МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
ФАКУЛЬТЕТ НАУК ПРО ЗДОРОВ'Я
КАФЕДРА ЦИВІЛЬНОЇ ТА ПРОМИСЛОВОЇ БЕЗПЕКИ
ІМ. ГЕРОЯ УКРАЇНИ ЧУБА ОЛЕКСАНДРА СЕРГІЙОВИЧА

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____Батир ХАЛМУРАДОВ
«____»_____2025р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР
ЗА СПЕЦІАЛЬНІСТЮ 263 «ЦИВІЛЬНА БЕЗПЕКА»

Тема: **«Підходи до визначення проєктних загроз об'єкту критичної інфраструктури з урахуванням міжнародного досвіду»**

Виконавець: студент групи М-263-24-1-ТП Артур ШЕВЧЕНКО
(студент, група, ім'я, прізвище)

Керівник: д.т.н., професор Олег ТРЕТЬЯКОВ
(науковий ступінь, вчене звання, ім'я, прізвище)

Консультант з розділу Екологія Оксана ТИХЕНКО
Консультант з розділу Охорона праці Олексій КОЗЛІТІН
Нормоконтролер: _____ Віталій НЕЧИПОРУК
(підпис) (ім'я, прізвище)

КИЇВ 2025

ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Факультет наук про здоров'я
Кафедра цивільної та промислової безпеки
Імені Героя України Чуба Олександра Сергійовича
Спеціальність: 263 «Цивільна безпека
(шифр, найменування)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Батир ХАЛМУРАДОВ
«____» _____2025р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи
Шевченка Артема Миколайовича

1. Тема роботи «**Підходи до визначення проєктних загроз об'єкту критичної інфраструктури з урахуванням міжнародного досвіду**» затверджена наказом ректора від «28» 08 2025р. № 1562/ст.

2. Термін виконання роботи з 01.10.2025 р. по 25.12.2025р.

3. Вихідні дані роботи:

Проаналізувати теоретичні основи міжнародного підходу до забезпечення безпеки критичної інфраструктури на етапах проектування промислових систем. Дослідити поточний стан розвитку та впровадження передових технологій для зменшення вразливості промислових споруд. Виконати оцінювання впливу помилок персоналу на стійкість об'єктів критичної інфраструктури. Розробити систему управління ризиками на основі міжнародного досвіду. Запропонувати заходи щодо впровадження заходів з підвищення стійкості критичної інфраструктури. Обґрунтувати економічну ефективність запропонованих рішень

4. Зміст пояснювальної записки: аналітичний огляд літературних джерел з тематики диплому. Організаційні заходи щодо забезпечення безпеки об’єктів критичної інфраструктури. Аналіз навчання персоналу правилам забезпечення безпеки об’єктів критичної інфраструктури.

5. Перелік обов’язкового ілюстративного матеріалу: таблиці, рисунки, діаграми, графіки.

6. Календарний план-графік

№ п/п	Завдання	Термін виконання	Підпис керівника
1	Аналітичний огляд літературних джерел	29.09.2025-01.10.2025	
2	Складання календарного плану дкваліфікаційної роботи, пошук та збір інформації, аналіз наукової літератури	02.10.2025-03.10.2025	
3	Загальна характеристика	04.10.2025-05.10.2025	
4	Підготовка додатків до пояснювальної записки	06.10.2025-08.10.2025	
5	Підготовка основної частини (Розділ I)	09.10.2025-19.10.2025	
6	Підготовка основної частини (Розділ II)	20.10.2025-30.10.2025	
7	Підготовка основної частини (Розділ III)	31.10.2025-10.11.2025	
8	Підготовка основної частини (Розділ IV), (Розділ V)	11.11.2025-21.11.2025	
9	На основі проаналізованої інформації написати загальні висновки	22.11.2025-26.11.2025	
10	Передзахист кваліфікаційної роботи	27.11.2025	
11	Підготовка до захисту: доповідь, презентація, ілюстративний (роздатковий) матеріал	28.11.2025-15.12.2025	
12	Захист кваліфікаційної роботи до	25.12.2025	

8.Дата видачі завдання: «29» 10 2025 р.

Керівник кваліфікаційної роботи: _____ Третьяков О.В.

Завдання прийняв до виконання: _____ Шевченко А. М.

ЗМІСТ

ВСТУП..... 10

Наукова новизна та практичне значення роботи..... 13

РОЗДІЛ 1 ОГЛЯД ЛІТЕРАТУРИ ТА НОРМАТИВНО-ПРАВОВОЇ БАЗИ 15

2.1. Теоретичні підходи до категоризації загроз і ризиків 15

1.2. Огляд міжнародних стандартів і нормативно-правових підходів до управління загрозами та ризиками об'єктів критичної інфраструктури 17

1.3. Аналіз національної нормативно-правової бази у сфері захисту критичної інфраструктури України..... 19

1.4. Порівняльний аналіз міжнародного та національного підходів до визначення загроз об'єктам критичної інфраструктури 24

1.4.1. Міжнародний підхід (ЄС, США, НАТО)..... 24

1.4.2. Національний підхід (Україна) 25

1.4.3. Порівняльний підхід 26

1.4.4. Ключові висновки та тренди..... 27

1.5.1 Законодавче закріплення поняття "Стійкість" (Resilience)..... 28

1.5.2. Розширення секторів КІ (Гармонізація Додатку до Директиви) 28

1.5.3. Впровадження динамічної оцінки ризиків (Risk Assessment) 29

1.5.4. Перевірка персоналу (Background Checks)..... 29

1.5.5 Визначення КІ європейського значення 29

РОЗДІЛ 2 МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ..... 34

2.1. Дизайн дослідження: комбінований (кількісний та якісний) підхід . 34

2.2. Методи збору даних..... 34

2.3. Методи аналізу та оцінки проєктних загроз..... 35

2.4. Забезпечення надійності та валідності результатів 36

2.5. Обмеження дослідження та етичні аспекти..... 36

РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ПІДХОДУ ДО ВИЗНАЧЕННЯ ПРОЄКТНИХ ЗАГРОЗ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 38

3.1. Розроблення методичного підходу до визначення проєктних загроз 38

3.2. Визначення «проєктних загроз» об’єкта критичної інфраструктури 39

3.2. Класифікація (таксономія) проєктних загроз об’єкта критичної інфраструктури 40

3.3. Відображення проєктних загроз на етапах життєвого циклу об’єкта критичної інфраструктури 43

3.4. Інтеграція таксономії проєктних загроз у модель оцінки ризиків 45

3.5. Модель ідентифікації та оцінки проєктних загроз 47

3.6. Апробація підходу на прикладі типового об’єкта критичної інфраструктури 48

3.7. Практичні рекомендації щодо впровадження підходу 49

РОЗДІЛ 4 ІНСТРУМЕНТИ ТА АЛГОРИТМИ ВИЯВЛЕННЯ ПРОЄКТНИХ ЗАГРОЗ 51

4.1. Процесна схема ідентифікації та оцінки загроз 51

4.2 Деталізація за етапами життєвого циклу Системи Фізичного Захисту (СФЗ) 53

4.2.1 Алгоритм застосування CARVER 56

4.3 Діаграма послідовності дій порушника (Adversary Sequence Diagram – ASD) 62

4.4 Розробка плану забезпечення стійкості кп "міськводоканал" 65

4.5 Розробка покрокової інстукції для персоналу водоканалу на випадок повного знеструмлення. 68

РОЗДІЛ 5 ОХОРОНА ПРАЦІ 73

5.1.1 Організація робочого місця 73

5.1.2 Перелік шкідливих та небезпечних виробничих чинників 74

5.1.3 Аналіз шкідливих та небезпечних чинників 74

5.2. Розробка заходів з охорони праці 77

5.3. Пожежна безпека. 78

5.4. Розрахункова частина. Розрахунок штучного освітлення 79

5.5. Висновки до розділу 81

РОЗДІЛ 6 ЕКОЛОГІЯ 82

6.1 Забруднення небезпечними речовинами 85

6.2 Забруднення від побутових стічних вод 86

6.3. Скорочення біомаси..... 87
6.4 Забруднення хімічними речовинами..... 91
ЗАГАЛЬНІ ВИСНОВКИ..... 94
Ключові аспекти системного підходу..... 94
Міжнародний та національний досвід..... 94
Практичне значення та рекомендації..... 95
СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ..... 96

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Підходи до визначення проєктних загроз об’єкту критичної інфраструктури з урахуванням міжнародного досвіду»: 98 с., 4 рис., 3 табл., 3 графіки, 54 літературних джерела.

Мета дослідження полягає у розробленні та обґрунтуванні системного підходу до визначення проєктних загроз об’єктам критичної інфраструктури з урахуванням міжнародного досвіду, з метою підвищення рівня їх безпеки на етапах проєктування, модернізації та впровадження.

Для досягнення поставленої мети у магістерській роботі передбачається розв’язання таких завдань дослідження:

1. Проаналізувати наукові підходи та термінологічні аспекти у сфері безпеки критичної інфраструктури, зокрема поняття загроз, ризиків і вразливостей.
2. Дослідити сучасні види кібернетичних і фізичних загроз, характерних для об’єктів критичної інфраструктури, з акцентом на загрози, що формуються на проєктному етапі.
3. Проаналізувати міжнародні стандарти, нормативні документи та практики щодо ідентифікації та управління загрозами об’єктів критичної інфраструктури.
4. Сформувати класифікацію (таксономію) проєктних загроз об’єктів критичної інфраструктури.
5. Розробити методичний підхід до ідентифікації та оцінки проєктних загроз з урахуванням міжнародного досвіду.
6. Апробувати запропонований підхід на прикладі конкретного об’єкта критичної інфраструктури або умовного кейсу.

7. Розробити практичні рекомендації щодо впровадження системи визначення проєктних загроз у діяльність операторів критичної інфраструктури.

Об’єктом дослідження є процес забезпечення безпеки об’єктів критичної інфраструктури.

Предметом дослідження є методи та підходи до визначення і оцінки проєктних загроз об’єктам критичної інфраструктури з урахуванням міжнародного досвіду.

Наукова новизна та практичне значення роботи

Наукова новизна дослідження полягає в тому, що в роботі:

уточнено зміст і місце поняття «проєктні загрози об’єктам критичної інфраструктури» у системі загроз безпеці критичної інфраструктури, з урахуванням їх формування на етапах проєктування, модернізації та впровадження інфраструктурних об’єктів;

удосконалено класифікацію загроз об’єктам критичної інфраструктури шляхом виділення окремої групи проєктних загроз та їх систематизації за джерелами виникнення, характером впливу та етапами життєвого циклу об’єкта;

дістало подальшого розвитку методичний підхід до ідентифікації та оцінки загроз об’єктам критичної інфраструктури на основі інтеграції проєктного управління ризиками з міжнародними стандартами та практиками у сфері безпеки;

запропоновано комплексний алгоритм визначення проєктних загроз, що поєднує кібернетичні, фізичні та організаційні аспекти безпеки і може застосовуватися на ранніх етапах життєвого циклу об’єкта критичної інфраструктури.

Практичне значення отриманих результатів полягає в можливості використання:

розробленої класифікації та методичного підходу операторами об’єктів критичної інфраструктури під час проєктування, модернізації та оцінки безпеки інфраструктурних об’єктів;

запропонованих інструментів і процедур ідентифікації проєктних загроз у діяльності органів державного управління та суб’єктів господарювання у сфері критичної інфраструктури;

результатів дослідження при розробленні внутрішніх регламентів, програм управління ризиками та безпекових вимог до проєктної документації;

матеріалів роботи в освітньому процесі під час викладання дисциплін з управління ризиками, безпеки критичної інфраструктури та проєктного менеджменту.

ВСТУП

Актуальність теми дослідження

У сучасних умовах розвитку держав і глобалізації економічних та інформаційних процесів критична інфраструктура (КІ) відіграє ключову роль у забезпеченні національної безпеки, сталого функціонування суспільства та життєдіяльності населення. До об’єктів критичної інфраструктури належать енергетичні, транспортні, водопостачальні, інформаційно-комунікаційні, фінансові та інші системи, порушення роботи яких може призвести до значних соціальних, економічних і безпекових наслідків.

Останніми роками спостерігається стійке зростання загроз для об’єктів критичної інфраструктури, що зумовлено поєднанням технологічних, геополітичних і соціальних чинників. З одного боку, цифровізація, впровадження автоматизованих систем управління, промислового Інтернету речей (IoT) та хмарних технологій суттєво підвищують ефективність функціонування інфраструктурних об’єктів, але водночас збільшують уразливість до кіберзагроз. Кібернапади на енергетичні мережі, транспортні системи та об’єкти зв’язку демонструють можливість завдання масштабної шкоди без фізичного втручання.

З іншого боку, фізичні загрози – диверсії, терористичні акти, саботаж, вплив збройних конфліктів і природних катастроф – залишаються не менш актуальними. Особливої гостроти ця проблема набуває в умовах гібридних загроз, коли кібер- та фізичні впливи застосовуються комплексно, взаємно підсилюючи наслідки один одного. У таких умовах традиційні підходи до безпеки, орієнтовані лише на експлуатаційну фазу об’єкта, виявляються недостатніми.

Важливим аспектом є те, що значна частина критичних вразливостей формується на етапі проєктування, модернізації або реконструкції об’єктів критичної інфраструктури. Неврахування потенційних загроз у проєктних

рішеннях, виборі технологій, постачальників або організаційних моделей управління може призвести до системних ризиків, усунення яких на етапі експлуатації є значно дорожчим або навіть неможливим. Це зумовлює потребу у виділенні та глибокому аналізі саме проєктних загроз як окремої категорії ризиків.

У зв'язку з цим зростає потреба у системному, структурованому підході до ідентифікації та оцінки загроз, який поєднує технічні, організаційні, кібернетичні та фізичні аспекти безпеки. Провідні міжнародні організації та держави (Європейський Союз, США, країни НАТО) уже впроваджують комплексні підходи до управління ризиками критичної інфраструктури, закріплені в міжнародних стандартах і нормативних документах (зокрема ISO 31000, директива NIS2, настанови ENISA та CISA). Ці підходи передбачають інтеграцію безпеки у весь життєвий цикл об'єкта, починаючи з етапу проєктування.

Для національного контексту актуальним є адаптація міжнародного досвіду з урахуванням правових, інституційних і безпекових особливостей. Відсутність уніфікованої методики визначення проєктних загроз для об'єктів критичної інфраструктури ускладнює процес прийняття управлінських рішень та знижує ефективність заходів захисту.

Таким чином, обрана тема магістерської роботи є актуальною з огляду на:

- зростання кібер- та фізичних загроз для критичної інфраструктури;
- необхідність раннього виявлення загроз на етапі проєктування об'єктів КІ;
- потребу у впровадженні системного підходу до управління проєктними загрозами;
- доцільність використання та адаптації міжнародних практик і стандартів у сфері захисту критичної інфраструктури.

Результати дослідження можуть мати як наукову, так і практичну цінність для фахівців у сфері безпеки, проєктного управління та державного регулювання критичної інфраструктури.

Мета, завдання, об’єкт і предмет дослідження

Мета дослідження полягає у розробленні та обґрунтуванні системного підходу до визначення проєктних загроз об’єктам критичної інфраструктури з урахуванням міжнародного досвіду, з метою підвищення рівня їх безпеки на етапах проєктування, модернізації та впровадження.

Для досягнення поставленої мети у магістерській роботі передбачається розв’язання таких **завдань дослідження**:

1. Проаналізувати наукові підходи та термінологічні аспекти у сфері безпеки критичної інфраструктури, зокрема поняття загроз, ризиків і вразливостей.
2. Дослідити сучасні види кібернетичних і фізичних загроз, характерних для об’єктів критичної інфраструктури, з акцентом на загрози, що формуються на проєктному етапі.
3. Проаналізувати міжнародні стандарти, нормативні документи та практики щодо ідентифікації та управління загрозами об’єктів критичної інфраструктури.
4. Сформувати класифікацію (таксономію) проєктних загроз об’єктів критичної інфраструктури.
5. Розробити методичний підхід до ідентифікації та оцінки проєктних загроз з урахуванням міжнародного досвіду.
6. Апробувати запропонований підхід на прикладі конкретного об’єкта критичної інфраструктури або умовного кейсу.
7. Розробити практичні рекомендації щодо впровадження системи визначення проєктних загроз у діяльність операторів критичної інфраструктури.

Об’єктом дослідження є процес забезпечення безпеки об’єктів критичної інфраструктури.

Предметом дослідження є методи та підходи до визначення і оцінки проєктних загроз об’єктам критичної інфраструктури з урахуванням міжнародного досвіду.

Наукова новизна та практичне значення роботи

Наукова новизна дослідження полягає в тому, що в роботі:

- уточнено зміст і місце поняття *«проєктні загрози об’єктам критичної інфраструктури»* у системі загроз безпеці критичної інфраструктури, з урахуванням їх формування на етапах проєктування, модернізації та впровадження інфраструктурних об’єктів;
- удосконалено класифікацію загроз об’єктам критичної інфраструктури шляхом виділення окремої групи проєктних загроз та їх систематизації за джерелами виникнення, характером впливу та етапами життєвого циклу об’єкта;
- дістало подальшого розвитку методичний підхід до ідентифікації та оцінки загроз об’єктам критичної інфраструктури на основі інтеграції проєктного управління ризиками з міжнародними стандартами та практиками у сфері безпеки;
- запропоновано комплексний алгоритм визначення проєктних загроз, що поєднує кібернетичні, фізичні та організаційні аспекти безпеки і може застосовуватися на ранніх етапах життєвого циклу об’єкта критичної інфраструктури.

Практичне значення отриманих результатів полягає в можливості використання:

- розробленої класифікації та методичного підходу операторами об’єктів критичної інфраструктури під час проєктування, модернізації та оцінки безпеки інфраструктурних об’єктів;
- запропонованих інструментів і процедур ідентифікації проєктних загроз у діяльності органів державного управління та суб’єктів господарювання у сфері критичної інфраструктури;

- результатів дослідження при розробленні внутрішніх регламентів, програм управління ризиками та безпекових вимог до проєктної документації;
- матеріалів роботи в освітньому процесі під час викладання дисциплін з управління ризиками, безпеки критичної інфраструктури та проєктного менеджменту.

РОЗДІЛ 1
ОГЛЯД ЛІТЕРАТУРИ ТА НОРМАТИВНО-ПРАВОВОЇ БАЗИ

2.1. Теоретичні підходи до категоризації загроз і ризиків

У наукових дослідженнях і нормативно-правових документах, присвячених безпеці та управлінню ризиками, ключове значення має чітке розмежування та коректне трактування базових понять, зокрема **«загроза»**, **«ризик»**, **«вразливість»** та їх взаємозв'язок у контексті функціонування об'єктів критичної інфраструктури.

