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 загроз для енергетичних об’єктів критичної інфраструктури»

Виконавець: студент групи 413 ЦБ Дрегула Трохим Ігорович

Керівник: к.т.н., доцент Кажан Катерина Іванівна

Нормконтролер: _____ Козлітін О. О.

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

Дрегули Трохима Ігоровича

1. Тема роботи «Оцінка загроз для енергетичних об’єктів критичної інфраструктури» 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:

- проаналізувати теоретичні концепції та підходи до визначення енергетичних об'єктів критичної інфраструктури, їх ролі у суспільстві та важливості для економічного розвитку;
- охарактеризувати інженерні заходи захисту населення від можливих наслідків пошкодження/руйнування енергетичних об’єктів;
- провести оцінку потенційних небезпек від технологічних неполадок, природних катастроф, воєнних дій, терористичних актів;
- проаналізувати існуючі підходи та методики оцінки загроз для енергетичних об'єктів критичної інфраструктури та визначити їхню ефективність і придатність до застосування;

- удосконалити методи та моделі для визначення рівня загроз та ризиків для енергетичних об'єктів;
- розробити стратегії та заходи захисту на основі аналізу отриманих результатів з метою забезпечення найвищого рівня безпеки енергетичних об'єктів критичної інфраструктури.

4. Зміст пояснювальної записки:

- загальні відомості про оцінку загроз енергетичних об’єктів критичної інфраструктури;
- інженерні та планувальні заходи від природних катастроф;
- ідентифікація небезпеки від воєнних дій;
- математичний розрахунок ризиків при виникненні конкретних загроз;
- планування заходів для забезпечення безпеки та стійкості об'єктів енергетичної інфраструктури

5. Перелік обов’язкового ілюстративного матеріалу:

- етапи розробки стратегій управління ризиками;
- моделі визначення рівня загроз для енергетики;
- графічне представлення прогресування надзвичайних ситуацій.

6. Календарний план-графік

№ з/п	Завдання	Термін виконання	Підпис керівника
1	2	3	4
1	Постановка задачі та аналіз інформаційних джерел	20.05.2024-22.05.2024	
2	Збір інформаційних даних та обґрунтування вибору рішення	22.05.2024-25.05.2024	
3	Аналіз даних та їх класифікація	26.05.2024	
4	Робота над розділом №1	26.05.2024-29.05.2024	
5	Робота над розділами №2, 3	29.05.2024-04.06.2024	
6	Підготовка графічного матеріалу, оформлення і друк пояснювальної записки	05.06.2024-06.06.2024	
7	Оформлення презентації в PowerPoint	07.06.2024-08.06.2024	

8	Отримання рецензій від опонентів	09.06.2024	
9	Захист в ДЕК	10.06.2024	

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

Керівник кваліфікаційної роботи: _____ Кажан К. І.

Завдання прийняв до виконання: _____ Дрегула Т. І

РЕФЕРАТ

Кваліфікаційна робота складається із вступу, основної частини, що містить 3 розділи, висновку й списку літератури. Загальний обсяг роботи – 53 сторінки. Робота містить 7 рисунків та 2 таблиці. Список бібліографічних посилань включає 31 джерело.

Ключові слова: КРИТИЧНА ІНФРАСТРУКТУРА, ЕНЕРГЕТИЧНІ ОБ’ЄКТИ, МОДЕЛІ ОЦІНКИ РИЗИКІВ, НАДЗВИЧАЙНІ СИТУАЦІЇ, ДНІПРОВСЬКА ГЕС, КИЇВСЬКА ТЕЦ, СИСТЕМИ БЕЗПЕКИ.

Об’єкт дослідження – енергетичні об'єкти критичної інфраструктури.

Предмет дослідження – оцінка загроз, які можуть виникнути для енергетичних об'єктів критичної інфраструктури, а також розробка стратегій та заходів захисту для запобігання або пом'якшення їхнього впливу.

Мета роботи – систематичний аналіз та оцінка загроз, які впливають на енергетичні об'єкти критичної інфраструктури, з метою визначення їхнього потенційного впливу на функціонування цих об'єктів та розробки ефективних заходів захисту.

Методи, застосовані в кваліфікаційній роботі: методи дослідження, що охоплюють збір та аналіз інформації про загрози, математичне моделювання та прогнозування, методи синтезу для розробки стратегій захисту енергетичних об'єктів. Також були використані елементи ймовірнісно-статистичних методів та геоінформаційних систем для оцінки ризику та візуалізації результатів моделювання.

Наукова новизна отриманих результатів полягає в проведеному моделюванні та прогнозуванні потенційних небезпек та оцінці загроз для енергетичних об’єктів критичної інфраструктури. Особлива увага приділяється розширенню області застосування моделей, включаючи не лише самі енергетичні об'єкти, а й їхнє навколишнє середовище та інфраструктуру, таку як транспортні мережі та промислові райони.

Основні висновки роботи – проведено моделювання та спрогнозовані потенційні небезпеки або ймовірність прояву небезпечних станів; оцінено загрози для енергетичних об’єктів критичної інфраструктури; запропоновано конкретні кроків для зменшення ризиків і підвищення стійкості енергетичних об'єктів; рекомендовано впровадити системи моніторингу та аналізу для постійного контролю стану енергетичних об'єктів та виявлення потенційних загроз.

Матеріали дипломної роботи надають практичні рекомендації для підвищення стійкості енергетичних об'єктів перед різноманітними загрозами, зменшуючи ймовірність виникнення негативних наслідків та мінімізуючи їх вплив на економіку та безпеку.

ЗМІСТ

ВСТУП

Актуальність теми. В умовах постійного розвитку технологій і зростаючої глобалізації світового економічного простору, енергетичні об'єкти критичної інфраструктури стають об'єктом особливої уваги з боку різних сторін. Надійна та безперебійна робота цих об'єктів має критичне значення для забезпечення життєвого рівня суспільства, економічного розвитку та національної безпеки.

Однак, зростаючі загрози та виклики, такі як кібератаки, терористичні акти, природні катастрофи та інші, ставлять під загрозу функціонування цих об'єктів. Дослідженнями в галузі вивчення загроз щодо енергетичних об’єктів інфраструктури займалися такі вчені як Качинський А. Б., Бірюков Д. С., Кодрик А.І., Яковлєв Є.О., Чумаченко С.М., Парталян А.С. [4-6].

Актуальність дослідження загроз для енергетичних об'єктів критичної інфраструктури визначається необхідністю забезпечення їхньої захищеності та стійкості перед потенційними небезпеками. Сучасний рівень технологічного розвитку, висока ступінь залежності суспільства від енергетичних ресурсів та швидкий розвиток кіберзлочинності вимагають комплексного підходу до вирішення цієї проблеми. Також варто додати, що в умовах триваючого військового конфлікту в Україні, енергетичні об’єкти стають ключовими точками, що зазнають значного впливу. Збільшення кількості кібератак, ракетних ударів та інших форм ворожих дій призводить до значних пошкоджень інфраструктури, що в свою чергу впливає на стабільність енергопостачання в країні.

У цьому контексті, дипломна робота спрямована на аналіз та оцінку різноманітних загроз, що стоять перед енергетичними об'єктами критичної інфраструктури, визначення їхнього потенційного впливу та розробку ефективних заходів захисту. Відповідно, вона має велике значення як для наукового співтовариства, так і для практичних застосувань в галузі енергетичної безпеки та національної оборони.

Метою дослідження є систематичний аналіз та оцінка загроз, які впливають на енергетичні об'єкти критичної інфраструктури, з метою визначення їхнього потенційного впливу на функціонування цих об'єктів та розробки ефективних заходів захисту.

Для досягнення поставленої мети було вирішено наступні завдання:

1. Проаналізувати теоретичні концепції та підходи до визначення енергетичних об'єктів критичної інфраструктури, їх ролі у суспільстві та важливості для економічного розвитку.

2. Проаналізувати існуючі підходи та методики оцінки загроз для енергетичних об'єктів критичної інфраструктури та визначити їхню ефективність і придатність до застосування.

3. Удосконалити методи та моделі для визначення рівня загроз та ризиків для енергетичних об'єктів критичної інфраструктури та їх практичну цінність.

4. Розробити стратегії та заходи захисту на основі аналізу отриманих результатів з метою забезпечення найвищого рівня безпеки енергетичних об'єктів критичної інфраструктури.

Об'єктом дослідження є енергетичні об'єкти критичної інфраструктури.

Предметом дослідження є оцінка загроз, які можуть виникнути для енергетичних об'єктів критичної інфраструктури, а також розробка стратегій та заходів захисту для запобігання або пом'якшення їхнього впливу.

У процесі написання дипломної роботи використано методи дослідження, що охоплюють збір та аналіз інформації про загрози, математичне моделювання та прогнозування, методи синтезу для розробки стратегій захисту **енергетичних об'єктів.** Також були використані елементи ймовірнісно-статистичних методів та геоінформаційних систем для оцінки ризику та візуалізації результатів моделювання.

Відмінність від отриманих раніше результатів полягає у розробці та вдосконаленні існуючих методів оцінки ризику. Особлива увага приділяється розширенню області застосування моделей, включаючи не лише самі енергетичні

об'єкти, а й їхнє навколишнє середовище та інфраструктуру, таку як транспортні мережі та промислові райони.

Прикладна цінність отриманих результатів наукової роботи полягає у покращенні здатності управління та захисту енергетичних об'єктів критичної інфраструктури від потенційних загроз. Проведені у даній роботі дослідження допомагають розробити більш точні та комплексні стратегії захисту, що враховують різноманітність та динаміку сучасних загроз. Отримані результати можуть бути використані органами управління, енергетичними компаніями та іншими зацікавленими сторонами для прийняття обґрунтованих рішень щодо забезпечення безпеки та надійності енергетичної інфраструктури. Додатково, висновки можуть послужити основою для подальших досліджень у галузі захисту критичних енергетичних об'єктів та розробки нових стратегій протидії загрозам.

Відмінність від отриманих раніше результатів. Результати попередніх досліджень підкреслюють необхідність ретельного аналізу загроз та розробки ефективних стратегій управління ризиками для енергетичних об'єктів. В рамках цієї роботи проведено оцінку потенційних загроз, таких як технічні відмови, природні катастрофи та кібератаки, а також їхню ймовірність виникнення. Далі проведено аналіз вразливості системи енергопостачання та оцінку рівня вразливості кожного об'єкта. Основною відмінністю цієї роботи є додатковий аналіз етапів управління ризиками, таких як розробка заходів превентивного характеру, створення планів реагування, навчання та тренування персоналу, вдосконалення систем моніторингу та контролю, а також постійний аналіз та оновлення стратегій управління ризиками. Ці етапи важливі для забезпечення ефективного управління ризиками та забезпечення стійкості енергетичних об'єктів у сучасному динамічному середовищі.

