямку забезпечення безпеки і стійкості критичної інфраструктури.

Рекомендації Ради ЄС визначають ряд цілеспрямованих заходів на рівні Євросоюзу та на національному рівні, які спрямовані на покращення стійкості критичної інфраструктури. Ці зусилля зорієнтовані на здатність виявляти потенційні загрози та ризики, покращення готовності до кризових ситуацій, зміцнення реагування на небезпеки та розвиток міжнародної співпраці у цій сфері.

Імплементація цих Рекомендацій спрямована на розширення можливостей Євросоюзу щодо захисту критичної інфраструктури. Директива CER встановлює чіткі норми та інструменти для моніторингу та регулювання, вводить нові обов'язки для держав-членів та операторів, а також розширює перелік регульованих секторів критичної інфраструктури. Крім того, оновлена Директива NIS2 вводить комплексні вимоги у сфері кібербезпеки по всіх відповідних секторах. Новий законодавчий акт зобов'язує Єврокомісію взяти на себе лідируючу роль у координації і надає їй відповідні повноваження.

Зміцнення політики ЄС у цій області має на меті підвищення здатності держав-членів до забезпечення надійності послуг, які відіграють критичну роль у підтриманні основних суспільних функцій, економічної активності, громадського здоров'я, безпеки та екологічної сталості.

Посилення захисту критичної інфраструктури ЄС, особливо від антропогенних загроз, визнано одним із ключових напрямків у безпековій стратегії Союзу. Звернено увагу на важливість приділення особливої уваги транскордонній інфраструктурі, оцінювання ризиків та поглиблення співпраці між державами-членами для аналізу загроз, а також обміну інформацією про виявлені вразливості і розробку відповідних реакцій.

Важливою є також інтенсифікація міжнародних зусиль для ефективного вирішення ризиків, що виникають у зв'язку з експлуатацією критичної інфраструктури, як у межах ЄС, так і за його межами. Це передбачає тісну взаємодію між державами-членами, Єврокомісією і Високим представником ЄС із закордонних справ та політики безпеки [36].

Висновки до розділу 1

1. Історичний аналіз підтверджує, що кожне суспільство в усі часи зазнавало зовнішніх та внутрішніх загроз. Форми та цілі цих загроз змінювалися залежно від рівня економічного, соціального та технологічного розвитку, а наслідки часто були катастрофічними, включно з людськими жертвами та матеріальними втратами. Історично, основною метою агресора

було знищення критично важливих об'єктів суспільства, таких як транспортні мережі та системи водопостачання, що були вирішальними для підтримки життєдіяльності держав. Згодом, з розвитком технологій, особливо в інформаційній сфері, з'явились нові види загроз, такі як кібератаки на критичну інфраструктуру. Сучасні війни часто ведуться з використанням гібридних методів, які включають комбінації конвенційної зброї, партизанських дій та терористичних актів.

Захист критичної інфраструктури в сучасному світі вимагає комплексного підходу, який включає фізичний захист, кіберзахист та готовність до різних видів надзвичайних ситуацій. Враховуючи глобалізацію та взаємозалежність національних інфраструктур, потребується також міжнародна співпраця для захисту від загроз, які мають транснаціональний характер. Визначення «критичної інфраструктури» постійно оновлюється і розширюється, включаючи не тільки фізичні об'єкти, але й важливі нематеріальні аспекти, такі як програмне забезпечення та дані, що визначають стабільне функціонування економіки та суспільства. Враховуючи динамічний характер загроз та їхній потенційний вплив на соціально-економічний розвиток та національну безпеку, сучасне законодавство повинно бути гнучким і здатним швидко адаптуватися до нових викликів.Класифікація об'єктів критичної інфраструктури відображає їх важливість і роль у підтримці стабільності та функціонування держави і суспільства. Об'єкти критичної інфраструктури можуть включати елементи фізичної інфраструктури, такі як транспортні мережі, енергетичні системи, системи водопостачання та комунікаційні вузли. Крім того, до критичної інфраструктури належать і кібернетичні системи, які забезпечують управління, контроль та захист важливих інформаційних потоків. Відмова чи пошкодження цих систем може призвести до серйозних наслідків для національної безпеки, економіки та здоров'я громадян. Визначення інфраструктурних об'єктів як критичних передбачає, що їх ушкодження або дестабілізація може мати широкомасштабні

негативні наслідки на національному або навіть міжнародному рівні, тому їх захист є пріоритетом для державних органів.

2. Аналізуючи сучасні умови управління ризиками та захисту об'єктів критичної інфраструктури, можна зазначити, що динаміка зміни загроз та розвиток технологій зумовлюють постійну адаптацію захисних механізмів. Події, що стосуються критичної інфраструктури, особливо з урахуванням кібератак, підкреслюють необхідність інтенсифікації зусиль у цих напрямках. Особлива увага приділяється не тільки фізичному захисту, але й кібербезпеці, що стає ключовим у контексті збереження функціональності і надійності систем управління.

Прогрес у цифрових технологіях, хоча і пропонує нові можливості для ефективного управління і моніторингу, також збільшує потенціал для кіберзлочинності, що може мати серйозні наслідки для національної безпеки. Це вимагає розробки комплексних стратегій, що включають законодавчі, технологічні, фінансові та освітні ініціативи для посилення резистентності критичної інфраструктури. Зокрема, важливість інформаційного обміну між державними органами та приватним сектором, а також міжнародне співробітництво, що дозволяє ефективно реагувати на транснаціональні загрози.

Також актуальним є розвиток імплементації міжнародних стандартів та практик управління ризиками, таких як ISO 31000:2018, що сприяє створенню уніфікованих підходів до оцінки, моніторингу та реагування на ризики, здатних вплинути на критичну інфраструктуру. Визначення чітких відповідальностей та ролей серед усіх зацікавлених сторін, у тому числі у сфері кібербезпеки, є суттєвим для забезпечення координованих та ефективних заходів безпеки.

3. Сучасні підходи до підвищення стійкості об'єктів критичної інфраструктури акцентують на інтеграції стратегій профілактики, стримування, мінімізації ризиків та ефективного відновлення після можливих аварій або атак. Важливими є також підготовка до надзвичайних ситуацій та

оперативне реагування. Стійкість об'єктів критичної інфраструктури, як енергетичних систем, транспорту, комунікацій та інших ключових секторів, є фундаментальною для забезпечення національної безпеки та стабільності держав, відновлення економіки та підтримки життєво важливих соціальних функцій.