У загальнотеоретичному розумінні **загроза** трактується як потенційна можливість або сукупність умов, дій чи факторів, здатних завдати шкоди об'єкту, системі або процесу. У сфері безпеки критичної інфраструктури загроза пов'язується з наявністю джерела впливу (природного, техногенного, антропогенного чи навмисного), яке за певних умов може порушити нормальне функціонування інфраструктурного об'єкта. Таким чином, загроза є категорією потенційною і не обов'язково реалізується, однак її існування вимагає врахування під час планування та управління.

Поняття ризику є більш комплексним і, на відміну від загрози, має імовірнісний характер. У більшості сучасних підходів ризик визначається як поєднання ймовірності реалізації загрози та тяжкості її наслідків. У стандартах з управління ризиками ризик розглядається як відхилення від очікуваного результату, яке може мати як негативний, так і позитивний характер, проте у сфері захисту критичної інфраструктури основна увага зосереджується саме на негативних наслідках. Таким чином, ризик є результатом взаємодії загрози, вразливості об'єкта та можливих наслідків.

Важливим елементом у цій тріаді є поняття вразливості, яке характеризує слабкі місця об'єкта, системи або процесу, що можуть бути використані загрозою. Вразливість може мати технічний, організаційний,

кадровий, інформаційний або нормативний характер. У контексті критичної інфраструктури вразливості часто виникають через застарілі технології, недостатній рівень кіберзахисту, помилки в організації управління, залежність від окремих постачальників або недосконаліть нормативної бази. Саме наявність вразливостей визначає, чи зможе конкретна загроза бути реалізованою.

У сучасних теоретичних підходах загроза, вразливість і ризик розглядаються як взаємопов'язані категорії, де загроза виступає джерелом потенційного впливу, вразливість – умовою реалізації цього впливу, а ризик – інтегральною оцінкою ймовірних наслідків для об'єкта критичної інфраструктури.

Окремого наукового інтересу набуває поняття «проєктні загрози», яке в традиційних дослідженнях безпеки розкривається недостатньо. Під проєктними загрозами доцільно розуміти сукупність загроз, що виникають або закладаються на національному рівні чи на рівні проектних загроз об'єктів критичної інфраструктури. На відміну від експлуатаційних загроз, проєктні загрози пов'язані з прийнятими технічними рішеннями, архітектурою систем, вибором технологій, підрядників і постачальників, а також організаційними моделями управління проєктом.

Проектна загроза – це визначені характеристики потенційних правопорушників та їхні можливості вчинити диверсію, крадіжку або інший злочин щодо критично важливих об'єктів (ЯКВ, ядерні матеріали, кіберінфраструктура, енергетика, медицина) або специфічні сценарії небезпек (кібератаки, епідемії, пожежі, стихійні лиха). Вона є основою для створення системи захисту, розробки планів реагування та забезпечення безпеки об'єктів критичної інфраструктури (КІ) від загроз національного та об'єктового рівні [1]

До проєктних загроз можуть належати: некоректне проєктування систем безпеки, ігнорування вимог кіберзахисту на етапі розробки, залежність від критичних компонентів одного виробника, недостатній аналіз фізичних і

природних факторів, а також недооцінка людського чинника. Особливістю таких загроз є те, що їх наслідки часто проявляються вже на етапі експлуатації, тоді як усунення закладених помилок потребує значних фінансових і часових ресурсів.

Таким чином, аналіз теоретичних підходів свідчить про необхідність розширення традиційного розуміння загроз безпеці критичної інфраструктури шляхом виокремлення проєктних загроз в окрему категорію. Це дозволяє забезпечити більш системний і превентивний підхід до управління ризиками, орієнтований на підвищення стійкості об’єктів критичної інфраструктури на всіх етапах їх життєвого циклу.

1.2. Огляд міжнародних стандартів і нормативно-правових підходів до управління загрозами та ризиками об’єктів критичної інфраструктури

У сучасній міжнародній практиці забезпечення безпеки об’єктів критичної інфраструктури ґрунтується на стандартизованих підходах до управління ризиками, які забезпечують системність, порівнюваність результатів та можливість інтеграції безпекових вимог у всі етапи життєвого циклу інфраструктурних об’єктів. Провідну роль у цьому процесі відіграють міжнародні стандарти та регуляторні документи, розроблені міжнародними організаціями та наднаціональними інституціями.

Базовим документом у сфері управління ризиками є міжнародний стандарт ISO 31000 “Risk management – Guidelines”, який визначає загальні принципи, рамкову структуру та процес управління ризиками. Стандарт не є галузевим і може застосовуватися до будь-яких організацій та об’єктів, у тому числі до критичної інфраструктури. Відповідно до ISO 31000, управління ризиками має бути інтегрованим у всі організаційні процеси, включаючи стратегічне планування та проєктну діяльність. Особливу увагу в стандарті приділено етапу ідентифікації ризиків, який передбачає систематичне виявлення джерел загроз, подій, причин і потенційних наслідків.

У контексті інформаційної та кібербезпеки важливе значення має стандарт ISO/IEC 27005, який деталізує підхід до управління ризиками інформаційної безпеки. Він орієнтований на ідентифікацію загроз, вразливостей та оцінку ризиків для інформаційних активів, що є критично важливим для об’єктів критичної інфраструктури, які широко використовують автоматизовані системи управління та інформаційно-комунікаційні технології. Цей стандарт підкреслює необхідність урахування ризиків ще на етапі проєктування систем, що безпосередньо пов’язано з концепцією проєктних загроз.

На рівні Європейського Союзу ключовим нормативним документом у сфері захисту критичної інфраструктури є Директива (ЄС) 2022/2555 (NIS2), спрямована на підвищення спільного рівня кібербезпеки в державах-членах. Директива розширює перелік суб’єктів, які підпадають під вимоги щодо управління ризиками, та встановлює обов’язок впровадження системного підходу до оцінки кібер- і фізичних загроз. Важливою особливістю NIS2 є вимога врахування ризиків ланцюгів постачання та безпеки підрядників, що має безпосереднє значення для проєктної діяльності у сфері критичної інфраструктури.

Доповненням до директиви NIS2 є рекомендації та методичні настанови Агентства ЄС з кібербезпеки (ENISA), які містять практичні підходи до аналізу ризиків, класифікації загроз та оцінки їх впливу на критичні сервіси. Документи ENISA орієнтовані на міждисциплінарний підхід і передбачають поєднання технічних, організаційних та управлінських заходів безпеки.

У Сполучених Штатах Америки питання захисту критичної інфраструктури регулюються через стратегічні документи та рекомендації Агентства з кібербезпеки та захисту інфраструктури (CISA). Американський підхід базується на концепції управління ризиками на національному рівні та активній взаємодії державного і приватного секторів. Значна увага приділяється превентивним заходам, зокрема ідентифікації загроз на ранніх стадіях проєктування та модернізації інфраструктурних об’єктів.

У військово-політичному вимірі важливу роль відіграють підходи НАТО, які акцентують увагу на стійкості (resilience) критичної інфраструктури та здатності швидко відновлювати функціонування у разі кризових ситуацій. Документи Альянсу підкреслюють необхідність міжвідомчої координації та врахування комплексних загроз, включно з гібридними, що поєднують кібер- і фізичні впливи.

Загалом аналіз міжнародних стандартів і нормативних підходів свідчить про тенденцію до інтеграції управління ризиками в проєктну діяльність, що дозволяє мінімізувати загрози ще на етапі прийняття технічних і організаційних рішень. Водночас більшість міжнародних документів не виокремлює проєктні загрози як самостійну категорію, що зумовлює необхідність подальших наукових досліджень у цьому напрямі та адаптації міжнародного досвіду до конкретних умов функціонування об'єктів критичної інфраструктури.

1.3. Аналіз національної нормативно-правової бази у сфері захисту критичної інфраструктури України

Формування та розвиток системи захисту критичної інфраструктури в Україні відбувається в умовах зростання внутрішніх і зовнішніх загроз, що обумовлює особливу увагу держави до нормативно-правового регулювання у цій сфері. Національна правова база спрямована на визначення засад державної політики, розподіл повноважень між суб'єктами безпеки та створення умов для комплексного управління ризиками об'єктів критичної інфраструктури.

Ключовим документом, що закладає основи державної політики у сфері захисту критичної інфраструктури, є Закон України «Про критичну інфраструктуру». У ньому визначено поняття критичної інфраструктури, її сектори, об'єкти та суб'єкти, а також основні принципи їх захисту. Закон закріплює необхідність комплексного підходу до забезпечення безпеки, що

включає запобігання, виявлення, реагування та відновлення після реалізації загроз. Водночас у законі основний акцент зроблено на експлуатаційній фазі функціонування об’єктів, тоді як питання врахування загроз на етапі проєктування розкриті недостатньо.

Важливе місце у системі нормативного регулювання посідають стратегічні документи у сфері національної безпеки, зокрема Стратегія національної безпеки України та Стратегія кібербезпеки України. У цих документах критична інфраструктура розглядається як один із ключових об’єктів захисту держави, а кібернетичні та гібридні загрози визначаються серед пріоритетних. Стратегічні документи підкреслюють необхідність запровадження ризик-орієнтованого підходу та гармонізації національної системи безпеки з міжнародними стандартами й практиками.

Окрему роль відіграє законодавство у сфері кібербезпеки, зокрема Закон України «Про основні засади забезпечення кібербезпеки України». Він визначає правові та організаційні основи захисту інформаційних ресурсів і критичної інформаційної інфраструктури, встановлює повноваження органів державної влади та обов’язки власників і операторів об’єктів. У контексті даного дослідження важливим є те, що закон орієнтує суб’єктів на впровадження систем управління ризиками, однак не містить деталізованих вимог щодо ідентифікації загроз на проєктних етапах створення або модернізації об’єктів.

Регуляторну основу також формують підзаконні нормативно-правові акти Кабінету Міністрів України, які визначають порядок категоризації об’єктів критичної інфраструктури, вимоги до їх захисту та механізми міжвідомчої взаємодії. Ці документи спрямовані на уніфікацію підходів до оцінки значущості об’єктів і рівня загроз, проте переважно мають описовий характер і залишають значну свободу у виборі конкретних методик оцінки ризиків.

У сфері технічного регулювання та стандартизації в Україні застосовуються національні стандарти (ДСТУ), частина з яких гармонізована

з міжнародними стандартами ISO та IEC. Зокрема, у практиці управління ризиками використовуються стандарти, що базуються на положеннях ISO 31000 та стандартів серії ISO/IEC 27000. Вони створюють методичне підґрунтя для впровадження ризик-орієнтованого підходу, однак їх застосування у сфері критичної інфраструктури має рекомендаційний характер і не завжди є обов'язковим.

Аналіз національної нормативно-правової бази свідчить про поступове формування в Україні комплексної системи захисту критичної інфраструктури, орієнтованої на протидію сучасним кібер- та фізичним загрозам. Водночас існує низка проблемних аспектів, зокрема фрагментарність регулювання, відсутність єдиної методики ідентифікації та оцінки загроз, а також недостатня увага до ризиків, що виникають на етапах проєктування і модернізації об'єктів.

Таким чином, національна нормативно-правова база України створює загальні умови для забезпечення безпеки критичної інфраструктури, проте потребує подальшого розвитку в частині інституалізації системного підходу до визначення проєктних загроз та адаптації кращих міжнародних практик до національних умов. Це обумовлює актуальність і практичну значущість дослідження, спрямованого на вдосконалення методичних підходів у цій сфері.

Таблиця 1.1

Відповідність нормативно-правової бази України вимогам NIS2 та ISO 31000 у сфері захисту критичної інфраструктури

Ключовий аспект	**Вимоги NIS2 / ISO 31000**	**Нормативно-правове регулювання в Україні**	**Рівень відповідності**	**Коментар**

Підхід до управління ризиками	ISO 31000: системний, безперервний, інтегрований у всі процеси організації	Закон України «Про критичну інфраструктуру», Стратегія національної безпеки	Часткова	Декларується ризик-орієнтований підхід, але відсутня уніфікована методика
Ідентифікація загроз	NIS2: обов'язкова ідентифікація кібер- та фізичних загроз	Закон України «Про критичну інфраструктуру»	Часткова	Визначено необхідність захисту, але без деталізації процедур
Оцінка ризиків	ISO 31000: оцінка ймовірності та наслідків	Підзаконні акти КМУ, галузеві методики	Часткова	Відсутні єдині шкали та критерії оцінювання
Урахування життєвого циклу об'єкта	ISO 31000, NIS2: ризики на всіх етапах (проєктування–експлуатація)	Непрямо відображено	Низька	Проєктний етап нормативно майже не регламентований
Проєктні загрози	ISO 31000: управління ризиками в проєктній діяльності	Прямі норми відсутні	Низька	Поняття «проєктні загрози» не закріплене

Кібербезпека КІ	NIS2: обов’язкові заходи кіберзахисту	Закон «Про основні засади забезпечення кібербезпеки України»	Висока	Загальні вимоги відповідають європейському підходу
Supply-chain ризики	NIS2: оцінка ризиків ланцюгів постачання	Фрагментарне регулювання	Низька	Відсутні комплексні вимоги до постачальників
Інцидент-менеджмент	NIS2: звітність, реагування, відновлення	Стратегія кібербезпеки, підзаконні акти	Часткова	Є вимоги щодо реагування, але слабка інтеграція з проєктною фазою
Взаємодія держави і операторів КІ	NIS2: чіткий розподіл відповідальності	Закон України «Про критичну інфраструктуру»	Середня	Норми визначені, але практична реалізація ускладнена
Гармонізація з міжнародними стандартами	ISO 31000, ISO/IEC 27000	ДСТУ, гармонізовані з ISO	Часткова	Застосування стандартів має переважно рекомендаційний характер

Узагальнюючий висновок до таблиці

Порівняльний аналіз свідчить, що нормативно-правова база України у сфері захисту критичної інфраструктури частково відповідає вимогам NIS2 та принципам ISO 31000, зокрема в частині декларування ризик-орієнтованого підходу та забезпечення кібербезпеки. Водночас найбільш суттєвими прогалинами залишаються:

- відсутність формалізованого підходу до ідентифікації проєктних загроз;
- недостатнє нормативне врахування етапу проєктування та модернізації об’єктів КІ;
- слабка регламентація ризиків ланцюгів постачання;
- відсутність єдиної національної методики оцінки ризиків.

Зазначені обставини підтверджують доцільність адаптації міжнародних підходів NIS2 та ISO 31000 до національних умов і обґрунтовують необхідність наукового дослідження, спрямованого на вдосконалення методів визначення проєктних загроз об’єктів критичної інфраструктури.

1.4. Порівняльний аналіз міжнародного та національного підходів до визначення загроз об’єктам критичної інфраструктури

1.4.1. Міжнародний підхід (ЄС, США, НАТО)

Міжнародна практика (зокрема, Директива ЄС **CER** 2022/2557 та стандарти США через CISA) базується на концепції "All-hazards approach" (підхід усіх небезпек).

- Фокус на стійкості (Resilience): Загроза розглядається не просто як подія, що може пошкодити об'єкт, а як фактор, що може порушити надання *життєво важливої послуги*. Мета – не "непробивна стіна", а здатність системи швидко відновитися після інциденту.

- Ризик-орієнтований підхід: Загрози не є статичним списком. Вони визначаються через матрицю ризиків:

Ризик = Загроза х Вразливість х Наслідки

- Класифікація**:** Зазвичай поділяється на три великі групи без жорсткої прив'язки до джерела:

1. Природні (стихійні лиха, кліматичні зміни).
2. Техногенні (аварії, збої систем).
3. Антропогенні (кібератаки, тероризм, саботаж, інсайдерські загрози).

- Кібер-фізична конвергенція**:** У міжнародних стандартах (наприклад, NIS2 в ЄС) кіберзагрози та фізичні загрози розглядаються як єдине ціле, оскільки кібератака може спричинити фізичні наслідки.

1.4.2. Національний підхід (Україна)

Український підхід регламентується ЗУ *"Про критичну інфраструктуру"* (2021) та постановами Кабміну. Він є більш централізованим та "безпековим".

- Поняття "Проектна загроза": Україна використовує унікальний термін – *проектна загроза*. Це офіційно затверджений документ, що визначає характеристики реальних та потенційних загроз для конкретного об'єкта. Це дещо більш статичний підхід порівняно з динамічним оцінюванням ризиків у ЄС.

- Вплив війни**:** На відміну від ЄС, де військова загроза розглядається як малоймовірна (або в контексті гібридних загроз), в Україні військова агресія, диверсії та теракти є пріоритетними загрозами.

- Категоризація (згідно із законодавством):

1. Соціально-політичні (блокування, страйки).
2. Воєнні (збройна агресія).
3. Кримінальні (теракти, кібератаки, крадіжки).
4. Техногенні (аварії).

5. Природні.

- Реєстровий принцип**:** Загрози визначаються для об'єктів, які внесені до Реєстру об'єктів критичної інфраструктури, з поділом на категорії критичності (I, II, III, IV).
-

1.4.3. Порівняльний підхід

Порівняльна таблиця підходів

Таблиця 1.2

Критерій	**Міжнародний підхід (ЄС/США)**	**Національний підхід (Україна)**
Ключова концепція	**Resilience (Стійкість)**: здатність витримати удар і відновитися.	**Protection (Захист)**: недопущення несанкціонованого втручання.
Методологія	**All-hazards approach**: врахування всіх можливих ризиків, включно з ланцюгами постачання.	**Категоризація загроз**: чіткий поділ на джерела (природні, техногенні, кримінальні тощо).
Визначення загроз	Динамічне, оператори КІ самі проводять оцінку ризиків (Risk Assessment).	Централізоване + локальне. Використання "паспортів безпеки" та "проектних загроз".
Кібербезпека	Повна інтеграція кібер- та фізичних загроз (Директиви NIS2 + CER).	Формально розділено: Держспецзв'язку (кібер) та нацсистема захисту КІ (фізична/загальна), хоча координація посилюється.
Роль держави	Регулятор та координатор.	Керівна та контролююча. Держава затверджує вимоги до захисту.

	Відповідальність лежить на операторі.	

1.4.4. Ключові висновки та тренди

1. Гармонізація: Україна активно імплементує європейські норми (зокрема, через впровадження вимог, схожих на NIS2). Постанова Кабміну №1176 вже впроваджує ризик-орієнтований підхід.

2. Гібридні загрози: Україна зараз є світовим лідером у практичному визначенні гібридних загроз (кібер + кінетичні удари по енергетиці). Цей досвід зараз вивчається міжнародними партнерами, що призводить до змін і в їхніх методологіях.

3. Відмінність у пріоритетах:

ЄС: Пріоритет на кліматичні зміни, пандемії, збої в ланцюгах постачання.

Україна: Пріоритет на ракетні обстріли, фізичні диверсії, блекаути.

Порівняльний аналіз міжнародних і національних підходів до визначення загроз об’єктам критичної інфраструктури дозволяє виявити спільні риси, відмінності та проблемні аспекти у сфері нормативно-методичного забезпечення безпеки. Такий аналіз є необхідним для обґрунтування доцільності адаптації кращих міжнародних практик до умов функціонування критичної інфраструктури України.

