МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ХАРЧОВИХ ТЕХНОЛОГІЙ

Інститут (факультет) Автоматизації і комп'ютерних систем
Кафедра Інформаційних систем

«До захисту в ЕК»	**«До захисту допущено»**
Директор інституту(декан факультету)	Завідувач кафедри
_____ Андрій Форсюк	_____ Сергій Чумаченко
(підпис) (ім'я та прізвище)	(підпис) (ім'я та прізвище)
«___» _____ 2022р.	«___» _____ 2022р.

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА

зі спеціальності 122 «Комп'ютерні науки»
(код та назва спеціальності)
освітньо-професійної програми «Інформаційні управляючі системи та технології»
на тему: «Інформаційно-аналітична система оцінки ризиків і загроз для об'єктів критичної інфраструктури на Сході України»

Виконав: здобувач 2 курсу, групи ІС-2-3М

Сорока Роман Сергійович _____
(прізвище, ім'я, по батькові повністю) (підпис)

Керівник Чумаченко Сергій Миколайович _____
(прізвище , ім'я та по батькові повністю) (підпис)

Консультанти Сергій Чумаченко _____
(ім'я та прізвище) (підпис)

_____ _____
(ім'я та прізвище) (підпис)

_____ _____
(ім'я та прізвище) (підпис)

Рецензент Ярослав Смітюх _____
(ім'я та прізвище) (підпис)

Я як здобувач(ка) Національного університету харчових технологій розумію і підтримую політику університету з академічної доброчесності. Я не надавав(-ла) і не одержував(-ла) недозволеної допомоги під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Здобувач_____
(підпис)

Київ – 2022 р.

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ХАРЧОВИХ ТЕХНОЛОГІЙ

Інститут (факультет) __Автоматизації і комп'ютерних систем_____
Кафедра __Інформаційних систем_____
Освітній ступінь__магістр_____
Спеціальність__122 «Комп'ютерні науки»_____
(код і назва)
Освітньо-професійна програма *«Інформаційні управляючі системи та технології»* _____
(назва)

ЗАТВЕРДЖУЮ

Завідувач
кафедри Інформаційних систем

_____Чумаченко С.М.
"____" _____2022року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧА
_____Сороки Романа Сергійовича_____
(прізвище, ім'я, по батькові)

1. Тема роботи «Інформаційно-аналітична система оцінки ризиків і загроз для об'єктів критичної інфраструктури на Сході України»
_____
керівник роботи___Чумаченко Сергій Миколайович д.т.н., с.н.с._____
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від "11"листопада 2021 року №884-кс
2. Строк подання здобувачем роботи 08 лютого 2022_____
3. Вихідні дані до роботи
Критична інфраструктура на Сході України, чинники промислового та військового техногенезу, інформація про розташування об'єктів критичної інфраструктури відносно лінії розмежування, можливі зони ураження, прилеглі населені пункти, що можуть бути уражені внаслідок аварій на потенційно-небезпечних об'єктах критичної інфраструктури_____
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Розділ 1. Системний аналіз стану предметної галузі. Розділ 2. Постановка наукового завдання на розробку інформаційно-аналітичної системи. Розділ 3. Інформаційно-аналітична система оцінювання воєнно-техногенних загроз і ризиків для об'єктів критичної інфраструктури на Сході України. Висновки та пропозиції. Список використаної літератури та інтернет-ресурсів. Додатки
5. Перелік графічного матеріалу
Презентація доповіді кваліфікаційної роботи, скріншоти роботи інформаційно-аналітичної системи, результати розрахунків оцінок загроз і ризиків для об'єктів критичної інфраструктури

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Вступ. Розділ 1	Чумаченко С.М., старший науковий співробітник	11.11.21р.	30.11.21
Розділ 2	Чумаченко С.М., старший науковий співробітник	11.11.21р.	24.12.21
Розділ 3	Чумаченко С.М., старший науковий співробітник	11.11.21р.	24.01.22

7. Дата видачі завдання 11 листопада 2021 року

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Приміпка
	Вступ Розділ 1 Системний аналіз стану предметної галузі	11.11.21-30.11.21	Виконано
	Розділ 2 Постановка наукового завдання на розробку інформаційно-аналітичної системи	01.12.21-24.12.21	Виконано
	Розділ 3. Інформаційно-аналітична система оцінювання воєнно-техногенних загроз і ризиків для об'єктів критичної інфраструктури на Сході України	25.12. 21-24.01.22	Виконано
	Висновки та пропозиції Список використаної літератури та інтернет-ресурсів.	25.01.22-01.02.22	Виконано
	Подання кваліфікаційної роботи на кафедру	02.02.2022	Виконано

Здобувач _____ Сорока Р.С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Чумаченко С.М.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Метою кваліфікаційної роботи на здобуття ступеня «Магістр» є підвищення рівня техногенної безпеки на об’єктах критичної інфраструктури в районах, наближених до лінії розмежування, за рахунок розробки інформаційно-аналітичної системи оцінювання ризиків і загроз для об’єктів критичної інфраструктури.

Об’єктом дослідження є процес оцінювання ризиків і загроз для об’єктів критичної інфраструктури в районах, прилеглих до лінії розмежування.

Предметом дослідження є інформаційно-аналітична система оцінювання ризиків і загроз для об’єктів критичної інфраструктури в районах прилеглих до лінії розмежування.

Наукова новизна кваліфікаційної роботи: вперше розроблено інформаційно-аналітичну систему оцінювання ризиків і загроз для об’єктів критичної інфраструктури в районах, прилеглих до лінії розмежування, з використанням методу аналізу ієрархій і аналітичних мереж, яка забезпечує розробку класифікації потенційно небезпечних об’єктів критичної інфраструктури за сукупністю небезпечних чинників воєнного і промислового техногенезу;

набула подальшого розвитку інформаційно-логічна модель експертного оцінювання загроз від впливу чинників воєнного і промислового техногенезу на техногенну безпеку об’єктів критичної інфраструктури на Сході України на основі модифікації методу багатокритеріальної оцінки загроз із згорткою їх до узагальненого індексу загрози для потенційно-небезпечних об’єктів критичної інфраструктури, яка відрізняється від існуючої тим, що враховує додаткові критерії, чинники та показники оцінки, а саме – дозволяє з більшою достовірністю оцінити рівень техногенної загрози виникнення надзвичайних ситуацій.

КЛЮЧОВІ СЛОВА: критична інфраструктура, оцінювання загроз і ризиків, модель, метод аналізу ієрархій, метод аналітичних мереж.

ABSTRACT

The purpose of the qualification work for the degree of Master is to increase the level of man-made safety at critical infrastructure in areas close to the line of demarcation, by developing an information and analytical system for assessing risks and threats to critical infrastructure.

The object of the research is the process of risk and threat assessment for critical infrastructure objects in the areas adjacent to the demarcation line.

The subject of the research is an information-analytical system of risk and threat assessment for critical infrastructure objects in the areas adjacent to the demarcation line.

Scientific novelty of the qualification work: for the first time an information-analytical system of risk and threat assessment for critical infrastructure objects in the areas adjacent to the demarcation line was developed, using the method of analysis of hierarchies and analytical networks. a set of dangerous factors of military and industrial technogenesis;

the information-logical model of expert assessment of threats from the impact of military and industrial technogenesis on man-caused safety of critical infrastructure in eastern Ukraine on the basis of modification of the method of multicriteria threat assessment with their reduction to a generalized threat index for potentially dangerous critical infrastructure that differs from the existing one in that it takes into account additional criteria, factors and indicators of assessment, namely - allows you to more accurately assess the level of man-made threat of emergencies.

KEYWORDS: critical infrastructure, threat and risk assessment, model, method of hierarchy analysis, method of analytical networks

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Системний аналіз воєнних та техногенних загроз для критичної інфраструктури (КІ) свідчить про стрімке зростання всього спектру небезпек для людини, суспільства та держави в районах ведення бойових дій на території проведення операції об’єднаних сил (ООС). Відповіддю з боку держави повинен бути такий же стрімкий ріст потенціалу самозахисту та управління воєнно-техногенними загрозами і ризиками в районах ведення бойових дій на Сході України.

Вирішення питань забезпечення техногенної безпеки об’єктів критичної інфраструктури (ОКІ), зокрема управління воєнно-техногенними загрозами та ризиками, обумовлено необхідністю наукового підходу до розбудови системи техногенної безпеки. Широкий спектр техногенних проблем, що виникають в сучасних умовах існування, розвитку та взаємодії природного, техногенного та соціального середовища, вказує на необхідність розробки ефективних заходів для своєчасного виявлення та попередження небезпек різного походження.

Перспективним напрямом розробки таких попереджувальних заходів є створення ефективної інформаційно-аналітичної системи оцінки ризиків і загроз для об'єктів критичної інфраструктури на Сході України з метою розробки та реалізації ефективних антикризових рішень щодо попередження надзвичайних ситуацій (НС) техногенного характеру на об’єктах критичної інфраструктури (ОКІ) в районах ведення бойових дій (БД).

За сучасних умов на тлі загострення обстановки в східних регіонах України відбувається зростання загроз екологічній і техногенній безпеці держави, у т. ч. внаслідок порушення технологічного режиму функціонування численних ОКІ. Наявний на Сході України комплекс гірничодобувних, хімічних, енергетичних об’єктів із значною кількістю промислово-міських агломерацій та високою щільністю населення зумовлює істотне зростання ризиків виникнення техногенних аварій і катастроф з масштабними негативними наслідками через загрозу руйнування потенційно небезпечних об’єктів (ПНО) у місцях їх дислокації, у т.ч.

внаслідок воєнних дій. Серед ОКІ особливу загрозу становлять просторово розподілені залізничні колії, нафто- та газопроводи, мости, ПНО, магістральні електромережі, водоканали та водоводи, безпечна експлуатація яких має першочергове значення для безпеки життєдіяльності населення та соціально-економічного розвитку України.

На сьогоднішній день експерти серед ОКІ особливу важливість надають об’єктам водопостачання, енергопостачання, газотранспортної системи та теплоенергетики. Саме вони породжують найбільш катастрофічні каскадні ефекти у випадку виникнення на них НС природного чи техногенного характеру.