Прикладна цінність отриманих результатів наукової роботи. Отримані результати наукової роботи надають практичні рекомендації для підвищення стійкості енергетичних об'єктів перед різноманітними загрозами, зменшуючи

ймовірність виникнення негативних наслідків та мінімізуючи їх вплив на економіку та безпеку. Це допомагає уникнути втрат та збільшує готовність персоналу до екстрених ситуацій, а також сприяє покращенню кібербезпеки енергетичних систем. Таким чином, результати дослідження мають важливе практичне значення для забезпечення безпеки та стабільності енергетичної інфраструктури.

РОЗДІЛ 1. ТЕОРЕТИЧНИЙ АНАЛІЗ БЕЗПЕКИ ЕНЕРГЕТИЧНИХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Визначення понять: енергетичні об'єкти критичної інфраструктури, загрози, безпека

У сучасному світі, енергетичні об’єкти критичної інфраструктури відіграють ключову роль у підтримці стабільності та розвитку суспільства. Вони є життєво важливими для функціонування економіки, безпеки держави, суспільства та населення. Однак, ці об’єкти також стикаються з численними загрозами, які можуть завдати шкоди або збитків. Ці загрози можуть бути різноманітними, включаючи природні катастрофи, технологічні неполадки, кібератаки та інше. Важливість безпеки в цьому контексті не можна переоцінити. Безпека означає стан, коли об’єкти, процеси та явища не можуть завдати шкоди, що є несумісною з життям та здоров’ям людини, її благополуччям [1]. Це означає, що ми повинні розробляти та впроваджувати стратегії та політики, які забезпечують безпеку наших критичних інфраструктурних об’єктів. У цьому підрозділі ми детально розглянемо визначення енергетичних об’єктів критичної інфраструктури, загроз та безпеки. Ми також обговоримо, як ці поняття взаємодіють одне з одним, та їх значення для сучасного суспільства. Крім того, ми розглянемо потенційні стратегії та рішення для забезпечення безпеки наших критичних інфраструктурних об’єктів від різноманітних загроз.

Енергетичні об'єкти критичної інфраструктури – це важливі елементи енергетичної системи країни, які відіграють ключову роль у підтримці стабільності та розвитку суспільства. Вони можуть включати електростанції, гідроелектростанції, атомні станції, вітряні ферми, сонячні панелі, енергетичні мережі та інші об'єкти, які генерують, передають або розподіляють енергію [2]. Ці об'єкти відіграють важливу роль у сучасному суспільстві, оскільки вони забезпечують надійне постачання енергії, яке необхідне для функціонування всіх секторів економіки, включаючи промисловість, транспорт, освіту, охорону

здоров'я та домашнє господарство. Без стабільного постачання енергії багато сфер життя суспільства були б неможливими.

На рис. 1.1 представлені приклади енергетичних об'єктів критичної інфраструктури

Рис 1.1 Приклади енергетичних об'єктів критичної інфраструктури

Джерело: розроблено автором *[3]*

Як видно з рис. 1.1 великі промислові комплекси - електростанції, що використовуються для генерації електроенергії з різних джерел енергії, таких як вугілля, газ, вітер або сонячне світло. Атомні станції, використовують ядерну енергію для того, щоб забезпечити електроенергією великі території. Гідроелектростанції використовують потік води для генерації електроенергії, що є важливим відновлювальним джерелом енергії. Нарешті, енергетичні мережі є системами передачі та розподілу енергії, які забезпечують зв'язок між виробниками та споживачами, забезпечуючи постачання електроенергії від джерел виробництва до кінцевих користувачів. Аналіз цих компонентів демонструє, як різноманітність енергетичних об'єктів сприяє надійності та стійкості енергетичної системи. Ці об'єкти є важливими елементами

національної інфраструктури, і їх безпека та надійність є важливими пріоритетами для будь-якої країни.

Слід зазначити, що загрози – це потенційні події, дії або обставини, які можуть завдати шкоди, збитків у певній сфері [4]. В контексті енергетичних об’єктів критичної інфраструктури, загрози можуть бути різноманітними і включати такі типи [5]:

1. Технологічні неполадки. Це можуть бути відмови обладнання, помилки програмного забезпечення, недоліки в проектуванні та інше.

2. Природні катастрофи. Землетруси, повені, урагани та інші природні явища можуть спричинити серйозні пошкодження енергетичних об’єктів.

3. Кібератаки. Зловмисники можуть спробувати зламати системи захисту для отримання несанкціонованого доступу до критичної інфраструктури.

4. Терористичні атаки. Терористи можуть цілеспрямовано атакувати енергетичні об’єкти з метою завдати шкоди.

Потенційні наслідки для енергетичних об’єктів критичної інфраструктури можуть бути дуже серйозними. Вони можуть включати втрату життя, значні матеріальні збитки, перебої в постачанні енергії, економічні втрати та навіть національну небезпеку. Щодо реальних прикладів, в Україні були випадки кібератак на енергетичні об’єкти, що призвели до перебоїв в електропостачанні. Також були випадки фізичних атак на енергетичні об’єкти в зоні ведення бойових дій. Ці приклади показують, що загрози для енергетичних об’єктів критичної інфраструктури є реальними і можуть мати серйозні наслідки.

В свою чергу, безпека – це стан, при якому явища, процеси, об’єкти, не можуть завдати шкоди, несумісної із здоров’ям та життям людини, її благополуччям1. В контексті енергетичних об’єктів критичної інфраструктури, безпека означає стан захищеності критичної інфраструктури, за якого забезпечується функціональність, безперервність роботи, цілісність й стійкість критичної інфраструктури. Основні принципи безпеки енергетичних об’єктів критичної інфраструктури включають [6]:

- Проактивність. Попереднє виявлення та запобігання потенційним загрозам.

- Відновлюваність. Здатність швидко відновлюватися після інциденту.

- Стійкість. Здатність витримувати та адаптуватися до змін у середовищі.

- Захист. Захист від небезпечних подій, що можуть завдати шкоди.

Методи та стратегії забезпечення безпеки енергетичних об’єктів критичної інфраструктури можуть включати:

- Технічні заходи. Використання технологій та обладнання для захисту об’єктів від фізичних та кібернетичних загроз.

- Організаційні заходи. Розробка процедур та політик для забезпечення безпеки.

- Регулятивні заходи. Дотримання відповідних законів та нормативів.

Приклади ефективних заходів безпеки можуть включати:

- Захист від кібератак. Встановлення вогневих стін, систем виявлення вторгнень та інших технологій кібербезпеки.

- Фізичний захист. Встановлення огорож, систем відеоспостереження, контролю доступу та інших фізичних заходів безпеки.

- Захист від природних катастроф. Розробка планів готовності до надзвичайних ситуацій та заходів зменшення ризику.

- Забезпечення надійного електроживлення. Використання резервних генераторів та систем безперебійного живлення

Отже, енергетичні об’єкти критичної інфраструктури відіграють важливу роль у сучасному суспільстві, оскільки вони забезпечують надійне постачання енергії, необхідне для функціонування всіх секторів економіки. Однак, ці об’єкти також стикаються з численними загрозами, які можуть завдати шкоди або збитків. Ці загрози можуть бути різноманітними, включаючи природні катастрофи, технологічні неполадки, кібератаки та інше. Безпека в цьому контексті означає стан захищеності критичної інфраструктури, за якого

забезпечується функціональність, безперервність роботи, цілісність й стійкість критичної інфраструктури.

Для забезпечення безпеки необхідно використовувати різні методи та стратегії, включаючи технічні, організаційні та регулятивні заходи. Висновки цього підрозділу підкреслюють важливість розуміння та управління цими поняттями в контексті енергетичних об’єктів критичної інфраструктури.

1.2 Аналіз існуючих підходів до оцінки загроз для енергетичних об'єктів

Оцінка загроз для енергетичних об'єктів критичної інфраструктури є важливим етапом у розробці стратегій їх захисту. Різноманіття загроз вимагає використання комплексних підходів та методів, що дозволяють адекватно оцінювати ризики та розробляти ефективні заходи для їх мінімізації. У цьому підрозділі буде проведено аналіз існуючих підходів до оцінки загроз, які застосовуються в сучасних умовах. Різні країни та організації використовують різні методології та інструменти для оцінки загроз, що відображає специфіку їхнього енергетичного сектору та рівень розвитку технологій. Важливими аспектами є ідентифікація потенційних загроз, їх класифікація, кількісна та якісна оцінка ризиків, а також розробка моделей для прогнозування можливих наслідків. Враховуючи сучасні виклики, такі як зростання кіберзагроз, зміна клімату та збройні конфлікти, оцінка загроз для енергетичних об'єктів набуває ще більшої актуальності. Аналіз існуючих підходів допоможе виявити їх сильні та слабкі сторони, а також визначити напрямки для вдосконалення методологій оцінки ризиків, зокрема, в умовах сучасної України [7].

Ідентифікація загроз є першим і надзвичайно важливим етапом у процесі оцінки ризиків для енергетичних об'єктів критичної інфраструктури. Основна мета цього етапу – виявлення всіх можливих загроз, які можуть вплинути на безпеку та стабільність функціонування енергетичних систем. Нижче наведені основні методи виявлення можливих загроз для енергетичної інфраструктури [8].:

- Експертні оцінки. Цей метод передбачає залучення фахівців з різних галузей для визначення можливих загроз. Експерти використовують свій досвід та знання для ідентифікації потенційних ризиків, аналізуючи наявні дані та оцінюючи ймовірність виникнення тих чи інших загроз.

- Аналіз історичних даних. Вивчення попередніх інцидентів та катастроф дозволяє виявити тенденції та повторювані загрози. Це дає можливість розробити сценарії, які можуть повторитися в майбутньому, та визначити заходи для їх запобігання.

- SWOT-аналіз. Цей метод включає вивчення сильних та слабких сторін енергетичних об'єктів, а також аналіз можливостей і загроз, що можуть виникнути. SWOT-аналіз допомагає систематизувати інформацію та визначити ключові фактори, які потребують уваги.

- Аналіз вразливостей. Виявлення вразливих місць у структурі та функціонуванні енергетичних об'єктів дозволяє визначити потенційні точки впливу загроз. Цей метод включає тестування систем на стійкість до різних типів впливу.

Методи класифікації загроз за походженням, впливом, частотою виникнення та іншими критеріями дозволяють систематизувати інформацію про загрози та забезпечити ефективне управління ризиками для енергетичних об'єктів критичної інфраструктури. Класифікація загроз за походженням включає техногенні, природні та кіберзагрози. Техногенні загрози виникають через людську діяльність, наприклад, аварії на виробництвах чи технологічні збої. Природні загрози пов'язані з природними явищами, такими як землетруси, повені та урагани. Кіберзагрози включають атаки на інформаційні системи, злам мереж та розповсюдження шкідливого програмного забезпечення. Класифікація загроз за впливом допомагає визначити основні наслідки загроз та сфокусувати зусилля на їх мінімізації. Фізичний вплив передбачає пряме фізичне пошкодження об'єктів, наприклад, руйнування будівель чи обладнання. Економічний вплив охоплює фінансові збитки, втрати продуктивності та зниження прибутків.