У міжнародній практиці, зокрема в країнах Європейського Союзу, США та державах – членах НАТО, домінує ризик-орієнтований і превентивний підхід до забезпечення безпеки критичної інфраструктури. Міжнародні стандарти та регуляторні документи (ISO 31000, NIS2, настанови ENISA та CISA) передбачають інтеграцію управління ризиками у всі етапи життєвого циклу інфраструктурних об’єктів – від стратегічного планування і проєктування до експлуатації та виведення з експлуатації. Особлива увага приділяється ранній ідентифікації загроз, що дозволяє мінімізувати потенційні втрати шляхом запобіжних заходів.

Характерною рисою міжнародного підходу є чітка структуризація процесу управління загрозами, яка включає формалізовані процедури ідентифікації, аналізу, оцінки та обробки ризиків. При цьому широко застосовуються стандартизовані методики, кількісні та якісні моделі оцінки, сценарний аналіз і моделювання наслідків. Значна увага приділяється також управлінню ризиками ланцюгів постачання та залученню підрядників, що є особливо важливим у контексті проєктної діяльності.

1.5 Рекомендації щодо адаптації Директиви ЄС 2022/2557 (CER) в Україні

Головна мета адаптації – перехід від парадигми "Охорона об'єкта" (фізичне недопущення ворога) до парадигми "Стійкість послуги" (гарантування того, що світло/вода/зв'язок будуть навіть під час атаки або швидко відновляться).

1.5.1 Законодавче закріплення поняття "Стійкість" (Resilience)

В українському законодавстві (ЗУ "Про критичну інфраструктуру") домінує термін "захист". Директива CER вимагає ширшого підходу.

- Суть зміни**:** Внести зміни до ст. 1 Закону, де визначити стійкість не як здатність протистояти, а як здатність: *попереджати, чинити опір, пом'якшувати наслідки, поглинати удар, адаптуватися та відновлюватися*.
- Практичне значення: Це зобов'яже операторів КІ інвестувати не лише в паркани та охорону, а й у резервні генератори, дублюючі канали зв'язку та плани відновлення (Business Continuity Plans).

1.5.2. Розширення секторів КІ (Гармонізація Додатку до Директиви)

Український перелік секторів є досить широким, але Директива CER виділяє 11 обов'язкових секторів. Необхідно уточнити український класифікатор для відповідності ЄС.

Рекомендація**:** Чітко виділити та регламентувати сектори, які в ЄС є критичними, а в Україні регулюються розмито:

Виробництво, переробка та дистрибуція продуктів харчування (продовольча безпека).

Водовідведення (окремо від водопостачання).

Космічний простір (наземна інфраструктура супутникового зв'язку).

1.5.3. Впровадження динамічної оцінки ризиків (Risk Assessment)

Замість статичного "Паспорта безпеки", який оновлюється рідко, Директива CER вимагає регулярної (що 4 роки або після інцидентів) переоцінки ризиків.

Рекомендація**:** Зобов'язати операторів КІ проводити оцінку ризиків "знизу-вгору", враховуючи:

Залежність від інших секторів (наприклад, як зупинка електростанції вплине на водоканал).

Ланцюги постачання (Supply Chain Security) – ризики від підрядників.

1.5.4. Перевірка персоналу (Background Checks)

Стаття 14 Директиви CER дозволяє державам-членам вимагати перевірки благонадійності персоналу, що займає критичні посади.

Проблема в Україні**:** Зараз це роблять спецслужби вибірково або самі підприємства як можуть.

Рекомендація**:** Створити прозорий законодавчий механізм, який дозволяє операторам КІ (навіть приватним) офіційно звертатися до держорганів для перевірки ключових співробітників на наявність зв'язків з державою-агресором або криміналом (боротьба з інсайдерськими загрозами та навідниками).

1.5.5 Визначення КІ європейського значення

Директива вводить поняття *Critical entities of particular European significance* (ті, що надають послуги в 6+ країнах ЄС).

Рекомендація**:** Ідентифікувати українські об'єкти, які є критичними для ЄС (газотранспортна система, інтерконектори електромереж, залізниця). Це відкриє доступ до фінансування ЄС на модернізацію їхньої безпеки.

Таблиця 1.3

Порівняльна таблиця змін (Було / Стане)

Аспект регулювання	**Поточний стан (Україна)**	**Пропоновані зміни (на базі CER)**
Фокус	Захист периметра та обладнання.	Безперервність надання послуги.
Документ планування	Паспорт безпеки / План захисту.	План забезпечення стійкості (Resilience Plan).
Взаємозалежність	Розглядається слабо. Об'єкт – ізольована одиниця.	Обов'язковий аналіз каскадних ефектів (Domino effects).
Звітність про інциденти	Повідомлення про факт атаки/аварії.	Повідомлення про "значні інциденти" (загроза зупинки послуги), навіть без атаки.
Співпраця	Вертикальна (Оператор -> Держорган).	Горизонтальна (SPOC – єдині контактні точки для обміну даними з ЄС).

Стратегічний висновок

Імплементація CER дозволить Україні перейти від реактивної моделі (гасіння пожеж після прильотів) до проактивної моделі стійкості, де система спроектована так, щоб функціонувати навіть за умов часткового руйнування.

Національний підхід України до захисту критичної інфраструктури перебуває на стадії становлення та розвитку. Нормативно-правова база визначає загальні засади державної політики у цій сфері, окреслює коло суб’єктів та їх повноваження, а також декларує необхідність застосування

ризик-орієнтованого підходу. Водночас на практиці цей підхід реалізується переважно фрагментарно та зосереджується на експлуатаційній фазі функціонування об’єктів критичної інфраструктури.

На відміну від міжнародних практик, у національному законодавстві України відсутні чітко регламентовані вимоги щодо ідентифікації загроз на етапі проєктування, модернізації або реконструкції об’єктів критичної інфраструктури. Проєктні загрози не виокремлюються як окрема категорія ризиків, що ускладнює їх системний аналіз і врахування під час прийняття проєктних рішень. Крім того, застосування міжнародних стандартів управління ризиками в українській практиці має здебільшого рекомендаційний характер.

Ще однією суттєвою відмінністю є рівень інституційної координації та взаємодії між державними органами і операторами критичної інфраструктури. У міжнародних моделях значна роль відводиться публічно-приватному партнерству, обміну інформацією про загрози та спільному реагуванню на інциденти. В Україні такі механізми лише формуються, що знижує ефективність системи управління ризиками та ускладнює впровадження комплексних безпекових рішень.

Водночас слід зазначити, що національний підхід має потенціал для розвитку та гармонізації з міжнародними практиками. Наявність базового законодавства у сфері критичної інфраструктури та кібербезпеки, а також курс на європейську інтеграцію створюють передумови для впровадження системного підходу до визначення загроз, у тому числі на проєктних етапах.

Таким чином, порівняльний аналіз показує, що ключовими напрямами зближення національного та міжнародного підходів мають стати: формалізація процедур ідентифікації загроз, інтеграція управління ризиками у проєктну діяльність, виокремлення проєктних загроз як самостійної категорії та розширення використання міжнародних стандартів і кращих практик. Реалізація цих напрямів дозволить підвищити стійкість об’єктів критичної інфраструктури та ефективність системи їх захисту в Україні.

Висновки до розділу 1

У 1 розділі магістерської роботи здійснено комплексний аналіз теоретичних, міжнародних та національних підходів до визначення загроз і ризиків об’єктів критичної інфраструктури, що дозволило сформувати цілісне уявлення про сучасний стан нормативно-методичного забезпечення у цій сфері.

У результаті аналізу теоретичних підходів встановлено, що поняття «загроза», «ризик» та «вразливість» є взаємопов’язаними категоріями, які в сукупності формують основу для управління безпекою об’єктів критичної інфраструктури. Загроза розглядається як потенційне джерело негативного впливу, вразливість – як умова її реалізації, а ризик – як інтегральна оцінка ймовірності та наслідків такого впливу. Обґрунтовано доцільність виокремлення проєктних загроз як окремої категорії, що виникає на етапах проєктування, модернізації та реконструкції об’єктів і значною мірою визначає рівень їх подальшої безпеки.

Аналіз міжнародних стандартів і нормативних документів (ISO 31000, ISO/IEC 27005, директива NIS2, настанови ENISA, підходи CISA та НАТО) показав, що у провідних країнах світу домінує системний, ризик-орієнтований і превентивний підхід до захисту критичної інфраструктури. Управління загрозами інтегрується у всі етапи життєвого циклу об’єктів, з особливим акцентом на ранню ідентифікацію ризиків, у тому числі під час проєктної діяльності та управління ланцюгами постачання.

Дослідження національної нормативно-правової бази України засвідчило наявність законодавчих та стратегічних передумов для забезпечення безпеки критичної інфраструктури. Водночас встановлено, що чинні нормативні акти переважно орієнтовані на експлуатаційну фазу функціонування об’єктів і не містять чітко визначених вимог щодо ідентифікації та оцінки загроз на етапі проєктування. Порівняльний аналіз показав часткову відповідність національного законодавства вимогам NIS2 та

принципам ISO 31000, зокрема у сфері кібербезпеки, за наявності суттєвих прогалин у регулюванні проєктних загроз і ризиків ланцюгів постачання.

Порівняння міжнародного та національного підходів дозволило визначити ключові напрями їх зближення, а саме: формалізацію процедур ідентифікації загроз, інтеграцію управління ризиками у проєктну діяльність, виокремлення проєктних загроз як самостійного об’єкта аналізу та розширення практики застосування міжнародних стандартів. Реалізація зазначених напрямів є необхідною умовою підвищення стійкості об’єктів критичної інфраструктури та ефективності державної політики у сфері їх захисту.

Отримані у розділі 1 висновки створюють теоретичне та нормативно-методичне підґрунтя для подальшого дослідження, зокрема для розроблення методичного підходу до визначення проєктних загроз об’єктів критичної інфраструктури з урахуванням міжнародного досвіду, що є предметом наступного розділу магістерської роботи.

РОЗДІЛ 2
МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

2.1. Дизайн дослідження: комбінований (кількісний та якісний) підхід

Методологічною основою дослідження обрано комбінований (змішаний) дизайн, що поєднує якісні та кількісні методи аналізу. Такий підхід зумовлений комплексним характером проєктних загроз об’єктам критичної інфраструктури, які формуються під впливом технічних, організаційних, кібернетичних та зовнішніх факторів і не можуть бути повною мірою досліджені в межах одного методологічного підходу.

Якісний компонент дослідження спрямований на виявлення сутності, джерел та умов виникнення проєктних загроз, а також на аналіз міжнародних і національних підходів до управління ними. Кількісний компонент забезпечує формалізацію експертних суджень, оцінку значущості загроз, їх ранжування та порівняння за встановленими критеріями. Поєднання цих підходів дозволяє підвищити достовірність результатів та забезпечити їх прикладну спрямованість.

2.2. Методи збору даних

У роботі використано сукупність взаємодоповнювальних методів збору даних, що відповідають обраному комбінованому дизайну дослідження.

Базовим методом є аналіз наукової літератури та нормативно-правових документів, який охоплює вивчення вітчизняних і зарубіжних наукових публікацій, міжнародних стандартів (ISO 31000, ISO/IEC 27005), директив ЄС (NIS2), рекомендацій профільних міжнародних організацій, а також чинного законодавства України у сфері захисту критичної інфраструктури.

Застосування цього методу дозволяє сформувати теоретичне підґрунтя дослідження та визначити нормативні обмеження і вимоги.

Емпіричні дані збираються за допомогою експертного опитування, що проводиться на основі структурованої анкети. До опитування залучаються фахівці з проєктного управління, кібер- та фізичної безпеки, а також представники операторів об’єктів критичної інфраструктури. Експерти здійснюють оцінювання ймовірності реалізації проєктних загроз та можливих наслідків їх впливу.

Для поглиблення та уточнення результатів анкетування застосовуються напівструктуровані експертні інтерв’ю, які дозволяють отримати розширені якісні пояснення щодо специфіки виникнення загроз, практичних труднощів їх ідентифікації та ефективності існуючих підходів до управління ризиками.

Додатково використовується метод кейс-стаді, що передбачає аналіз типового об’єкта або проєкту у сфері критичної інфраструктури з метою апробації запропонованого методичного підходу в практичних умовах.

2.3. Методи аналізу та оцінки проєктних загроз

Для обробки та інтерпретації зібраних даних у дослідженні застосовано комплекс аналітичних методів. На етапі якісного аналізу використовуються методи порівняльного аналізу, узагальнення та систематизації, що дозволяють сформувати класифікацію проєктних загроз та встановити їх взаємозв’язок із вразливостями об’єктів критичної інфраструктури.

Кількісна оцінка проєктних загроз здійснюється за допомогою методу експертних оцінок. Для кожної загрози визначаються показники ймовірності реалізації та тяжкості наслідків за шкалою, що дозволяє розрахувати інтегральний показник ризику. Отримані результати використовуються для побудови матриці ризиків та ранжування загроз за рівнем критичності.

Крім того, застосовується сценарний аналіз, який дозволяє оцінити можливі наслідки реалізації проєктних загроз за різних умов та варіантів

розвитку подій. Це сприяє обґрунтуванню управлінських рішень щодо мінімізації ризиків на етапі проєктування.

2.4. Забезпечення надійності та валідності результатів

Надійність і валідність результатів дослідження забезпечуються шляхом тріангуляції методів, що передбачає поєднання різних джерел даних і способів їх аналізу. Використання як якісних, так і кількісних методів дозволяє зменшити суб’єктивність експертних оцінок та підвищити обґрунтованість отриманих висновків.

Додатково застосовується перевірка узгодженості експертних оцінок та логічна верифікація отриманих результатів шляхом їх порівняння з положеннями міжнародних стандартів і нормативних вимог.

2.5. Обмеження дослідження та етичні аспекти

До основних обмежень дослідження належать обмежена кількість залучених експертів, а також складність доступу до повної інформації щодо функціонування окремих об’єктів критичної інфраструктури з огляду на вимоги безпеки. Разом із тим зазначені обмеження не впливають критично на загальні висновки роботи.

У процесі дослідження дотримано етичних принципів наукової діяльності, зокрема конфіденційності інформації, добровільності участі експертів та використання отриманих даних виключно з науковою метою.

Висновки до розділу 2

У третьому розділі магістерської роботи сформовано та обґрунтовано методологію дослідження проєктних загроз об’єктів критичної інфраструктури з урахуванням міжнародного досвіду. Обраний методологічний підхід відповідає меті та завданням роботи і забезпечує комплексність та наукову обґрунтованість отриманих результатів.

У ході дослідження встановлено доцільність застосування комбінованого (кількісного та якісного) дизайну, який дозволяє поєднати глибокий теоретичний аналіз природи проєктних загроз із формалізованою оцінкою їх значущості. Такий підхід забезпечує врахування як експертних знань і міжнародних практик, так і кількісних характеристик ризиків, що є важливим для прийняття управлінських рішень у сфері безпеки критичної інфраструктури.

У розділі визначено та обґрунтовано систему методів збору даних, зокрема аналіз наукових і нормативних джерел, експертне опитування, напівструктуровані інтерв'ю та кейс-стаді. Їх поєднання дозволяє отримати репрезентативну та багатовимірну інформацію про проєктні загрози, умови їх виникнення та практичні проблеми їх ідентифікації на етапах проєктування і модернізації об'єктів критичної інфраструктури.

Обґрунтовано застосування методів аналізу та оцінки проєктних загроз, зокрема експертного оцінювання, побудови матриці ризиків і сценарного аналізу. Використання зазначених методів дозволяє здійснити систематизацію загроз, їх ранжування за рівнем критичності та визначити пріоритетні напрями мінімізації ризиків у проєктній діяльності.

У розділі також визначено підходи до забезпечення надійності та валідності результатів дослідження, зокрема шляхом тріангуляції методів та перевірки узгодженості експертних оцінок. Окрему увагу приділено аналізу обмежень дослідження та дотриманню етичних принципів наукової роботи, що підвищує довіру до отриманих результатів.

Загалом розроблена методологія створює необхідне підґрунтя для подальшої практичної реалізації дослідження, зокрема для апробації запропонованого методичного підходу до визначення проєктних загроз об'єктів критичної інфраструктури та формування практичних рекомендацій, що буде здійснено у наступному розділі магістерської роботи.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ ПІДХОДУ ДО ВИЗНАЧЕННЯ ПРОЄКТНИХ ЗАГРОЗ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1. Розроблення методичного підходу до визначення проєктних загроз

На основі результатів теоретичного аналізу та обґрунтованої методології дослідження у роботі розроблено методичний підхід до визначення проєктних загроз об'єктів критичної інфраструктури, орієнтований на етапи проєктування, модернізації та впровадження інфраструктурних рішень.

Запропонований підхід базується на принципах ризик-орієнтованого управління (ISO 31000), вимогах директиви NIS2 та кращих міжнародних практиках у сфері захисту критичної інфраструктури. Його ключовою особливістю є інтеграція безпекових процедур безпосередньо у процес проєктного управління.

Методичний підхід включає такі основні етапи:

1. Визначення контексту проєкту (тип об'єкта критичної інфраструктури, етап життєвого циклу, нормативні обмеження, зацікавлені сторони).
2. Ідентифікація проєктних загроз, з урахуванням технічних, організаційних, кібернетичних та зовнішніх факторів.
3. Виявлення вразливостей, що можуть сприяти реалізації загроз.
4. Оцінка ризиків, пов'язаних з проєктними загрозами, на основі експертних оцінок.
5. Ранжування загроз та вибір заходів реагування.
6. Інтеграція результатів оцінки у проєктні рішення та документацію.

7.

3.2. Визначення «проєктних загроз» об’єкта критичної інфраструктури

У контексті забезпечення безпеки об’єктів критичної інфраструктури загрози традиційно розглядаються як фактори, що можуть негативно впливати на їх функціонування під час експлуатації. Водночас сучасні міжнародні підходи до управління ризиками дедалі більше акцентують увагу на необхідності аналізу загроз, які формуються на етапах проєктування, модернізації, будівництва та ре-конфігурації інфраструктурних об’єктів. Такі загрози доцільно виокремлювати в окрему категорію – *проєктні загрози*.

Проєктні загрози об’єкта критичної інфраструктури – це сукупність потенційних факторів і умов, що виникають або закладаються на етапах проєктування, реконструкції, модернізації чи технічного переоснащення об’єкта та можуть призвести до зниження рівня його безпеки, стійкості або надійності протягом усього життєвого циклу.

Ключовою відмінністю проєктних загроз від загальних загроз є їх причинно-наслідковий зв’язок із проєктними рішеннями, а не лише з процесом експлуатації. Якщо загальні загрози, як правило, пов’язані з зовнішнім впливом або порушенням функціонування об’єкта, то проєктні загрози формуються внаслідок:

- помилкових або недостатньо обґрунтованих технічних рішень;
- ігнорування вимог безпеки на ранніх етапах проєкту;
- неврахування сучасних кібернетичних і фізичних загроз;
- обмежень ресурсів, часу або кваліфікації учасників проєкту.