Відсутність на сьогоднішній день науково обґрунтованих інформаційно-аналітичних методів і показників моніторингу ОКІ в зоні проведення ООС, які є головною ланкою забезпечення безпеки життєдіяльності населення та збройних формувань, суттєво стримують виконання законодавчих та нормативних актів в галузі техногенної безпеки та цивільного захисту держави.

Аналіз публікацій вітчизняних і зарубіжних авторів підтвердив, що проблематика розробки програмно-апаратних засобів для інформаційно-аналітичної системи оцінки ризиків і загроз для об'єктів критичної інфраструктури на Сході України на сьогоднішній день є актуальною через наступні причини:

- відсутність цілісної системи показників і критеріїв для оцінки та прогнозування впливу воєнно-техногенних загроз на техногенну безпеку ОКІ в районах ведення бойових дій (БД);
- неможливістю повноцінного використання існуючих методів моніторингу НС без їх адаптації до умов реального застосування систем зброї і військової техніки на цих територіях та врахування їх уражаючого впливу на ОКІ;
- реальним застосуванням різноманітних систем зброї і військової техніки, які відрізняються високою енерго-ресурсоємністю і тому є головними чинниками впливу на ОКІ;
- наявністю потенційних загроз від джерел техногенної небезпеки воєнного походження та реальних постійно і періодично діючих джерел воєнно-

техногенного навантаження в районах ведення бойових дій на ОКІ, які внаслідок комплексності і високої концентрації суттєво відрізняються за природою впливу від звичайних джерел антропогенного навантаження;

- відсутністю на сьогоднішній день у Збройних Силах України дієвих та ефективних засобів моніторингу ОКІ в районах ведення БД;
- сформованим у наш час розумінням тієї обставини, що в системі національної безпеки України цивільний захист є винятково важливим і ключовим компонентом.

Тому, виникає необхідність створення інформаційно-аналітичної системи оцінки ризиків і загроз для об'єктів критичної інфраструктури на Сході України в цих регіонах держави в районах ведення БД.

Таким чином, проблематика розробки інформаційно-аналітичних методів попередження НС на ОКІ на території районів ведення бойових дій розкрита лише частково і потребує подальшого удосконалення.

На сьогодні існує протиріччя: з одного боку необхідно забезпечити стабільність і розвиток техногенної безпеки ОКІ районів ведення бойових дій, а з іншого боку - немає відповідних методів, засобів і показників для адекватної оцінки та прогнозування загроз і ризиків виникнення НС на ОКІ.

Метою дослідження є підвищення рівня техногенної безпеки на об’єктах критичної інфраструктури в районах, наближених до лінії розмежування, за рахунок розробки інформаційно-аналітичної системи оцінювання ризиків і загроз для об’єктів критичної інфраструктури.

Основні задачі дослідження:

1. Проаналізувати наслідки впливу чинників промислового і воєнного техногенезу для критичної інфраструктури, природного середовища і соціуму.
2. Провести постановку задачі оцінювання оцінювання ризиків і загроз на об’єктах критичної інфраструктури в районах, наближених до лінії розмежування.
3. Розробити інформаційно-аналітичну систему для оцінювання ризиків і загроз на об’єктах критичної інфраструктури в районах, наближених до лінії розмежування, з використанням аналізу ієрархій і аналітичних мереж.

4. Запропонувати можливі варіанти впровадження розробленого методу.

Межі дослідження – при виборі початкових даних в основу дослідження закладається сучасний стан системи техногенної безпеки ОКІ, геополітична обстановка у світі та тенденції їх розвитку до 2030 року.

Дослідження проводиться на основі існуючої законодавчої бази щодо національної безпеки та оборони України.

Об'єкт дослідження – процес оцінювання ризиків і загроз для об'єктів критичної інфраструктури в районах, прилеглих до лінії розмежування.

Предмет дослідження – інформаційно-аналітична система оцінювання ризиків і загроз для об'єктів критичної інфраструктури в районах прилеглих до лінії розмежування.

Методологія дослідження базується на принципах системного підходу з використанням теорії прийняття рішень в умовах апріорної невизначеності.

Методи дослідження. Під час дослідження застосовувалися методи системного аналізу, математичної статистики, аналізу ієрархій, аналітичних мереж, стратифікації, причинно-наслідкових діаграм, багатокритеріальних оцінок та комп'ютерного моделювання для вирішення часткових завдань. Експериментальні дослідження адекватності запропонованого методу і показників здійснювались шляхом проведення експериментів і досліджень та обчислювального експерименту, шляхом комп'ютерного моделювання.

Наукова новизна отриманих результатів полягає в тому, що:

уперше розроблено:

- розроблено інформаційно-аналітичну систему оцінювання ризиків і загроз для об'єктів критичної інфраструктури в районах, прилеглих до лінії розмежування, з використанням методу аналізу ієрархій і аналітичних мереж, яка забезпечує розробку класифікації потенційно небезпечних об'єктів критичної інфраструктури за сукупністю небезпечних чинників воєнного і промислового техногенезу;

набула подальшого розвитку:

- інформаційно-логічна модель експертного оцінювання загроз від впливу чинників

воєнного і промислового техногенезу на техногенну безпеку об’єктів критичної інфраструктури на Сході України на основі модифікації методу багатокритеріальної оцінки загроз із згорткою їх до узагальненого індексу загрози для потенційно-небезпечних об’єктів критичної інфраструктури, яка відрізняється від існуючої тим, що враховує додаткові критерії, чинники та показники оцінки, а саме – дозволяє з більшою достовірністю оцінити рівень техногенної загрози виникнення надзвичайних ситуацій.

Практичне значення отриманих результатів полягає в розробленні рекомендацій щодо практичного впровадження інформаційно-аналітичної системи оцінки ризиків і загроз для об'єктів критичної інфраструктури на Сході України.

Результати дослідження забезпечують розробку класифікації потенційно небезпечних об’єктів критичної інфраструктури за сукупністю небезпечних чинників промислового та воєнного техногенезу, що дозволяє з більшою достовірністю оцінити рівні загроз виникнення надзвичайних ситуацій на об’єктах критичної інфраструктури і розробити сукупність можливих сценаріїв розвитку надзвичайних ситуацій та рекомендації щодо їх попередження.

РОЗДІЛ 1 СИСТЕМНИЙ АНАЛІЗ СТАНУ ПРЕДМЕТНОЇ ГАЛУЗІ

1.1 Поняття критичної інфраструктури в розвинутих країнах світу

Відповідно до "Закону про патріотизм" (USA Patriot Act), прийнятим конгресом 26 жовтня 2001 року, критична інфраструктура визначається як "сукупність фізичних або віртуальних систем і засобів, важливих для США такою мірою, що їх вихід з ладу або знищення можуть призвести до згубних наслідків в області оборони, економіки, охорони здоров'я та безпеки нації " [1].

Поняття критичної інфраструктури охоплює такі ключові галузі народного господарства і економіки США як національна оборона, сільське господарство (2 мільйони ферм), виробництво харчових продуктів (87 тисяч заводів), цивільна авіація (5000 аеропортів), морський транспорт (300 портів), автомобільні дороги і мости (590000), тунелі (400), дамби (80000), трубопроводи (2 мільйони миль), водопостачання (3400 резервуарів), охорона здоров'я (5800 госпіталів), служби екстреної допомоги (87 тисяч бригад), органи державного управління (3000 об'єктів), військове виробництво (250 тисяч фірм), інформаційні та телекомунікаційні системи і мережі (2 мільярди миль кабелів), енергетика (2800 електростанцій), атомні електростанції (104), транспорт, банківська і фінансова системи (26600 відділень), хімічна промисловість (66 000 заводів), поштова служба (137 мільйонів скриньок для листів), висотні будинки (460), національні та історичні пам'ятки (5800). 85% об'єктів критичної інфраструктури США належить приватним підприємцям.

Кульмінацією законотворчої діяльності Конгресу в галузі внутрішньої безпеки країни стало прийняття 25 листопада 2002 року довгоочікуваного для американців "Закону про внутрішню безпеку" (Home Security Act) і створення спеціального комітету (House Homeland Security Committee), що здійснює постійний нагляд за його виконанням. У відповідності з цим законом з метою забезпечення безпеки громадян перед обличчям загроз з боку міжнародного тероризму створено Міністерство внутрішньої безпеки (Department of Homeland Security), на яке покладаються функції по запобігання терористичним актам, зниженню вразливості інфраструктури, ліквідації наслідків терористичних актів, а

також координації дій інших міністерств і відомств по ліквідації наслідків техногенних, антропогенних і природних катастроф на території США [2].

Враховуючи постійно зростаючі масштаби поширення і практичного використання інформаційних технологій в США, особливо в сфері державного і військового управління, і тієї ролі, яка відводиться інформаційним технологіям у вирішенні кризових ситуацій, DARPA проводить науково-дослідницька розробки з метою забезпечення інформаційної безпеки та дієвості відповідних систем і мереж критичної інфраструктури в надзвичайних умовах.

Становлення нормативно-правової бази в сфері захисту критичної інфраструктури є тривалим процесом. Напевно найбільших успіхів в даній сфері досягли США. Адміністративний наказ Президента США № 13010 «Про роботу з дослідження вразливості захисту критичної інфраструктури від кібернетичних та фізичних загроз» (липень 1996 р.), а згодом Директива Президента США № 63 започаткували в США національну програму «Захист критичної інфраструктури» травень 1998 р. Продовження роботи з підсилення захисту критичної інформаційної інфраструктури відобразилося в Національному плані з захисту інформаційних систем (січень 2000 р.). Але переломним моментом у становленні концепції захисту критичної інфраструктури стала необхідність реагувати на терористичні акти, вчинені 11 вересня 2001 р. у Нью-Йорку. Після цієї екстраординарної події уряд США кардинально переглянув підходи щодо забезпечення внутрішньої безпеки держави (як в технічному, так і в організаційному плані). Важливим висновком з трагедії стало прийняття нормативно-правового документу, абревіатура назви якого перекладається як «Акт про патріотизм» (*USA PATRIOT ACT*), в ньому термін критична інфраструктура набув свого сучасного вигляду [3].