Соціальний вплив стосується впливу на населення, наприклад, загибель або поранення людей та соціальні потрясіння. Класифікація загроз за частотою виникнення дозволяє оцінити ймовірність загроз та розподілити ресурси для протидії найбільш імовірним подіям [9]. Часті загрози, такі як сезонні повені, виникають регулярно або з високою ймовірністю. Рідкісні загрози, наприклад, великі землетруси, трапляються рідко, але мають значні наслідки. Несподівані загрози, такі як терористичні атаки або нові види кібератак, є непередбачуваними подіями.

Переваги класифікації загроз за походженням включають чітке розрізнення джерел загроз, що сприяє розробці специфічних заходів захисту для кожного типу загрози. Однак, може бути складно класифікувати комплексні загрози, що мають змішане походження, як-от техногенно-природні катастрофи. Класифікація за впливом допомагає визначити основні наслідки загроз та сфокусувати зусилля на їх мінімізації, але може не враховувати всі аспекти загрози, зосереджуючись лише на певних типах впливу. Класифікація за частотою виникнення дозволяє оцінити ймовірність загроз та розподілити ресурси для протидії найбільш імовірним подіям, але рідкісні, але катастрофічні події можуть бути недооцінені через їх низьку ймовірність [10]. Використання комбінованих методів класифікації загроз дозволяє створити більш повну та всебічну оцінку ризиків для енергетичних об'єктів критичної інфраструктури. Це забезпечує більш ефективне управління ризиками, враховуючи всі можливі аспекти та наслідки загроз.

Оцінка ризиків є критично важливим етапом у забезпеченні безпеки енергетичних об'єктів критичної інфраструктури. Для цього використовуються кількісні та якісні методи оцінки ризиків. Кількісні методи базуються на числових даних і включають використання статистичних моделей та аналітичних інструментів, що дозволяє точно визначити ймовірність та вплив потенційних загроз. Якісні методи, з іншого боку, передбачають використання експертних оцінок та описових підходів для оцінки ризиків на основі якісної інформації.

Аналіз поширених моделей ризику, таких як матриця ризиків та сценарний аналіз, є важливим інструментом у процесі оцінки ризиків. Матриця ризиків дозволяє візуалізувати ризики за двома вимірами - ймовірністю та впливом, що сприяє ідентифікації пріоритетних загроз [11]. Сценарний аналіз використовується для моделювання різних сценаріїв розвитку подій та їх впливу на енергетичні об'єкти, що допомагає передбачати можливі наслідки та розробляти відповідні стратегії реагування. Використання статистичних методів та моделей є невід'ємною частиною оцінки ризиків. Статистичні методи дозволяють аналізувати історичні дані, визначати тенденції та прогнозувати майбутні загрози на основі минулого досвіду. Моделі, що використовуються в статистичному аналізі, можуть включати регресійний аналіз, аналіз часових рядів та інші математичні інструменти.

Прогнозування наслідків загроз є наступним важливим етапом після оцінки ризиків. Моделі прогнозування можливих наслідків загроз допомагають визначити, яким чином ті чи інші загрози можуть вплинути на енергетичні об'єкти та інфраструктуру загалом. Інструменти та методи, що використовуються для прогнозування, включають симуляції та аналітичні моделі, які дозволяють відтворити різні сценарії розвитку подій та оцінити їх наслідки. Симуляції є ефективним засобом для тестування різних сценаріїв та аналізу їх можливих наслідків без необхідності реальних випробувань. Вони дозволяють відтворювати різноманітні умови та оцінювати, як системи будуть реагувати на різні загрози. Аналітичні моделі, з іншого боку, надають можливість точно розраховувати вплив загроз на основі математичних формул та алгоритмів, що забезпечує високий рівень точності прогнозування.

Порівняння міжнародних підходів до оцінки загроз є важливим для розуміння найкращих практик та адаптації їх до місцевих умов. Огляд підходів, що використовуються у різних країнах, дозволяє виявити ефективні методології та стратегії, які можуть бути застосовані для підвищення безпеки енергетичних об'єктів критичної інфраструктури [12].

Порівняння методологій, що використовуються в міжнародній практиці, включає аналіз стандартів та рекомендацій, розроблених міжнародними організаціями та провідними країнами у сфері безпеки енергетичної інфраструктури. Це дозволяє виявити спільні риси та відмінності у підходах, оцінити їх ефективність та визначити можливості для вдосконалення національних систем управління ризиками. Використання міжнародного досвіду допомагає забезпечити більш комплексний та ефективний підхід до захисту енергетичних об'єктів від потенційних загроз [13].

Отже, після докладного аналізу різноманітних підходів до оцінки загроз для енергетичних об'єктів стає очевидним, що існують різні методи та стратегії, які використовуються для виявлення, класифікації та оцінки потенційних небезпек. Відмінності в підходах до аналізу загроз визначаються особливостями конкретного об'єкту, його контексту та вимог безпеки. Подальший аналіз принципів та методів ідентифікації, класифікації, оцінки ризиків та прогнозування наслідків виявив різноманітність підходів і їхню ефективність у різних ситуаціях.

1.3. Огляд методів та моделей для визначення рівня загроз та ризиків

У сучасному світі, де енергетичні об'єкти стають об'єктом постійно зростаючих загроз і викликів, важливо мати належний огляд методів та моделей для визначення рівня загроз та ризиків. Цей розділ присвячений дослідженню різноманітних підходів, що застосовуються для оцінки потенційних небезпек у сфері енергетики. Огляд цих методів та моделей має вирішальне значення для розуміння сучасного стану справ у галузі безпеки енергетичних об'єктів. Не лише він допомагає виявити наявні загрози, але й надає засади для ефективного управління ризиками та прийняття обґрунтованих стратегій захисту. Враховуючи складність сучасних викликів, таких як кібератаки, терористичні загрози та природні катастрофи, огляд методів та моделей для визначення рівня загроз та ризиків стає невід'ємною частиною стратегій забезпечення стійкості та безпеки енергетичних систем.

Методи визначення рівня загроз можуть бути різними і залежать від конкретного контексту. Деякі з них наведені на рис 1.2.

Рис. 1.2 Деякі загальні методи визначення рівня загроз для енергетики

Джерело: розроблено автором[14]

Як видно з рис. 1.2 моделювання загроз допомагає ідентифікувати можливі небезпеки та вразливості, що можуть виникнути, допомагаючи відповісти на запитання щодо найбільш актуальних загроз та шляхи захисту. Оцінка ризиків, в свою чергу, допомагає визначити вплив внутрішніх та зовнішніх чинників на ступінь ризику, що дозволяє розробити ефективні заходи для мінімізації цього ризику. Визначення рівнів загроз виходить за рамки простого ідентифікування потенційних небезпек, воно також включає аналіз можливого впливу на людей, поширення загрози та можливі наслідки небезпечних ситуацій [15]. Такий комплексний аналіз дозволяє зрозуміти і оцінити всі аспекти, пов'язані з ризиками та загрозами для енергетичних об'єктів критичної інфраструктури. Кожен з цих методів має свої переваги та недоліки, і вибір конкретного методу залежить від специфіки ситуації та цілей дослідження. Наприклад, моделювання загроз може бути корисним для систематичного аналізу потенційних векторів атаки, але цей метод може бути часозатратним і вимагати значних технічних знань. З іншого боку, оцінка ризиків може бути менш технічною, але вона може не враховувати всі можливі вектори атаки. Деякі загальні моделі визначення рівня загроз для енергетики представлені на рис 1.3.

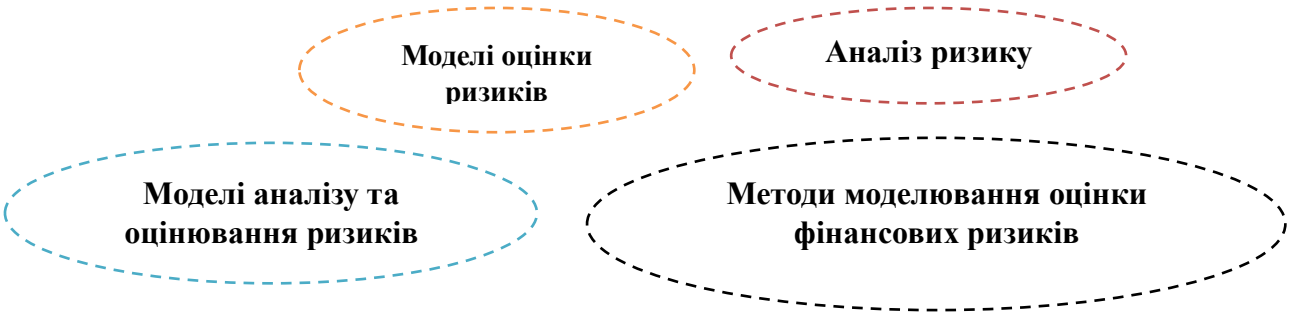


Рис. 1.3 Деякі загальні моделі визначення рівня загроз для енергетики

Джерело: розроблено автором [16]

Як видно з рис 1.3 моделі оцінки ризиків надають можливість оцінити рівень потенційного ризику, враховуючи як первинний, так і залишковий ризик, що є ключовим для прийняття відповідних заходів з мінімізації небезпеки. Аналіз ризиків, у свою чергу, включає в себе систематичне визначення впливу зовнішніх та внутрішніх факторів на ступінь ризику, і може бути проведений як у кількісному, так і у якісному форматі, залежно від конкретної ситуації та доступних ресурсів. Моделі аналізу та оцінювання ризиків допомагають структурувати процес визначення ризику та розробити ефективні стратегії управління ним. Нарешті, методи моделювання оцінки фінансових ризиків використовують економіко-математичні підходи, такі як VAR-метод, для аналізу статистичних характеристик ринку та визначення можливих фінансових втрат. Цей широкий спектр моделей надає комплексний підхід до аналізу та управління ризиками, що важливо для забезпечення стійкості та безпеки енергетичних об'єктів критичної інфраструктури.

Кожна з цих моделей має свої переваги та недоліки, і вибір конкретної моделі залежить від специфіки ситуації та цілей дослідження. Наприклад, моделі оцінки ризиків можуть бути корисними для систематичного аналізу потенційних векторів атаки, але цей метод може бути часозатратним і вимагати значних технічних знань. З іншого боку, аналіз ризику може бути менш технічним, але він може не враховувати всі можливі вектори атаки. Застосування методів та моделей для визначення рівня загроз та ризиків є важливим етапом в процесі управління ризиками. Це допомагає організаціям краще розуміти свої

вразливості та потенційні загрози, а також розробляти ефективні стратегії їх мінімізації. Методи визначення рівня загроз, такі як моделювання загроз, допомагають ідентифікувати потенційні загрози та визначити, які з них є найбільш актуальними. Це може включати в себе аналіз структурної вразливості, відсутність відповідних гарантій та інші фактори, які можуть збільшити ризик. Моделі визначення рівня ризиків, такі як моделі оцінки ризиків та аналіз ризику, допомагають організаціям краще розуміти ймовірність та потенційний вплив різних видів ризиків. Це може включати в себе визначення внутрішніх та зовнішніх чинників, які можуть збільшити або зменшити ступінь ризику, а також розробку стратегій для їх мінімізації.