Проєктні загрози мають латентний характер, оскільки можуть не проявлятися безпосередньо під час реалізації проєкту, але стають критичними на етапі експлуатації об’єкта. Саме тому їх своєчасна ідентифікація є важливим елементом превентивного управління безпекою.

До основних характеристик проєктних загроз належать:

- виникнення на докомісійних етапах життєвого циклу об’єкта;
- довгостроковий вплив на рівень безпеки та стійкості об’єкта;
- складність усунення після завершення проєкту;
- тісний зв’язок із організаційними, управлінськими та технічними рішеннями.

Таким чином, проєктні загрози слід розглядати як самостійну категорію загроз, що потребує окремих методів ідентифікації, оцінки та управління. Їх врахування на етапах проєктування, модернізації та ре-конфігурації об’єктів критичної інфраструктури є необхідною умовою підвищення рівня національної безпеки та стійкості критичних систем.

3.2. Класифікація (таксономія) проєктних загроз об’єкта критичної інфраструктури

З метою систематизації та підвищення ефективності ідентифікації проєктних загроз у роботі запропоновано таксономію проєктних загроз об’єктів критичної інфраструктури, яка ґрунтується на поєднанні міжнародних підходів до управління ризиками та особливостей національного контексту.

Запропонована класифікація дозволяє структурувати проєктні загрози за джерелами виникнення, характером впливу та етапами життєвого циклу об’єкта, що забезпечує можливість їх практичного використання у проєктному управлінні.

Таблиця 3.1

Таксономія проєктних загроз об’єктів критичної інфраструктури

Група проєктних загроз	**Характеристика**	**Типові приклади**

Технічні проєктні загрози	Загрози, пов’язані з технічними рішеннями та інженерними параметрами проєкту	Використання застарілих технологій; помилки у проєктній документації; відсутність резервування критичних систем
Кібернетичні проєктні загрози	Загрози, що формуються внаслідок недоліків ІКТ-архітектури та цифрових компонентів проєкту	Відсутність принципу security by design; недостатній захист SCADA/ICS; слабка сегментація мереж
Організаційно-управлінські загрози	Загрози, пов’язані з процесами управління проєктом та людським фактором	Низька кваліфікація персоналу; відсутність контролю за підрядниками; неузгодженість між стейкхолдерами
Регуляторні та правові загрози	Загрози, зумовлені невідповідністю проєкту чинним або перспективним нормативним вимогам	Ігнорування вимог NIS2; неврахування змін у законодавстві; відсутність сертифікації
Загрози ланцюгів постачання	Загрози, пов’язані з залежністю від постачальників, обладнання та програмного забезпечення	Використання недовірених постачальників; відсутність оцінки ризиків third-party
Фінансово-ресурсні загрози	Загрози, що виникають унаслідок обмеженості ресурсів проєкту	Недостатнє фінансування заходів безпеки; скорочення строків проєктування

Зовнішні та контекстні загрози	Загрози, пов’язані з умовами зовнішнього середовища	Воєнні ризики; геополітична нестабільність; зміни кліматичних умов

Пояснення до таксономії проєктних загроз

Запропонована таксономія відображає багатовимірний характер проєктних загроз та дозволяє розглядати їх не ізольовано, а у взаємозв’язку з управлінськими рішеннями та контекстом реалізації проєкту.

Особливістю технічних і кібернетичних проєктних загроз є те, що вони закладаються у проєктну архітектуру об’єкта та можуть мати довгострокові наслідки, усунення яких після введення об’єкта в експлуатацію є складним або економічно недоцільним. Саме тому міжнародні стандарти акцентують увагу на принципах *security by design* та *resilience by design*.

Організаційно-управлінські та регуляторні загрози відіграють системоутворюючу роль, оскільки вони визначають якість прийняття проєктних рішень та рівень відповідності об’єкта чинним і перспективним вимогам безпеки. Їх ігнорування призводить до формування прихованих вразливостей, що можуть бути реалізовані на будь-якому етапі життєвого циклу.

Загрози ланцюгів постачання та фінансово-ресурсні загрози є особливо актуальними в умовах глобалізації та обмеженості ресурсів. Вони безпосередньо впливають на можливість впровадження сучасних технічних і безпекових рішень та повинні враховуватися вже на стадії формування технічного завдання.

Загалом запропонована класифікація створює практичну основу для подальшої кількісної оцінки проєктних загроз, формування матриці ризиків та розроблення адресних заходів з їх мінімізації. Вона може бути використана як універсальний інструмент у проєктах зі створення, модернізації та реконфігурації об’єктів критичної інфраструктури.

3.3. Відображення проєктних загроз на етапах життєвого циклу об’єкта критичної інфраструктури

Проєктні загрози об’єктів критичної інфраструктури проявляються нерівномірно на різних етапах їх життєвого циклу. Водночас саме рішення, прийняті на ранніх етапах, мають визначальний вплив на рівень безпеки, стійкості та надійності об’єкта протягом усього періоду його функціонування. Тому важливим елементом практичної реалізації запропонованої таксономії є відображення проєктних загроз на етапах життєвого циклу об’єкта.

У межах дослідження життєвий цикл об’єкта критичної інфраструктури розглядається як послідовність взаємопов’язаних етапів: планування та концептуального проєктування, детального проєктування, будівництва або впровадження, введення в експлуатацію, модернізації (ре-конфігурації) та експлуатації.

Таблиця 3.2

Відображення проєктних загроз на етапах життєвого циклу об’єкта критичної інфраструктури

Етап життєвого циклу	**Характерні проєктні загрози**	**Потенційні наслідки**
Планування та концептуальне проєктування	Неврахування вимог безпеки; неправильне визначення критичності об’єкта; ігнорування міжнародних стандартів	Формування системних вразливостей; неможливість подальшого підвищення рівня безпеки
Детальне проєктування	Помилки у проєктній документації; відсутність резервування; слабка кібер-архітектура	Зниження стійкості; високі витрати на доопрацювання

Будівництво / впровадження	Неналежний контроль підрядників; використання несертифікованих компонентів	Поява прихованих дефектів; зростання ризиків відмов
Введення в експлуатацію	Недостатнє тестування безпеки; відсутність перевірок кіберзахисту	Реалізація загроз одразу після запуску
Модернізація / реконфігурація	Несумісність нових компонентів; порушення цілісності системи	Тимчасова або постійна втрата функціональності
Експлуатація	Обмежені можливості усунення проєктних помилок	Зростання вартості управління ризиками

Аналітичне пояснення

Аналіз відображення проєктних загроз на етапах життєвого циклу показує, що найбільш критичними з точки зору формування загроз є етапи планування та проєктування. Саме на цих стадіях закладаються базові архітектурні, технічні та організаційні рішення, які в подальшому визначають рівень захищеності об’єкта.

На етапі детального проєктування ключовими стають технічні та кібернетичні загрози, пов’язані з помилками в архітектурі систем, відсутністю резервування та слабкою інтеграцією безпекових механізмів. Недоліки, допущені на цьому етапі, є складними для усунення без суттєвих фінансових і часових витрат.

Етапи будівництва та впровадження характеризуються підвищеною роллю організаційно-управлінських та загроз ланцюгів постачання, що зумовлено залученням підрядників і постачальників обладнання та програмного забезпечення. Недостатній контроль на цих етапах може призвести до появи прихованих вразливостей.

Під час модернізації та ре-конфігурації об’єктів критичної інфраструктури виникає ризик порушення цілісності системи, особливо за відсутності комплексної оцінки проєктних загроз. Це підтверджує необхідність застосування запропонованого підходу не лише при створенні нових об’єктів, а й при оновленні існуючих.

Загалом відображення проєктних загроз на етапах життєвого циклу об’єкта підтверджує превентивний характер запропонованого підходу, який дозволяє зменшити рівень ризиків шляхом їх ідентифікації до моменту введення об’єкта в експлуатацію. Це відповідає міжнародним стандартам управління ризиками та підвищує практичну цінність дослідження.

3.4. Інтеграція таксономії проєктних загроз у модель оцінки ризиків

Інтеграція розробленої таксономії проєктних загроз у модель оцінки ризиків є ключовим етапом практичної реалізації результатів дослідження. Такий підхід дозволяє перейти від описової класифікації загроз до **формалізованої системи прийняття рішень**, орієнтованої на зниження ризиків на етапах проєктування, модернізації та ре-конфігурації об’єктів критичної інфраструктури.

Запропонована модель оцінки ризиків базується на принципах ISO 31000 та поєднує елементи проєктного управління з безпековими процедурами. Таксономія проєктних загроз використовується як **вхідний структурований перелік ризик-факторів**, що забезпечує повноту та системність процесу ідентифікації ризиків.

Алгоритм інтеграції таксономії у модель оцінки ризиків

Інтеграція здійснюється за таким послідовним алгоритмом:

1. **Формування переліку проєктних загроз**

На основі таксономії визначається повний перелік потенційних проєктних загроз, релевантних конкретному об’єкту критичної інфраструктури та етапу його життєвого циклу.

2. Прив’язка загроз до етапів життєвого циклу Кожна загроза співвідноситься з відповідним етапом (проєктування, будівництво, модернізація), що дозволяє визначити часові «вікна ризику».

3. Експертна оцінка параметрів ризику. Для кожної загрози визначаються:

- ймовірність реалізації;
- тяжкість можливих наслідків. Оцінювання здійснюється за уніфікованою шкалою.

4. Розрахунок інтегрального рівня ризику. Рівень ризику визначається як функція ймовірності та наслідків і відображається у матриці ризиків.

5. Ранжування та пріоритезація загроз. Загрози групуються за рівнем критичності (високий, середній, прийнятний ризик), що дозволяє визначити пріоритетні напрями реагування.

6. Вибір заходів реагування. Для критичних загроз визначаються заходи уникнення, зниження, передачі або прийняття ризику з обов’язковою інтеграцією у проєктну документацію.

Переваги інтегрованої моделі

Інтеграція таксономії проєктних загроз у модель оцінки ризиків забезпечує низку практичних переваг:

- повноту ідентифікації ризиків за рахунок структурованого підходу;
- можливість раннього виявлення критичних загроз;
- підвищення обґрунтованості управлінських рішень;
- узгодженість із міжнародними стандартами управління ризиками;
- зниження витрат на усунення наслідків реалізації загроз на пізніх етапах життєвого циклу.

Таблиця 3.3

Використання таксономії проєктних загроз у моделі оцінки ризиків

Елемент моделі	Роль таксономії
Ідентифікація ризиків	Формує повний перелік релевантних загроз
Аналіз ризиків	Забезпечує групування та структуризацію
Оцінка ризиків	Дає змогу порівнювати загрози за єдиними критеріями
Управління ризиками	Сприяє вибору адекватних заходів реагування

Узагальнююча оцінка

Запропонована інтеграція таксономії проєктних загроз у модель оцінки ризиків забезпечує перехід від фрагментарного реагування на загрози до системного, превентивного управління безпекою об’єктів критичної інфраструктури. Такий підхід є особливо актуальним в умовах зростання кібернетичних і фізичних загроз та відповідає курсу України на гармонізацію з міжнародними стандартами у сфері захисту критичної інфраструктури.

3.5. Модель ідентифікації та оцінки проєктних загроз

Для практичної реалізації методичного підходу запропоновано модель ідентифікації та оцінки проєктних загроз, що поєднує якісні та кількісні елементи аналізу.

На першому етапі формується перелік потенційних проєктних загроз за такими групами:

- технічні (помилки проєктних рішень, застарілі технології);
- кібернетичні (вразливості ІКТ-архітектури, відсутність вимог безпеки за замовчуванням);
- організаційні (недостатня кваліфікація персоналу, слабке управління підрядниками);

- зовнішні (регуляторні зміни, залежність від постачальників, воєнні ризики).

На другому етапі здійснюється експертна оцінка кожної загрози за двома основними критеріями:

- ймовірність реалізації;
- тяжкість можливих наслідків.

Інтегральний рівень ризику визначається шляхом поєднання зазначених показників і відображається у матриці ризиків, що дозволяє наочно ідентифікувати критичні та прийнятні рівні ризику.

Застосування моделі дає змогу:

- визначити найбільш критичні проєктні загрози;
- обґрунтувати пріоритетність заходів безпеки;
- зменшити ймовірність помилок на ранніх етапах реалізації проєкту.

3.6. Апробація підходу на прикладі типового об’єкта критичної інфраструктури

З метою перевірки прикладної ефективності запропонованого підходу проведено його апробацію на прикладі типового об’єкта критичної інфраструктури (енергетичного, транспортного або інформаційно-комунікаційного – залежно від обраного профілю).

У межах апробації:

- визначено контекст проєкту та основні функціональні вимоги;
- ідентифіковано перелік проєктних загроз;
- проведено експертну оцінку ризиків;
- сформовано матрицю ризиків та запропоновано заходи з їх мінімізації.

Результати апробації показали, що застосування підходу дозволяє виявити загрози, які не враховуються у традиційних процедурах безпеки,

зокрема на ранніх стадіях проєктування, та підвищити обґрунтованість управлінських рішень.

3.7. Практичні рекомендації щодо впровадження підходу

На основі проведеного дослідження розроблено практичні рекомендації для суб'єктів у сфері критичної інфраструктури:

- інтегрувати процедури ідентифікації проєктних загроз у стандарти проєктного управління;
- використовувати ризик-орієнтований підхід відповідно до ISO 31000 на всіх етапах життєвого циклу об'єктів;
- передбачати обов'язкову експертну оцінку проєктних рішень з позицій безпеки;
- гармонізувати внутрішні регламенти з вимогами NIS2 та міжнародними практиками;
- посилити міжвідомчу та публічно-приватну взаємодію у сфері обміну інформацією про загрози.

Запропоновані рекомендації можуть бути використані як операторами об'єктів критичної інфраструктури, так і органами державного управління при формуванні політики безпеки.

Висновки до розділу 3

У четвертому розділі магістерської роботи розроблено та обґрунтовано системний прикладний підхід до визначення проєктних загроз об'єктів критичної інфраструктури, який поєднує таксономію загроз, модель оцінки ризиків і практичні рекомендації щодо їх мінімізації.

У роботі уточнено поняття «проєктні загрози» як окремої категорії загроз, що формуються на етапах планування, проєктування, будівництва, модернізації та ре-конфігурації об'єктів критичної інфраструктури і мають довгостроковий вплив на рівень їх безпеки та стійкості. Доведено принципову відмінність проєктних загроз від загальних експлуатаційних загроз.

Запропоновано таксономію проєктних загроз, яка охоплює технічні, кібернетичні, організаційно-управлінські, регуляторні, загрози ланцюгів постачання, фінансово-ресурсні та зовнішні загрози. Розроблена класифікація забезпечує повноту ідентифікації загроз та створює основу для їх системного аналізу в межах проєктної діяльності.

У межах розділу проаналізовано прояв проєктних загроз на різних етапах життєвого циклу об’єкта критичної інфраструктури та показано, що найбільш критичними з точки зору формування вразливостей є ранні етапи планування та проєктування. Підтверджено превентивний характер запропонованого підходу, який дозволяє зменшити ризики ще до введення об’єкта в експлуатацію.

Розроблено модель інтеграції таксономії проєктних загроз у систему оцінки ризиків, що базується на експертному оцінюванні та матриці ризиків і відповідає принципам ISO 31000. Застосування цієї моделі забезпечує обґрунтоване ранжування загроз та вибір пріоритетних заходів реагування з урахуванням етапу життєвого циклу об’єкта.

Отримані у розділі результати мають практичну цінність для операторів об’єктів критичної інфраструктури та органів державного управління, оскільки дозволяють інтегрувати управління проєктними загрозами у процеси проєктного управління та гармонізувати національну практику із міжнародними стандартами та підходами.

РОЗДІЛ 4
ІНСТРУМЕНТИ ТА АЛГОРИТМИ ВИЯВЛЕННЯ ПРОЄКТНИХ ЗАГРОЗ

4.1. Процесна схема ідентифікації та оцінки загроз

Ця схема описує алгоритм розробки документа «Проєктна загроза» (DBT), який стає основою для проєктування інженерно-технічних засобів охорони.

Загальний алгоритм (Схема процесу)

Процес ідентифікації загроз для критичної інфраструктури є циклічним і складається з 4 основних фаз:

Фаза 1: Характеристика об'єкта (Target Identification)

- Мета: Визначити, *що* ми захищаємо (життєво важливі місця, радіоактивні матеріали, інформаційні сервери).
- Дія: Категоризація цілей за ступенем критичності (наслідки від втрати/руйнування).

Фаза 2: Збір даних про джерела загроз (Intelligence Gathering)

- Мета: Зрозуміти, *хто* може атакувати та *які* природні явища можливі.
- Категорії джерел:

1. Зовнішні порушники: Терористи, кримінал, диверсанти, активісти.
2. Внутрішні порушники (Інсайдери): Персонал, охорона, підрядники (ризик змови, саботажу).
3. Природні та техногенні явища: Землетруси, повені, пожежі, аварії на сусідніх об'єктах.

Фаза 3: Аналіз атрибутів та характеристик (Threat Characterization)

- Мета: Визначити *потенціал* загрози (на що вони здатні).
- Аналізовані параметри (Атрибути порушника):

- *Мотивація:* Політична, фінансова, ідеологічна.
- *Чисельність:* Група чи одинак.
- *Озброєння:* Стрілецька зброя, вибухівка, спецзасоби, БПЛА (дрони).
- *Навички:* Військова підготовка, знання систем кібербезпеки, знання об'єкта.
- *Тактика:* Приховане проникнення, силовий штурм, обман, кібератака.

Фаза 4: Формулювання Проєктної Загрози (DBT Definition)

- Мета: Створити офіційний документ, який фіксує максимальний рівень загрози, для протидії якому система *зобов'язана* бути спроєктована.
- Результат**:** Опис сценаріїв (наприклад: "Група з 4 осіб, озброєна автоматичною зброєю та 2 кг вибухівки, за підтримки 1 інсайдера").

Інструменти та Методи (Tools Breakdown)

Для реалізації цієї схеми використовуються специфічні інструменти безпеки:

Таблиця 4.1

Інструменти безпеки

Інструмент / Метод	**Опис та Застосування в Проєктній Загрозі**
Метод CARVER	Матриця кількісної оцінки привабливості цілі для диверсанта. Оцінює цілі за критеріями: **C**riticality (Критичність), **A**ccessibility (Доступність), **R**ecuperability (Відновлюваність), **V**ulnerability (Вразливість), **E**ffect (Ефект), **R**ecognizability (Впізнаваність).
Аналіз шляхів (Adversary Sequence Diagrams - ASD)	Алгоритмічний метод побудови шляхів проникнення порушника від периметра до цілі. Допомагає виявити найвірогідніші маршрути атаки для конкретних сценаріїв.