У США керівні документи з організації захисту та реагування на загрози критичній інфраструктурі постійно вдосконалюються, відповідні плани реагування та евакуації населення при надзвичайних ситуаціях періодично переглядаються. Відбувається оновлення технічних засобів попередження та реагування на надзвичайні ситуації, удосконалення способів та засобів інформування населення.

В директиві Президента США з національної безпеки № 7 (грудень 2003 р.)

визначено відповідальність Міністерства внутрішньої безпеки, інших міністерств та федеральних агентств, які є відповідальними за окремі сектори критичної інфраструктури. На Міністерство внутрішньої безпеки покладено обов'язок формувати Національний план захисту критичної інфраструктури. Аналізуючи національні плани захисту критичної інфраструктури США (останній розроблений у 2009 р. та попередній – 2006 р.), можна зробити висновки про те, що зміни та вдосконалення були здійснені на таких головних напрямах: планування регіонального захисту, вдосконалення загального підходу до управління ризиком, вдосконалення методики оцінок безпеки за секторами.

Усвідомлення зростання терористичних загроз в Європі призвело до того, що Європейська Комісія у листопаді 2005 р. випустила Зелену книгу щодо Європейської програми захисту критичної інфраструктури [4], а згодом, у 2006 р., коли завершився етап консультацій між членами ЄС, була запущена в дію Європейська програма захисту критичної інфраструктури. Особливості підходу ЄС, як об'єднання суверенних держав, у подальшому знайшли своє відображення у документі ЄК "Захист критичної енергетичної та транспортної інфраструктури Європи" (лютий 2007) [1] та у спеціальній директиві щодо визначення об'єктів критичної інфраструктури та оцінку потреб у підвищенні рівня їхнього захисту (грудень 2008) [5]. Захист критичної інфраструктури енергопостачання Декларацією Чиказького саміту (20 травня 2012 р.) було віднесено до числа пріоритетних напрямів забезпечення енергетичної безпеки для держав-членів НАТО та самого Альянсу.

На відміну від США, де було створено єдиний орган виконавчої влади (Міністерство внутрішньої безпеки), на який покладено функції координації захисту критичної інфраструктури США, в ЄС такого органу немає, а функції захисту критичної інфраструктури виконують відповідні органи окремих країн-членів ЄС.

В ЄС загальноєвропейський підхід до захисту критичної інфраструктури задекларовано в Директиві Європейської Комісії № 786 2006 р. До загальноєвропейської критичної інфраструктури відносять ті елементи національних критичних інфраструктур країн-членів ЄС, відмова, інцидент або

атака на які може мати значний вплив як на країну, в який ця подія відбудеться, так і хоча б на одну іншу країну-члена ЄС. Згадана директива започаткувала Європейську програму з захисту критичної інфраструктури, яка розроблена з метою підвищення рівня захищеності критичної інфраструктури шляхом створення спільного підходу до її захисту в країнах-членах ЄС і гармонізації національних законодавств в даній сфері. Слід відзначити, що провідні країни світу здійснюють захист своїх національних інтересів, не обмежуючись національними кордонами. Окрім національних критичних інфраструктур, розглядаються зарубіжні об'єкти, безпека яких має важливе значення для тієї чи іншої держави.

Об'єднання народних економік держав ЄС, їх взаємозалежність, але і необхідність протистояти сумісним або подібним загрозам, відбилися в ухваленні документа Critical Inrastructure protection in the fight against terrorism. У цьому документі критична інфраструктура визначена як фізичні засоби виробництва, інформаційні технології, мережі (транспортні, енергетичні і т. п.), служби і інші активи, розлад або руйнування яких мав би серйозні наслідки на здоров'я, охорону, надійність або життєвий рівень громадян або на штатне функціонування урядів в цих державах. За цією дефініцією в сектор критичної інфраструктури входять [6]:

- енергетичні об'єкти і мережі, наприклад, електричні розподільні мережі, газопроводи, нафтопроводи, сховища пального і т. ін.;

- комунікаційні і інформаційні технології (наприклад, телекомунікації, радіомовні і телевізійні передавачі і мережі, інтернет);

- фінансова система(банкова справа, капіталові ринки, інвестування);

- охорона здоров'я, особливо лікарні, поліклініки, установи постачання крові, лабораторії, сантехнічна рятувальна служби;

- харчова промисловість, сільське господарство, торгівля і постачання продовольством;

- вода, особливо греблі, гідроресурси;

- транспорт, особливо авіаційний, шосейний, залізничний, комбінований, комунікаційні вузли, а також системи управління транспортом;

- виробництво, зберігання і транспорт небезпечних товарів, особливо хімічних, біологічних, радіологічних ядерних матеріалів;

- державне управління, зокрема критичні служби і установи, інформаційні мережі, важливі економічні об’єкти, стратегічні об’єкти, а також культурні пам’ятники.

1.2 Поняття критичної інфраструктури в Україні та особливості впливу на неї воєнно-політичного конфлікту гібридного типу на Донбасі

Як і в інших країнах, в Україні існують такі системи, об'єкти та ресурси, знищення або пошкодження яких матиме суттєвий негативний вплив на громадян, суспільство і державні інституції. При цьому було б невірно стверджувати, що в нашій країні не приділяється увага їх захисту та безпеці. Навпаки, на сьогоднішній день діє ціла низка законодавчих і нормативних актів, що визначає повноваження та компетенцію державних органів у цій сфері, встановлює особливості забезпечення охорони та безпечного функціонування зазначених об’єктів і систем. Проте, в Україні й досі відсутній системний підхід на національному рівні до управління захистом та безпекою усього комплексу таких систем, об'єктів та ресурсів, які прийнято відносити до критичної інфраструктури. В результаті чого спостерігається домінування відомчих підходів, низький рівень взаємодії, координації дій та управління ресурсами, особливо, у випадку надзвичайних ситуацій державного рівня.

Термін «критична інфраструктура» неодноразово використовувався в нормативно-правових документах в Україні, проте його дефініція й досі відсутня в чинному законодавстві [7]. Вперше в офіційних документах термін «критична інфраструктура» з‘явився у 2006 р. у тексті Рекомендацій парламентських слухань з питання розвитку інформаційного суспільства. На жаль, у подальшому активна робота у цьому важливому напрямі припинилася.

В Стратегії національної безпеки «Україні у світі, що змінюється» в четвертому розділі «Стратегічні цілі та основні завдання політики національної безпеки» серед ключових завдань політики національної безпеки у внутрішній сфері одним із шляхів зміцнення енергетичної безпеки названий: «дієвий захист

критичної інфраструктури паливно-енергетичного комплексу від еколого-техногенних впливів та зловмисних дій», а одним із напрямів забезпечення інформаційної безпеки — «забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури» [8].

Відсутність чітко визначеного терміну «критична інфраструктура» в українському законодавстві, і як наслідок, відсутність переліку об’єктів, які слід віднести до неї, створюють перешкоду для ефективного виконання п.6 рішення Ради національної безпеки і оборони України від 1 березня 2014 року «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» (введеного в дію указом Президента України №189/2014 від 02.03.2014р.), на виконання якого Міністерству внутрішніх справ України наказується забезпечити «посилену охорону об’єктів енергетики та критичної інфраструктури».

На сьогоднішній день у Верховній Раді України знаходиться проект Закону України “Про критичну інфраструктуру та її захист” у якому визначено, що критична інфраструктура це сукупність об’єктів, які є стратегічно важливими для економіки і національної безпеки, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам.

Як вже відзначалося, українське законодавство щодо захисту об’єктів, які згідно зі світовою практикою відносять до критичної інфраструктури, є достатньо розгалуженим і включає численні нормативно-правові акти, які, проте, носять переважно внутрішньовідомчий характер.

Дійсно, чинне законодавство визначає такі категорії об’єктів, для яких встановлюються особливі умови забезпечення їх захисту та функціонування:

підприємства, які мають стратегічне значення для економіки та безпеки держави [9];

об’єкти, які включені до Державного реєстру потенційно небезпечних об’єктів [10];

об’єкти підвищеної небезпеки [11] (в т.ч. Перелік особливо небезпечних

підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров'ю громадян, майну, спорудам, навколишньому природному середовищу [12]);

об'єкти, які віднесені до категорій з цивільного захисту;

важливі державні об'єкти [13];

об'єкти, що підлягають обов'язковій охороні підрозділами Державної служби охорони за договорами [14];

об'єкти, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період [15];

особливо важливі об'єкти електроенергетики [16];

особливо важливі об'єкти нафтогазової галузі [17];

Національна система конфіденційного зв'язку [18];

платіжні системи [19];

чергово-диспетчерська система екстреної допомоги населенню за єдиним безкоштовним телефонним номером виклику екстрених служб 112 [20];

аварійно-рятувальні служби;

нерухомі об'єкти культурної спадщини [21].

Нині паралельно функціонують Єдина система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (Положення затверджене Постановою Кабінету Міністрів України № 1051 від 15.08.2007 р.), Єдина державна система цивільного захисту (Положення затверджене Постановою Кабінету Міністрів України № 11від 9 січня 2014 р. [22]). Названі системи створені в тому числі для захисту життєво важливих для держави об'єктів від окремих видів загроз, у зв'язку з чим створюється ситуація, що характеризується домінуванням відомчих підходів до розв'язання безпекових проблем національного масштабу.

Через об'єктивну необхідність забезпечення захисту від кіберзагроз, активізувалася робота щодо створення національного центру кіберзахисту та протидії кіберзагрозам, а також національного центру оперативно-технічного управління мережами телекомунікацій України для забезпечення потреб обороноздатності держави в особливий період (відповідне завдання згадується у рішенні РНБОУ [23]).