Важливо пам’ятати, що жоден метод або модель не є абсолютно точним, і всі вони мають свої переваги та недоліки. Вибір конкретного методу або моделі залежить від специфіки ситуації та цілей дослідження. Наприклад, моделювання загроз може бути корисним для систематичного аналізу потенційних векторів атаки, але цей метод може бути часозатратним і вимагати значних технічних знань. З іншого боку, оцінка ризиків може бути менш технічною, але вона може не враховувати всі можливі вектори атаки. Завжди важливо враховувати ці фактори при виборі методу або моделі для визначення рівня загроз та ризиків.

Отже, методи та моделі визначення рівня загроз та ризиків є важливими інструментами в процесі управління ризиками. Вони допомагають організаціям краще розуміти свої вразливості та потенційні загрози, а також розробляти ефективні стратегії їх мінімізації. Жоден метод або модель не є абсолютно точним, і всі вони мають свої переваги та недоліки. Вибір конкретного методу або моделі залежить від специфіки ситуації та цілей дослідження. Моделювання загроз може бути корисним для систематичного аналізу потенційних векторів атаки, але цей метод може бути часозатратним і вимагати значних технічних знань.

РОЗДІЛ 2. ЗАСТОСУВАННЯ ТА АНАЛІЗ МОДЕЛІ ОЦІНКИ РИЗИКІВ ДЛЯ ЕНЕРГЕТИЧНИХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1. Розробка моделі оцінки ризиків для енергетичних об'єктів критичної інфраструктури

У цьому підрозділі буде розглянуто процес розробки моделі оцінки ризиків для енергетичних об'єктів критичної інфраструктури. Зважаючи на важливість забезпечення безперебійного функціонування енергетичних систем та необхідність адекватного реагування на потенційні загрози, розробка ефективної моделі оцінки ризиків є критично важливою. Модель повинна враховувати різноманітні фактори, які впливають на ступінь ризику, та надавати можливість точної ідентифікації, аналізу та управління цими ризиками. У цьому підрозділі буде детально описано підхід до розробки моделі, вибір методології та інструментів, процес формалізації моделі [17], введення вхідних даних, побудова моделі, а також її тестування та валідація. Окрім цього, буде висвітлено питання документації моделі та подальших напрямків її розвитку.

Основною метою розробки моделі оцінки ризиків для енергетичних об'єктів критичної інфраструктури є забезпечення їхньої надійності та безпеки. Модель має допомогти ідентифікувати, оцінити та управляти потенційними загрозами, що можуть вплинути на функціонування енергетичних систем. Досягнення цієї мети сприятиме мінімізації ризиків, підвищенню стійкості інфраструктури до різноманітних загроз, включаючи природні катастрофи, техногенні аварії та кібератаки.

Конкретними завданнями моделі є [18]:

- Ідентифікація та класифікація можливих загроз для енергетичних об'єктів.

- Оцінка ймовірності виникнення цих загроз та їх потенційного впливу на об'єкти критичної інфраструктури.

- Визначення ступеня ризику для кожної з ідентифікованих загроз.

- Розробка рекомендацій щодо зниження та управління виявленими ризиками.

- Верифікація та валідація моделі для забезпечення її надійності та точності.

Розробка моделі оцінки ризиків потребує ретельного вибору методологій та інструментів, що забезпечать ефективність та точність аналізу. Огляд існуючих методологій включає аналіз таких підходів, як кількісна та якісна оцінка ризиків, використання матриць ризиків, сценарного аналізу, ймовірнісно-статистичних методів та інструментів моделювання. Обґрунтування вибору методології базується на специфіці енергетичних об'єктів та характері потенційних загроз. Для моделювання ризиків буде обрано комплексний підхід, що включає як кількісні, так і якісні методи оцінки. Це дозволить отримати всебічну картину ризиків та врахувати різноманітні фактори впливу[17].

Опис використаних інструментів та технологій включає застосування спеціалізованого програмного забезпечення для моделювання та аналізу ризиків, використання геоінформаційних систем (ГІС) для просторового аналізу загроз, а також статистичних пакетів для обробки та аналізу даних. Це забезпечить точність розрахунків, візуалізацію результатів та можливість їх інтеграції у системи управління ризиками. Формалізація моделі оцінки ризиків для енергетичних об'єктів критичної інфраструктури включає кілька ключових етапів, кожен з яких забезпечує систематичний підхід до аналізу ризиків. Ключові параметри та змінні, які використовуються при розробці моделі оцінки ризиків для енергетичних об'єктів критичної інфраструктури, включають такі компоненти, які представлені на рис 2.1

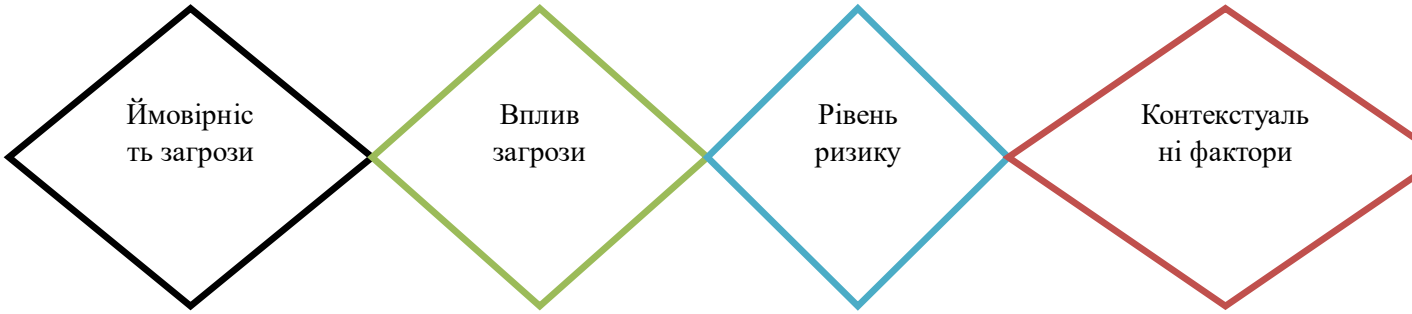


Рис. 2.1 Ключові параметри та змінні, які використовуються при розробці моделі оцінки ризиків для енергетичних об'єктів критичної інфраструктури

Джерело: розроблено автором[16]

Як видно з рис 2.1 для аналізу ризику потрібно враховувати ймовірність загрози, її вплив та рівень загрози. Ймовірність визначає шанс виникнення конкретної загрози, вплив вказує на ступінь можливих пошкоджень або негативних наслідків, а рівень ризику є комбінованою оцінкою ймовірності та впливу, що допомагає визначити загальний ризик для об'єкта. Для роботи моделі оцінки ризиків необхідні різноманітні типи даних. Історичні дані про інциденти надають інформацію про попередні інциденти та загрози, які вже виникали на подібних об'єктах. Технічні характеристики об'єктів включають детальну інформацію про конструкцію, функціональні можливості та стан енергетичних об'єктів. Експертні оцінки важливі для отримання відгуків та думок експертів у галузі енергетичної безпеки. Дані про навколишнє середовище надають інформацію про природні умови, у яких розташовані енергетичні об'єкти, включаючи кліматичні умови та можливі природні катастрофи. Кібердані включають відомості про потенційні кіберзагрози та вразливості в інформаційних системах енергетичних об'єктів.

Ризик для кожної загрози може бути розрахований як добуток ймовірності загрози на її потенційний вплив:

$$R = P \cdot I; \qquad (2.1)$$

де:

R – ризик.

P – ймовірність загрози.

I – вплив загрози.

Розглянемо спрощений приклад розрахунку для однієї загрози –землетрусу для гідроелектростанції. Припустимо, що в досліджуваному регіоні за останні 50

років сталося 5 землетрусів силою понад 6 балів. Ймовірність землетрусу на рік становить:

$$P = \frac{N}{T}; \qquad (2.2)$$

де:

P – Ймовірність загрози.

N – Кількість землетрусів за певний період.

T – Період за який виник землетрус.

Розраховуємо ймовірність загрози використовуючи формулу (2.2):

$$P = \frac{5}{50} = 0{,}1$$

Далі проводимо орієнтовану оцінку наслідків від землетрусу або іншої загрози (I):

- Приблизна вартість ремонту та відновлення: 150 мільйонів гривень.

- Втрати від простоїв виробництва електроенергії: 50 мільйонів гривень.

- Приблизна вартість компенсації: 2 мільйона гривень на людину, тобто загальна кількість збитків на 50 осіб: 100 мільйонів гривень.

- Загальний вплив оцінюється в 300 мільйонів гривень (включаючи економічні збитки і вартість людських життів).

Підставляємо отримані значення у (2.1):

$$R = 0.1 \cdot 300 \text{ млн. грн.} = 30 \text{ млн. грн.}$$

Цей приклад демонструє, як оцінка ризиків дозволяє кількісно визначити загрози і розробити стратегії для мінімізації їх впливу на критичну інфраструктуру.

Верифікація та валідація вхідних даних є критично важливими для забезпечення точності та надійності моделі. Цей процес включає оцінку достовірності та актуальності джерел даних, з яких отримуються дані. Також важливо перевірити повноту зібраних даних, щоб упевнитися, що нічого не пропущено [19]. Перехресна перевірка даних з різних джерел допомагає виявити та усунути невідповідності. Крім того, тестування моделі на реальних прикладах дозволяє перевірити її точність та адекватність. Таким чином, створення чітко структурованої моделі оцінки ризиків з використанням надійних вхідних даних та ефективних методів обробки даних сприятиме забезпеченню високого рівня безпеки та стійкості енергетичних об'єктів критичної інфраструктури. Процес тестування моделі оцінки ризиків для енергетичних об'єктів критичної інфраструктури є ключовим етапом, що забезпечує її практичну цінність та надійність.

Тестування включає кілька кроків, які будуть описані нижче. Спочатку модель тестується на стимуляційних даних, що дозволяє оцінити її поведінку в контрольованих умовах. Це можуть бути сценарії, що відтворюють різні типи загроз, наприклад, кібератаки або природні катастрофи. Симуляції допомагають виявити потенційні слабкі місця в моделі та зрозуміти, як вона реагує на різні типи вхідних даних [20].