РОЗДІЛ 2. ПРАКТИЧНІ АСПЕКТИ ПІДВИЩЕННЯ СТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1 Аналіз існуючого стану захищеності об'єктів критичної інфраструктури в Україні

Забезпечення цивільної безпеки та захист об'єктів критичної інфраструктури (КІ) стали ключовими питаннями в Україні, особливо після повномасштабного вторгнення Росії, що почалося 24 лютого 2022 року. Ця подія значно змінила підходи та вимоги до національної системи захисту КІ, висвітливши низку критичних недоліків та вразливостей, які потребують негайного перегляду та удосконалення.

Від початку конфлікту, Україна зіткнулася з масштабними та координованими атаками на свою інфраструктуру, що включають не лише фізичні удари по об'єктах енергетики, транспорту та зв'язку, але й кібернетичні атаки, які спрямовані на дестабілізацію внутрішньої стабільності та підрив державних функцій. Такі атаки підкреслили критичну потребу в розробці більш ефективних механізмів реагування та відновлення після надзвичайних ситуацій.

Аналізуючи існуючий стан КІ в Україні, можна констатувати, що до війни багато зусиль було спрямовано на модернізацію та підвищення фізичної стійкості ключових об'єктів. Проте, заходи були неоднорідні та не завжди систематичні, що частково пояснюється обмеженими ресурсами та складнощами в координації між різними рівнями управління та приватним сектором, який володіє значною частиною КІ.

З моменту ескалації конфлікту було вжито низку заходів для зміцнення обороноздатності критичних об'єктів, зокрема через введення жорсткіших стандартів безпеки, підвищення готовності до кіберзагроз та залучення міжнародних партнерів для обміну досвідом та ресурсами.

Україна ініціює розробку системи захисту своєї критичної інфраструктури, ґрунтуючись на передових міжнародних практиках та вимогах європейського законодавства. Вивчення та адаптація європейських директив, таких як NIS 2 (EU 2022/2555) та RCE (EU 2022/2557), відбувається у співпраці з державами, що уже розпочали цей процес. Україна також здійснила кроки взаємодії з Американською агенцією з кібербезпеки (CISA), зокрема підписавши меморандум про співпрацю та організувавши тренінги згідно з їх методиками.

Паралельно, триває формування правової бази, потрібної для цих цілей. Вже створено секторальні каталоги об'єктів критичної інфраструктури (ОКІ), і незабаром планується ухвалення урядової постанови про процедуру ведення Реєстру критичної інфраструктури, який включатиме дані про ОКІ, включно з реєстраційними номерами, формами власності та основними діяльностями.

Відповідальність за категоризацію і подання даних до Реєстру покладена на секторальні органи та операторів ОКІ. Оператори критичної інфраструктури також несуть пряму відповідальність за її захист.

Ключові установи держави, як-от Збройні сили України, Служба безпеки України та Держспецзв'язку, беруть активну участь у відповідях на кризові ситуації, спрямовані на забезпечення безпеки критичної інфраструктури, такі як ракетні обстріли, диверсії та кібератаки.

Уповноважений орган координує зусилля усіх учасників національної системи захисту, формулюючи та реалізуючи державну політику в цій сфері, і виступає представником інтересів критичної інфраструктури у владних структурах.

Продовжується робота над законодавчим урегулюванням процесів паспортизації ОКІ та розробки загроз національного масштабу [41].

Дослідження українського законодавства щодо забезпечення безпеки та правового режиму функціонування критичної інфраструктури під час особливих умов, зокрема під час воєнного стану, виявило, що ці аспекти регулюються наступними законами: «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», «Про функціонування єдиної транспортної системи України в особливий період», «Про оборону України», «Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України», «Про державну таємницю», «Про місцеве самоврядування в Україні», «Про місцеві державні адміністрації», «Про основні засади забезпечення кібербезпеки України», «Про національну безпеку України».

Закон України «Про критичну інфраструктуру» встановлює визначення: «безпека критичної інфраструктури – стан захищеності критичної інфраструктури, за якого забезпечуються її функціональність, безперервність діяльності, відновлюваність, цілісність та стійкість» [28]. Цей закон також окреслює основні принципи створення системи захисту критичної інфраструктури та ефективності її роботи, особливо в умовах воєнного стану, включаючи: завдання державної політики у цій сфері; структуру керування такою системою; категорії критичності об'єктів; реєстр критичної інфраструктури; процедури паспортизації об'єктів; суб'єкти системи захисту критичної інфраструктури; режими її функціонування; уповноважений орган у цій сфері; функціональні та секторальні органи; місцеві виконавчі органи, у тому числі військово-цивільні адміністрації; завдання, права та обов'язки операторів; моніторинг безпеки; взаємодія різних систем захисту у сфері національної безпеки; державно-приватне партнерство, парламентський контроль, громадський нагляд; відповідальність за порушення законодавства; міжнародне співробітництво у сфері захисту критичної інфраструктури.

З введенням воєнного стану в Україні відбулись значні зміни у законодавчих актах, що стосуються регулювання об'єктів критичної інфраструктури, адаптуючи їх до нових умов. Серед оновлених нормативних документів:

– Постанова КМУ «Деякі питання об’єктів критичної інфраструктури», яка встановлює «Порядок формування переліку об’єктів критичної

інформаційної інфраструктури» та «Порядок внесення об’єктів критичної інформаційної інфраструктури до державного реєстру об’єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування» [6];

– Постанова КМУ «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури», включає Перелік базових вимог для кіберзахисту [25];

– Постанова КМУ «Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури», визначає Акт оцінки стану захищеності об’єкта критичної інфраструктури [27];

– Розпорядження КМУ «Про схвалення Концепції створення державної системи захисту критичної інфраструктури», оновлює стратегічний підхід до захисту систем, об'єктів та ресурсів, критичних для держави [32];

– Постанова КМУ «Деякі питання ідентифікації об’єктів підвищеної небезпеки», визначає процедуру ідентифікації та ведення обліку таких об’єктів, а також починає формування Державного електронного реєстру об’єктів підвищеної небезпеки [5];

– Постанова Правління НБУ «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», описує перелік критичних об’єктів у банківській системі [26];

– Постанова КМУ «Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України», регулює створення відповідного центрального органу виконавчої влади [33];

– Постанова КМУ «Деякі питання проведення зовнішнього аудиту діяльності уповноваженого органу у сфері захисту критичної інфраструктури України», задає рамки для складення звіту про зовнішній аудит Рахунковою палатою [7].