Термін «критична інфраструктура» не використовується в Женевських конвенціях про захист жертв війни. Проте сама ідея ресурсів і персоналу, життєво важливих для цивільних і гуманітарних цілей, добре опрацьована в ряді статей Конвенції, які історично висувають суворі вимоги до ресурсів і персоналу, що перебувають під їх захистом:

- «що займають незначну частину території ...»;

- «малонаселені порівняно з можливістю розміщення.»;

- «далеко віддалені від військових об'єктів або великих промислових потужностей.»;

- «не розташовані на території, значимій для ведення військових дій.»;

- «засоби комунікації та транспорту не повинні використовуватися для військового персоналу або матеріалів ...»;

- «не захищаються військовими засобами ...»;

- «відзначені червоними хрестами (червоними півмісяцями, червоними левами і сонцями) ...»;

- «всі необхідні кроки повинні бути вчинені, щоб звільнити ... будівлі, що використовуються в цілях релігії, мистецтва, науки або благодійності, історичні будівлі, госпіталі та будівлі, де розміщені хворі і поранені ... в тому випадку, якщо вони не використовуються у військових цілях »;

- «підводні кабелі, що з'єднують окуповану територію з нейтральними територіями» [1].

У найбільш широкому розумінні критичні інфраструктури - це системи, що мають найбільш важливе значення в захисті людського життя, забезпеченні економічної стабільності та національної безпеки. Незважаючи на те, що термін «захист критичних інфраструктур» не використовується у Конвенціях, у них визнається безпека людини, зокрема цивільного населення. Велике значення в праві збройних конфліктів надається захисту цивільних об'єктів - «цивільні об'єкти не повинні бути об'єктом нападу або репресій». Конвенції виключають такого роду об'єкти з числа можливих об'єктів атаки, а також гарантує їм захист і обережне поводження. У разі припинення дії такого статусу цивільних об'єктів, атакуюча сторона зобов'язується зробити належне попередження.

Цілком ефективно можуть застосовуватися положення Додаткового протоколу 1 Гаазької конвенції 1907 р., що забороняють піддавати нападу або знищенню об'єкти, необхідні для виживання цивільного населення (запаси прісної води, запаси продуктів харчування та ін.). Особлива увага приділяється установкам і спорудам, що стримують небезпечні сили, таким, як греблі, дамби та ін. Такі установки і споруди не повинні піддаватися нападу навіть якщо відносяться до військових об'єктів, «якщо такий напад може викликати вивільнення небезпечних сил і наступні тяжкі втрати серед цивільного населення».

1.3 Вплив локальних чинників воєнного і промислового техногенезу для критичної інфраструктури, природного середовища і соціуму

Розглянемо «воєнно-політичний конфлікт гібридного типу» - протистояння суб’єктів політики як в середині держави так і на міждержавному рівні, спрямованого на досягнення власних політичних інтересів із застосуванням різних засобів та способів впливу у політичній, воєнній, економічній, соціальній, інформаційній та інших сферах життєдіяльності [24]. Якраз сценарії такого збройного конфлікту відпрацьовуються на Донбасі.

Аналіз воєнно-політичних конфліктів гібридного типу дозволяє нам систематизувати основні специфічні ознаки цього суспільного явища, якими є:

- комплексне застосування невоєнних та воєнних засобів, форм і методів впливу на усіх етапах розвитку воєнно-політичного конфлікту, що охоплюють весь спектр прямого конфлікту, тилову зону, а також простір міждержавних взаємовідносин; зростання ролі непрямих (невоєнних) методів впливу на противника: політичних, дипломатичних, економічних, екологічних, інформаційно-психологічних операцій та інших. Тобто відбувається «стирання» чіткої межі між політичним конфліктом та початком збройного протистояння (воєнними діями);

- широке використання засобів масової інформації як фактору впливу на супротивника для досягнення необхідних політичних або воєнних переваг, спонукання до прийняття сприятливих для сторони-ініціатора інформаційного впливу рішень, а також впливу на свідомість людини, внаслідок якого вона

здійснює необхідні дії; використання сучасних інформаційних комп'ютерних технологій для руйнування (дезорганізації) систем військово-цивільного управління супротивника, а також із розвідувальною метою;

- стратегічні цілі воєнно-політичного конфлікту часто досягаються шляхом внутрішніх підривних дій у країнах-суперниках з використанням осередків політичних, громадських та інших організацій, партизансько-повстанських, терористичних і інших недержавних формувань, включаючи транснаціональну злочинність, що широко застосовують сепаратистські методи;

- застосування психологічного тиску та фізичного насилля до органів державної влади, збройних сил, правоохоронних органів і спеціальних служб з метою їх примусу до переходу на сторону противника;

- широке застосування для вирішення цих завдань сил спеціальних операцій, повітряно-десантних військ, що створює загрозу для постійного розширення масштабів конфлікту;

- широкомасштабне застосування засобів повітряно-космічного нападу, високоточної зброї, засобів радіоелектронної боротьби по всій території держави. Тобто основні завдання вирішуватимуться не в результаті прямого зіткнення учасників воєнно-політичного конфлікту, а завдяки застосуванню засобів дальнього вогневого ураження, інтенсивність якого зросте;

- спостерігається стрімкий перехід до застосування автоматизованих комплексів та систем ведення бойових дій (розвідувально-ударних, інформаційно-бойових тощо), а бойові системи зі штучним інтелектом стають одним із головних засобів збройної боротьби. При цьому має місце випереджальний розвиток засобів і способів ураження порівняно із засобами захисту;

- зростання вірогідності застосування зброї на нових фізичних принципах, так званої «зброї гуманної дії» (зброя яка несмертельна для людини, але виводить із ладу техніку, озброєння, засоби управління та комунікації, інженерні мережі);

- пріоритетом під час воєнно-політичного конфлікту стає ураження не військових об’єктів, а об’єктів критичної інфраструктури (руйнування електростанцій, ліній зв’язку, систем життєзабезпечення, об’єктів комунального обслуговування, транспорту, медичних закладів, елементів фінансової системи);

- неможливо повністю виключити вірогідність застосування під час воєнно-політичного конфлікту ядерної зброї та інших видів зброї масового ураження (їх компонентів). У воєнних доктринах більшості ядерних держав передбачається, так зване «обмежене застосування ядерної зброї»;

- сучасні воєнно-політичні конфлікти приймають все більш терористичний характер, а терористичні атаки стають одним із основних видів збройної боротьби. При цьому об'єктами терористичних дій, у більшості випадків, є цивільне населення, громадські та культурні об'єкти, системи життєзабезпечення, а також навколишнє середовище. При цьому зростає загроза використання терористами зброї масового ураження, або її компонентів.

Вищенаведене дозволяє нам також сформувати перелік можливих наслідків впливу сучасних воєнно-політичних конфліктів гібридного типу на безпеку життєдіяльності цивільного населення:

- прямі втрати серед мирного населення, а також значна кількість поранених та травмованих осіб; збільшення інтенсивності міграційних процесів, ріст кількості біженців, внутрішньо переміщених осіб та евакуйованих;

- спад економіки, і як наслідок, зниження рівня життя населення та його соціального захисту;

- порушення системи державного управління (у більшості випадків - бездіяльність влади), і як наслідок, неефективність діяльності системи ЦЗ;

- пошкодження та руйнування об'єктів ЦЗ (будівель та споруд пожежно-рятувальних служб, систем оповіщення та інформування, захисних споруд, тимчасових притулків, пунктів евакуації та медичних закладів, тощо);

- порушення діяльності систем життєзабезпечення, пошкодження та руйнування об'єктів критичної інфраструктури, і як наслідок, створення нестерпних умов життя для населення; виникнення осередків ураження від вторинних факторів застосування зброї (руйнування ядерних об'єктів (у першу чергу атомних електростанцій (АЕС), хімічно небезпечних об'єктів, гідротехнічних споруд інше), масштаби аварій на яких співвимірні із наслідками застосування зброї масового знищення;

- приховане використання під час воєнних дій чи терористичних операцій

зброї масового ураження або її компонентів (у першу чергу проти цивільного населення);

- нанесення збитків навколишньому середовищу, наслідком чого стануть екологічні катастрофи, голод, хвороби, пандемії;

- масштабний інформаційно-психологічний тиск на населення з метою придушення його спротиву та спонукання до колабораціонізму;

- створення атмосфери страху та незахищеності унаслідок терористичних дій, розгулу мародерства та бандитизму;

- порушення норм міжнародного гуманітарного права (у тому числі щодо цивільного населення), в основному партизансько-повстанськими, терористичними та іншими недержавними формуваннями, які є основними учасниками цих конфліктів.

Наразі можна виділити чотири принципово різних напрямки протистояння у сфері критичної інфраструктури, що знаходяться в районах ведення БД:

- використання традиційних озброєнь проти традиційної критичної інфраструктури (ситуація, аналогічна війнам XX століття, підпадає під дію міжнародного гуманітарного права);

- використання традиційних озброєнь проти мережевої критичної інфраструктури (критичної інформаційної інфраструктури), що є малоймовірним;

- використання інформаційних озброєнь проти традиційної критичної інфраструктури - атака з використанням глобальної системи позиціонування транспортних та інших інфраструктурних мереж, атака з відео-підтримкою, атака дистанційно-керованого літального апарату на об'єкти критичної інфраструктури;

- використання інформаційних озброєнь проти мережевої критичної інфраструктури (критичної інформаційної інфраструктури).

Останніх сім років територія Луганської та Донецької областей потерпає від дій російських окупантів, у зв’язку чим здійснюється комплекс військових та спеціальних організаційно-правових заходів українських силових структур, спрямований на протидію діяльності незаконних російських та проросійських збройних формувань у війні на сході України – ООС [26-28].

Площа території, на якій відбувається збройний конфлікт, становить до 20 тис. км^2, тут проживає до 7 млн. людей [25]. Це – старопромисловий регіон, насичений об`єктами критичної інфраструктури: шахтами, каналами, продуктопроводами, підприємствами військово-промислового комплексу тощо. Загалом на території Донецької, Луганської, Харківської областей є понад 5700 ПНО (23 % від їхньої загальної кількості в Україні), при цьому господарську діяльність тут продовжують підприємства, що входять до Переліку 100 об'єктів, які є найбільшими забруднювачами довкілля в Україні [27, 28].