Після успішного тестування на симуляційних даних модель застосовується до реальних даних, зібраних з енергетичних об'єктів. Це дозволяє перевірити її точність та ефективність у реальних умовах. Тестування на реальних даних включає аналіз історичних інцидентів та поточних загроз, а також використання даних від моніторингових систем та датчиків, встановлених на об'єктах.

Валідація (процес підтвердження відповідності) моделі здійснюється шляхом порівняння результатів, отриманих за допомогою моделі, з відомими даними та подіями. Основними етапами валідації є [21]:

- Перевірка точності прогнозів. Оцінка, наскільки точно модель передбачає виникнення та вплив загроз. Це включає порівняння прогнозованих результатів з реальними подіями.

- Аналіз відхилень. Виявлення та аналіз відхилень між прогнозованими та фактичними результатами. Це дозволяє зрозуміти, де модель може давати неточності або помилки.

- Аналіз чутливості. Перевірка, як зміна вхідних даних впливає на результати моделі. Це допомагає визначити, які параметри мають найбільший вплив на оцінку ризиків.

Після завершення тестування та валідації результати аналізуються для внесення необхідних коригувань. Основні кроки цього процесу включають:

- Оцінка результатів тестування. Розгляд та аналіз усіх результатів тестування, щоб виявити можливі помилки або недоліки моделі.

- Внесення коригувань. Модифікація моделі для усунення виявлених недоліків. Це може включати зміну параметрів моделі, додавання нових компонентів або уточнення існуючих методів оцінки ризиків.

- Повторне тестування. Після внесення змін модель повторно тестується для підтвердження, що коригування покращили її точність та адекватність.

- Постійне вдосконалення. На основі результатів повторних тестувань модель постійно вдосконалюється, щоб забезпечити її максимальну ефективність у різних сценаріях та умовах.

Для розробки моделі оцінки ризиків для енергетичних об'єктів критичної інфраструктури можна використати комплексний підхід, який включатиме в себе різні аспекти, такі як технічні, економічні, соціальні та природні чинники.

Приклад структури такої моделі, яка була розроблена у даній дипломній роботі представлений на рис 2.2.

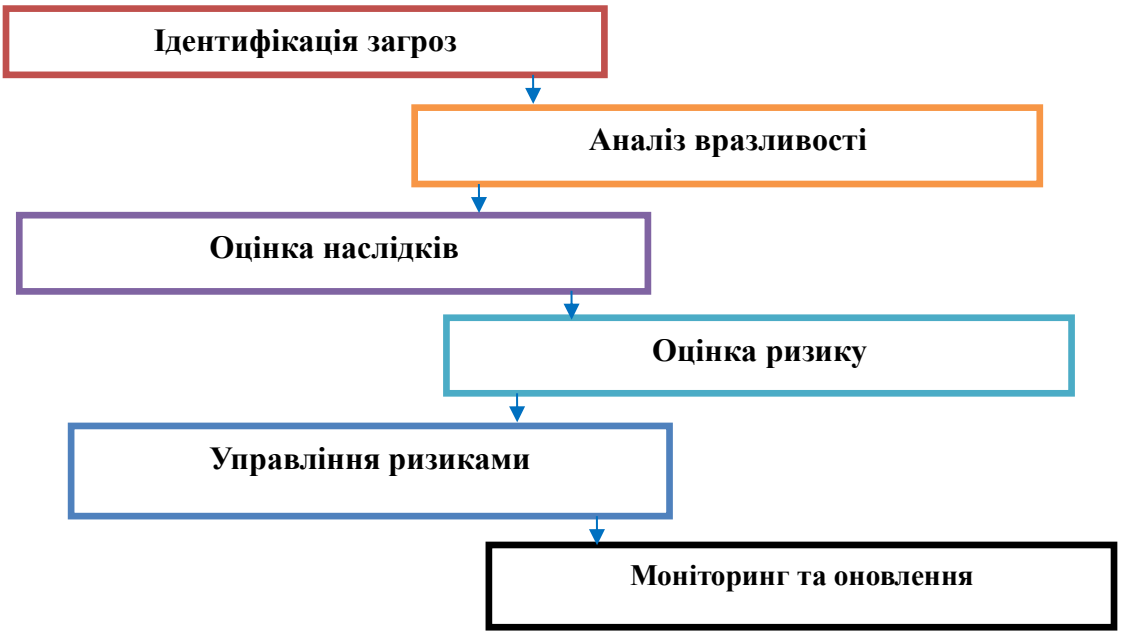


Рис. 2.2 Структура моделі оцінки ризиків для енергетичних об'єктів

Джерело: розроблено автором

Як видно рис 2.2 процес оцінки ризиків за розробленою моделлю починається з ідентифікації потенційних загроз для енергетичних об'єктів, таких як технічні відмови, природні катастрофи та кібератаки. Потім проводиться оцінка ймовірності виникнення кожної загрози, а також аналіз вразливості системи енергопостачання та оцінка рівня вразливості кожного об'єкта. Далі визначаються можливі наслідки для кожної загрози, такі як економічні втрати, втрати людських життів та припинення енергопостачання, і проводиться оцінка їхньої серйозності. Після цього інформація про ймовірність, вразливість та можливі наслідки комбінується для визначення загального рівня ризику. Управління ризиками, що включає в себе розробку стратегій мінімізації ризиків та забезпечення стійкості енергетичних об'єктів, а також визначення заходів превентивного характеру та реагування в разі виникнення небезпек. Нарешті, важливо здійснювати постійний моніторинг рівня ризиків та оновлення моделі з урахуванням нових загроз та змін у системі енергопостачання. Ця модель може бути адаптована для конкретних умов та потреб дослідження енергетичних

об'єктів критичної інфраструктури, дозволяючи забезпечити ефективне управління ризиками та забезпечення безпеки.

Отже, розроблена модель оцінки ризиків для енергетичних об'єктів критичної інфраструктури є комплексним інструментом, що враховує всі ключові аспекти ризиків та забезпечує їх ефективну оцінку. Модель може бути використана для ідентифікації та мінімізації ризиків, що сприятиме підвищенню захищеності та стійкості енергетичних об'єктів перед потенційними загрозами.

2.2. Застосування розробленої моделі до конкретних енергетичних об'єктів

Розробка моделі оцінки ризиків для енергетичних об'єктів критичної інфраструктури є лише першим кроком у комплексному процесі забезпечення їхньої безпеки. Наступним етапом є застосування цієї моделі до реальних об'єктів з метою оцінки її ефективності та практичної цінності. Це дозволить не лише перевірити модель у реальних умовах, але й отримати цінні дані для подальшого вдосконалення методології оцінки ризиків.

Вибір об'єктів для дослідження є важливим етапом у процесі оцінки ризиків для енергетичних об'єктів критичної інфраструктури. Вибір здійснювався на основі кількох критеріїв, які дозволили відібрати об'єкти, що мають значну важливість для енергетичної системи та є потенційно вразливими до різних загроз [23]. Основними критеріями вибору були: стратегічне значення об'єкта, тип енергетичного об'єкта (електростанції, атомні станції, гідроелектростанції, енергетичні мережі), географічне розташування, а також доступність даних для проведення аналізу [24]. Опис обраних об'єктів та їх характеристик включає детальну інформацію про кожен об'єкт, зокрема його потужність, тип використовуваної енергії, рік введення в експлуатацію, кількість персоналу та основні технологічні процеси.

У даній дипломній роботі для проведення досліджень та аналізу були обрані два об'єкти енергетичної інфраструктури: Київська теплоелектроцентраль (ТЕЦ) та Дніпровська гідроелектростанція (ГЕС). У додатку А представлена Київська теплоелектроцентраль (ТЕЦ), а у додатку Б Дніпровська

гідроелектростанція (ГЕС). Обидва ці об'єкти представляють важливі компоненти енергетичної інфраструктури України і мають стратегічне значення для забезпечення енергетичної безпеки країни.

Київська ТЕЦ є однією з ключових теплових електростанцій столиці України, що забезпечує постачання тепла та електроенергії для жителів та промислових підприємств міста. Цей об'єкт має велике значення для стабільності енергопостачання у регіоні та економічного розвитку Києва. Дніпровська ГЕС є однією з найбільших гідроелектростанцій на території України та має велике значення для виробництва електроенергії та регулювання водних ресурсів на Дніпрі. Ця гідроелектростанція відіграє важливу роль у забезпеченні енергетичної безпеки країни та сталого розвитку енергетичного сектору. Обидва об'єкти є об'єктами критичної інфраструктури, на які можуть впливати різноманітні загрози, тому проведення аналізу ризиків для них є актуальною та важливою задачею. Використання розробленої моделі оцінки ризиків дозволить здійснити комплексний аналіз потенційних загроз та прийняти ефективні заходи для забезпечення безпеки та стійкості цих об'єктів енергетичної інфраструктури.

Застосування розробленої моделі до Київської ТЕЦ дозволило провести аналіз ризиків та визначити потенційні загрози для надійності та безпеки енергопостачання Києва. Результати цього дослідження можуть бути корисні для розробки стратегій управління ризиками та підвищення стійкості енергетичних систем у місті. Такий підхід сприяє покращенню ефективності управління критичною інфраструктурою та забезпеченню безперебійного енергопостачання міста у найрізноманітніших ситуаціях.

Для застосування розробленої моделі оцінки ризиків до Київської ТЕЦ, спочатку необхідно провести ідентифікацію потенційних загроз, які можуть вплинути на роботу цього енергетичного об'єкту. Це можуть бути технічні відмови обладнання, природні катастрофи, кібератаки або інші фактори, що можуть призвести до порушення енергопостачання. Після визначення загроз потрібно проаналізувати вразливість Київської ТЕЦ до кожної з них. Наприклад,

вразливими місцями можуть бути паливні системи, електротехнічне обладнання або системи управління. Оцінка рівня вразливості дозволить визначити, наскільки ефективно об'єкт здатний протистояти потенційним загрозам. Після цього проводиться оцінка можливих наслідків для кожної загрози. Це може включати економічні втрати від зупинки роботи ТЕЦ, втрати електропостачання для мешканців та підприємств, а також можливість погіршення екологічної ситуації у разі аварій.

Далі проводиться оцінка ризику, підсумком якої буде визначення загального рівня ризику для Київської ТЕЦ. Залежно від результатів, розробляються стратегії мінімізації ризиків та плани дій у разі виникнення небезпек. Наприклад, можуть виконуватися заходи щодо підвищення надійності обладнання, створення резервних джерел енергії або вдосконалення систем моніторингу та контролю за станом об'єкту. Також важливим є постійний моніторинг рівня ризиків та оновлення моделі в залежності від змін у функціонуванні ТЕЦ та зовнішніх загроз. Додатковим потенційним чинником ризику для Київської ТЕЦ є можливість військових дій або терористичних актів, зокрема внаслідок конфлікту з російською федерацією. Умови воєнного стану та військових дій можуть створювати серйозні загрози для енергетичних об'єктів, включаючи можливість порушення роботи електростанцій через напади, обстріли або інші форми військової агресії. Такі сценарії можуть призвести до значного зниження енергопостачання та порушення безпеки енергетичних систем, що становить серйозну загрозу для економіки та безпеки країни в цілому. Тому необхідно враховувати цей фактор під час оцінки ризиків та розробки стратегій управління ризиками для Київської ТЕЦ.