Ці оновлення правової бази критично важливі для забезпечення стійкості інфраструктури в умовах постійної загрози воєнних дій.

Всі ці заходи демонструють стратегію державної політики, спрямовану на захист та оперативне відгукування на загрози, які можуть призвести до ушкоджень або руйнування об'єктів критичної інфраструктури. Ефективна реалізація цієї стратегії вимагає різногалузевої консолідації ресурсів. Згідно з діючим законодавством, за критичні сектори інфраструктури відповідають такі уповноважені органи державної влади: Міністерство енергетики відповідає за паливно-енергетичний комплекс, Міністерство цифрової трансформації — за інформаційний сектор, Міністерство розвитку громад і територій України — за системи життєзабезпечення, Міністерство економіки — за харчову промисловість та агропромисловий комплекс, Міністерство охорони здоров'я — за охорону здоров'я, Національна комісія з цінних паперів та фондових ринків — за ринки капіталу та організовані товарні ринки, Міністерство інфраструктури — за транспорт і пошту, Міністерство з питань стратегічних галузей промисловості — за промислові галузі, Міністерство внутрішніх справ — за цивільний захист населення та територій, Міністерство фінансів — за фінансовий сектор. Окрім того, воєнний період мобілізує для захисту критичної інфраструктури такі органи виконавчої влади, як Національна поліція України, Міністерство з надзвичайних ситуацій, Служба безпеки України, Національна гвардія, Збройні сили України, військові адміністрації, Державна служба спеціального зв’язку та захисту інформації, Державна інспекція ядерного регулювання України.

Військовий контекст висуває підвищені вимоги до контррозвідувальної, контртерористичної та контрдиверсійної безпеки критичної інфраструктури, зокрема у секторах енергетики та ядерної енергетики, нафтогазовій галузі, харчовій промисловості, ІТ та електронних комунікаціях, системах життєзабезпечення, агропромисловому комплексі, транспорті, пошті, зв'язку, медичній сфері, стратегічно важливих сферах національного господарства, а також у банківському секторі. Основними загрозами для стабільності та

безпеки цих секторів є кібератаки, терористичні акції та диверсії, військові операції, які можуть спричинити аварії на об'єктах підвищеної небезпеки та, відповідно, викликати надзвичайні ситуації регіонального, державного чи глобального масштабу.

Воєнні дії, що проводяться на території України збройними силами країни-агресорки, не оминули навіть об'єкти ядерної енергетики, такі як Запорізька та Південноукраїнська АЕС, створюючи значні ризики не тільки для країни, а й для міжнародної безпеки.

Ракетні та артилерійські обстріли мали величезний вплив на безпеку об'єктів критичної інфраструктури, особливо в енергетичному секторі. Пошкодження отримали гідроелектростанції, такі як Дніпровська, Кременчуцька, Київська, Каховська, а також теплові електростанції: Київська, Трипільська, Харківська, Старобешівська, Слов'янська, Миронівська, Луганська, Курахівська, Зуївська, Зміївська, Запорізька, Вуглегірська.

Важливі інфраструктурні об'єкти, що підтримують життєдіяльність населення — як електромережі, системи водопостачання, тепло- та газопроводи, телефонні лінії — постійно зазнають обстрілів. Найбільше це торкається Запорізької, Херсонської та Миколаївської областей, які включають окуповані, деокуповані та активні зони бойових дій.

Через бойові дії також серйозно постраждали портові споруди, ключові транспортні артерії, мости, переправи, промислові об'єкти, нафто- та газопроводи, а також інші важливі елементи критичної інфраструктури по всій Україні.

Уряд України здійснив додаткове виділення коштів з резервного фонду держбюджету, спрямованих на фінансування відновлення пошкоджених внаслідок воєнних дій, диверсій, та терористичних актів, об'єктів критичної інфраструктури, пошкоджених внаслідок агресії Російської Федерації. Серед регулятивних документів, ухвалених в цьому контексті, можна відзначити Постанову КМУ «Про внесення змін до Порядку виконання повноважень Державною казначейською службою в умовах воєнного стану», Постанову

КМУ «Про деякі питання здійснення оборонних та публічних закупівель товарів, робіт і послуг у воєнний час», Розпорядження КМУ «Про виділення коштів для фінансової підтримки комунального підприємства “Облводоканал” Запорізької обласної ради», Постанова КМУ «Про деякі питання отримання, розподілу, використання та обліку гуманітарної допомоги для енергетики під час воєнного стану» та інші. Такі значні пошкодження об'єктів національної мережі критичної інфраструктури вимагають міжнародного реагування та застосування ефективних фінансових санкцій.

Наразі триває законодавча робота щодо удосконалення правового регулювання цих питань. У сфері державної регіональної політики та відновлення критичної інфраструктури в умовах воєнного стану діє низка законів України, серед яких: «Про внесення змін до деяких законодавчих актів України щодо засад державної регіональної політики та політики відновлення регіонів і територій», «Про засади внутрішньої і зовнішньої політики», «Про місцеві державні адміністрації», «Про місцеве самоврядування в Україні», «Про регулювання містобудівної діяльності», «Про транскордонне співробітництво», «Про державне прогнозування та розроблення програм економічного і соціального розвитку України», «Про державні цільові програми», «Про Генеральну схему планування території України» та інші. Запропоновані заходи спрямовані на підвищення ефективності та прискорення робіт з відновлення конкретних об'єктів критичної інфраструктури по всій країні.

Також обговорюється внесення в законодавство положень про застосування санкцій за порушення безпекових норм щодо об'єктів критичної інфраструктури, включно з можливістю введення дисциплінарних, адміністративних і кримінальних заходів примусу стосовно відповідальних осіб, а також фінансових санкцій або обмежень для юридичних осіб [17, с. 71–72].

Стан захищеності об'єктів критичної інфраструктури визначається як ключовий аспект національної безпеки країни. У зв'язку з військовими

конфліктами, суттєві проблеми виникають з фінансовим та матеріально-технічним забезпеченням постраждалих об'єктів критичної інфраструктури. Відповідно, було оперативно внесено зміни до нормативно-правової бази, що сприяло створенню ефективних умов для функціонування та швидкого відновлення цих об'єктів в умовах воєнного стану. Ці заходи стали фундаментом для розробки продуктивних механізмів, які забезпечують захист національних інтересів у сфері безпеки України.