За загальним рівнем техногенної насиченості та кількістю промислових підприємств Донеччина веде першість не лише в Україні, а й у Європі. Ці об'єкти представляють собою небезпеку, навіть у штатному режимі експлуатації [29]. Ескалація конфлікту у зоні ООС спричиняє значне зростання загроз техногенного та екологічного характеру, в тому числі внаслідок порушення технологічного режиму на численних ПНО [30].

Найбільшого руйнування в цих умовах зазнала критична інфраструктура водопостачання цього регіону. Схема забезпечення водою Донбасу із незахищених поверхневих джерел наведена на рис. 1.1 у вигляді 2-х схем.

а) канал Дніпро-Донбас

б) канал Сіверський Донець-Донбас та Південно-Донбаський водопровід

Рисунок 1.1 - Схема забезпечення водою Донбасу із незахищених поверхневих джерел

Перша включає канал Дніпро-Донбас, друга включає Сіверський Донець, канал Сіверський Донець-Донбас та Південно-Донбаський водопровід. Обидві ці схеми значно уразливі до зовнішній чинників впливу, про що свідчать данні, отримані від представників аналітичних центрів у Донецькій та Луганській обласних військово-цивільних адміністраціях. Під час проведення ремонтно-відновлювальних робіт на водогонах загинуло близько 12 чоловік, за свідченнями спостерігачів з розведення конфліктуючих сторін. Наземні та низько заглиблені водогони піддаються артилерійським обстрілам та диверсійним актам терористичного характеру.

За оцінками експертів [31], в умовах ведення бойових дій найбільшу загрозу для безпеки життєдіяльності населення і можливості відновлення виробництва формує небезпека втрати водовідливу і вентиляції шахт Донбасу, значна частина яких є гідравлічно пов’язаними. Нині зі 150 вугільних шахт 115 перебувають на окупованих територіях; повністю зруйновано 7 вугледобувних шахт Донбасу, ще

63 працюють у режимі відкачування води, працюючими є лише 24 шахти. З 90 шахт, підпорядкованих Міністерству енергетики та вугільної промисловості України, лише 35 знаходяться на контрольованій Україною території, тоді як інші 55 (у т.ч. шахти, що видобувають вугілля антрацитової групи) перебувають на території Донецької та Луганської областей, підконтрольній терористам. Із 35 контрольованих Україною шахт близько 10 працюють у режимі підтримання життєдіяльності .

На рис. 1.2 для ілюстрації наведено мінімальні рівні залягання ґрунтових вод за умови зняття з експлуатації шахт Донецько- Макіївсько-Горлівсько-Єнакіївської та Стаханівської гірничо-міських агломерацій. Зеленим кольором наведено результати підтоплення за умови зупинення шахт в цьому регіоні.

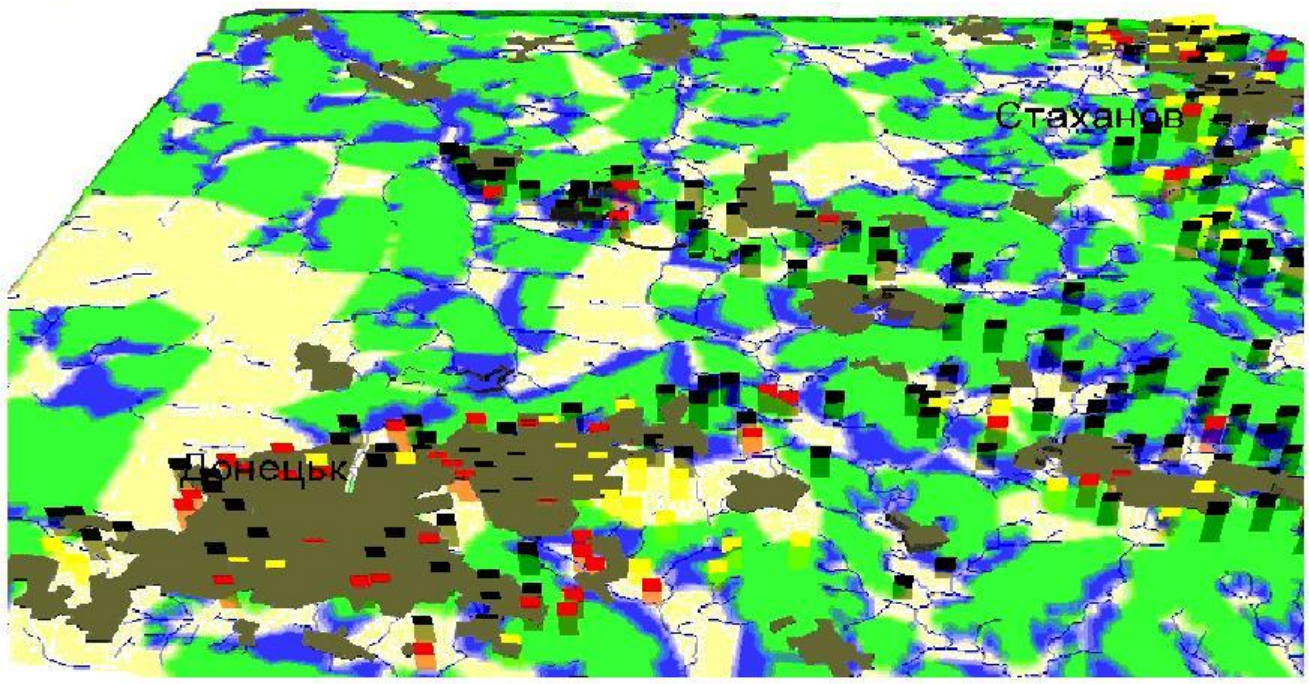
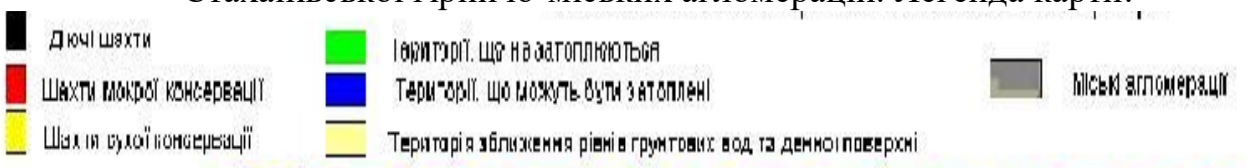


Рисунок 1.2 - Мінімальні рівні залягання ґрунтових вод за умови зняття з експлуатації шахт Донецько- Макіївсько-Горлівсько-Єнакіївської та Стаханівської гірничо-міських агломерацій. Легенда карти:



Більшість шахт в цьому регіоні є гідравлічно зв’язаними і затоплення однієї шахти може призвести до затоплення інших шахт, що розташовані поруч.

Наслідком некерованого затоплення шахт буде підтоплення і затоплення великих площ прилеглих міст та селищ, забруднення підземних і поверхневих водозаборів мінералізованими шахтними водами, додаткові просідання і зрушення (деформації) денної поверхні, руйнування нафтогазопроводів, магістральних та місцевих ліній електропередач та інших об’єктів критичної інфраструктури.

Потенційну загрозу радіаційного забруднення підземних вод несе у собі шахта Юнком, з камерою підземного атомного вибуху на глибині 860 м.

Радіаційну небезпеку несуть також терикони та теплові електростанції, біля яких виявлено підвищений радіаційний фон з рівнями радіації до 58 Мкр.

Рівні небезпеки для окремих територій на Сході України можна характеризувати інтегральними показниками як узагальненими критеріями комплексів воєнно-техногенних загроз, що можуть реалізуватися на ОКІ при певних умовах і спричинити надзвичайні ситуації воєнно-техногенного характеру. Тому визначення інтегральних показників воєнно-техногенної небезпеки є актуальним завданням, оскільки на території Донбасу знаходиться велика кількість ПНО та ОПН, переважно в зонах з великою концентрацією населення, що збільшує ризики надзвичайних ситуацій, які загрожують життю та здоров’ю особового складу ЗС України і місцевого населення, завдають значних матеріальних збитків, забруднюють навколишнє природне середовище [32-34].

Що стосується воєнно-техногенної безпеки, то існують проблеми безпечної роботи шахт, металургійних і коксо-хімічних підприємств, хімічно-небезпечних об’єктів, дамб хвостосховищ та шламонакопичувачів, вибухо- і пожежонебезпечних об'єктів, транспортних вузлів (залізничних станцій), магістральних трубопроводів та інших об’єктів в зоні впливу збройного конфлікту.

Тому системний підхід до вивчення воєнно-техногенних загроз надзвичайних ситуацій на ОКІ, оцінка рівнів техногенної та природної небезпеки окремих територій Донбасу, зниження ризиків аварій та катастроф є актуальним завданням, вирішення якого сприятиме підвищенню рівня національної безпеки у державі.

Значного ураження зазнала критична інфраструктура об’єктів водопостачання та водовідведення. Пошкоджено канал “Сіверський Донець–Донбас”. Внаслідок чинників воєнного і промислового техногенезу 10 червня 2014 року на території насосної станції каналу “Сіверський Донець – Донбас” поранено двох працівників КП “Компанія “Вода Донбасу” і пошкоджено обладнання водопостачання. Аварії на насосних станціях (НС) призвели до того, що в кількох містах Донецької області не було води. Повністю без води залишився Волноваський район. 2 липня 2014 року в результаті обстрілу пошкоджено насосну станцію І-го підйом каналу “Сіверський Донець – Донбас”, тоді смертельно поранило працівника “Компанії “Вода Донбасу”.

Водночас, екологічні проблем стосуються хімічного та радіаційного забруднення водних ресурсів, забруднення атмосферного повітря та ґрунтів, розсіювання хімічних речовин внаслідок розривів снарядів, мін, бомб тощо, руйнування місць зберігання небезпечних хімічних речовин (НХР), відходів та їхнє згоряння. При цьому відсутність належного державного контролю за техногенно-небезпечними об’єктами, сприяє збільшенню кількості випадків потрапляння до водойм НХР промислового і комунального походження. За час проведення АТО й ООС, від обстрілів артилерії загорілось кілька ПНО: Авдіївський та Ясинівський коксохімічні заводи, Лисичанський нафтопереробний та Краматорський верстатобудівельний заводи. Також, атак зазнав завод “Стирол”, який виготовляє аміак та завод “Точмаш” (Донецьк). Так, у результаті пожеж на коксохімічному заводі в Макіївці в повітря потрапила значна кількість НХР. Загалом на окупованій території знаходиться близько двох десятків ОПН. І в разі їхньої руйнації територія стане не придатна для проживання [35, 36].