За допомогою розробленої моделі оцінки ризиків також було проведено аналіз безпеки та стійкості Дніпровської гідроелектростанції (ГЕС) в умовах можливих загроз. Під час застосування моделі виконувалися такі етапи, які представлені у таблиці 2.1.

Таблиця 2.1 [23]

Етапи застосування моделі оцінки ризиків для енергетичних об'єктів на прикладі Дніпровської гідроелектростанції (ГЕС)

Етап	Опис
Ідентифікація загроз	Визначені потенційні загрози для Дніпровської ГЕС, такі як природні катастрофи, технічні відмови обладнання та можливі воєнні дії, включаючи постріли, які можуть виникнути в умовах конфлікту з російською федерацією.
Аналіз вразливості	Встановлені вразливі місця у системі Дніпровської ГЕС, такі як електрогенеруючі агрегати та системи автоматизації, які можуть бути піддані впливу внаслідок військових дій або технічних проблем.
Оцінка наслідків	Визначені можливі наслідки для Дніпровської ГЕС у разі виникнення загроз, такі як втрати виробництва електроенергії, екологічні збитки та ризики для працівників станції.
Оцінка ризику	Проведена оцінка загального рівня ризику для Дніпровської ГЕС, яка враховувала імовірність виникнення загроз, вразливість об'єктів та серйозність можливих наслідків.
Управління ризиками	Управління ризиками. Розроблені стратегії мінімізації ризиків для Дніпровської ГЕС, включаючи вдосконалення систем безпеки, розробку планів евакуації та підвищення свідомості персоналу щодо можливих небезпек.
Моніторинг та оновлення	Розроблено план постійного моніторингу рівня ризиків та оновлення моделі з урахуванням нових загроз та змін у системі Дніпровської ГЕС, зокрема з урахуванням геополітичних подій та можливих воєнних конфліктів.

Як видно з табл. 2.1 Основні етапи розробленої моделі включають визначення загроз, аналіз вразливостей, оцінку можливих наслідків, розрахунок загального рівня ризику, розробку стратегій мінімізації ризиків та встановлення моніторингу та оновлення планів. Цей підхід спрямований на забезпечення безпеки та стійкості функціонування станції в умовах можливих загроз.

Отже, проведена ідентифікація потенційних загроз для Дніпровської ГЕС дозволила чітко визначити різноманітні можливі сценарії ризику, включаючи технічні відмови, природні катастрофи, кібератаки та можливі військові загрози внаслідок конфлікту з Російською Федерацією. Це допомогло підготувати підґрунтя для подальшої оцінки ризиків та розробки стратегій управління ризиками. Використання розробленої методології дозволило здійснити оцінку ризиків для Дніпровської ГЕС, враховуючи різноманітні потенційні загрози. Обґрунтовано вибір методології та інструментів, що найкращим чином

відповідають характеру досліджуваного об'єкту. Формалізація моделі оцінки ризиків для Дніпровської ГЕС включила чітке визначення ключових компонентів та змінних, що дозволило систематизувати процес оцінки ризиків та забезпечити його ефективність. Проведений аналіз вказав на необхідність ретельного збору та обробки вхідних даних для вивчення ризиків для енергетичних об'єктів. Застосування розробленої моделі оцінки ризиків до Дніпровської ГЕС надало можливість ідентифікувати основні загрози та вразливості енергетичного об'єкту, що є важливим кроком у розробці стратегій управління ризиками та забезпеченні стійкості енергетичних об’єктів.

РОЗДІЛ 3. АНАЛІЗ ОТРИМАНИХ РЕЗУЛЬТАТІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ

3.1. Детальний аналіз отриманих результатів дослідження

В цьому підрозділі проводиться детальний аналіз результатів дослідження, що стосується застосування розробленої моделі оцінки ризиків до конкретних енергетичних об'єктів - Київської ТЕЦ та Дніпровської ГЕС. Цей аналіз дозволить глибше зрозуміти виявлені загрози, вразливості та потенційні наслідки для об'єктів інфраструктури.

Під час ідентифікації загроз для Київської ТЕЦ та Дніпровської ГЕС було проведено аналіз потенційних небезпек, які можуть вплинути на їхню нормальну експлуатацію та функціонування. Цей аналіз включав в себе виявлення технічних відмов, що можуть виникнути через поломки у обладнанні, недоліки у системі безпеки або несправності у виробництві. Природні катастрофи також були враховані, оскільки вони можуть призвести до затримок у постачанні палива, пошкодження інфраструктури або навіть призупинення роботи електростанцій. Крім того, потенційні кібератаки та військові загрози були розглянуті як можливі ризики, оскільки вони можуть призвести до порушень у роботі систем керування та управління енергетичними об'єктами [24-26].

У Додатку В представлений послідовний розвиток екологічних катастроф при руйнуванні об’єктів критичної інфраструктури, а у додатку Г показано графічне представлення ефекту доміно, яке може виникнути внаслідок реалізації потенційних загроз та небезпек по відношенню до енергетичної галузі.

Слід також зазначити, що визначення загроз для енергетичної інфраструктури стало першим етапом у процесі оцінки ризиків та розробки стратегій управління ними для забезпечення стійкості та безпеки енергетичних об'єктів.

Після ідентифікації потенційних загроз було проведено оцінку рівня вразливості енергетичних систем, зокрема Київської ТЕЦ та Дніпровської ГЕС. Цей аналіз включав в себе визначення вразливих місць у системі

енергопостачання, які можуть бути особливо схильні до негативного впливу у разі виникнення загроз. Такі вразливі місця можуть включати в себе слабкі моменти у системі безпеки, технічні недоліки у виробництві електроенергії, а також недостатню захищеність інфраструктури від природних або техногенних катастроф. Оцінка рівня вразливості була спрямована на визначення критичних точок, де можуть виникнути проблеми, а також розробку стратегій та заходів для їхнього усунення або зменшення ризику впливу загроз на енергетичні системи.

Після ідентифікації потенційних загроз та визначення рівня вразливості систем енергопостачання Київської ТЕЦ та Дніпровської ГЕС, була проведена оцінка можливих наслідків для кожної з цих загроз. Цей етап аналізу включав визначення потенційних наслідків у разі виникнення кожної загрози, таких як економічні втрати, втрати людських життів, припинення енергопостачання тощо. Для оцінки наслідків було важливо врахувати різні аспекти, такі як масштаб і тривалість можливих наслідків, вплив на довкілля та суспільство, а також економічні втрати для держави та громадян. Результати оцінки наслідків надали інформацію для подальшого визначення загального рівня ризику та розробки стратегій управління ризиками для забезпечення стійкості енергетичних об'єктів.

Оцінка ризику включала комбінування інформації про ймовірність виникнення загроз, рівень вразливості системи енергопостачання та потенційні наслідки в разі реалізації цих загроз. За допомогою цієї інформації визначався загальний рівень ризику для Київської ТЕЦ та Дніпровської ГЕС. Ризик оцінювався з урахуванням його серйозності та імовірності виникнення. Чим вище ймовірність виникнення загрози та її серйозність, тим вищий загальний рівень ризику. Визначений ризик допомагав ідентифікувати найбільш критичні аспекти безпеки енергетичних об'єктів та спрямовував увагу на розробку пріоритетних стратегій управління ризиками. Управління ризиками включало розробку стратегій для мінімізації виявлених ризиків та забезпечення стійкості енергетичних об'єктів.

Етапи розробки стратегій управління ризиками представлені на рис 3.1.

Рис 3.1 Етапи розробки стратегій управління ризиками

Джерело: розроблено автором [25]

Як видно з рис 3.1 у першому етапі виконується розробка заходів превентивного характеру, спрямованих на запобігання виникненню потенційних загроз. Це може включати оновлення систем безпеки, підвищення рівня технічного обслуговування та планування екстрених ситуацій. Другий етап передбачає створення планів реагування на небезпечні ситуації.

Ці плани включають процедури екстреного реагування, розробку евакуаційних планів та інші заходи для забезпечення безпеки персоналу та майна. Третій етап - навчання та тренування персоналу. Проведення навчальних семінарів, тренувань та симуляційних вправ допомагає підготувати персонал до екстрених ситуацій та впровадження в практику реагування на них. Нарешті, четвертий етап передбачає вдосконалення систем моніторингу та контролю [27]. Це включає вдосконалення систем відслідковування та контролю за станом обладнання, робочих процесів та потенційних загроз для вчасного виявлення проблем та запобігання негативним наслідкам.

Крім того, важливим аспектом є постійний аналіз та оновлення стратегій, що передбачає проведення регулярного аналізу ризиків та ефективності заходів управління ризиками для виявлення нових загроз та оновлення стратегій управління відповідно до змін у середовищі.

Ці етапи розробки стратегій спрямовані на забезпечення оптимального рівня безпеки та стійкості енергетичних об'єктів у випадку виникнення небезпечних ситуацій. Моніторинг та оновлення включають в себе низку дій, спрямованих на постійне відслідковування рівня ризиків, оновлення моделі оцінки ризиків та впровадження нових заходів управління ризиками.

Основні етапи моніторингу та оновлення процесу управління ризиками представлені на рис 3.2.

Рис 3.2 Основні етапи моніторингу та оновлення процесу управління ризиками

Джерело: розроблено автором [28]

Як видно з рис 3.2 постійний моніторинг полягає в аналізі потенційних загроз, оновленні даних та відслідковуванні змін у середовищі. Оновлення моделі оцінки ризиків є необхідним для врахування нових даних та знань. Аналіз ефективності заходів включає оцінку ефективності вжитих заходів та їхнього коригування. Навчання та підготовка персоналу є важливим для готовності до дій у разі небезпеки. Комунікація та співпраця з іншими сторонами допомагають у обміні інформацією та ресурсами в разі потреби.

Отже, проведений детальний аналіз результатів дослідження показав, що обидва енергетичні об'єкти, як Київська ТЕЦ, так і Дніпровська ГЕС, стикаються з різноманітними потенційними загрозами, включаючи технічні відмови, природні катастрофи, кібератаки та можливі військові конфлікти. Ці загрози можуть призвести до серйозних наслідків, таких як припинення енергопостачання, економічні втрати та загрози безпеці.

3.2 Розробка практичних рекомендацій

У цьому підрозділі проведено розробку практичних рекомендацій щодо управління ризиками в контексті енергетичних об'єктів, зокрема Київської ТЕЦ та Дніпровської ГЕС. Рекомендації розроблялись з урахуванням результатів аналізу загроз, вразливостей, наслідків та ризиків, отриманих під час дослідження, з метою забезпечення оптимального функціонування енергетичних об'єктів в умовах можливих загроз та викликів.