2.2 Розробка рекомендацій щодо підвищення стійкості об'єктів критичної інфраструктури

Для підвищення стійкості об'єктів критичної інфраструктури в Україні, особливо в умовах військових загроз, можна розробити комплексний підхід, який включатиме наступні рекомендації:

1. Для підвищення стійкості об'єктів критичної інфраструктури особливу увагу слід приділити посиленню їхнього фізичного захисту. Це передбачає встановлення міцніших захисних бар'єрів та загороджень, які можуть ефективно обмежити доступ до об'єктів ззовні і таким чином ускладнити проникнення потенційних зловмисників. Паралельно з цим, важливим аспектом є модернізація систем відеоспостереження та охорони, яка включає оновлення камер високої роздільної здатності та покращення програмного забезпечення для кращого моніторингу та аналізу ситуацій в реальному часі. Це дозволить оперативно реагувати на будь-які спроби несанкціонованого доступу чи інші підозрілі дії.

Також значне місце в стратегії захисту відіграє покращення протипожежних заходів та систем аварійного реагування. Важливо забезпечити, щоб всі системи пожежогасіння були належно обслуговувані та повністю функціональні, а персонал регулярно проходив навчання з пожежної безпеки. Вдосконалення систем аварійного реагування передбачає

встановлення чітких процедур евакуації та швидкого реагування на аварії, що допоможе мінімізувати ризики для здоров'я та життя персоналу, а також знизити потенційні втрати від надзвичайних подій.

Ці заходи, реалізовані разом, забезпечать комплексне підвищення безпеки об'єктів критичної інфраструктури, значно зменшуючи ризики, пов'язані з військовими діями, терористичними актами, техногенними катастрофами та іншими потенційними загрозами.

2. У контексті посилення кібербезпеки критичної інфраструктури, важливо зосередитися на комплексному підході, який включає кілька ключових аспектів. Перш за все, необхідно запровадити передові технології кіберзахисту, що дозволить захищати системи від хакерських атак, які можуть призвести до серйозних збоїв в роботі життєво важливих об'єктів. Це означає впровадження надійних шифрувальних рішень, систем виявлення та запобігання вторгненням, а також засобів для моніторингу та аналізу мережевого трафіку в реальному часі.

Паралельно із запровадженням передових технологій, критично важливим є регулярне проведення аудитів безпеки, що дозволяє ідентифікувати та усувати потенційні вразливості у системах. Аудити повинні проводитися як зовнішніми, так і внутрішніми фахівцями для об'єктивної оцінки стану кіберзахисту, а результати цих перевірок мають спонукати до швидкого впровадження необхідних оновлень безпеки.

Крім технічних заходів, надзвичайно важливим є навчання персоналу. Підготовка співробітників до розуміння основ кібергігієни та вміння адекватно реагувати на кіберінциденти забезпечує, що вся команда здатна ефективно виявляти підозрілу активність та діяти відповідно до встановлених процедур. Це включає навчання з користування паролями, фішинговими атаками, захистом даних та використанням антивірусного програмного забезпечення.

Такий комплексний підхід до кібербезпеки не лише знижує ризики потенційних атак, але й забезпечує стійкість критичної інфраструктури в умовах постійно змінюваних кіберзагроз.

3. Розробка та впровадження планів аварійного реагування є критично важливою для забезпечення безпеки об'єктів критичної інфраструктури. Цей процес включає створення детальних планів, які описують кроки реагування на різноманітні кризові ситуації, включаючи техногенні аварії, природні катастрофи та інші потенційні небезпеки. Ці плани повинні містити чіткі інструкції для всіх рівнів персоналу, від оперативних працівників до вищого керівництва, а також механізми зв'язку та координації дій із зовнішніми службами аварійного реагування.

Крім того, регулярне проведення тренувань та навчань для персоналу є не менш важливим. Ці заходи допомагають підтримувати високий рівень готовності персоналу до дій в екстремальних умовах. Навчання мають включати як теоретичні, так і практичні заняття, які моделюють різні сценарії криз. В процесі таких тренувань персонал вчиться швидко і адекватно реагувати, забезпечуючи особисту безпеку та мінімізуючи можливі збитки для об'єкта інфраструктури.

Такий підхід не тільки дозволяє знизити ризики втрати життів і майна в разі виникнення надзвичайних ситуацій, але й забезпечує стабільність функціонування критично важливих об'єктів навіть у найскладніших умовах.

4. Удосконалення системи моніторингу та діагностики обладнання та інфраструктури є важливим кроком у підвищенні стійкості об'єктів критичної інфраструктури. Цей процес передбачає впровадження новітніх технологій, які дозволяють вести неперервний моніторинг стану всіх критичних систем та компонентів в реальному часі. Використання сучасних сенсорів та аналітичного програмного забезпечення допомагає відслідковувати роботу обладнання, виявляючи будь-які ознаки зносу або неполадок до того, як вони можуть призвести до серйозних збоїв.

Крім того, розробка ефективної системи раннього попередження грає ключову роль у запобіганні аварійних ситуацій. Така система базується на алгоритмах штучного інтелекту та машинного навчання, що аналізують вхідні дані від сенсорів в реальному часі, ідентифікуючи потенційні загрози та

аномалії у роботі систем. Завдяки цьому можливо оперативно реагувати на зміни, що відбуваються, мінімізуючи ризик виникнення великих технічних проблем або навіть катастроф.

В цілому, інтеграція передових систем моніторингу та діагностики є вирішальною для підтримки безперебійної та безпечної роботи об'єктів критичної інфраструктури, забезпечуючи їх здатність витримувати різні виклики та зовнішні впливи.

5. Зміцнення міжвідомчого співробітництва є ключовим елементом у забезпеченні стійкості та ефективності роботи критичної інфраструктури, особливо в контексті національної безпеки. Цей процес включає покращення координації та взаємодії між різними державними органами та відомствами, кожне з яких несе відповідальність за окремі аспекти функціонування критичної інфраструктури. Важливо створити єдиний координаційний механізм, який би забезпечував оперативний обмін інформацією та ресурсами у кризових ситуаціях, а також під час планування заходів щодо забезпечення безпеки.