Після масштабного мародерства і неконтрольованого вуглевидобутку на тимчасово окупованій території поступово затоплюються “копанки”, заповнюючи підземними водами порожнечі, що утворилися.

Сьогодні, у зоні проведення ООС, через зупинку насосів і потрапляння в шахти ґрунтових та підземних вод більшість з них не придатні для експлуатації,

затоплено 35 шахт у тому числі шахта “Юний комунар” в Єнакієве, де на глибині 903 метра у 1979 році був проведений ядерний вибух (об’єкт “Кліваж”). Повністю або частково затопленні шахти “Бутовська” і “Ясинівка-Глибока” в Макіївці, шахти Моспінська, “Трудовська” і “Жовтнева” в Донецьку, шахта “Білоріченська” в Лутугинському районі Луганської, шахта імені Мельникова в Лисичанську, шахта “Комсомолець Донбасу” в Кіровському районі Донецької області, шахти ім. Вахрушева в Ровеньках і ім. Коротченка в Селідово. Зруйновані шахти “Прогрес” у Торезі і “Червоний Партизан” в Свердловську, шахти Іловайська і Волинська із Розсипного, повністю затоплені шахти “Луганська” та “Машинський блок”, шахти “Марія Глибока” в Первомайську і Єнакіївська.

Затоплення шахт призводить до виходу шахтних вод на поверхню, забруднення та отруєння поверхневих вод басейнів р. Сіверський Донець і малих річок Приазов’я, джерел питної води та інших складових навколишнього природного середовища. Шахтні води виштовхують на поверхню вибухонебезпечний і отруйний газ метан, який накопичується у підвалах і на перших поверхах будинків та може спричинити масові вибухи у комунальних та промислових будівлях [37].

Ще в 1989 року у Горлівці на шахті “Олександр-Захід” зафіксована надзвичайна ситуація з потрапляння токсичних хімічних речовин в гірничі виробки і як наслідок сталося отруєння шахтарів. Ця шахта протягом тривалого часу була законсервованою та передана на ліквідацію з переведенням її в водовідливний режим. У результаті її затоплення є ризик забруднення небезпечними хімічними сполуками водоносних горизонтів ЦРД. Відсутність оперативного реагування на цю ситуацію може призвести також до забруднення отруйними хімічними речовинами всієї гідрографічної мережі річки Сіверський Донець та акваторії Азовського моря.

Серйозного забруднення в зоні проведення ООС зазнає атмосферне повітря. Після підриву моста в Новій Кіндрашівці залізничні поставки вугілля на Луганську ТЕС були припинені, а невдовзі, через пошкодження ліній електропередач, її

ізолювали від енергосистеми України. В результаті теплоелектростанція, що забезпечує електроенергією більше ніж 90 % споживачів Луганської області, була змушена самостійно регулювати частоту енергомережі, використовуючи доступне високосірчане і високозольне вугілля, що спричинило до різкого погіршення якості атмосферного повітря в цьому районі [38].

Дані інформаційної системи про стан навколишнього середовища Донбасу свідчить про насиченість даної території об'єктами критичної інфраструктури в районах ведення бойових дій може призвести до виникнення надзвичайного стану різного рівня (рис.1.3).

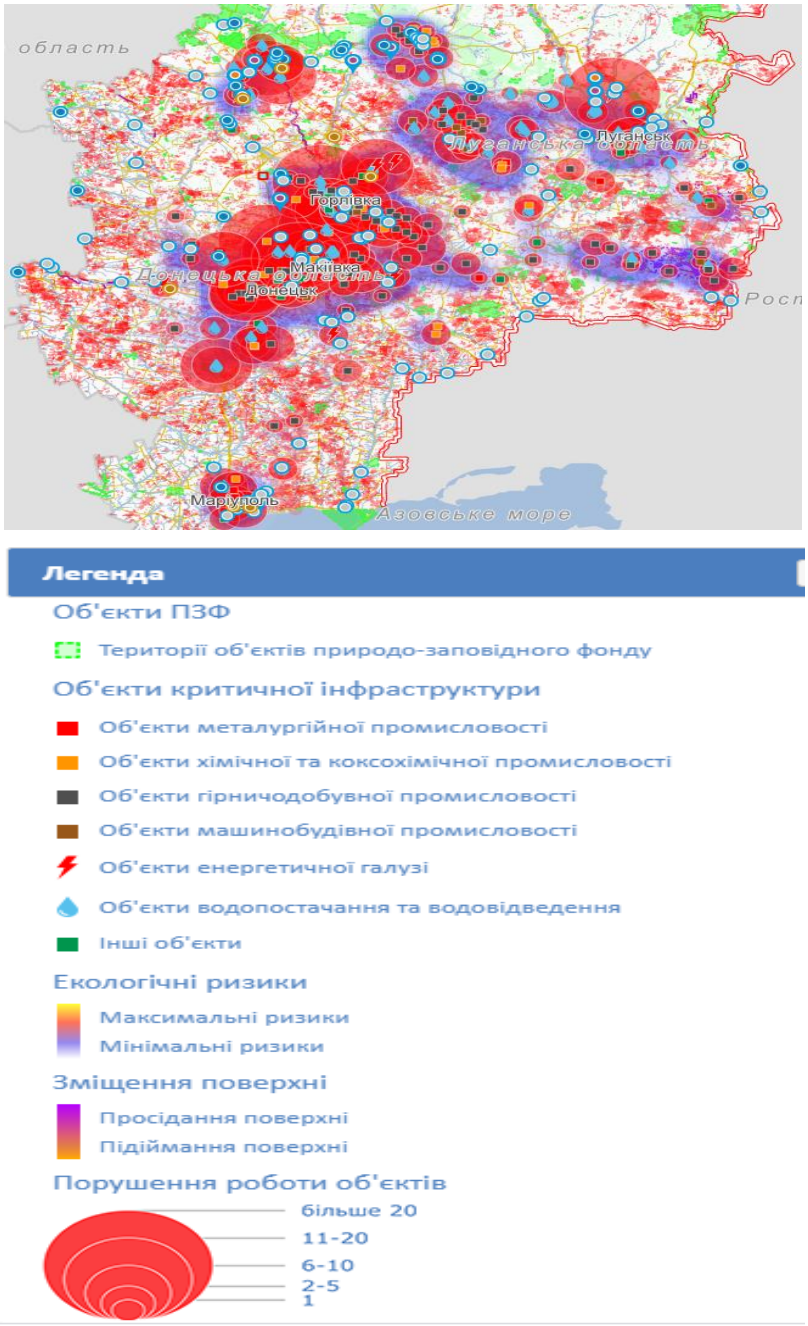


Рис.1.3- Техногенно – екологічна обстановка в зоні розташування обєктів критичної інфраструктури

1.4 Висновки до розділу 1

1. Проаналізовані підходи до поняття «критична інфраструктура» в США та Європейському союзі.

2. Проаналізована нормативно – правова база в сфері захисту об'єктів критичної інфраструктури розвинених країн.

3. Визначений сектор критичної інфраструктури розвинених країн:

- енергетичні об'єкти і мережі, наприклад, електричні розподільні мережі, газопроводи, нафтопроводи, сховища пального і т. ін.;

- комунікаційні і інформаційні технології (наприклад, телекомунікації, радіомовні і телевізійні передавачі і мережі, інтернет);

- фінансова система(банкова справа, капіталові ринки, інвестування);

- охорона здоров'я, особливо лікарні, поліклініки, установи постачання крові, лабораторії, сантехнічна рятувальна служби;

- харчова промисловість, сільське господарство, торгівля і постачання продовольством;

- вода, особливо греблі, гідроресурси;

- транспорт, особливо авіаційний, шосейний, залізничний, комбінований, комунікаційні вузли, а також системи управління транспортом;

- виробництво, зберігання і транспорт небезпечних товарів, особливо хімічних, біологічних, радіологічних ядерних матеріалів;

- державне управління, зокрема критичні служби і установи, інформаційні мережі, важливі економічні об'єкти, стратегічні об'єкти, а також культурні пам'ятники.

4. Визначено законодавчі категорії об'єктів, для яких встановлюються особливі умови забезпечення їх захисту та функціонування в Україні:

- підприємства, які мають стратегічне значення для економіки та безпеки держави;

- об'єкти, які включені до Державного реєстру потенційно небезпечних об'єктів;

- об’єкти підвищеної небезпеки (перелік особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров’ю громадян, майну, спорудам, навколишньому природному середовищу);

- об’єкти, які віднесені до категорій з цивільного захисту;

- важливі державні об’єкти;

- об’єкти, що підлягають обов’язковій охороні підрозділами Державної служби охорони за договорами;

- об’єкти, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період;

- особливо важливі об’єкти електроенергетики ;

- особливо важливі об’єкти нафтогазової галузі ;

- Національна система конфіденційного зв’язку ;

- платіжні системи ;

- чергово-диспетчерська система екстреної допомоги населенню за єдиним безкоштовним телефонним номером виклику екстрених служб 112 ;

- аварійно-рятувальні служби;

-нерухомі об’єкти культурної спадщини .

5. Встановлено вплив чинників воєнного і промислового техногенезу на об’єкти критичної інфраструктури природного середовища і соціуму на Сході України .

РОЗДІЛ 2 ПОСТАНОВКА НАУКОВОГО ЗАВДАННЯ НА РОЗРОБКУ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ

Ефективна реалізація державної політики у сфері захисту населення і територій від техногенних та природних надзвичайних ситуацій, їх попередження, зниження можливих людських жертв та майнових втрат в зоні проведення ООС вимагає визначення раціональних пропорцій при виділенні матеріальних і фінансових ресурсів на попередження надзвичайних ситуацій та зниження ризиків їх виникнення. Очевидно, що розмір ресурсів, які виділяються для цієї мети, повинен відповідати рівням техногенної небезпеки для ОКІ і життєдіяльності населення на відповідних територіях проведення операції об'єднаних Сил.