Під час розробки практичних рекомендацій для управління ризиками енергетичних об'єктів, таких як Київська ТЕЦ та Дніпровська ГЕС, було враховано різноманітні фактори, що впливають на їхню стійкість та надійність. Основні аспекти рекомендацій включають:

1. Підвищення технічної готовності. Рекомендується посилення технічного обслуговування та ремонту обладнання енергетичних об'єктів, щоб зменшити ймовірність технічних відмов та аварій.

2. Вдосконалення систем безпеки. Рекомендується впровадження сучасних систем моніторингу, виявлення та запобігання кібератак, а також підвищення рівня фізичної безпеки на об'єктах.

3. Розробка планів надзвичайних ситуацій. Рекомендується розробка та впровадження планів дій у випадку надзвичайних ситуацій, таких як природні катастрофи або військові загрози.

4. Забезпечення резервного живлення. Рекомендується створення резервних джерел енергії та систем енергозабезпечення для забезпечення безперебійної роботи об'єктів у разі відмов основних джерел енергії.

5. Підготовка персоналу. Рекомендується проведення регулярних навчань та тренувань персоналу з метою ефективної реакції на надзвичайні ситуації та мінімізації можливих наслідків.

6. Постійний моніторинг та аналіз. Рекомендується встановлення систем постійного моніторингу та аналізу ризиків з метою вчасного виявлення потенційних загроз та прийняття відповідних заходів з управління ризиками.

Ці рекомендації спрямовані на покращення стійкості та безпеки енергетичних об'єктів в умовах постійно мінливого середовища та можливих загроз.

Отже, основна частина розробки практичних рекомендацій полягає в аналізі отриманих результатів та визначенні конкретних кроків для зменшення ризиків і підвищення стійкості енергетичних об'єктів, таких як Київська ТЕЦ та Дніпровська ГЕС. Покращення технічної інфраструктури: Важливо провести оновлення технічного обладнання та мереж, а також забезпечити регулярне обслуговування для запобігання технічним відмовам. Захист від кібератак: Рекомендується впровадження сучасних систем кібербезпеки, включаючи програмне та апаратне забезпечення, а також проведення регулярних аудитів безпеки. Розробка планів надзвичайних ситуацій: Необхідно розробити детальні плани дій у випадку природних катастроф, технічних аварій, кібератак або військових загроз. Забезпечення навчання персоналу: Важливо забезпечити регулярні тренування та навчання персоналу з питань безпеки, а також ознайомлення з процедурами реагування на надзвичайні ситуації. Впровадження систем моніторингу та аналізу: Рекомендується встановлення систем постійного моніторингу за станом енергетичних об'єктів та аналізу потенційних загроз.

ВИСНОВКИ

Енергетичні об’єкти критичної інфраструктури є невід'ємною складовою сучасного суспільства, оскільки вони забезпечують незмінне постачання енергії, необхідне для функціонування всіх галузей економіки. Проте, ці об'єкти також стикаються з різними загрозами, такими як природні катастрофи, технологічні збої, кібератаки та інші. Безпека в цьому контексті визначається рівнем захищеності критичної інфраструктури, який забезпечує її функціональність, безперервність роботи, цілісність та стійкість. Для забезпечення безпеки використовуються різноманітні методи та стратегії, включаючи технічні, організаційні та регулятивні заходи. Висновки цього аспекту підкреслюють необхідність ретельного розуміння та ефективного управління цими поняттями в контексті енергетичних об'єктів критичної інфраструктури. Це сприятиме кращому захисту критичних інфраструктурних об'єктів від потенційних загроз та забезпечить їх безперервну роботу та стійкість, сприяючи стабільності та прогресу суспільства.

Після ретельного аналізу різноманітних підходів до оцінки загроз для енергетичних об'єктів стає очевидним, що існують різні методи та стратегії, які застосовуються для виявлення, класифікації та оцінки потенційних небезпек. Різноманітність в підходах до аналізу загроз визначається особливостями кожного конкретного об'єкту, його контекстом та вимогами безпеки. Детальний аналіз принципів та методів ідентифікації, класифікації, оцінки ризиків та прогнозування наслідків розкриває широкий спектр підходів та їхню ефективність у різних умовах.

Кожен із цих підходів має свої переваги та обмеження, і вибір конкретного методу повинен враховувати специфіку досліджуваного об'єкту та мети оцінки загроз. Незважаючи на різноманітність методів, важливо пам'ятати про постійну зміну загроз та викликів, зокрема, у зв'язку з технологічними розвитками та геополітичною ситуацією. Тому гнучкість та адаптивність оціночних методів відіграють ключову роль у забезпеченні ефективного контролю та захисту

енергетичних об'єктів критичної інфраструктури. Методи та моделі для визначення рівня загроз та ризиків є важливими інструментами у процесі управління ризиками. Вони допомагають організаціям отримати краще розуміння своїх слабких місць та потенційних загроз, а також розробляти ефективні стратегії для їх зменшення. Жоден метод або модель не є абсолютно точним, і всі вони мають свої переваги та недоліки. Вибір конкретного методу або моделі залежить від конкретної ситуації та цілей дослідження. Моделювання загроз може бути корисним для систематичного аналізу потенційних шляхів атаки, але цей метод може бути часо- та ресурсозатратним і потребувати значних технічних знань. Оцінка ризиків може бути менш технічною, проте вона може не враховувати всі можливі шляхи атаки.

У даній дипломній роботі була розроблена модель оцінки ризиків для енергетичних об'єктів критичної інфраструктури є комплексним інструментом, що враховує всі ключові аспекти ризиків та забезпечує їх ефективну оцінку. Модель може бути використана для ідентифікації та мінімізації ризиків, що сприятиме підвищенню захищеності та стійкості енергетичних об'єктів перед потенційними загрозами. Після проведеної ідентифікації потенційних загроз для Дніпровської ГЕС стало можливим чітко визначити різноманітні можливі сценарії ризику, такі як технічні відмови, природні катастрофи, кібератаки та можливі військові загрози у зв'язку з конфліктом з Російською Федерацією. Цей аналіз став фундаментом для подальшої оцінки ризиків та розробки стратегій управління ними. Використання розробленої методології дозволило провести оцінку ризиків для Дніпровської ГЕС, враховуючи різноманітні потенційні небезпеки. Обґрунтувано було вибір методології та інструментів, найбільш відповідних для даного об'єкту. Формалізація моделі оцінки ризиків включала чітке визначення ключових компонентів та змінних, що сприяло систематизації процесу оцінки та його ефективності.

Проведений аналіз підкреслив необхідність ретельного збору та обробки вхідних даних для дослідження ризиків енергетичних об'єктів. Верифікація та

валідація отриманих даних виявилися важливими етапами у процесі розробки моделі оцінки ризиків. Тестування та валідація моделі на прикладі Дніпровської ГЕС дозволили підтвердити її точність та адекватність для конкретних енергетичних об'єктів. Використання розробленої моделі оцінки ризиків для Дніпровської ГЕС допомогло ідентифікувати основні загрози та вразливості цього енергетичного об'єкту, що є важливим кроком у розробці стратегій управління ризиками та забезпеченні стійкості енергетичних об'єктів.

Після ретельного аналізу результатів дослідження стало очевидним, що як Київська ТЕЦ, так і Дніпровська ГЕС, мають різноманітні потенційні загрози, включаючи технічні невдачі, природні катастрофи, кібератаки та можливі військові конфлікти. Ці загрози можуть призвести до серйозних наслідків, таких як припинення енергопостачання, великі економічні втрати та порушення безпеки. В аналізі виявлено основні слабкі місця систем, які можуть бути особливо вразливими в разі загроз. Проведена оцінка ризиків дозволила встановити загальний рівень ризику для обох об'єктів та визначити конкретні пріоритети для подальшого управління ризиками. Не менш важливим було розроблення стратегій для мінімізації ризиків з метою забезпечення стійкості та безпеки енергетичних об'єктів у випадку можливих загроз. Результати дослідження підкреслюють потребу в постійному моніторингу, оновленні та удосконаленні стратегій управління ризиками для забезпечення ефективної роботи енергетичної інфраструктури. Впровадження відповідних заходів допоможе зменшити вплив потенційних загроз та забезпечить надійність та стабільність енергетичних об'єктів у складних умовах зовнішнього середовища.

Ключова частина розробки практичних рекомендацій полягає в оцінці отриманих результатів та формулюванні конкретних заходів для зменшення ризиків та підвищення стійкості енергетичних об'єктів, таких як Київська ТЕЦ та Дніпровська ГЕС. Першим етапом є покращення технічної інфраструктури, включаючи оновлення обладнання та мереж і проведення регулярного обслуговування для запобігання технічним проблемам. Другим заходом є

забезпечення захисту від кібератак шляхом впровадження сучасних систем кібербезпеки та проведення регулярних аудитів безпеки. Третім кроком є розробка докладних планів надзвичайних ситуацій для реагування на природні катастрофи, технічні аварії, кібератаки та військові загрози. Крім того, важливо забезпечити навчання персоналу з питань безпеки та проведення регулярних тренувань з процедур реагування на надзвичайні ситуації. Нарешті, рекомендується встановлення систем моніторингу та аналізу для постійного контролю за станом енергетичних об'єктів та виявлення потенційних загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Указ Президента України №392/2020 Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/3922020-35037

2. Постанова Кабінету Міністрів України від 23.12.2004 № 1734 «Про затвердження переліку підприємств, які мають стратегічне значення для економіки та безпеки держави»

3. Рішення Ради національної безпеки і оборони України від 28 серпня 2014 року "Про невідкладні заходи щодо захисту України та зміцнення її обороноздатності" http://president.gov.ua/documents/18125.html

4. Качинський А. Б. Безпека, загрози і ризик : наукові концепції та математичні методи / А. Б. Качинський// – К.: 2023. – 472 с

5. Бірюков Д. С. Захист критичної інфраструктури в Україні: від наукового осмислення до розробки засад політики [Електронний ресурс] / Д. С. Бірюков // Наук.- інформ. вісн. Акад. нац. безпеки. – 2022. – № 3-4. – С. 155- 170.

6. Кодрик А.І., Яковлєв Є.О., Чумаченко С.М., Парталян А.С. Методичні підходи до геоінформаційного аналізу еколого-техногенних загроз для вуглепромислових районів Донбасу (на прикладі ПАО “Лисичанськвугілля” та ДП “Первомайськвугілля”) // Математичне моделювання в економіці. Міжнародний науковий журнал. № 4 (13), жовтень-грудень 2018 р. С. 5-17

7. Бобро Д.Г. Методологія оцінки рівня в критичній інфраструктурі / Д.Г. Бобро // Стратегічні пріоритети. – Серія «Економіка». – 2015. – № 4 (37). – С. 83-93.