Крім того, розробка міжвідомчих планів спільних дій є фундаментальною для забезпечення готовності до різноманітних загроз, що можуть вплинути на функціонування важливих об'єктів. Ці плани повинні включати чітко визначені ролі та обов'язки кожного з учасників, процедури евакуації, відновлення роботи об'єктів після аварій, а також методи реагування на терористичні атаки, техногенні катастрофи та природні надзвичайні ситуації. Важливим аспектом також є регулярне проведення спільних тренувань та навчань, які допомагають відпрацювати взаємодію між різними службами, підвищити їхню злагодженість та готовність до дій у складних умовах.

Забезпечення ефективного міжвідомчого співробітництва не тільки покращує реагування на надзвичайні ситуації, але й сприяє підвищенню загальної резилієнтності критичної інфраструктури, що є важливим для забезпечення стабільності та безпеки на національному рівні.

6. Створення резервних систем та розробка альтернативних шляхів постачання є критичними кроками для забезпечення стійкості об'єктів критичної інфраструктури, особливо в умовах, коли основні системи можуть бути пошкоджені або знищені через різні надзвичайні ситуації, включаючи природні катастрофи чи військові дії. Інтеграція резервних систем дозволяє забезпечувати неперервність постачання основних ресурсів, таких як електроенергія і вода, що є життєво необхідними для підтримки функціонування критичної інфраструктури та загальної соціальної стабільності.

Впровадження резервних систем включає не тільки створення додаткових джерел енергії, таких як генератори або акумуляторні батареї, але й розробку систем, що можуть автоматично включатися при відключенні основного постачання. Це забезпечує неперервність важливих операцій та знижує ризики, пов'язані з можливими аваріями або зупинками виробництва.

Крім створення резервних систем, ключовим аспектом є планування альтернативних маршрутів постачання та розвиток логістичних мереж. Це дозволяє диверсифікувати джерела ресурсів і зменшує залежність від одного постачальника або транспортного шляху, що може бути критично важливим у кризових ситуаціях. Розробка альтернативних логістичних маршрутів забезпечує гнучкість та адаптивність в управлінні ланцюгами постачання, дозволяючи швидко реагувати на зміни у зовнішньому середовищі та запобігати потенційним перебоям у постачанні.

Таким чином, розробка та впровадження резервних систем та альтернативних шляхів постачання є невід'ємною частиною стратегії забезпечення стійкості та ефективності критичної інфраструктури, зміцнюючи її здатність витримувати різні виклики і забезпечувати стабільне функціонування у всіх умовах.

7. Залучення міжнародного досвіду та технологій є важливим аспектом вдосконалення системи захисту критичної інфраструктури в Україні. Це включає налагодження співпраці з міжнародними організаціями та

партнерами, які мають багаторічний досвід і передові знання в області безпеки. Співробітництво з такими організаціями дозволяє Україні впроваджувати кращі світові практики та інноваційні технології, які були успішно застосовані у різних країнах для захисту важливих об'єктів інфраструктури.

Така співпраця також передбачає адаптацію міжнародних стандартів і рекомендацій до українського контексту. Це означає, що міжнародні норми і методики повинні бути переглянуті та модифіковані таким чином, щоб вони враховували місцеві особливості, регуляторну базу та специфічні загрози, які існують в Україні. Адаптація стандартів включає не тільки технічні аспекти, але й організаційні, що забезпечує цілісний підхід до забезпечення безпеки.

Впровадження кращих практик і стандартів на міжнародному рівні дозволяє Україні підвищити ефективність системи захисту критичної інфраструктури, зменшити ризики від потенційних загроз та підвищити стійкість країни до різних викликів, що можуть виникнути в майбутньому. Такий підхід також сприяє інтеграції України у світову спільноту, зміцнюючи її позиції на міжнародній арені у сфері безпеки та оборони.

Реалізація рекомендацій щодо підвищення стійкості критичної інфраструктури в Україні вимагатиме застосування інтегрованого підходу та алокації значних ресурсів. Проте, належне впровадження цих заходів має потенціал значно зміцнити здатність країни протистояти різноманітним загрозам, що ставлять під ризик національну безпеку та стабільність.

Такий інтегрований підхід включає систематичне планування та координацію дій між різними органами влади, приватним сектором, і міжнародними партнерами. Важливо забезпечити, щоб всі елементи цієї складної системи працювали злагоджено, з чітким розумінням своїх ролей та відповідальностей. Застосування передових технологій, покращення фізичного та кіберзахисту, а також розробка адаптивних планів аварійного реагування і резервних систем — усе це має бути інтегровано у загальнодержавну стратегію.

Фінансування таких ініціатив також вимагає особливої уваги. Забезпечення достатнього бюджетування та ефективне використання ресурсів будуть ключовими для успішного впровадження запланованих заходів. Можливість використання міжнародних грантів та фінансування, а також співпраця з міжнародними організаціями можуть допомогти у залученні необхідних інвестицій для розвитку та модернізації інфраструктури.

Завдяки всебічному виконанню цих стратегій, Україна не тільки покращить захист своєї критичної інфраструктури, але й зможе ефективніше реагувати на сучасні виклики, що, в свою чергу, сприятиме збільшенню загальної стабільності та безпеки країни.

2.3 Оцінка ефективності запропонованих заходів щодо підвищення стійкості об'єктів критичної інфраструктури

Оцінка ефективності заходів щодо підвищення стійкості об'єктів критичної інфраструктури в Україні може здійснюватися через комплексні методи, які включають кілька ключових компонентів:

1. Аналіз ризиків та вразливостей є важливим етапом перед запровадженням будь-яких заходів безпеки в області критичної інфраструктури. Цей процес включає в себе глибоке дослідження поточного стану об'єктів, що визначається через ідентифікацію їх слабких місць та потенційних загроз. Такий підхід дозволяє не тільки зрозуміти, які саме ризики існують, але й визначити, які заходи захисту будуть найбільш ефективними в конкретних умовах, забезпечуючи цілеспрямоване і обгрунтоване планування безпеки.

2. Імплементація запропонованих заходів включає впровадження рекомендованих технічних рішень, що передбачає модернізацію наявних систем безпеки, встановлення резервних систем постачання та покращення кіберзахисту. Цей процес вимагає детальної уваги до відповідності міжнародним стандартам та адаптації до специфіки місцевих умов. Важливо,

щоб кожен крок впровадження був ретельно спланований та виконаний з урахуванням всіх потреб та особливостей об'єкта, щоб забезпечити не тільки функціональність, але й високий рівень безпеки і надійності інфраструктури.