Рівні небезпеки для окремих територій на Сході України можна характеризувати інтегральними показниками як узагальненими критеріями комплексів воєнно-техногенних загроз, що можуть реалізуватися при певних умовах і спричинити надзвичайні ситуації воєнно-техногенного характеру на ОКІ.

2.1. Обґрунтування показників для оцінки впливу чинників воєнного і промислового техногенезу на об'єктах критичної інфраструктури

Питання про показники моніторингу ОКІ районів ведення БД відноситься до найважливіших теоретичних і методичних положень прецизійної воєнної екології. На сьогодні, найбільш детальне опрацьовування концепції показників моніторингу представлене в роботах [39, 40, 41, 42]. У найзагальнішому вигляді задача обґрунтування показників зводиться до вибору з певної множини розроблених індикаторів та індексів таких, що забезпечують стійку оцінку індикаторних значень впливу ВТН на НПС та ОКІ, які не викликають протягом невизначено тривалого періоду відхилень в нормальному функціонуванні екосистем, розташованих біля джерел впливу.

Такий підхід, безумовно, максимально враховує інтереси екосистеми і її структуру, але майже не враховує внутрішньої структури впливу ВТН, розглядаючи його як інтегральний.

Системний підхід до вивчення ОКІ, складається з [43, 44, 45]:

- визначення утворюючих її складових частин - $\Gamma_1, \Gamma_2, \ldots, \Gamma_n$ і взаємодіючих з нею об'єктів навколишнього середовища - $S_1, S_2, \ldots, S_k$;

- встановлення структури, тобто сукупності внутрішніх зв'язків і відносин ОКІ, а також зв'язків між ОКІ і навколишнім середовищем $\Sigma_1, \Sigma_2, \ldots, \Sigma_r$;

- побудови функцій (законів функціонування) системи ОКІ F, що визначає характер зміни компонентів системи ОКІ і зв'язків між ними під дією зовнішніх об'єктів $S_1(t), S_2(t), \ldots, S_k(t)$.

Елементи ОКІ $\Gamma_1, \Gamma_2, \ldots, \Gamma_n$, які пов'язані між собою різними зв'язками і відносинами, називаються системоутворюючими, тому що саме їхня наявність перетворює набір елементів у цілісну систему (див. рис. 2.1).

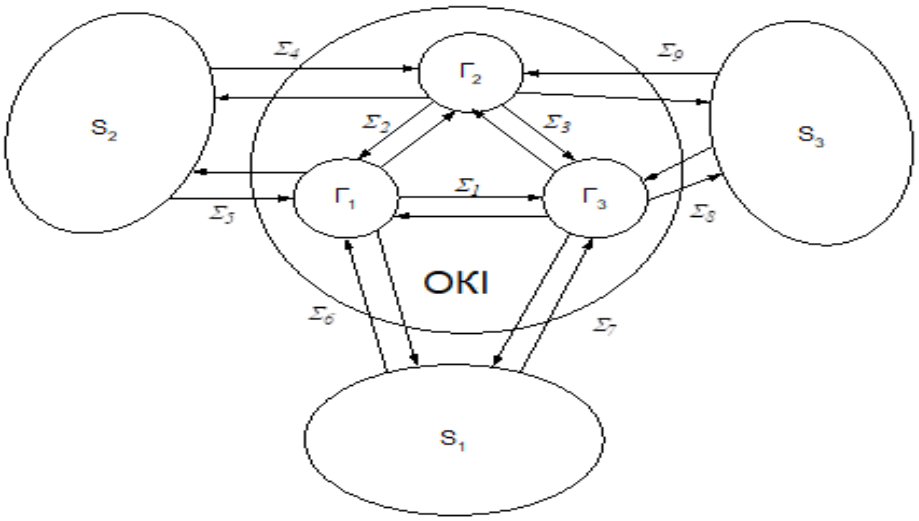


Рисунок 2.1 - Принципова схема системи ОКІ як простору

$$ОКІ = \{\Gamma, V, \Sigma, F\}, \quad (2.1)$$

де $\Gamma = \{\Gamma_1, \Gamma_2, \Gamma_3\}$- внутрішні елементи системи ОКІ; $V = \{S_1, S_2, S_3\}$- зовнішні системи; $\Sigma = \{\Sigma_1, \Sigma_2, \Sigma_3, \Sigma_4, \Sigma_5, \Sigma_6, \Sigma_7, \Sigma_8, \Sigma_9\}$- структурні зв'язки; F - функція перетворення параметрів і структури

Однак крім того, що ці елементи пов'язані між собою, на них впливають зовнішні об'єкти, а вони, в свою чергу, самі впливають на них. Це приводить до

необхідності залучення поняття про навколишнє середовище як по відношенню до системи ОКІ, так і до систем, що входять до її складу.

З формальної точки зору система ОКІ впливає сама і зазнає впливу з боку незліченної кількості зовнішніх стосовно неї систем $S_1, S_2, \ldots, S_m$ (див. рис. 2.1). Однак, обравши поріг визначеної міри інтенсивності впливу, можна встановити кінцеве число зовнішніх систем $S_1, S_2, \ldots, S_k, k < m$, що знаходяться з даною системою у взаємодії з інтенсивністю не меншою деякого заданого порогу. Множину, що складається з усіх зовнішніх систем, які знаходяться в істотному зв'язку (у вищезазначеному розумінні) з даною системою ОКІ, назвемо безпосереднім зовнішнім середовищем і позначимо:

$$V = \{S_1, S_2, \ldots, S_k\}. \tag{2.2}$$

Множину зв'язків (відносин) елементів системи ОКІ між собою, а також елементів цієї системи з зовнішнім середовищем назвемо структурою системи ОКІ, яку можна представити у вигляді

$$\Sigma = \{\Sigma_1, \Sigma_2, \ldots, \Sigma_r\}, \tag{2.3}$$

де r — число всіх розглянутих зв'язків, що утворюють структуру системи ОКІ.

Зовнішнє середовище, склад і структура ОКІ можуть змінюватися з часом:

$$\begin{cases} \Gamma(t) = \{\Gamma_1(t), \Gamma_2(t), \ldots, \Gamma_n(t)\} \\ V(t) = \{S_1(t), S_2(t), \ldots, S_k(t)\}. \\ \Sigma(t) = \{\Sigma_1(t), \Sigma_2(t), \ldots, \Sigma_r(t)\} \end{cases} \tag{2.4}$$

Функцією ОКІ називається закон (сукупність правил) F, за яким в залежності від зовнішніх факторів $V(t)$ відбувається зміна в часі внутрішніх елементів $\Gamma(t)$ і структури $\Sigma(t)$ системи.

Остаточно математичне визначення поняття ОКІ набуває змісту простору $\text{ОКІ}(t) = \{V(t), X(t), \Sigma(t), F\}$, який складається із кортежу елементів систем $\Gamma(t)$, зовнішніх систем $V(t)$, сукупності зв'язків $\Sigma(t)$ та функції параметричних і структурних змін в $\Gamma(t)$ та $\Sigma(t)$.

Для обґрунтування показників моніторингу ОКІ районів ведення БД застосуємо індикаторно-індексний підхід, що спирається на кількісні оцінки індикаторів та індексів ВТН, показників стану абіотичного середовища ВПТГС та реакції на ВТН.

Слово індикатор (походить від латинського indicio − вказую, визначаю) − частина інформації або даних (кількісних або якісних), що характеризує екологічний стан НПС. Індикатор використовується для оцінки ситуації та прийняття рішень і визначається таким чином, щоб великий об'єм первинної інформації узагальнити і зробити висновки про стан та тенденції розвитку ситуації [46,47]. Параметр – це величина властива процесу чи явищу, що оцінюється або досліджується. Показники – наочні конкретні дані про результати якогось процесу. Індекс − набір сукупних або зважених параметрів, показників або індикаторів.

Надалі під індикатором розуміємо ознаку, властиву системі чи процесу, на підставі якої проводиться якісна чи кількісна оцінка тенденцій змін в ВПТГС чи оціночна класифікація стану ОКІ, процесів і явищ.

Під індикатором в прецизійній військовій екології розуміють елемент інформації, який може бути складовою компонентою вектора екологічного стану ВПТГС, і відповідає вимогам:

- бути характеристикою, яка використовується в інтересах моніторингу ОКІ районів ведення БД та процесів управління їх станом, і може застосовуватися для планування цього процесу в майбутньому;

- відігравати роль показника стану ОКІ чи ВТН;

- описувати відхилення від рівня екологічного стану ВПТГС, прийнятого за базовий.

Одночасно з цим необхідно відзначити, що кожний окремий індикатор

повинен відповідати наступним вимогам [48]:

- бути науково обґрунтованим;

- мати відповідну чутливість до зміни воєнно-техногенної обстановки;

- мати просту інтерпретацію;

- мати здатність до агрегування;

- відповідати набору національних пріоритетів і концепції сталого розвитку;

- бути вихідним елементом екологічної інформації, на основі якої можуть проводитись кількісні оцінки рівня воєнно-техногенної безпеки;

- мати високу інформаційну ємність і нести нові цінні дані для систем підтримки прийняття рішень.

Під екологічним індексом розуміємо комплексну величину, яка може складатися з декількох індикаторів, які описують процеси, і характеризує відхилення від рівня екологічного стану ВПТГС, прийнятого за базовий. Один індекс у собі може об’єднувати й агрегувати цілий пакет індикаторів [42, 49-51].

Таким чином, застосування екологічних індикаторів та індексів дозволяє виконати агрегування значних об’ємів екологічної інформації (вимірів і параметрів стану природного середовища), що зазвичай використовуються для формування багатовимірного вектору стану ОКІ.

На сьогоднішній день у проблематиці індикаторів та індексів вимагають свого вирішення ряд непростих задач, серед яких слід зазначити як найбільш значимі наступні [49-51]:

- проблема невизначеності вхідної інформації;

- критерії вибору індикаторів;

- проблема агрегування екологічних даних;

- способи і форми представлення інформації на основі індикаторів для систем підтримки прийняття рішень;

- зв'язок індикаторів із загрозою та ризиком;

- вибір одиниць виміру і шкали.