Моделювання "Червона Команда" (Red Teaming)	Імітація дій реального супротивника (етичні хакери або фізичні групи проникнення) для перевірки гіпотез про загрози та вразливості на етапі планування або експлуатації.
TVRA (Threat, Vulnerability and Risk Assessment)	Комплексна методологія оцінки загроз, вразливостей та ризиків. Дозволяє пов'язати ймовірність атаки з ефективністю наявних засобів захисту.
OSINT (Open Source Intelligence)	Розвідка на основі відкритих джерел для моніторингу намірів терористичних груп, соціальних настроїв або нових технологічних загроз (наприклад, нові типи дронів).

4.2 Деталізація за етапами життєвого циклу Системи Фізичного Захисту (СФЗ)

1. Ініціація (Передпроєктна стадія):
   - *Дія:* Розробка Концепції безпеки. Визначення нормативних вимог (державні стандарти для ядерних/енергетичних об'єктів).
   - *Інструмент:* Аналіз історичних даних про інциденти в галузі.
2. Планування (Проєктування СФЗ):
   - *Дія:* Розробка Документа Проєктної Загрози (ПЗ). Моделювання ефективності системи захисту проти визначених загроз.
   - *Інструмент:* Програмне забезпечення для симуляції (наприклад, EASI - Estimate of Adversary Sequence Interruption), побудова дерев відмов (Fault Tree Analysis).
3. Реалізація (Будівництво/Впровадження):
   - *Дія:* Контроль відповідності збудованих бар'єрів та систем визначеним загрозам.

- *Загроза етапу:* Впровадження "закладок" або вразливостей підрядниками (supply chain risks).

4. Експлуатація:

- *Дія:* Періодичний перегляд DBT (зазвичай раз на 1-3 роки або при зміні обстановки).
- *Інструмент:* Навчання персоналу, перевірка планів реагування на реальні інциденти.

У контексті фізичного захисту та визначення проєктної загрози (Design Basis Threat), **CARVER** – це методика, яка дозволяє подивитися на об'єкт очима потенційного зловмисника (диверсанта, терориста). Вона допомагає виявити найбільш привабливі цілі всередині вашої критичної інфраструктури.

Мета методу: ранжувати активи об'єкта, щоб зрозуміти, куди саме потрібно спрямувати найбільші ресурси захисту.

Розшифровка абревіатури CARVER

Кожен елемент оцінюється за бальною шкалою (зазвичай від 1 до 10), де **10** – це максимально приваблива умова для зловмисника (і максимальний ризик для вас), а **1** – мінімальна.

Таблиця 4.2

Можливе обгрунтування зловмисника

Критерій	**Англійська**	**Значення**	**Питання для аналізу (Погляд зловмисника)**	**Шкала (Приклад)**
C	**Criticality** (Критичність)	Наскільки важливий цей вузол для функціонуван	"Якщо я знищу це, чи зупиниться весь	**10**: Повна зупинка об'єкта.

		ня всієї системи?	завод/станція ?"	**1**: Вплив непомітний.
A	**Accessibility** (Доступність)	Наскільки легко фізично дістатися до цілі?	"Чи зможу я підійти до цілі непоміченим, обійти охорону та бар'єри?"	**10**: Відкритий доступ (без паркану). **1**: Бункер, біометрія, озброєна охорона.
R	**Recuperability** (Відновлюваність)	Скільки часу займе відновлення роботи після атаки?	"Як довго об'єкт буде виведений з ладу? Чи є запасні частини?"	**10**: Роки/неможливо відновити. **1**: Години/миттєва заміна.
V	**Vulnerability** (Вразливість)	Наскільки легко ціль пошкодити наявними засобами?	"Чи вистачить мені молотка, чи потрібна вибухівка С4?"	**10**: Можна знищити підручними засобами. **1**: Витримує пряме влучання ракети.

E	**Effect** (Ефект)	Який прямий та непрямий ефект від атаки (паніка, політика, екологія)?	"Чи викличе це резонанс у новинах, страх населення або екологічну катастрофу?"	**10**: Міжнародний скандал, жертви, катастрофа. **1**: Тільки локальні збитки.
R	**Recognizability** (Впізнаваність)	Наскільки легко ідентифікувати ціль серед інших об'єктів?	"Чи зможу я знайти потрібний кабель/сервер без спеціальних знань і карт?"	**10**: Яскраво підписано, очевидно. **1**: Замасковано, виглядає як звичайна стіна.

4.2.1 Алгоритм застосування CARVER

Процес оцінки зазвичай виконується групою експертів (служба безпеки, інженери, технологи) за наступним алгоритмом:

Крок 1: Декомпозиція об'єкта

Розбийте об'єкт критичної інфраструктури на конкретні вузли (активи).

- *Приклад:* Трансформаторна підстанція, Серверна кімната, Склад палива, КПП охорони, Адміністративна будівля.

Крок 2: Оцінка кожного активу

Заповніть матрицю, виставляючи бали (1-10) для кожного активу за кожною літерою CARVER.

Таблиця 4.3

Приклад розрахунку (порівняння двох цілей на Енергооб'єкті):

Актив (Ціль)	**C**	**A**	**R**	**V**	**E**	**R**	**СУМА**	**Інтерпретація**
Головний силовий трансформатор	10 (Зупинить все)	4 (Запериметром)	10 (Замовлення нового – 6 міс.)	8 (Вразливий до куль/вибуху)	9 (Відключення міста)	10 (Великий, очевидний)	**51**	**Критична ціль №1.** Потребує додаткового захисту (габіони, екрани).
Склад офісних меблів	1 (Робота не стане)	8 (Слабка охорона)	1 (Купити нові легко)	10 (Легко спалити)	1 (Ніхто не помітить)	10 (Підписано)	**31**	**Низький пріоритет.** Витрачати бюджет на посилений захист

								недоціл ьно.

Крок 3: Аналіз результатів

Активи з найвищими сумами балів є найбільш вірогідними цілями для зловмисника. Саме вони формують основу Проєктної Загрози.

- Якщо "Головний трансформатор" набрав 51 бал, система безпеки має бути спроєктована навколо нього.
- Якщо у активу високий бал R (Recognizability), можливо, варто прибрати таблички або замаскувати його.
- Якщо високий бал **A** (Accessibility), потрібно додати бар'єри або датчики руху.

Чому це важливо для "Проєктної загрози"?

Метод CARVER перетворює абстрактне поняття "безпека" на конкретну математичну модель. Він дозволяє обґрунтувати бюджет перед замовником або керівництвом:

"Ми ставимо дорогу систему відеоспостереження та бар'єри саме біля цього вузла, тому що за методом CARVER його індекс привабливості – 51, що є найвищим на об'єкті".

Це також допомагає визначити характеристики зловмисника. Наприклад, якщо ціль має низьку вразливість (**V=2**), це означає, що загрозою є не хуліган з каменем, а підготовлена група з вибухівкою. Відповідно, в паспорт проєктної загрози вписується "озброєна група з вибуховими речовинами".

проведемо експрес-оцінку CARVER для двох різнопланових об'єктів у межах одного гіпотетичного підприємства критичної інфраструктури (наприклад, станція водопостачання або енергооб'єкт).

Це дозволить нам порівняти ризики для IT-інфраструктури (Серверна) та виробничого обладнання (Насосна станція).

Умови симуляції

- Об'єкт: Стратегічне підприємство.
- Потенційний агресор: Диверсійна група, що має на меті зупинити роботу підприємства на тривалий час.

Об'єкт №1: Серверна кімната (IT/SCADA)

Опис: Приміщення всередині адміністративної будівлі, де розташовані сервери управління технологічними процесами та бази даних.

Критерій	**Бал (1-10)**	**Обґрунтування оцінки (Логіка агресора)**
C - Criticality (Критичність)	**10**	**Максимальна.** Це «мозок» системи. Знищення серверів зупиняє всі автоматизовані процеси та моніторинг.
A - Accessibility (Доступність)	**3**	**Низька.** Потрібно пройти зовнішній периметр, увійти в адмінбудівлю (охорона), пройти СКУД (картки/біометрія) на поверсі.
R - Recuperability (Відновлюваність)	**6**	**Середня.** "Залізо" можна купити/замінити за пару днів. Якщо є *резервні копії (бекапи)* у хмарі або на віддаленому майданчику, дані відновлюються швидко. Якщо ні – бал зростає до 10.
V - Vulnerability (Вразливість)	**9**	**Висока.** Електроніка дуже вразлива. Вогонь, вода, відключення кондиціонування або кілька ударів молотком знищать обладнання.
E - Effect (Ефект)	**8**	**Високий.** Зупинка виробництва, втрата даних, репутаційні ризики, можлива паніка.
R - Recognizability (Впізнаваність)	**4**	**Низька/Середня.** Без таблички на дверях це просто «офіс №305». Потрібен інсайд або схема будівлі, щоб знайти саме серверну.

ЗАГАЛЬНА СУМА	**40**	*Результат:* Ціль дуже важлива, але до неї важко дістатися і її важко знайти без знань.

Об'єкт №2: Насосна станція

Опис: Окрема технічна споруда на території, яка забезпечує подачу води для охолодження реакторів або водопостачання міста.

Критерій	**Бал (1-10)**	**Обґрунтування оцінки (Логіка агресора)**
C - Criticality (Критичність)	**9**	**Дуже висока.** Без насосів технологічний процес зупиняється (або стається аварія через перегрів).
A - Accessibility (Доступність)	**7**	**Висока.** Часто такі станції стоять ближче до периметра (біля річки/водойми). Охорона може бути слабшою, ніж в адмінкорпусі.
R - Recuperability (Відновлюваність)	**9**	**Дуже складна.** Промислові насоси – це замовні позиції. Виготовлення та доставка нового агрегату може зайняти **6-12 місяців**. Швидко замінити нічим.
V - Vulnerability (Вразливість)	**5**	**Середня.** Чавун і сталь важко пошкодити молотком. Потрібна вибухівка, щоб підірвати трубу або сам насос, або знання, який вентиль перекрити.
E - Effect (Ефект)	**8**	**Високий.** Екологічна загроза або відсутність води у населення.
R - Recognizability (Впізнаваність)	**10**	**Максимальна.** Характерний шум, вібрація, труби, що входять у будівлю. Її видно на

		супутникових картах (Google Maps) і легко ідентифікувати візуально.
ЗАГАЛЬНА СУМА	**48**	*Результат:* Ціль більш приваблива для диверсанта, ніж серверна.

Аналіз результатів та Висновки

За результатами розрахунку CARVER:

1. Насосна станція (48 балів) є більш привабливою ціллю ("м'якою ціллю"), ніж Серверна (40 балів).

- *Чому?* Хоча Серверна критичніша (10 проти 9), Насосну набагато легше знайти (Recognizability 10) і до неї легше дістатися (Accessibility 7). Також її відновлення (Recuperability 9) триває набагато довше.

2. Вплив на Проєктну Загрозу (ПЗ) та Систему Захисту:

- Для Насосної станції:
  - *Пріоритет:* Зменшити **A** (Доступність) та **R** (Впізнаваність).
  - *Дії:* Посилити фізичний бар'єр (паркан, колючий дріт), встановити вібраційні сповіщувачі, встановити відеоспостереження з аналітикою перетину лінії. Можливо, застосувати маскувальні сітки або екрани, щоб приховати труби (знизити впізнаваність).
  - *План реагування:* Мати резервний насос на складі (знизити Recuperability з 9 до 3).
- Для Серверної:
  - *Пріоритет:* Утримувати **A** на низькому рівні та зменшити **V** (Вразливість).
  - *Дії:* Контроль доступу (двофакторна аутентифікація). Щодо вразливості – встановити газову систему пожежогасіння (щоб не залило водою), броньовані двері.
  - *План реагування:* Регулярне тестування розгортання бекапів (знизити Recuperability).

Цей метод наочно показує, що іноді дороге обладнання в центрі будівлі менш пріоритетне для захисту, ніж "грубе" залізо на периферії, втрата якого паралізує роботу на місяці.

4.3 Діаграма послідовності дій порушника (Adversary Sequence Diagram – ASD)

Діаграма послідовності дій порушника – це інструмент моделювання, який візуалізує шлях диверсанта від зовнішнього середовища («вулиці») безпосередньо до цілі (нашого насосу).

Оскільки за методом CARVER насосна станція набрала високі бали за Доступністю (A) та Впізнаваністю (R), наше завдання в ASD – розкласти цей шлях на кроки, щоб знайти найслабше місце, де ми можемо виявити ворога і затримати його достатньо довго для приїзду охорони.

Нижче наведено процес формування ASD для сценарію «Підрив насосу диверсійною групою».

1. Структура Діаграми (Шари захисту)

ASD будується за принципом «цибулини» (шарів). Для насосної станції виділяємо 4 фізичні зони:

1. Зовні (Off-site).
2. Периметр та Територія (Protected Area).
3. Будівля станції (Vital Area).
4. Ціль (Target – сам насос).

2. Формування Сценарію (Крок за кроком)

Ми описуємо дії порушника на межі кожної зони. Для кожного кроку визначаємо два параметри:

- Ймовірність виявлення (P_D): Чи побачить його система?
- Час затримки (T_{delay}): Скільки часу йому знадобиться, щоб подолати бар'єр?

Крок А: Подолання зовнішнього периметра

- *Дія:* Група підходить до паркану з боку лісу/річки.
- *Метод:* Перерізання сітки рабиці кусачками.
- *Характеристика:*
  - Затримка: 30 секунд.
  - Виявлення**:** Якщо на паркані немає вібраційного кабелю – **0%**. Якщо є камера, але оператор п'є каву – низька.

Крок Б: Переміщення територією

- *Дія:* Біг від паркану до дверей насосної станції (наприклад, 50 метрів).
- *Метод:* Швидке переміщення.
- *Характеристика:*
  - Затримка: 10 секунд.
  - Виявлення: Якщо є датчики руху (ІЧ-бар'єри) або відеоаналітика – висока.

Крок В: Проникнення в будівлю

- *Дія:* Вхід через технічні двері.
- *Метод:* Злам замка ломом або використання накладної вибухівки для вибивання дверей.
- *Характеристика:*
  - Затримка: 60 секунд (злам) або 10 секунд (вибух).
  - Виявлення: Датчик відкриття дверей (геркон), датчик розбиття скла.

Крок Г: Знищення цілі (Саботаж)

- *Дія:* Закладання вибухівки (С4) на корпус насосу та детонація.
- *Характеристика:*
  - Затримка**:** 40 секунд (встановити таймер, відбігти).

3. Математичний Аналіз (Критичний момент)

Головна формула фізичного захисту:

Tdelay > Tresponse

(Час затримки порушника має бути більшим за час реакції охорони)

Давайте порахуємо сценарій для нашої Насосної станції (найгірший варіант):

1. Загальний час порушника (Tadv):

- Паркан (30 с) + Біг (10 с) + Двері (60 с) + Мінування (40 с) = 140 секунд (2 хв 20 с).

2. Час реакції охорони ($T_{response}$):

- Оператор побачив сигнал тривоги: 10 с.
- Доповідь і збір групи реагування: 60 с.
- Доїзд/добіг до насосної станції: 3 хвилини (180 с).
- Разом: 250 секунд (4 хв 10 с).

ВИСНОВОК ASD: 140 < 250.

Результат: Диверсія успішна. Охорона приїде через 2 хвилини після вибуху. Система не працює.

4. Оптимізація системи на основі ASD

Дивлячись на діаграму, ми бачимо, що нам потрібно або збільшити час затримки порушника, або раніше його виявити.

Що робити (Коригувальні заходи):

1. Посилити бар'єр (Збільшення Tdelay):

- Замінити звичайні двері на броньовані 2-го класу захисту (час злому зростає з 60 с до 5 хвилин).
- *Новий час атаки:* 30 + 10 + **300** + 40 = 380 секунд.
- *Порівняння:* 380 > 250. **Перемога.** Група реагування встигає схопити диверсанта, поки він возиться з дверима.

2. Раніше виявити (Зсув точки детекції):

- Встановити на паркані надійну систему сигналізації. Тривога спрацьовує на етапі перерізання сітки (Крок А), а не на етапі вибивання дверей (Крок В).
- Це дає охороні додаткові дорогоцінні секунди на старті.

Підсумок

Діаграма послідовності дій порушник для Насосної станції дозволяє перетворити абстрактний страх "нас можуть підірвати" у чіткий таймлайн.

Вона показує, що навіть якщо у вас є зброя і охорона, але двері надто слабкі (або паркан "сліпий"), ви програєте змагання у часі.

Саме так формується **Проєктна Загроза**: ми фіксуємо, що система повинна витримувати натиск інструментів (брухт, пила) протягом мінімум 5 хвилин.

4.4 Розробка плану забезпечення стійкості кп "міськводоканал"

Мета плану: Забезпечити постачання питної води та відведення стоків за умов будь-яких збоїв, включаючи військові дії, відключення енергії та кібератаки.

Розділ 1. Паспорт критичної послуги

Замість опису будівель, ми описуємо процеси.

1.1. Визначення критичних функцій:

- Забір води (насосні станції 1-го підйому).
- Очищення та знезараження (станції водопідготовки).
- Транспортування (магістральні водогони, насосні 2-3 підйому).
- Водовідведення (каналізаційні насосні станції - КНС).

1.2. Параметри допустимих збоїв:

- RTO (Recovery Time Objective): Максимальний час, протягом якого місто може бути без води (наприклад, 4 години для лікарень, 24 години для населення).
- RPO (Recovery Point Objective): Допустима втрата даних (наприклад, даних білінгу чи SCADA).
- Мінімальний рівень послуги: Який тиск та обсяг води вважається "аварійним мінімумом" (санітарна норма).

Розділ 2. Динамічна оцінка ризиків

Аналіз загроз у реальному часі (All-hazards approach).

2.1. Кінетичні загрози: Ракетні удари по насосних станціях, руйнування дамб, ушкодження трубопроводів вибухами.

2.2. Енергетичні ризики: Повний блекаут, перепади напруги, дефіцит палива для генераторів.

2.3. Ланцюги постачання**:** Неможливість підвезення реагентів (хлоп, коагулянти) через блокування доріг.

2.4. Гібридні загрози: Одночасна кібератака на систему управління (SCADA) та повідомлення про замінування.

2.5. Каскадні ефекти: Як зупинка КНС вплине на екологію та санітарний стан міста (ризик епідемії).

Розділ 3. Технічні заходи стійкості (Resilience Measures)

Що зроблено, щоб система "поглинула удар".

3.1. Енергетична автономність:

- Наявність дизель-генераторів для критичних вузлів.
- Контракти на пріоритетне постачання палива.
- Альтернативні вводи електроживлення.

3.2. Фізичний захист (фортифікація):

- Габіони та бетонні блоки навколо трансформаторів та насосних агрегатів.
- Антидронові сітки.
- Захист ємностей з хлором/хімікатами (локалізація викидів).