3. Тренування персоналу є ключовим компонентом забезпечення готовності до надзвичайних ситуацій. Це включає регулярні навчання та практичні тренування, які допомагають персоналу розвинути необхідні навички для ефективного реагування на різноманітні кризові ситуації. Проведення таких заходів зазвичай охоплює симуляції та навчання, що імітують реальні умови, де персонал може випробувати та вдосконалити свої реакції на потенційні загрози. Це дозволяє не тільки підвищити особисту компетентність кожного члена команди, але й покращує загальну координацію та спроможність колективу швидко та ефективно вирішувати непередбачені проблеми.

4. Моніторинг та оцінка впроваджених систем захисту є неперервним процесом, який забезпечує постійне спостереження за їхньою функціональністю та ефективністю у реальних умовах. Важливою складовою цього процесу є систематичний збір даних про всі інциденти, що виникають, їх детальний аналіз з метою ідентифікації можливих слабких місць у системах безпеки. На основі зібраної інформації та проведеного аналізу, проводиться перегляд існуючих планів захисту та вносяться корективи, що дозволяє адаптувати заходи безпеки до змінюваних умов і нових загроз. Такий підхід не тільки підвищує загальну надійність і резистентність критичної інфраструктури, але й забезпечує її здатність ефективно реагувати на потенційні кризи.

5. Зворотний зв'язок від залучених сторін є критично важливим для оцінки впливу заходів, що були запроваджені для підвищення стійкості об'єктів критичної інфраструктури. Цей процес включає збір відгуків від осіб, які безпосередньо залучені до її функціонування, включно з оперативним персоналом, керівництвом, службами екстреної допомоги та іншими зацікавленими сторонами. Важливо систематично аналізувати зібрану

інформацію, щоб зрозуміти, наскільки ефективно запроваджені зміни сприяють збільшенню безпеки та оперативної ефективності. Такий підхід не тільки дозволяє виявити потенційні недоліки в роботі систем, але й забезпечує можливість швидко реагувати на виклики, оптимізувати процеси та підвищити загальну ефективність управління критичною інфраструктурою.

6. Адаптація та оптимізація стратегій безпеки є важливою частиною забезпечення стійкості та ефективності критичної інфраструктури. Враховуючи зібрану інформацію та зворотний зв'язок від усіх залучених сторін, необхідно регулярно проводити оновлення та адаптації існуючих планів і методик. Цей процес передбачає аналіз отриманих даних для ідентифікації трендів та виявлення потенційних викликів, що виникають унаслідок змін у зовнішньому середовищі та нових загроз. Реагування на ці зміни через постійну оптимізацію стратегій дозволяє збільшувати ефективність заходів безпеки, забезпечувати гнучкість в управлінні ризиками та підтримувати надійність критичних систем на високому рівні.

Оцінка ефективності запроваджених заходів безпеки є ключовою для забезпечення того, що інвестиції в захист об'єктів критичної інфраструктури виправдані, а ресурси використовуються максимально ефективно. Цей процес вимагає не лише аналізу витрат і вигод, але й детального вивчення, як впроваджені зміни впливають на рівень безпеки та стійкість інфраструктури. Ретельне оцінювання дозволяє виявити, наскільки ефективно забезпечено протидію потенційним загрозам та як це сприяє підтримці постійної роботоздатності і надійності систем. В результаті, такий підхід сприяє формуванню надійної та стійкої інфраструктурної системи в Україні, що забезпечує безпечне та стабільне середовище для економічного та соціального розвитку країни.

Висновки до розділу 2

1. Вивчення сучасного стану захищеності об'єктів критичної інфраструктури в Україні виявило низку викликів, посилення відповідальності

та адаптацію правової бази, що зумовлено військовими діями, розпочатими 24 лютого 2022 року. Російське вторгнення привело до значного збільшення фізичних та кібернетичних атак, зокрема, пошкодження ключових енергетичних об'єктів та кіберінфраструктури, висвітливши критичні вразливості в національній системі захисту. У відповідь, Україна активізувала розробку та впровадження нових заходів безпеки на основі міжнародних стандартів та європейського законодавства, включаючи паспортизацію критичної інфраструктури та формування Реєстру критичної інфраструктури. Важливим аспектом є взаємодія із міжнародними організаціями та впровадження системи координації між усіма рівнями управління. Оновлення правової бази та стратегічне планування сприяють підвищенню рівня захищеності об'єктів, забезпечуючи функціональність, безперервність діяльності та відновлюваність в умовах воєнного стану.

2.Рекомендації щодо підвищення стійкості об'єктів критичної інфраструктури в Україні охоплюють важливі аспекти фізичного та кіберзахисту, аварійного реагування, та моніторингу систем. Особливу увагу приділено зміцненню фізичних бар'єрів, оновленню систем відеоспостереження та пожежогасіння. У сфері кібербезпеки наголошується на впровадженні передових технологій, регулярному проведенні аудитів безпеки та навчанні персоналу. Ефективність кіберзахисту підсилюється через комплексний підхід, що включає шифрування, системи виявлення вторгнень, і аналіз мережевого трафіку. Для аварійного реагування розроблено детальні плани, що включають чіткі процедури евакуації та забезпечення безпеки, з постійними тренуваннями персоналу. Загалом, ці заходи спрямовані на забезпечення комплексного підвищення безпеки та зменшення ризиків від різних загроз, підвищуючи здатність України ефективно реагувати на виклики сучасного безпекового середовища.

3. Ефективність заходів щодо підвищення стійкості об'єктів критичної інфраструктури в Україні оцінюється через комплексний підхід, який включає аналіз ризиків, імплементацію запропонованих заходів, тренування персоналу,

а також моніторинг та адаптацію заходів. Ретельний аналіз допомагає ідентифікувати вразливі місця та оптимізувати стратегії захисту, забезпечуючи обгрунтованість впровадження технічних рішень. Тренування персоналу зосереджене на підвищенні готовності до надзвичайних ситуацій. Останній крок — моніторинг ефективності заходів — забезпечує постійне вдосконалення системи захисту на основі реальних даних і зворотного зв'язку від учасників процесу. Такий підхід дозволяє адаптувати та оптимізувати заходи безпеки відповідно до змінюваних умов і забезпечує високий рівень надійності та ефективності критичної інфраструктури.

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:

1. Поняття та класифікація об'єктів критичної інфраструктури є фундаментальними для розуміння та захисту систем, життєво важливих для функціонування суспільства та держави. Об'єкти критичної інфраструктури охоплюють широкий спектр секторів, від енергетики до кібернетичного простору, кожен з яких має свої унікальні вразливості та значення для національної безпеки. Історичний аналіз показує, що важливість та складність захисту цих об'єктів постійно зростає у відповідь на зміну форм загроз і викликів сучасності.