8. Лещенко О. Я. «Гібридна війна» як науковий конструкт: проблеми пошуку термінологічної та концептуальної сутності. Гілея: науковий вісник. К.: 2017. Вип.117. С. 262-267.

9. Чумаченко С. М., Парталян А. С., Туровець Ю. С. Система підтримки прийняття рішень щодо управління станом навколишнього середовища на

військових об’єктах у зоні збройного конфлікту // Форми та способи застосування військ (сил) за досвідом проведення антитерористичної операції на території Донецької та Луганської областей: зб. матер. наук.-практ. конф. (Київ, 15 листопада 2017 р.) / Київ: ЦНДІ ЗС України, 2017. С. 232–234. Інв. № 17806 (ЦНДІ ЗС України).

10. Морщ Є.В. Особливості розробки та реалізації комп’ютерної моделі для оцінки економічної шкоди від надзвичайних ситуацій техногенного походження з використанням геоінформаційних технологій і методу системної динаміки / С.М. Чумаченко, Є.О. Яковлєв, Є.В. Морщ, А.С. Парталян, О.Г. Гуйда // Вчені записки Таврійського національного університету ім. В.І. Вернадського. – Київ: Видавничий дім «Гельветика», 2020. – Том 31 (70), ч. 1. №6. – С. 156 – 164.

11. Операція об'єднаних сил [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/ Операція об'єднаних сил

12. Закон України «Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях».

13. Омаров Азад Енвер огли. Проблеми та протиріччя в реалізації політики екологічної безпеки в Україні / Омаров Азад Енвер огли. // Теорія і практика державного управління. – 2016. – №4. – С. 1–6.

14. Іванюта С. П. Екологічні і техногенні загрози у зоні військового конфлікту на Сході України / С. П. Іванюта. // Енергетична, екологічна і техногенна безпека Стратегічна панорама. – 2017. – №1. – С. 53–60.

15. Побережна Л. Я. Оцінка потенційних екологічних ризиків внаслідок проведення антитерористичної операції / Л. Я. Побережна, А. І. Станецький. // Науково-технічний журнал "Техногенно-екологічна безпека". – 2017. – С. 45–52.

16. Настасенко О. Г. Системний підхід щодо ліквідації загроз екологічної катастрофи у зоні антитерористичної операції / О. Г. Настасенко, О. І. Бондар, О. А. Машков. // Науково-практичний журнал "Екологічні науки". – С. 5–20.

17. Морщ Є.В. Аналіз впливу воєнно-техногенного навантаження бойових дій на складові навколишнього природного середовища / Є.В. Морщ // Техногенноекологічна безпека та цивільний захист. – Київ: ДУ «ІГНС НАНУ», 2018. – Вип. 3 (13). –Инв. № 63.– С. 110 – 116

18. Чумаченко С. М. Особливості застосування методів екологічної оцінки для оцінювання впливу бойових дій на складові військових природно-техногенних геосистем / С. М. Чумаченко, С. Л. Данилюк // Зб. наук. пр. ЦНДІ ЗС України. – К., 2015. – № 2 (72). –С. 100–114. – (Таємно; інв. № 45179).

19. Чумаченко С.М. Оцінювання загроз об'єктам критичної інфраструктури / С. М. Чумаченко, В.В. Троцько // Науковий вісник: Цивільний захист та пожежна безпека– Вип. 1 (3). – К.: УкрНДІ ЦЗ, 2017. – С. 41-47

20. Чернега В.М. Аналіз критичної інфраструктури та напрямки досліджень систем життєзабезпечення об'єктів України : Аналітична записка. [Електронний ресурс]. – Режим доступу: file:///C:/Users/Student/Desktop/96-4193-1-10-20161205.pdf.

21. Морщ Є.В. Обґрунтування показників для оцінки впливу бойових дій на об'єкти критичної інфраструктури / С.М. Чумаченко, Є.В. Морщ // Техногенно екологічна безпека та цивільний захист. – Київ: ДУ «ІГНС НАНУ», 2017. – Вип. 3 (9). –Инв. № 59. – С. 121-127.

22. Дудкін О. В. Оцінка і напрямки зменшення загроз біорізноманіттю України / О. В. Дудкін, А. В. Єна, С. М. Чумаченко та ін. – К.: Хімджест, 2003. – 400 с.

23. Чумаченко С. М. Метод оцінки екологічних загроз від заходів бойової підготовки на військовому полігоні / С. М. Чумаченко // Зб. наук. пр. – Вип. 4 (29). – К.: ННДЦ ОТ і ВБ України, 2005. – С. 93-103. − (Таємно; інв. №39110).

24. Довгий О.С., Коржнєв М.М., Трофимчук О.М., Чумаченко С.М., Яковлев Є.О. та ін. Екологічні ризики, збитки та раціональні межі використання надр в Україні. - К.: Ніка-Центр, 2013. - 314 с.

25. Стан басейну Сіверського Дінця та фактори впливу в умовах військових дій. Технічний звіт. - ОБСЄ, 2018. – 88 с.

26. Морщ Є.В. Методика комплексного оперативного експертного оцінювання військово-техногенних загроз в зоні проведення операції об'єднаних сил / Чумаченко С.М., Морщ Є.В., Михайлова А.В., Парталян А.С. // Науковий вісник: Цивільний захист та пожежна безпека. №1 (9), 2020. С. 23-33

27. Дядченко В.В. Бойові токсичні хімічні речовини: підручник у 3 т. Т. 1 Хімічна зброя / В.В. Дядченко, С.Ю. Петрухін, О.І. Новіков. – Х.: ФОП Бровін О.В., 2018. – 532 с.

28. 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.

29. Y Yakovliev, S Chumachenko Ecological Threats in Donbas, Ukraine - Centre for Humanitarian Dialogue. Ceneva, 2017. 60 c.

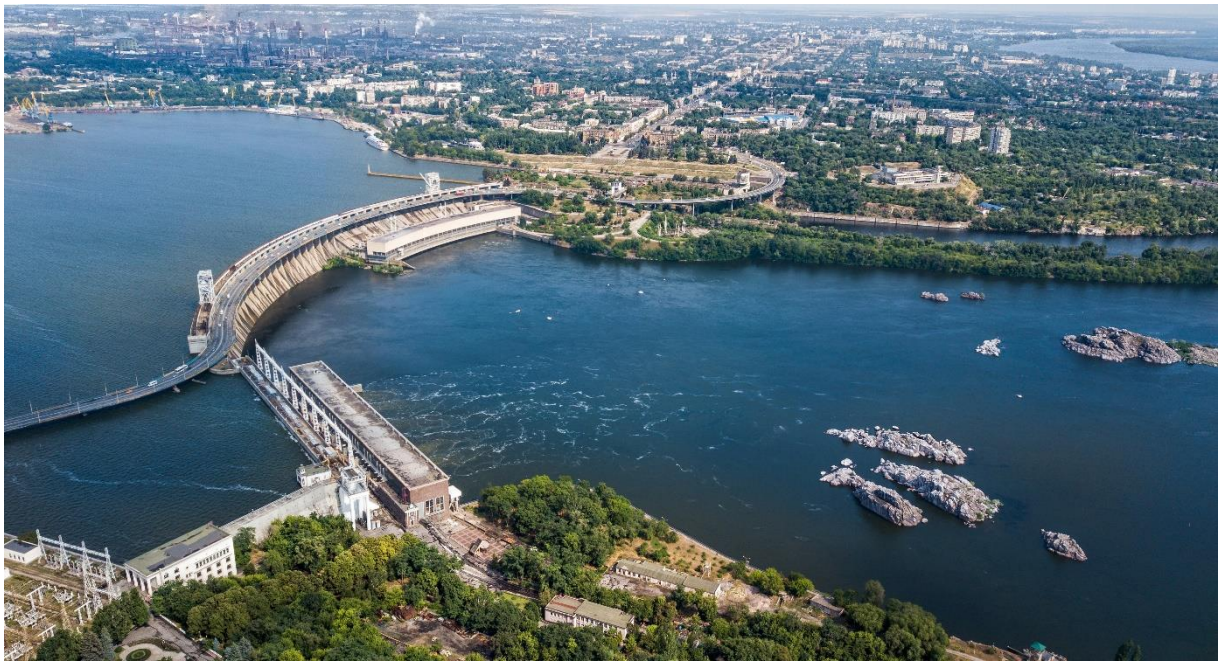
30. Critical Infrastructure Protection Month: Presidential Proclamation / The White House. – 2011. – November 30 [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/the-press-office/2011/11/30/presidentialproclamation-criticalinfrastructure-protection-month-2011.

31. On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection: Council Directive 2008/114/EC [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu.

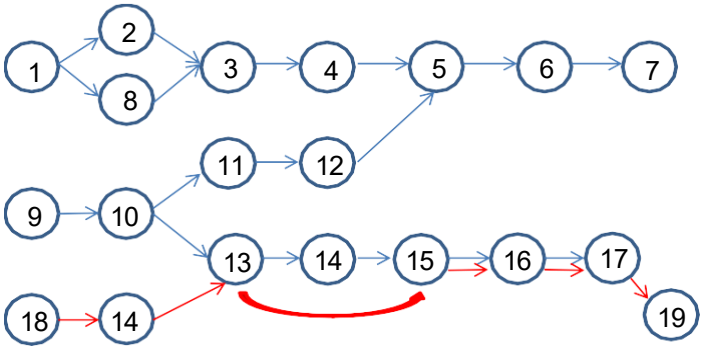
ДОДАТКИ

Додаток А. ТЕЦ-5 – Київ

Додаток Б. Історія Дніпровської ГЕС



Додаток В. Послідовний розвиток екологічних катастроф при руйнуванні об'єктів критичної інфраструктури



№	Опис події
1	Прорив дамби шламонакопичувача
2	Затоплення села Красногорівка
3	Загибель людей і сільських тварин
4	Забруднення значної території відходами із шламонакопичувача
5	Забруднення річок Кам'янка й Очеретувата та р. Кривий Торець
6	Забруднення басейну річки Сіверський Донець
7	Транскордонне забруднення басейну нижнього Дону
8	Затоплення села Веселе
9	Влучення снаряду в хімічний накопичувач
10	Руйнування гідро бар'єру
11	Вторинне забруднення грун. вод
12	Вторинне забруднення шламонакопичувача хім. речовинами з хім. накопичувача
13	Виникнення пожежі на хім. накопичувачі
14	Виникнення пожежі на породному відвалі
15	Забруднення приземного шару повітря
16	Задимлення прилеглої території (залізничного полотна і полігону тв. побут. відходів)
17	Перекидання пожежі на прилеглу територію (залізницю і полігон тв. побут. відходів)
18	Влучення снаряду в породний відвал
19	Перекидання пожежі на територію міста

Додаток Г. Графічне представлення ефекту доміно