3.3. Дублювання систем:

- Резервні свердловини (бювети), що працюють автономно.
- Кільцювання водопровідної мережі (можливість подати воду в обхід пошкодженої ділянки).

Розділ 4. Кіберстійкість та зв'язок

Інтеграція з вимогами NIS2.

4.1. Захист OT/SCADA: Ізоляція технологічної мережі від інтернету, ручне керування засувками у разі злому системи.

4.2. Резервний зв'язок:

- Наявність терміналів супутникового зв’язку (Starlink) для диспетчерів.
- Захищений радіозв'язок (на випадок падіння мобільної мережі).

Розділ 5. Управління персоналом

Люди – найвразливіший актив.

5.1. Кризові ролі: Хто приймає рішення, якщо директор недоступний.

5.2. Кадровий резерв: Список колишніх працівників або пенсіонерів, яких можна викликати у разі мобілізації основного персоналу.

5.3. Безпека персоналу:

- Алгоритм дій під час повітряної тривоги (укриття на території).
- Засоби індивідуального захисту (хімзахист, бронежилети для ремонтних бригад).
- Перевірка персоналу на наявність інсайдерських загроз.

Розділ 6. Реагування та Відновлення (Crisis Management)

Алгоритми дій.

6.1. Протоколи реагування (Playbooks):

- Дії при повному знеструмленні.
- Дії при хімічній аварії (витік хлору).
- Дії при фізичному руйнуванні магістрального водогону.

6.2. Взаємодія зі стейкхолдерами:

- Механізм запиту допомоги у ДСНС, Обленерго, міської влади.
- Інформування населення (графіки подачі води).

6.3. План підвезення води: Маршрути автоцистерн, точки видачі води населенню.

Розділ 7. Матеріальний резерв

7.1. Стратегічний запас:

- Запас труб, засувок, хомутів для швидкого ремонту ("аварійний набір").
- Запас реагентів мінімум на 30 діб.
- Запас питної води у резервуарах чистої води (РЧВ).

Чому ця структура краща за старий "План цивільного захисту"?

1. Акцент на послузі: Старий план рятував людей і майно. Цей план рятує функцію (щоб вода текла з крана).
2. Реальність війни: Враховано Starlink, генератори, габіони та мобілізацію персоналу.
3. Гнучкість: Це не статична папка паперів, а набір протоколів ("якщо сталося А, робимо Б"), що відповідає сучасним стандартам NATO та ЄС.
4.

4.5 Розробка покрокової інстукції для персоналу водоканалу на випадок повного знеструмлення.

ОПЕРАЦІЙНИЙ ПРОТОКОЛ № В-01

Тема: Дії персоналу при повному знеструмленні (BLACKOUT)

Об'єкт: КП "Міськводоканал"

Статус: Для службового користування

🟥 **Етап 0: "Стоп" та Оцінка (0 – 15 хвилин)**

Мета: Запобігти пошкодженню обладнання та з'ясувати масштаб проблеми.

Таблиця 4.1

№	Дія	Відповідальний	Примітки
0.1	**Фіксація знеструмлення.** Перевірити показники телеметрії (SCADA). Якщо зв'язок з об'єктами	Диспетчер	⚠️ Не намагатися перезавантажувати систему дистанційно.

	втрачено – вважати їх знеструмленими.		
0.2	**Перекриття засувок (Anti-Hydraulic Shock).** На насосних станціях (НС) 2-го підйому автоматично або вручну перекрити напірні засувки.	Черговий машиніст НС	Це критично, щоб вода не пішла "назад" і не розірвала труби/насоси гідроударом.
0.3	**Зв'язок з енергетиками.** Зв'язатися з диспетчером Обленерго/РЕМ для з'ясування причини та орієнтовного часу відновлення.	Головний енергетик	Використовувати спецлінію або Starlink, якщо мобільний зв'язок "ліг".
0.4	**Оповіщення.** Повідомити керівництво підприємства та чергового міськради за формою: *"Повне знеструмлення. Переходимо на аварійний протокол".*	Диспетчер	

🟧 Етап 1: Запуск резервного живлення (15 – 60 хвилин)

Мета: Відновити критичний мінімум водопостачання.

Пріоритетність запуску ДЕС (Дизель-електростанцій):

1. НС другого підйому (подача в місто).
2. НС першого підйому (забір води) – *якщо є запас у резервуарах чистої води (РЧВ), цей крок можна відкласти на 2-3 години.*
3. Очисні споруди (КНС) – для запобігання виливу стоків.

№	Дія	Відповідальний	Примітки
1.1	**Відключення від мережі.** Переконатися, що вводний рубильник від зовнішньої мережі ВИМКНЕНО (розрив ланцюга).	Черговий електрик	⚠ **СМЕРТЕЛЬНО НЕБЕЗПЕЧНО!** Якщо дадуть світло під час роботи генератора без розриву – згорить генератор.
1.2	**Перевірка ДЕС.** Рівень мастила, охолоджуючої рідини, палива. Візуальний огляд на відсутність протікань.	Механік / Електрик	
1.3	**Запуск та прогрів.** Запустити генератор. Дати пропрацювати на холостому ходу 3-5 хв для стабілізації напруги.	Електрик	
1.4	**Подача навантаження.** Поступово (ступінчасто) вмикати насосні агрегати. Спочатку один, перевірка струмів, потім наступний.	Машиніст НС	**Заборонено** запускати всі насоси одночасно (пускові струми "виб'ють" генератор).

🟦 Етап 2: Робота в аварійному режимі (1 – 4 години)

Мета: Стабілізація системи та економія ресурсів.

1. **Режим тиску:** Знизити тиск у мережі до **мінімального санітарного** (наприклад, 2.5 атм замість 5.0 атм). Вода буде доходити до 3-4 поверхів. Верхні поверхи – без води.

2. **Графік подачі:** Якщо палива мало або потужності ДЕС не вистачає, перейти на погодинний графік (наприклад: 06:00–09:00 та 18:00–21:00).

3. **Водовідведення:** Забезпечити роботу головних КНС. Другорядні КНС можуть працювати в режимі накопичення (слідкувати за рівнем у приймальних відділеннях).

🟧 Етап 3: Логістика та "Довга гра" (4+ години)

Мета: Забезпечення безперервності роботи понад добу.

№	Дія	Відповідальний	Інструкція
3.1	**Моніторинг палива.** Щогодини заміряти залишок палива в баках ДЕС.	Черговий	Дані передавати в логістичний центр підприємства.
3.2	**Дозаправка.** Замовити паливозаправник, коли рівень бака досягне 40%.	Завгосп / Логіст	Не чекати "червоної лампочки". Врахувати затори на дорогах.
3.3	**Підвезення води.** Якщо район міста без води понад 12 годин – направити автоцистерни до лікарень та точок роздачі.	Начальник автотранспорту	Згідно з затвердженими маршрутами.
3.4	**Ротація персоналу.** Організувати зміну бригад,	HR / Адмін. відділ	

	гаряче харчування та пункти обігріву для чергових.		

🟩 Етап 4: Відновлення нормального режиму (Світло дали)

Мета: Безпечний перехід на мережу.

1. **Очікування (10-15 хв):** Не вмикатися одразу після появи світла. Можливі стрибки напруги або повторне відключення.
2. **Зворотний перехід:**
   - Зняти навантаження з генератора (зупинити насоси).
   - Зупинити генератор.
   - Увімкнути ввідний рубильник зовнішньої мережі.
3. **Плавний пуск:** Запуск насосних агрегатів по черзі з інтервалом 5-10 хвилин для уникнення гідроударів та перевантаження міської електромережі.
4. **Розповітрення:** Перевірити вантузи (клапани випуску повітря) на магістралях, щоб уникнути повітряних пробок.

Додаткові рекомендації для візуалізації

Для кращого сприйняття персоналом, я рекомендую додати до цього тексту схематичні зображення (інфографіку):

– Схема перемикача "Мережа-0-Генератор" (щоб електрик візуально пам'ятав положення ручки).

Карта-схема території з позначенням місць підключення генераторів.

QR-коди на обладнанні з посиланням на відеоінструкцію запуску конкретної моделі генератора.

РОЗДІЛ 5
ОХОРОНА ПРАЦІ

За для забезпечення необхідного рівня безпеки праці на виробництвах та наукових лабораторіях була створена система охорони праці. Дотримання правил безпеки і виробничої санітарії залежить від того, наскільки кожен працівник знає і виконує ці правила під час роботи. Порушення правил і вимог техніки безпеки та охороні праці. може призвести до виробничого травматизму.

За стан техніки безпеки та охороні праці в лабораторії відповідає керівник лабораторії. При цьому усі співробітники лабораторії несуть персональну відповідальність за забезпечення безпеки на своєму робочому місці.

Для аналізу умов праці було обрано лабораторію КАІ - 7.410.

Метою аналізу умов праці є визначення небезпечних і шкідливих чинників при виконанні певної роботи, та потреби в розробленні засобів і заходів для усунення ризику травмування та професійних захворювань і створення умов для високопродуктивної праці [96].

5.1 Аналіз умов праці

5.1.1 Організація робочого місця

Робоче місце– місце постійного або тимчасового перебування працівника або групи працівників в процесі трудової діяльності, оснащене всім необхідним для успішного здійснення роботи [97].

Параметри хімічної лабораторії, в якій проводилися досліди, становлять:

- Довжина приміщення a = 7,0 м;
- Ширина приміщення b = 5,0 м;
- Висота приміщення h = 3,2 м.

Таким чином, площа цього приміщення $S^{/}=a\cdot b=35м^2$, загальна площа столів, шаф, приладів $S_п = 20$ м^2, а корисна площа $S=S^{/}-S_п=15$ м^2.

Об’єм приміщення становить V=S·h=48 м^3.

В приміщенні працює 2 особи.

Розрахуємо значення площі і об’єму приміщення на одну особу (табл.5.1).

Таблиця 5.1

Дійсні і нормативні параметри приміщення, що приходяться на одну людину

Параметр Приміщення	Норма	Дійсне значення
Площа, S	Не менше 4,5 м^2	7,5 м^2
Об’єм , V	Не менше 15 м^3	24 м^3
Висота	Не менше 3 м	3,2 м

Значення об’єму приміщення, що приходиться на одну людину і корисної площі більші за нормативні у відповідності з СН 245-94 і ОНТП-24-92.

5.1.2 Перелік шкідливих та небезпечних виробничих чинників.

До основних шкідливих і небезпечних факторів, що впливають на дослідника в хімічній лабораторії відносять:

- несприятливі параметри мікроклімату;
- виробниче освітлення;
- наявність шкідливих речовин;
- електронебезпека;
- вибухо-пожежна небезпека.

5.1.3 Аналіз шкідливих та небезпечних чинників

5.1.3.1 Мікроклімат приміщення.

Мікрокліматичні умови виробничих приміщень характеризуються такими показниками[98]:

- температура повітря,

- відносна вологість повітря,

- швидкість руху повітря,

- інтенсивність теплового (інфрачервоного) випромінювання,

- температура поверхонь.

За ступенем впливу на тепловий стан людини мікрокліматичної умови поділяють на оптимальні та допустимі.

Відповідно до ДСТУ 12.1.005-02 і ДСН 3.3.6.042-99, робота, яку я виконувала у приміщенні, відноситься до першої категорії Іб. До неї належать роботи, що виконуються сидячи, стоячи або пов'язані з ходінням та супроводжуються деяким фізичним навантаженням. Величини показників мікроклімату у робочій зоні для робіт категорії Іб наведені в табл. 5.2.

В розглянутому приміщенні підтримуються належні вимоги метеорологічних умов для виконання робіт I (легкої) категорії.

Таблиця 5.2

Оптимальні і припустимі норми температури, відносної вологості повітря і швидкості руху повітря в робочій зоні виробничих приміщень для категорії робіт Іб

Період року	Температура повітря, ^{0}C		Відносна вологість повітря, %		Швидкість руху повітря, м/с	
	Опти-мальна	Допус-тима	Опти-мальна	Допус-тима	Опти-мальна	Допустима
Холодний	21-23	20-24	60-40	Не більше 75	0,1	не більше 0,1
Теплий	22-24	21-28	60-40	60 - при 27 ^{0}C	0,1	0,3-0,1
Існуючі умови на	22-23		50		0,1	

робочому місці			

5.1.3.2. Природне та штучне освітлення

Згідно зі СНіП 23-05-95 дослідження, які проводились за характером зорової роботи відноситься до робіт середньої точності, розряд зорової роботи IV.

У приміщенні лабораторії присутнє суміщене освітлення: природне і штучне. У приміщенні присутні 11 світильників на стелі , загальною кількістю ламп в них – 44 шт. За типом: лампи люмінесцентні T8 TL-D Standard Colours 18W/54-765 G13 Philips. Ще існує освітлення у витяжних шафах: місцеве штучне, кількість ламп- 3 шт., тип - T8 TL-D Standard Colours 36W/54-765 G13 Philips.

5.1.3.3 Електронебезпека

Небезпека ураження людей електричним струмом істотно залежить від конструкції електричної мережі, роду струму (постійного чи змінного), робочої напруги, режиму нейтралі джерела живлення, стану ізоляції, огороджень і блокувань. Коли людина торкається неізольованої струмоведучої частини електроустановки, що перебуває під напругою, струм який проходить через тіло людини, визначається напругою установки і опором тіла людини. Якщо людина торкається ізольованої струмоведучої частини, то опір ізоляції включається в мережу струму послідовно з опором тіла людини. Це збільшує повний опір кола струму, а оскільки опір ізоляції значно більший за опір людини, зменшується сила струму до безпечної величини, а відтак і захищається людина від ураження.

У лабораторії електрична мережа має наступні характеристики: напруга - 220 Вт, частота струму - 50 Гц, кількість фаз - 1, вид струму - змінний.

Усі приміщення, в яких існує небезпека ураження людей електричним струмом, щодо техніки електробезпеки поділяються на приміщення з підвищеною небезпекою, особливо небезпечні приміщення та приміщення без

підвищеної небезпеки. Лабораторія, в якій виконувалась дипломна робота відноситься, щодо техніки електробезпеки, до приміщень без підвищеної небезпеки, у яких відсутні умови, що створюють підвищену чи особливу небезпеку.

Умовно безпечною для життя людини прийнято вважати напругу, що не перевищує 42 В змінного струму (в Україні така стандартна напруга становить 36 та 12 В), при якій не повинен статися пробій шкіри людини, що призводить до різкого зменшення загального опору її тіла.

Гранично допустимий струм, що проходить крізь тіло людини при нормальному (неаварійному) режимі роботи електроустановки, не повинен перевищувати 0,3 мА для змінного струму і 1 мА для постійного.

Гранично допустима напруга на людину при нормальному (неаварійному) режимі роботи електроустановки не повинна перевищувати 2-3 В для змінного струму і 8 В для постійного.

5.2. Розробка заходів з охорони праці

У цьому підрозділі розглянемо заходи для нормалізації мікрокліматичних умов, що забезпечують здоров’я працівників.

Для нормалізація несприятливих мікрокліматичних умов здійснюється ряд заходів і комплексів, які включають: будівельно-планувальні, організаційно-технологічні, санітарно-технічні та ін. заходи колективного захисту. Для профілактики перегрівань та переохолоджень робітників використовуються засоби індивідуального захисту, медико-біологічні тощо. У приміщеннях з вікнами, що займають велику площу здійснюються заходи щодо захисту від перегрівання при попаданні прямих сонячних променів в теплий період року (орієнтація віконних прорізів схід - захід, улаштування жалюзі та ін.), від радіаційного охолодження - в зимовий (екранування робочих місць). При температурі внутрішніх поверхонь огороджуючих

конструкцій, засклення нижче або вище допустимих величин робочі місця повинні бути віддалені від них на відстань не менше 1 м.

Для нормалізації температури приміщень у виробничих приміщеннях з надлишком тепла використовують природну вентиляцію. Аераційні ліхтарі та шахти розташовують безпосередньо над основними джерелами тепла на одній осі. У разі неможливості або неефективності аерації встановлюють механічну загальнообмінну вентиляцію.

5.3. Пожежна безпека.

Кількість горючих і вибухонебезпечних матеріалів, які використовуються в хімічних лабораторіях невелика- тому приміщення відноситься до категорії «В» (НАПБ Б.07.005-86. Згідно з правилами улаштування електроустановок (ПУЕ) приміщення хімічних лабораторій відносяться до класу В-1б, оскільки роботи навіть з горючими і вибухонебезпечними речовинами ведуться у витяжних шафах без застосування відкритого вогню і відкритих нагрівальних пристроїв.

У випадку виникнення пожежі, евакуація із лабораторії здійснюється відповідно до плану

Затверджений план евакуації на випадок виникнення пожежі наведено нижче на рис. 5.1

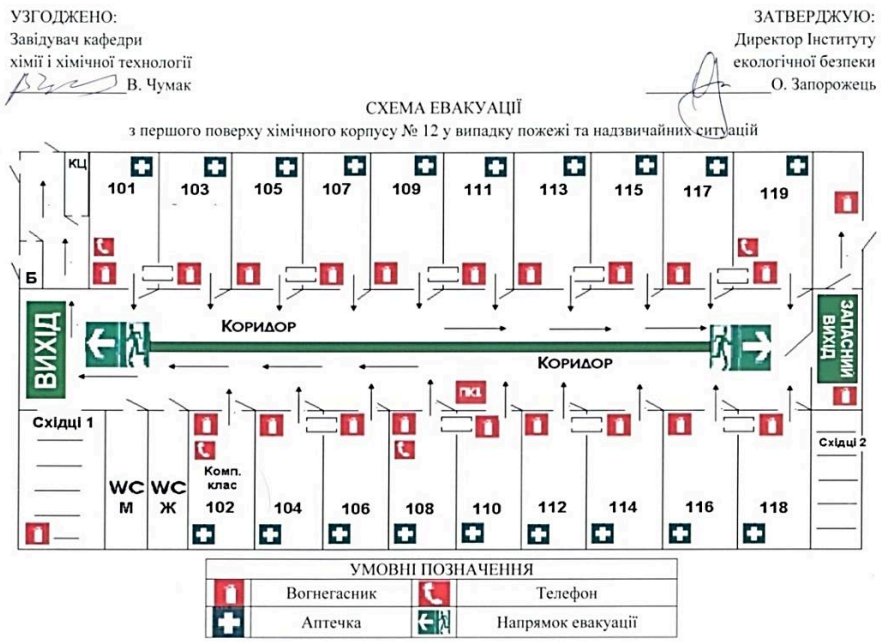

Рис. 5.1 – Схема евакуації з першого поверху корпусу №12 Національного авіаційного університету у випадку виникнення надзвичайної ситуації.

В розглянутій лабораторії знаходиться дорогі прилади, тому пожежа може привести до великих матеріальних втрат.

У приміщенні лабораторії знаходяться:

вогнегасник ВП-5(3) (ДСТУ 3675-98) – 1шт.;

вогнегасник ВВК–1.4 (ДСТУ 3675-98) – 1шт.