Класифікація об'єктів критичної інфраструктури дозволяє організувати ефективний захист та розподіл ресурсів, особливо у випадку кризових ситуацій, гарантуючи стійкість і продовження життєво важливих функцій. Розробка та впровадження стратегій захисту цих об'єктів вимагає координації між урядами, приватним сектором та міжнародними організаціями для забезпечення комплексного підходу до ризиків, які постійно еволюціонують.

Національна та міжнародна увага до критичної інфраструктури, її регулярна оцінка та модернізація захисних заходів є ключовими для забезпечення ефективного реагування на потенційні загрози та зміцнення загальної безпеки.

2. Дослідження загроз та ризиків для об'єктів критичної інфраструктури є ключовим для забезпечення національної безпеки, особливо в контексті посилення глобальних викликів, таких як тероризм, кіберзагрози та техногенні катастрофи. Існуючий стан фізичного зносу основних фондів промисловості та ветхість інфраструктури комунальних мереж значно підвищує ризики аварій, які можуть мати катастрофічні наслідки на рівні держави або регіону.

Наявність критичної інфраструктури, яка займає центральне місце в економічному і соціальному житті країни, зобов'язує до розробки комплексних механізмів її захисту. Це включає ідентифікацію ризиків, систематичний моніторинг стану інфраструктури, регулярні оновлення стратегій забезпечення безпеки та розробку резервних планів для кризового реагування.

Стратегічне планування і імплементація превентивних заходів, таких як модернізація та оновлення інфраструктури, посилення кіберзахисту та підготовка кадрів, стають вирішальними для зменшення вразливості перед зовнішніми і внутрішніми загрозами. Також важливим є міжнародне співробітництво та обмін інформацією для забезпечення адекватного реагування на сучасні загрози критичній інфраструктурі.

Забезпечення безпеки критичної інфраструктури є невід'ємною частиною забезпечення стабільності держави, підтримки її економічного розвитку та захисту громадян від потенційних загроз. В умовах зростання комплексності і взаємозалежності систем життєзабезпечення суспільства, ці дії набувають особливої актуальності.

3. Вивчення сучасних підходів до підвищення стійкості об'єктів критичної інфраструктури є актуальним для підтримки національної безпеки та стабільності держави у відповідь на збільшення залежності від комплексних технологій. Розвиток стійкості критичної інфраструктури, що охоплює важливі сектори економіки, стає вирішальним для підтримання функціональності та виживання національної економіки у кризових умовах.

Практики стійкості, використовувані в США та інших країнах, акцентують на важливості профілактики, стримування та мінімізації ризиків, спрямованих на захист критичної інфраструктури від потенційних загроз, включаючи терористичні атаки. Важливими складовими є також підготовка до надзвичайних ситуацій, оперативне реагування, а також швидке відновлення пошкоджених систем.

Згідно з міжнародною практикою, стійкість описується як здатність системи адаптуватися та відновлюватися після збоїв, забезпечуючи

продовження функціонування необхідних сервісів. Це включає поняття як статичної, так і динамічної стійкості, де перша відноситься до базової здатності системи відновитися до прийнятного рівня після збоїв, а друга описує швидкість і ефективність процесу відновлення.

На основі аналізу стійкості інфраструктур можна зробити висновок, що інтеграція міжнародного досвіду і впровадження комплексних стратегій забезпечення стійкості є ключовими для зміцнення національної безпеки. Уряди повинні враховувати не тільки захист фізичних активів, але й підвищення загальної відновлювальної здатності економіки та суспільства перед лицем зростаючих і все більш складних глобальних викликів.

4. Аналіз стану захищеності об'єктів критичної інфраструктури в Україні виявив значні виклики, які виникли через повномасштабне вторгнення Росії, що зумовило необхідність негайного перегляду та удосконалення захисних стратегій. Незважаючи на певні дії, спрямовані на модернізацію та зміцнення фізичної стійкості об'єктів до початку війни, існуючі заходи виявилися неоднорідними та частково неефективними у контексті реальних загроз, як фізичних, так і кібернетичних.

Ескалація конфлікту спричинила активізацію державних зусиль щодо введення жорсткіших стандартів безпеки, підвищення готовності до кіберзагроз та залучення міжнародних партнерів для підтримки та обміну досвідом. Це допомогло посилити обороноздатність та реакційну здатність критичної інфраструктури.

Наразі Україна розвиває свою систему захисту критичної інфраструктури на основі міжнародних практик та вимог європейського законодавства, що включає формування правової бази та структуризацію відповідності об'єктів критичної інфраструктури. Також значний акцент робиться на категоризацію об'єктів і забезпечення їхньої реєстрації та захисту на національному рівні.

Спільні дії державних органів та критичних операторів, підкріплені законодавчими актами та міжнародною підтримкою, стали ключем до

підвищення захищеності критичної інфраструктури. Продовження такої роботи є вирішальним для забезпечення стабільності та безпеки національної інфраструктури в умовах сучасних викликів і загроз.

5. У зв’язку з посиленням військових загроз та необхідністю забезпечення національної безпеки, розробка ефективних рекомендацій щодо підвищення стійкості об'єктів критичної інфраструктури в Україні є актуальним завданням. Основні напрямки включають посилення фізичного захисту, покращення систем відеоспостереження та охорони, зміцнення протипожежних заходів, і розширення систем аварійного реагування. Важливо також зосередити увагу на комплексному підході до кібербезпеки, включаючи впровадження передових технологій, проведення регулярних аудитів безпеки та навчання персоналу.

Запропоновані рекомендації спрямовані на створення умов, що мінімізують вразливість критичних об'єктів до військових дій, терористичних актів, техногенних катастроф і інших загроз. Реалізація цих рекомендацій забезпечить більш високий рівень безпеки та оперативне реагування на надзвичайні ситуації, що є ключовим для збереження життєво важливих соціальних функцій і національної економіки.

6. Оцінка ефективності заходів щодо підвищення стійкості об'єктів критичної інфраструктури в Україні є важливим компонентом забезпечення національної безпеки і стабільності. Процес оцінювання включає в себе аналіз ризиків, впровадження запропонованих заходів, тренування персоналу, моніторинг ефективності систем та зворотний зв'язок від залучених сторін. Важливість регулярного перегляду і адаптації стратегій з огляду на змінні умови і виявлені прогалини є ключем до підтримання високого рівня захищеності і функціональності інфраструктури. На основі отриманих даних, можна коригувати та оптимізувати заходи безпеки, що сприяє підвищенню загальної стійкості критичної інфраструктури до потенційних загроз.

СПИСОК РЕФЕРОВАНОЇ 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

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. URL: https://shron1.chtyvo.org.ua/Bobro_Dmytro/Metodolohiia_otsinky_rivnia_krytych no sti_obiektiv_infrastruktury.pdf?PHPSESSID=e42scruak1ifebqfqsm81bcun7

5. Деякі питання ідентифікації об’єктів підвищеної небезпеки : Постанова КМУ від 13 вересня 2022 р. № 1030. Дата оновлення: 16.09.2022. URL: https://zakon.rada.gov.ua/ laws/show/1030-2022-%D0%BF#Text (дата звернення: 20.05.2024).

6. Деякі питання об’єктів критичної інфраструктури : Постанова КМУ від 9 жовтня 2020 р. № 1109. Дата оновлення: 07.09.2022. URL: https://zakon.rada.gov.ua/laws/ show/1109-2020-%D0%BF#Text (дата звернення: 21.05.2024).

7. Деякі питання проведення зовнішнього аудиту діяльності уповноваженого органу у сфері захисту критичної інфраструктури України : Постанова КМУ від 10 червня 2022 р. № 675. Дата оновлення: 15.06.2022. URL: https://zakon.rada.gov.ua/ laws/show/675-2022-%D0%BF#Text (дата звернення: 12.05.2024).

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.

9. Єрменчук О.П. Складові національної інфраструктури // *Науковий вісник ДДУВС*. 2017. № 4. С. 109-115

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

11. 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

12. Закон України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс] // Верховна Рада. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

13. Захист критичної інфраструктури. Концепція основних заходів захисту. Рекомендація для підприємств // Bundesministerium des Innern, 2006. URL:https://www.bmi.bund.de.

14. 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.

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

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

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

18. Лядовська В.М. Визначення критичної інформаційної інфраструктури та її захист: аналіз підходів / В.М. Лядовська, М.О. Рябий, С.О. Гнатюк. Зв'язок. 2014. № 4. С. 3–7.

19. Магда Є. Гібридна агресія Росії: уроки для Європи К.: Каламар, 2017. С. 21.

20. Марек Сметана. Захист критичної інфраструктури. Підходи держав Європейського Союзу щодо визначення елементів критичної інфраструктури. Острава: ВШБ – Техніч. ун-т Острава, 2014/2015. 60 с. (Текст для курсів, що готуються в рамках співробітництва Чеська республіка – Молдова). С. 32.

21. 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. DOI: https://doi.org/10.35432/1993-8330appa1812020201816

22. Мунтіян В.І. Економічна безпека України / В.І. Мунтіян. К.: КИИЦ, 1999. 463 с.

23. Об'єкти критичної інфраструткури [Електронний ресурс] // Wikipedia – Режим доступу до ресурсу: 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

24. 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. No 8. С. 74-82. doi:10.15407/visn2021.08.074 (дата звернення : 19.05.2024)

25. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова КМУ від 19 червня 2019 р. № 518. Дата

оновлення: 7.09.2022. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 19.05.2024).

26. 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. Дата оновлення:

20.08.2022. URL: https://zakon.rada.gov.ua/laws/show/ v0178500-22#Text (дата звернення: 13.05.2024).

27. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури : Постанова КМУ від 22 липня 2022 р. № 821. Дата оновлення: 22.07.2022. URL: https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#Text (дата звернення: 15.05. 2024)

28. Про критичну інфраструктуру. Закон України від 16.11.2021 №1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

29. Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні. Постанова Верховної Ради України від01.12.2005 №3175-IV. URL:https://zakon.rada.gov.ua/ laws/show/3175-15#Text

30. 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

31. 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

32. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : розпорядження КМУ від 6 грудня 2017 р. № 1009-р. Дата оновлення: 6.12.2017. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (дата звернення: 10.05.2024)

33. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України : Постанова КМУ від 12 липня 2022 р. № 787. Набуває чинності. URL: https://zakon.rada.gov.ua/laws/show/787-2022- %D0%BF#Text (дата звернення: 17.05.2024)

34. Ризик. Вікіпедія. URL: https://uk.wikipedia.org/wiki/%D0%A0%-D0%B8%D0%B7%D0%B8%D0%BA (дата звернення: 02.05.2019).

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

36. Стійкість критичної інфраструктури ЄС: посилення політики та координації. 24.02.2023. https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/stiykist-krytychnoyi-infrastruktury-yes-posylennya-polityky-ta

37. Стійкість систем / матеріал з Вікіпедії – вільної енциклопедії / URL: https://uk.wikipedia.org/wiki/Стійкість_систем (дата звернення: 19.05.2024).

38. 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

39. 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.

40. Термін «Управління ризиками». База даних: «Законодавство України». URL: https://zakon.rada.gov.ua/ laws/term/31450 (дата звернення: 02.05.2024).

41. Україна починає будувати систему захисту критичної інфраструктури відповідно до вимог європейського законодавства. 25 квітня 2023. https://biz.ligazakon.net/news/219095_ukrana-pochina-buduvati-sistemu-zakhistu-kritichno-nfrastrukturi-vdpovdno-do-vimog-vropeyskogo-zakonodavstva

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

43. 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.

44. 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: 20.05.2024).

45. 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

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

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

48. 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

49. 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.

50. 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).

51. 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.

52. 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: 19.05.2024).

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

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

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

56. Hoffman F. Onnot-so-newwarfare: political war fare vs hybrid threats. URL: http://warontherocks.com.

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

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

59. 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: 19.05.2024).

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

61. 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

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

63. National Infrastructure Delivery Plan 2016 – 2021. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attach

ment_data/file/5 20086/2904569_nidp_deliveryplan.pdf (дата звернення: 19.05.2024).

64. 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: 16.05.2024).

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

66. Quadrennial Homeland Security Review, 2010, 2014. URL: https://www.dhs.gov/quadrennial-homeland-security-review (дата звернення: 19.05.2024).

67. 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.

68. Resilience Analysis and Practice, The Resilience Alliance. Research organization. URL: http://www.resalliance.org/index.php/resilience (дата звернення: 19.05.2024).

69. 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)

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

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

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

73. 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: 23.05.2024).

.