Така кількість вогнегасників відповідає вимогам ISO3941-87, якими передбачене обов'язкова наявність двох вогнегасників на 100 м^2 площі підлоги для приміщень.

У робочому приміщенні виконуються усі вимоги по пожежонебезпеці відповідно до вимог НАПБ.А.01.001- 95 “Правила пожежної безпеки в Україні”.

5.4. Розрахункова частина. Розрахунок штучного освітлення

Мета розрахунку загального освітлення методом коефіцієнта використання світлового потоку – визначити, чи достатня кількість

світильників і потужність ламп, для забезпечення в приміщенні нормованої освітленості Emin.

При розрахунку по вказаному методу необхідний світловий потік однієї лампи визначається по формулі:

$$\Phi_{Л} = \frac{E_{MIN} \cdot k \cdot S \cdot Z}{N \cdot n \cdot \eta} \quad (5.1)$$

або нормованої освітленосі:

$$E_{MIN} = \frac{\Phi_{Л} \cdot N \cdot n \cdot \eta}{k \cdot S \cdot Z} \quad (5.2)$$

де E_{min} – мінімальна нормована освітленість, лк;

k - коефіцієнт запасу;

S - освітлювана площа, м^2;

Z - коефіцієнт мінімальної освітленості (коефіцієнт нерівномірності освітлення);

N - число світильників;

n - число ламп в світильнику;

η - коефіцієнт використання світлового потоку в долях одиниці.

Вихідні дані:

Мінімальна нормована освітленість для приміщень даного типу становить 200 лк. Коефіцієнт запасу для приміщень з запиленням менше 1 мг/м^3 при використанні люмінесцентних ламп становить 1,2. Площа аудиторії становить 35 м^2. Коефіцієнт мінімальної освітленості для люмінесцентних ламп становить 1,1. Світловий потік ламп, що використовуються у приміщені становить 1080 лв.

Для визначення коефіцієнта використання світлового потоку знаходять індекс приміщення ***i.*** Для розрахунку індексу приміщення використовують формулу:

$$i = \frac{A \cdot B}{h \cdot (A + B)}, \quad (5.3)$$

де A, B, h – довжина, ширина і розрахункова висота приміщення, м:

$$h = H - h_{зв} - h_{р} \quad (5.4)$$

де Н – геометрична висота приміщення;

$h_{зв}$ – висота звисання світильника. $h_{зв}$=0 м.

$h_р$ – висота робочої поверхні. $h_р$ = 0,9 м.

$$h = 3,2 - 0 - 0,9 = 2,3 \text{ м.},$$

$$i = \frac{5 \cdot 7}{2,3 \cdot (5+7)} = 1,25 .$$

Отже, користуючись значенням індексу приміщення з табличних даних визначаємо, що η=55.

Отже, необхідна кількість світильників становить:

$$E_{MIN} = \frac{1080 \cdot 11 \cdot 4 \cdot 0,55}{1,2 \cdot 35 \cdot 1,1} = 565 \text{ лм.}$$

Такої кількості освітлення достатньо, для проведення вказаного типу робіт, тому необхідності у застосуванні додаткових джерел загального чи місцевого освітлення у даному випадку немає.

5.5. Висновки до розділу

Під час досліджень було проведено аналіз умов праці у приміщенні лабораторії № 7.410 корпусу №7 Національного університету Київський авіаційний інститут. Було розглянуто вплив різних чинників на організм людини, а саме: вплив мікроклімату, освітлення, ураження електричним струмом. Розглянута пожежна безпека та план евакуації у разі виникнення пожежі. Було пораховано необхідну кількість світильників для даної лабораторії, вона становить 565лм.

РОЗДІЛ 6
ЕКОЛОГІЯ

У цьому розділі досліджується зв’язок між дамбами та навколишнім середовищем – як вплив дамб на навколишнє середовище, так і вплив навколишнього середовища на дамби – та економічний аналіз цих наслідків. Дамби – це великі соціальні інвестиції, побудовані для виконання однієї або кількох із чотирьох основних цілей: побутове та промислове водопостачання, виробництво енергії, зрошення та контроль за повенями. На додаток до цих прямих вигод існує багато пов’язаних екологічних і соціальних наслідків, деякі з яких є вигодами, але більша частина яких, ймовірно, буде витратами. (Переселення є основною соціальною проблемою, пов’язаною з більшістю проектів гребель, і детально розглядається в інших технічних документах.) Економічний аналіз гребель повинен включати всі пов’язані вигоди та витрати, як прямі, так і непрямі, як при оцінці запропонованого проекту, так і при оцінці альтернативи.

У цьому розділі розглядаються фактори навколишнього середовища, пов’язані з проектами великих акумулюючих гребель, і економічний аналіз впливу на навколишнє середовище. Розглядаються впливи на навколишнє середовище, які виникають нагорі за течією, на місці та вниз за течією, а також методи економічного аналізу, які можна використовувати для оцінки впливу на навколишнє середовище в грошовому еквіваленті.

Великі греблі – це великі соціальні інвестиції, які зазвичай будуються для виконання однієї чи кількох із чотирьох основних цілей:

- побутове та промислове водопостачання;
- виробництво енергії;
- зрошення;
- контроль повеней.

За своєю природою греблі та пов’язані з ними водосховища створюють зміни в існуючому середовищі. Води затоплені, райони вище за течією

затоплені, люди часто витісняються з території водосховища. Існують також ефекти вниз за течією, які є результатом змін кількості, якості, часу та використання водних потоків. Деякі з цих впливів позитивні, інші негативні.

Термін «вплив на навколишнє середовище» у своєму широкому визначенні включає як фізичні, так і соціальні аспекти. Зміни в кількості або якості води, або ерозія ґрунту та осадження є фізичними наслідками навколишнього середовища. Вимушене переселення людей і порушення їх виробничих систем і способу життя є соціальними наслідками, а також впливом переселення на населення, яке населяє нові території проживання. Ключ до цього підходу полягає в тому, щоб підкреслити, що всі ці впливи разом спричинені проектом будівництва греблі та впливають на життєздатність проекту, його вигоди та витрати. Було б помилкою брати до уваги лише фізичні аспекти чи лише соціальний вплив. Непрямий вплив також необхідно брати до уваги так само, як і прямий вихід води для поливу, енергії, боротьби з повенями або побутового та промислового водопостачання.

Один із способів представлення цього різноманіття взаємодій (насамперед фізичних) використовує лінійний підхід до більшої системи, всередині якої розташована гребля. У верхній частині вододілу (у цьому розділі використовується для позначення басейну/водозбірного басейну, що стікає у водойму) існують екологічні умови, які впливають на водойму. Водосховище, у свою чергу, має різні впливи (як сприятливі, так і негативні) як на місці, так і на навколишнє середовище, розташоване нижче за течією.

Нарешті, існує непрямий або вторинний вплив на основні «зони обслуговування» нижче за течією – зрошення, побутове та промислове водопостачання та гідроенергію.

Зростання чисельності населення та розвиток технологій і будівництва, наприклад будівництво великих міст і доріг, мостів і дамб, призвели до дисбалансу в екосистемі та втрати екологічного балансу (Huesemann and Huesemann, 2011). З кожним днем інтерес до навколишнього середовища зростає, і в міру того, як інтерес до нього зростає, виникають протиріччя між

екологічними чиновниками та інженерами, які знають, що будівництво інженерних проектів, особливо дамб, завдає великої шкоди (Gadgil and Guha, 1994) . З інших аспектів ми знаємо, що будівництво інженерних будівель або промислових проектів сприяє розвитку та розвитку країни з усіх аспектів, економічного та соціального (Tibaijuka, 2009). Плануючи будівництво будь-якого проекту, слід звернути увагу на екологічні проблеми та те, як цей проект вплине на громаду та організми, не обов'язково звертати увагу лише на економічну цінність (Richter et al., 2010). Серед проектів розвитку великий інтерес для агентств і Світового банку становлять великі греблі (Ledec and Quintero, 2003).

Екологи говорили про екологічні та соціальні наслідки будівництва дамб, такі як міграція населення та зміна біорізноманіття, тоді як власники гідроелектростанцій говорили про те, що дамби є джерелом відновлюваної енергії (Бассон, 2004). Греблі спричиняють багато негативних впливів на навколишнє середовище та суспільство, у тому числі під час будівництва, і вони закінчуються після завершення будівництва, але найсерйозніший вплив спостерігається на етапі експлуатації, який триває тисячі років. Це також може бути результатом будівельних робіт, таких як будівництво доріг, буріння, лінії електропередач тощо. У цьому документі узагальнено несприятливий вплив на навколишнє середовище, пов'язаний з дамбами під час створення водосховища, будівництва та експлуатації, разом із типовими видами заходів пом'якшення.

Будівельні майданчики можуть бути джерелом забруднення води в результаті діяльності, яка неналежним чином керується та контролюється, що може вплинути на якість води нижче за течією.

Впливи, які зазвичай спостерігаються за таких обставин, стосуються виділення надмірних наносів у річковий потік, викидів хімікатів (Skaggs et al., 1994). Крім того, розподіл і кругообіг хімічних сполук у водоймах, таких як дамби, тісно пов'язані з рухом води в ландшафті та на них впливають процеси в гідрологічних і біологічних циклах (Lewis, 2002).

Викид високого вмісту наносів у воду може відбуватися головним чином під час робіт у руслі річки або поблизу нього: будівництво водовідвідного каналу, земляні роботи на ділянці дамби, будівництво захисних дамб і кофферів, кар'єрні роботи, запозичення піску в руслі річки, створення ґрунту. території, розташовані надто близько до берега річки або з нестабільними схилами тощо. Усі ці види діяльності можуть мати значний вплив на наноси, що скидаються в річку (Wahlstrom, 2012). Більшість цих робіт проводитиметься в сухий сезон, коли річка низька. Під час робіт необхідно буде відкачати воду, що просочилася з наносного горизонту в виїмку. Закачувана вода з великим навантаженням наносів часто просто скидається в сусідній потік, який зазвичай складається з низького потоку дуже чистої води, що дренується з поверхневих водоносних горизонтів (Jean-Baptiste et al., 2007).

Великі наноси можуть досягати річки на початку сезону дощів, коли перші сильні шторми розмивають нестійкі схили звалищ або оголені ґрунти на будівельних майданчиках, у таборах або вздовж під'їзних доріг. Однак вплив у цей період року є менш згубним через набагато вищий потік у річці, яка вже містить високий вміст наносів (Віссер та ін., 2002 та Муракамі, 1995).

6.1 Забруднення небезпечними речовинами

Під час будівництва дамб велика кількість бензину, мастильних матеріалів, а також велика кількість вибухових речовин і хімікатів (бетонна заливка, розчинники, фарби, розчинники, кислоти) будуть зберігатися та перероблятися на будівельному майданчику, і існує ризик витоку або оточення випадкового витоку. Цей ризик можна ефективно зменшити шляхом впровадження підрядником процедур превентивного управління: відповідне розташування зон зберігання з дизайном, що відповідає передовій міжнародній практиці (таможне зберігання), збір і переробка відпрацьованих масел, моніторинг усіх небезпечних продуктів із спеціальним поводженням процедури та плани на випадок непередбачених обставин (Webb et al., 1995 та

Basnyat et al., 2000). Іншим джерелом забруднення є заводи з дозуванням, зокрема стічні води від очищення бетоновозів, які складаються зі стічних вод із високим pH та забруднюючих речовин із добавок до бетону. У разі прямого викиду в річку може виникнути серйозний вплив на населення нижче за течією, яке покладається на річку для домашнього водопостачання та водопостачання великої рогатої худоби, миття та зрошення (Ellison, 2007).

6.2 Забруднення від побутових стічних вод

Регіон оператора та інші тимчасові робочі табори, ймовірно, вміщатимуть кілька тисяч працівників. Без відповідної системи санітарії та очищення стічних вод викид патогенів і коліформ у річку може серйозно вплинути на населення нижче за течією (Jafarinejad, 2016).

Забруднення твердими відходами

Під час будівництва дамби утворюватиметься дуже велика кількість твердих відходів як комунального, так і будівельного характеру. Більшість цих відходів, якщо не поводитися належним чином, може призвести до забруднення ґрунту та води з можливим шкідливим впливом на навколишнє середовище та здоров’я населення. Побутові відходи вироблятимуться в робочих таборах (Chandrappa і Das, 2012; Tatsi і Zouboulis, 2002).

Вплив під час захоронення водосховища

Коли наземна територія затоплюється підйомною водою одразу після закриття дамби, відбувається кілька процесів, які мають різкий вплив на якість води, що збирається. Розпочнеться процес евтрофікації, коли рослини, позбавлені атмосферного кисню, гинуть і починають розкладатися, що в поєднанні з розкладанням органічної речовини з верхнього шару ґрунту виснажує розчинений кисень у воді водойми. Якщо цю дезоксигеновану воду не замінити досить швидко, то на дні водойми виникнуть безкисневі умови (Spoor, 1990).

Гіпоксія викликає відновлювальне середовище, яке за допомогою анаеробних бактерій перетворює нерозчинні сполуки на розчинні з значними несприятливими наслідками: виділенням аміаку, металів, таких як залізо, марганець, іноді ртуть. Крім того, сульфат буде відновлено до висококислого водню, що постачається бактеріями, які можуть роз'їдати металеві компоненти турбін (Naja and Volesky, 2009). Ризикованість цих змін дуже шкідлива як для водних організмів, так і для електромеханічного обладнання. Ступінь і серйозність аноксичної області залежить від кількох параметрів, основними з яких є кількість затопленої органічної речовини та характеристики водойми. Іншим наслідком затоплення рослинності є вивільнення поживних речовин, таких як азот і фосфор, які беруть участь у процесі евтрофікації водойми, що має драматичні наслідки для якості води в довгостроковій перспективі.

Затоплена біомаса

Найбільш активною частиною біомаси щодо процесу гниття та споживання розчиненого кисню є м'яка біомаса: свіжі трави, листя дерев, плоди та гілки. Жорстка біомаса, представлена деревиною, дуже повільно розкладається у воді, і при постійному затопленні може залишатися десятиліттями. Органічні речовини, розташовані в перших кількох сантиметрах верхнього шару ґрунту, разом із м'якою біомасою також швидко сприяють швидкому процесу розпаду. Чим щільніший затоплений рослинний покрив, тим вищою є деградація води протягом перших кількох років після затоплення (Zimmer, 2008).

6.3. Скорочення біомаси

Можна вжити певних заходів до створення водойм, щоб максимально зменшити ризик зміни води. Найбільш очевидним заходом є видалення свіжої рослинності шляхом розчищення. Можна розглянути два заходи:

- Луки, чагарники та перелоги, розташовані в межах водосховища: спалювання рослинності протягом останніх двох-трьох місяців перед захороненням, щоб уникнути будь-якого значного відростання рослинності.

- Лісисті території: це невеликі та локалізовані території, переважно розташовані у верхній частині водойм. Фізичне очищення із заготівлею деревини місцевим населенням та спалюванням деревних відходів не зібрано.

Спалювання доцільно як з точки зору збереження якості води, так і для запобігання глобальному потеплінню. Дійсно, горіння споживає атмосферний кисень і вивільняє вуглекислий газ, тоді як розпад споживає розчинений у воді кисень і, коли кисень більше не доступний у воді (це відбувається дуже швидко), він перетворюється на анаеробний процес із виділенням метану. Ця ситуація є більш згубною з точки зору глобального потепління, оскільки метан у 25 разів більш шкідливий, ніж вуглекислий газ.

Плаваючі уламки

За наявності рослинного покриву очікується значна кількість плаваючого сміття під час етапу захоронення. На водозливі знадобляться деякі засоби для збору та транспортування будь-якого великого сміття (дерева), принесеного повінню.

Вплив на зону нижньої течії

Як тільки почнеться заповнення, деякий вантаж органіки буде транспортовано водою та випущено вниз за течією.

Вода, ймовірно, матиме знижений вміст розчиненого кисню, якщо тимчасово не буде безкисневою, і деякі загибелі риби можуть спостерігатися нижче за течією від греблі.

Зі збільшенням органічного навантаження вниз за течією вода може мати неприємний смак і, можливо, протягом кількох місяців бути несумісною з її використанням для пиття вдома та тварин. Типовим заходом пом’якшення

є забезпечення відповідних сіл водопостачанням, незалежним від річкової води, як правило, ручними насосами, під'єднаними до поверхневого алювіального водоносного горизонту (Baxter, 1977).

Впливи під час експлуатації водосховища

Прогнозування найбільш вірогідного стану водойми після захоронення та протягом років експлуатації є небезпечною справою. Однак спостереження за явищами в існуючих водосховищах по всьому світу і особливо в Африці заклали основу для емпіричного моделювання для оцінки, головним чином, поживних речовин і потенційної продуктивності в майбутньому водоймі. Таким чином, були встановлені спеціальні критерії, які дозволяють порівнювати та прогнозувати, пов'язані головним чином з морфометрією (формою) водойми та управлінням водними ресурсами (Gruner, 1963).

Прогнози щодо можливих майбутніх характеристик водосховищ Дамб представлені в наступному:

Час перебування

Гідравлічний час перебування пов'язаний із тривалістю очікуваного перебування води в резервуарі. Це відношення об'єму водосховища до річного притоку. Дійсно, чим довше залишається вода, тим вище концентрація поживних речовин і ризик евтрофікації водойми. Чим швидше оновлюється вода у водоймі, тим менший ризик погіршення її якості порівняно з якістю притоку.

Розвиток берегової лінії

Розвиненість берегової лінії водойми виражає відношення периметра водойми до довжини кола еквівалентної площі. Коли водосховище має високу дендритність, існує ризик недостатньої циркуляції та оновлення води в деяких ізольованих частинах з локальним ризиком евтрофікації та розвитку водної рослинності (Ветцель, 2001).

Температури і стратифікація пласта

Прогноз температури водойм залежить від географічних і метеорологічних критеріїв. Обмежена середня глибина водойм означає, що

значна площа водойм складатиметься з мілководдя, яке зазвичай має вищу температуру (Loucks, 2017).

Електропровідність і солоність

Електропровідність або солоність має збільшуватися з часом у водоймах в результаті накопичення солі в результаті випаровування. Зрештою це може становити загрозу для зрошення.

Завантаження поживними речовинами та первинна продуктивність

Оскільки фосфор, як правило, є фактором, що обмежує поживні речовини для первинного виробництва, він вважається ключовим критерієм для прогнозування ризику евтрофікації водойми.

Фосфор (P) є важливим макроелементом. Продуктивність водних систем знижується через дефіцит або недостатню біодоступність первинних продуцентів.

І навпаки, додавання розчиненого P до водних екосистем часто стимулює евтрофікацію, що призводить до цвітіння водоростей, фітопланктону або плаваючих макрофізичних речовин на поверхні води (Carpenter et al., 1998).

Відкладення пласта

Річки несуть чотири різні типи відкладень вниз за течією, які дозволяють утворювати річкові береги, такі як дельти, мул, річковий дрейф, озера у формі півмісяця, дамби та прибережні пляжі. Будівництво дамб перешкоджає потоку цих відкладень вниз за течією, що призводить до ерозії русла річки від цього осадового середовища та збільшення накопичених відкладень у водосховищах або дамбах (McCully, 1996). Швидкість опадів змінюється між кожною дамбою та річкою, а водосховища припиняють накопичення води завдяки обміну місця зберігання осадами. Зниження ємності накопичувачів призводить до зменшення потужності для виробництва гідроенергії, наприклад, до зменшення доступності води для зрошення, і якщо її не обробити, це може зрештою призвести до провалу греблі, а також річки.

Контроль осаду

Від зацікавлених Підрядників вимагатиметься дренаж будівельних майданчиків та використання відстійників у критичних місцях усередині або поблизу русла річки.

6.4 Забруднення хімічними речовинами

Надайте контейнери для всіх хімікатів і хімічних відходів, включаючи паливо, моторне масло та гідравлічні рідини. Також буде потрібно моніторинг і реєстрація кількості використаних масел і використаних гідравлічних рідин. Ці відходи становитимуть більшу частину небезпечних відходів, які виробляються на місці.

Підрядники повинні мати можливість переробки, наприклад виробництва низькоякісного дизельного палива або використання як альтернативного палива. Підрядники також зобов'язані підготувати та впровадити план ліквідації розливів, включаючи управління місцями зберігання та обладнанням, пов'язаним із контролем розливів (Кумарі та Сінгх, 2018).

Забруднення з робочих таборів

Робочі табори повинні бути обладнані санітарною системою для збору та очищення всіх сірих і чорних вод, що утворюються в таборах, перед викидом у навколишнє середовище. Будівельні майданчики будуть обладнані достатньою кількістю туалетів, щоб контролювати скидання забруднень у річкові потоки.

Під час будівництва необхідно проводити регулярний контроль фекальних коліформ, щоб забезпечити ефективність очищення стічних вод перед скиданням (Adams et al., 2008).

Забруднення твердими відходами

Основні підрядні компанії повинні розробити план заходів щодо поводження з ТПВ. Цей план має охоплювати (1) поводження з побутовими

відходами з таборів, (2) поводження з безпечними будівельними відходами та (3) поводження з небезпечними твердими відходами (Robles, 2010).

Необхідні заходи для очищення забрудненої води (такі як очисні споруди або забезпечення дотримання промислових норм) можуть знадобитися для покращення якості води у водоймах. Вибіркові ліси в межах території водосховища повинні бути видалені та знищені перед заповненням, щоб уникнути гниття зануреної біомаси, що спричиняє погіршення якості води.

Вплив на водну екологію

Закриття річок дамбами глибоко змінює місцеву водну екологію, яка переміщується з річкового середовища існування в озерне. Постійні повені затоплюють навколишні водно-болотні угіддя, ліси та інші середовища проживання в річці, і це призводить до подальшого порушення екосистеми, яке відбувається вздовж берегів річки та естуарію, оскільки території, що оточують береги річки характеризуються найбагатшим біорізноманіттям (Ward et al., 1998).

Дамби пригнічують відкладення, які могли б природним чином відновити екосистеми нижче за течією, і через це деякі ендемічні види можуть або не можуть пережити зміни навколишнього середовища. Нові види, ймовірно, будуть залежати від адаптивних середовищ існування.

Однак дамби змінили і зробили основну екосистему.

Він адаптується до цих змін, і з будівництва дамб і водосховищ стає зрозуміло, що вони зменшують різноманітність дикої природи, на краще чи на гірше, а також призводять до втрати місць існування для багатьох організмів.

На базі аналізу наданих даних було зроблено висновок, що найважливішим впливом дамб є вплив на якість води та повітря, оскільки вони є основними елементами, які безпосередньо впливають на людей, тварин і рослини. Ефективність на якість води через надмірне виділення осаду, забруднення небезпечними матеріалами; побутові стічні води та ТПВ. Тоді як

найбільш небезпечним впливом на якість повітря є викид парникових газів (вуглекислого газу, метану).

ЗАГАЛЬНІ ВИСНОВКИ

Аналіз виділеного тексту свідчить про високий рівень систематизації та комплексного підходу до питань безпеки, охорони праці, екології та управління ризиками у сфері критичної інфраструктури та промислових об'єктів. Основна увага приділяється розробці та впровадженню системних підходів, що базуються на міжнародних стандартах, таких як ISO 31000, ISO/IEC 27005, а також нормативно-правових актах України, що регламентують безпеку та захист об'єктів критичної інфраструктури.

Ключові аспекти системного підходу

- Врахування життєвого циклу об'єктів – від етапів планування та проєктування до експлуатації та модернізації, що дозволяє виявляти та мінімізувати проєктні загрози ще на ранніх стадіях.
- Використання класифікаційних таксономій для систематизації проєктних загроз за джерелами виникнення, характером впливу та етапами життєвого циклу, що сприяє більш точному управлінню ризиками.
- Застосування сучасних інструментів і методів, таких як CARVER, ASD, сценарний аналіз, що дозволяє не лише ідентифікувати потенційні загрози, а й моделювати сценарії їх реалізації та оцінювати рівень ризиків.

Міжнародний та національний досвід

Міжнародний досвід, зокрема стандарти ISO, директиви NIS2, рекомендації ENISA та CISA, демонструє тенденцію до інтеграції управління ризиками у всі етапи життєвого циклу об'єктів, з особливим акцентом на превентивних заходах та системній ідентифікації загроз. Українська практика, хоча і базується на законодавчих нормах, потребує подальшого розвитку для гармонізації з міжнародними стандартами, зокрема щодо формалізації процедур ідентифікації та оцінки проєктних загроз.

Важливим є те, що в Україні зростає увага до гібридних загроз, що поєднують кібернетичні та фізичні елементи, а також до управління

ланцюгами постачання та людським фактором. Це відповідає глобальним тенденціям і підкреслює необхідність системного підходу, що враховує всі можливі джерела та сценарії загроз.

Практичне значення та рекомендації

Результати аналізу мають важливе практичне значення для операторів критичної інфраструктури, органів державної влади та інших зацікавлених сторін. Вони дозволяють розробляти та впроваджувати системи управління проєктними загрозами, що базуються на міжнародних стандартах і адаптовані до національних умов. Це сприятиме підвищенню рівня безпеки, стійкості та надійності об'єктів, а також зменшенню потенційних збитків у разі реалізації загроз.

Рекомендується посилити нормативно-правову базу щодо формалізації процедур ідентифікації та оцінки проєктних загроз, а також розробити єдину методику їх аналізу. Важливо також активізувати міжвідомчу та публічно-приватну взаємодію, що дозволить більш ефективно реагувати на сучасні виклики та загрози.

Загалом, робота підтверджує необхідність системного, ризик-орієнтованого підходу до управління безпекою об'єктів критичної інфраструктури. Впровадження міжнародних стандартів, формалізація процедур і підвищення рівня міжвідомчої координації є ключовими факторами підвищення рівня безпеки та стійкості. Це дозволить не лише ефективніше протидіяти сучасним кібер- та фізичним загрозам, а й створити передумови для розвитку національної системи безпеки у відповідності до світових тенденцій.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Asters розробила положення законопроєкту, які допоможуть посилити кіберзахист державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури в Україні. Site. URL: https://eba.com.ua/asters-rozrobyla-polozhennya-zakonoproyektu-yaki-dopomozhut-posylyty-kiberzahyst-derzhavnyh-informatsijnyh-resursiv-ta-ob-yektiv-krytychnoyi-informatsijnoyi-infrastruktury-v-ukrayini/

2. Анісімова О. М., Вітка Н. Є. Управління ризиками зовнішньоекономічної діяльності високотехнологічного підприємства : монографія. Донецьк : Ноулідж (донецьке відділення), 2011. 175 с.

3. Блага Н.В., Гобела В.В. Удосконалення комунікаційних процесів на підприємстві у контексті зміцнення інформаційної безпеки. Соціально-правові студії: науково-аналітичний журнал. Гол.ред. О.Балинська. Львів: ЛьвДУВС. 2021. Вип. 3(13). С 156-162. 15

4. Варналій З., Бондаренко С. Фінансова безпека підприємств України в умовах війни та повоєнного відновлення // Економ. вісник університету. 2023. Випуск № 56. С. 106-113. https:// doi.org/10.31470/2306-546X-2023-56-106-113.

5. Варналій З.С. Економічна безпекологія в умовах глобалізаційних викликів і загроз // Економічна безпека: держава, регіон, підприємство: 19 Матеріали VI Всеукраїнської науково-практичної Інтернет-конференції з міжнародною участю, 21 грудня 2020 р. – 21 січня 2021 р. Полтава: НУПП, 2021. С. 34-39.

6. Гобела В. В. Економіко-безпекова екологізація: теорія і практика : монографія. Львів: ЛьвДУВС, 2021. 244 с. http://dspace.lvduvs.edu.ua/handle/1234567890/3757

7. Гобела В. В. Управління зовнішньоекономічною діяльністю & Management of Foreign Economic Activity : навчальний посібник. Львів : ЛДУВС, 2021. 244 с. http://dspace.lvduvs.edu.ua/handle/1234567890/3732

8. Грибіненко О. М. Сутність та шляхи забезпечення економічної безпеки підприємства. Науковий вісник Херсонського державного 26 університету. 2017. Вип. 1. С.98-100. URL:https://ep.nmu.org.ua/ua/kaf/gribinenko.php?print=Y.

9. Гук О. В. Стратегічне управління економічною безпекою як спосіб запобігання падіння економічної безпеки у підприємства / О. В. Гук // Економіка: реалії часу. 2015. № 6 (22). С. 193–198. URL : https://economics.opu.ua/files/archive/2015/No6/193.pdf

10. Діденко Є. О. Управління економічною безпекою підприємства на основі формування стратегії його безпечного розвитку. Формування ринкових відносин в Україні. 2015. № 5 (168) С. 35–40.

11. Кабінет Міністрів України. Постанова від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» {Із змінами, внесеними згідно з Постановою КМ № 991 від 02.09.2022}. Site. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

12. Кизим М. О., Хаустова В. Є., Трушкіна Н. В. Сутність поняття «критична інфраструктура» з позицій національної безпеки України. Бізнес Інформ. 2022. № 12. С. 58-78. https://doi.org/10.32983/2222-4459-2022-12-58-78.

13. Кібератаки на українські державні сайти. Site. URL: https://uk.wikipedia.org/wiki/Кібератаки_на_українські_державні_сайти_(2022)

14. Колесник І. Релокація бізнесу в умовах війни: варіанти та покрокова інструкція. URL: https://www.prostir.ua/?news=relokatsiya-biznesu-v-umovahvijny-varianty-ta-pokrokova-instruktsiya

15. Коляденко І. І. Наукові підходи до сутності стратегічного управління економічною безпекою. Бізнес-навігатор. 2018. № 2-2 (45). С. 7–10.

16. Ляшенко О. М. Управління економічною безпекою підприємств в умовах гібридної війни. URL: https://cyberleninka.ru/article/n/upravlinnyaekonomichnoyubezpekoyu pidpriemstv-v-umovah-gibridnoyi-viyni

17. Михайлов Д. За рік війни інфраструктурі України завдано збитків майже на $144 млрд – KSE. URL: https://suspilne.media/422019-za-rik-vijniinfrastrukturi-ukraini-zavdano-zbitkiv-majze-na-144-mlrd-kse.

18. Наказ Адміністрації Держспецзв'язку від 06 жовтня 2021 року № 601 Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Site. URL: https://dut.edu.ua/ua/news-1-569-9870-metodichni--rekomendacii--schodo--pidvischennya--rivnya-kiberzahistu-kritichnoi-informaciynoi-infrastrukturi_kafedra-cistem-tehnichnogo-zahistu-informacii.

19. Національний банк України - "Безпека у кіберпросторі": веб-сайт URL:https://bank.gov.ua/control/uk/publish/article?art_id=81635567&cat_id=81634361

20. Піцур Я. С., Гобела В. В. Теоретико-методологічний аналіз процесу формування оптимальної системи управління економічною безпекою суб'єктів господарювання. Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна. 2018. Випуск 1. С. 227-335. http://dspace.lvduvs.edu.ua/handle/1234567890/996

21. Піцур Я. С., Гобела В. В. Теоретико-методологічний аналіз процесу формування оптимальної системи управління економічною безпекою суб'єктів господарювання. Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна. 2018. Випуск 1. С. 227-335. http://dspace.lvduvs.edu.ua/handle/1234567890/996

22. Постанова Правління Національного банку України від 12 серпня 2022 року № 178 «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».

Національний банк України. 12 серп. 2022. Site. URL: https://bank.gov.ua/ua/legislation/Resolution_12082022_178.

23. Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури. Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України. 15.01.2021 № 23. Site. URL: https://zakon.rada.gov.ua/rada/show/v0023519-21#Text.

24. Про затвердження Порядку проведення огляду стану кіберзахисту інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. Постанова Кабінету Міністрів України від 11 листопада 2020 р. № 1176. Site. URL: https://ips.ligazakon.net/document/KP201176?an=1.

25. Рогов П. Д. Шляхи забезпечення кібернетичної безпеки об’єктів критичної інформаційної інфраструктури держави у воєнній сфері / П. Д. Рогов, Б. О. Ворович, В. А. Ткаченко // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2017. № 1. С. 64-72. URL: http://nbuv.gov.ua/UJRN/Znpcvsd_2017_1_13

26. Розроблені вимоги до функціонування системи кіберзахисту в банківській системі України. Національний банк України. 19 серп. 2022. Site. URL: https://bank.gov.ua/ua/news/all/rozrobleni-vimogi-do-funktsionuvannya-sistemi-kiberzahistu-v-bankivskiy-sistemi-ukrayini.

27. Сініцин І. П., Ігнатенко П. П., Слабоспицька О. О., Артеменко О. В.. Комплексний підхід до побудови системи кіберзахисту критичної інформаційної інфраструктури держави. Проблеми програмування. 2017. № 3. С. 128-148. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/144499/08-Sinitsyn.pdf?sequence=1.

28. Статистика кібератак на українську критичну інфраструктуру. Site/ URL: https://www.cip.gov.ua/ua/news/statistika-kiberatak-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-15-22-bereznya

29. Субач, І. Архітектура та функціональна модель перспективної проактивної інтелектуальної SIEM-системи для кіберзахисту об'єктів критичної інфраструктури / Ігор Субач, Артем Микитюк, Володимир Кубрак // Information Technology and Security. 2019. Vol. 7, Iss. 2 (13). Pp. 208–215.

30. Ткачук Н.А. Організаційно-правові засади формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. Інформація і право. № 1(24)/2018. С. 133-138. URL: http://ippi.org.ua/sites/default/files/16_4.pdf

31. Франчук В. І. Економічна безпека суб'єктів господарської діяльності : підручник. Львів : ЛьвДУВС, 2015. 236 с.

32. Штангрет А. М. Основи економічної безпеки підприємств : навчальний посібник. Львів : УАД. 2013. 284 с.

33. Bezpartochnyi M., Trushkina N., Birca I. Critical infrastructure development management mechanism: theoretical aspects. Current issues of the management of socio-economic systems in terms of globalization challenges: scientific monograph. Košice: Vysoká škola bezpečnostného manažérstva v Košiciach, 2023. P. 612-628. https://doi.org/10.5281/zenodo.7799542.

34. Chen, Y.-C., & Chang, I.-C. (2019). The Impact of Information Security Management on Organizational Performance: An Empirical Study. Journal of Business Research, 98, 365-377.

35. Cybersecurity Act 2018 operative from 31 August 2018 to protect critical information infrastructure against cybersecurity threats. Site. URL: https://www.allenandgledhill.com/media/2996/ag-cybersecurity-act-2018-operative-from-31-august-2018-to-protect-critical-information-infrastructure.pdf.

36. Cybersecurity and Critical Infrastructure. Homeland Security. Site. URL: https://www.dhs.gov/archive/coronavirus/cybersecurity-and-critical-infrastructure

37. David Biello,Is High-Tech Security at Public Events Counterproductive? [Електронний ресурс]. – Режим доступу: https://www.scientificamerican.com/article/how-to-better-protect-public-events/

38. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high overall level of security for network and information systems within the Union territory. Site. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

39. Hnylytska L., Franchuk V., Melnyk S., Nakonechna N., Leskiv H., & Hobela V. (2022). Security-oriented model of business risk assessment. Financial and Credit Activity Problems of Theory and Practice, 4(45), 202–210. http://dspace.lvduvs.edu.ua/handle/1234567890/4938

40. Jorgensen, R. (2019). Cyber Security and the Protection of Consumer Rights: The Role of Governments. Journal of Consumer Policy, 42(4), 635-650.

41. Khaustova V., Tirlea M. R., Dandara L., Trushkina N., Birca I. Development of Critical Infrastructure from the Point of View of Information Security. UNIVERS STRATEGIC – Revistă de Studii Strategice Interdisciplinare și de Securitate. 2023. Anul XIV. Nr. 1(53). P. 170-188.

42. Leck, A., Chia, K. Singapore: New initiatives to ensure digital security and enhanced cyber resilience. Global Compliance News. March 26, 2022. Site. URL: https://www.globalcompliancenews.com/2022/03/26/singapore-new-initiatives-to-ensure-digital-security-and-enhanced-cyber-resilience-17032022/

43. Lee, M., & Kuo, Y. (2018). The role of information sharing in enhancing supply chain resilience and performance. International Journal of Production Economics, 201, 221-233.

44. Li, S., Wang, K., & Liu, H. (2019). Trust and distrust in e-commerce platforms: An investigation of the role of customer reviews and ratings. Decision Support Systems, 119, 1-9.

45. MCI response to PQ on Steps to Protect Singapore's Critical Infrastructure from Malware Threat. Parliament Sitting on 4 July 2022. Site. URL: https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2022/7/mci-

response-to-pq-on-steps-to-protect-singapore-critical-infrastructure-from-malware-threat

46. Security of Critical Infrastructure Act 2018, №. 29, 2018. Ausrtalia, Compilation No. 4. Compilation date: 2 April 2022. Includes amendments up to: Act №. 33, 2022. Registered: 2 May 2022. Site.URL:https://www.legislation.gov.au/Details/C2022C00160

47. Terry L. Schell, Brian G. Chow, and Clifford Grammich, Designing Airports for Security: An Analysis of Proposed Changes at LAX. Public Safety and Justice. RAND Co.https://www.rand.org/pubs/issue_papers/IP251.html

48. The Critical Infrastructure Information Act of November 25, 2002. Homeland Security. Site.URL: https://www.dhs.gov/publication/critical-infrastructure-information-act#:~:text=The%20Critical%20Infrastructure%20Information%20Act,reducing%20the%20nation's%20vulnerability%20to