Змістовне і цільове призначення індикаторів та індексів в системі

моніторингу ОКІ районів ведення БД полягає в представленні в стиснутій формі інформації за наступними основними напрямками [51, 52]:

- кількісна чи якісна інтегральна оцінка ВТН та його факторів в цілому чи за окремими його компонентами;

- визначення чисельного значення величини чи сукупності величин, що характеризують взаємодію і взаємозв'язки між окремими військовими екосистемами, їх стану і динаміки;

- визначення чисельного значення характеристик досліджуваних процесів і явищ, що протікають у військових екосистемах;

- визначення чисельних значень показників, що описують властивості досліджуваних військових екосистем.

Будучи відносно новими показниками в системах моніторингу районів ведення БД індикатори та індекси можуть стати основою для генерації інтегральної інформації про техногенні впливи військового походження в системах підтримки прийняття рішень щодо забезпечення необхідного рівня техногенної безпеки на ОКІ.

Основними передумовами до обґрунтування головної ідеї застосування індикаторів і індексів в якості компонент ВЕС ВПТГС є системний підхід до оцінки процесів у військових екосистемах, що ґрунтується на [53]:

- декомпозиції ВПТГС на складові компоненти біоценозу, біотопу та критичної інфраструктури;

- агрегації відповідних показників воєнно-техногенного впливу, стану ВПТГС та відгуку екосистеми до екологічних індикаторів та індексів;

- гнучкому представленні отриманих індикаторів та індексів у відповідних шкалах.

Для обґрунтування показників моніторингу ОКІ районів ведення БД пропонується розглянути наступну ієрархічну структурно-логічну модель на рис. 2.3, яку було побудовано на основі застосування методу стратифікації, системного підходу та основних принципів прикладної екології.

В результаті ведення БД формується потік ВТН на компоненти вектору

стану ОКІ.

Для формалізації ВТН від ведення БД відповідно до структурно-логічної моделі введемо поняття потоку ВТН

$$\Phi_{BTH} = \Phi_{BTH}(F) \tag{2.5}$$

де $F^T = (F_1^T, F_2^T, F_3^T)$ − вектор потоку ВТН.

Елементи вектора потоку ВТН F_1, F_2, F_3 представляють собою вектори інтенсивності факторів воєнно-техногенного навантаження. Назвемо їх спектрами типів ВТН

$$\begin{cases} F_1^T = (f_{11}, \ldots, f_{1k}, \ldots, f_{1N}), \\ F_2^T = (f_{21}, \ldots, f_{2k}, \ldots, f_{2M}), \\ F_3^T = (f_{31}, \ldots, f_{3k}, \ldots, f_{3K}), \end{cases} \tag{2.6}$$

де f_{ij} − фактори воєнно-техногенного навантаження.

2.2 Математична модель оцінювання загроз і ризиків на об'єктах критичної інфраструктури в районах ведення бойових дій

Розглянемо воєнно-техногенний вплив на ОКІ, який може призводити до покращення стану ОКІ, перебування ОКІ у врівноваженому стані, чи до погіршення стану ОКІ. Покращення стану здійснюється за рахунок цілеспрямованих заходів цивільного захисту, які перевищують ступінь негативного воєнно-техногенного впливу на ОКІ. Врівноважений стан обумовлено незначним воєнно-техногенним негативним впливом на ОКІ, у межах екологічної ємності, коли система ОКІ здатна до самовідновлення. Погіршення стану спостерігається за умови значного негативного впливу на ОКІ, коли відновлення екологічної системи самостійно не можливе.

Забезпечення безпеки населення та навколишнього середовища в умовах ведення БД - складна соціо-еколого-економічна проблема, вирішення якої залежить від характеру взаємодії військових, економічних, соціальних,

екологічних і демографічних факторів, що визначають розвиток як окремих держав, так і цивілізації в цілому.

Аналіз воєнно-техногенних загроз виводить нас на широкий спектр проблем, з них виділимо чотири головні:

- виявлення елементів загрози;

- аналіз та кількісний вимір загрози;

- визначення допустимого рівня загрози;

- заходи щодо запобігання аварій та катастроф, управління в умовах аварійних ситуацій, зниження рівня загрози.

Причини виникнення надзвичайних ситуацій на ОКІ можна умовно поділити на три основні групи:

- технічні причини, зумовлені недоліками у технологічних схемах, або дефекти обладнання, конструкторськими недоробками;

- причини пов'язані з «людським фактором»;

- причини пов'язані з веденням БД.

Аналіз багатьох аварій показує, що значна їх частина зумовлена неправильною поведінкою операторів та іншого обслуговуючого персоналу. У зв'язку з цим сьогодні поряд із розв'язанням задач щодо підвищення надійності обладнання, його якості та своєчасного технічного обслуговування все більша увага приділяється особливостям поведінки служб безпеки, навчання персоналу та працюючих на складних технічних системах та дій у надзвичайних ситуаціях, що виникають на виробництві.

Розглянемо визначення загрози, що висвітлює кількісні аспекти і може бути застосовано до будь-якого виду оцінюваної загрози. Для цього спочатку обговоримо якісні оцінки ідеї загрози, а потім перейдемо до кількісних показників.

Загроза – це фізична ситуація з потенційними пошкодженнями для ОКІ, людини, пошкодження майна, власності, навколишнього середовища та їх комбінаціями. Тоді ризик – це сукупність специфічних небажаних подій, що мають

місце в певний період часу, або за певних обставин, і виникають через реалізацію певних загроз.

Перший якісний аспект, який ми розглянемо, це відмінність між ідеями ризику та загрози. Якщо пошукати ці слова в різних словниках, то можна знайти значне співпадіння в значенні, та різницю в акцентах. Загроза зазвичай визначається як джерело шкоди або збитку, в той час як визначення ризику звичайно включає ідею ймовірності того, що шкода або збиток дійсно будуть нанесені:

$$\text{Ризик} = \text{Загроза/Заходи запобігання, або } R=Z/S. \quad (2.7)$$

Формула (2.7) - символічна, а не чисельна рівність, у тому розумінні, що ні R, ні Z, ні S не є числами. Не можна поділити два з них, щоб отримати третє. Зміст цього співвідношення в тому, що для вказаного Z, чим більше S, тим менший ризик R.

Кількісна оцінка загрози є важливою складовою частиною в проблемі запобігання виникненню надзвичайних ситуацій на об’єктах критичної інфраструктури в районах ведення БД.

Кількісний аналіз загрози, тобто числове визначення ступеню окремих загроз, або загрози окремого виду ОКІ, є складною проблемою.

Математично загрозу можна подати як множину дуплетів [54]

$$Z = \{<s_j, p_j>\}s \ , \quad (2.8)$$

де s_j – j-й сценарій поведінки джерела загрози; p_j – j-а ймовірність виникнення сценарію для джерела загрози.

Тобто у відповідності з формулою (2.8) загроза – це ризик, але без врахування ймовірності сценарію. Це дещо спрощене розуміння загрози але воно відповідає словесному його визначенню, а також практиці.

Отже, поняття загрози у випадку виникнення надзвичайних ситуацій на об’єктах критичної інфраструктури пов’язане із сценарієм. Така парадигма загрози полягає у переході від джерела загрози до наслідків її реалізації.

Загроза у випадку виникнення надзвичайної ситуації на ОКІ може бути кількох типів:

- загроза для людського здоров'я на довгому чи короткому проміжку часу;

- загроза для флори і фауни, включаючи поняття харчових ланцюгів;

- загроза в екосистемі в цілому, враховуючи розмаїття;

- загроза для майна (активів), навіть за умови, що реалізація не обов'язково запланована;

- загроза для використання земель;

- загроза від недотримання певних норм та можливості несплати законодавчих штрафів;

- загроза іміджу підприємства та/або державі загалом;

- загроза ґрунтовим водам та іншим ресурсам, таким як рекреаційні.

Часто ці загрози можуть бути одночасними і поєднаними, та багато з них можуть перекриватися. З даного переліку типів загроз видно, що діапазон будь-якого набору методів аналізу загроз повинен бути набагато ширшим, аби цей аналіз був ефективним.

Систематичне та кількісне застосування методології «джерело - шлях - наслідки» дає змогу перенести проблему оточуючого середовища на джерелі до характеристики об’єкта критичної інфраструктури.

Задача оцінки та ранжування загроз в умовах невизначеності розв'язується методами системного аналізу з використанням багатокритеріальної оцінки загроз [55, 56].

Для оцінки загрози необхідно здійснити наступні кроки:

- навести всі можливі комбінації «джерело - шлях - наслідки», включаючи протиріччя;

- створити набір даних для об’єкта критичної інфраструктури, що базуються на доступній інформації, здоровому глузді;

- використати набір даних та відповідну модель аналізу загрози, щоб оцінити вплив джерела на наслідок. На цьому етапі багато чи більшість потенційних сценаріїв «джерело - шлях - наслідки» буде відкинуто, залишаючи лише реалістичні комбінації;

- провести аналіз чутливості на залишених зв'язках, щоб визначити ті, де оцінка чутлива до параметрів, які мало відомі;

- провести аналіз вигідності (зменшення вартості) між наслідками від не знання певних параметрів, для більш високого рівня впевненості та між вартістю переоцінки параметрів;

- визначити «потребу знати» параметри та повторювати кроки до цього пункту, доки до бази даних не має високої довіри;

- оцінити вихідні характеристики розповсюдження, які тільки зменшать вплив джерела нижче максимально допустимого;

- розробити та побудувати схему оновлення, що досягне такої характеристики розповсюдження;

- оцінити чуттєвість впливу джерела до помилок та відмов у проекті і/або реалізації схеми управління.

Якщо існує значна можливість недопустимої відмови, продовжувати виконувати аналіз при зменшенні цієї можливості.

Дослідження загрози потребує також відповіді на наступні запитання: Чи методологія дослідження загрози безпечна? Які загрози приймаються як важливі? Які рівні ризику допустимі, хто визначає це і як?

Для оцінки і ранжування загроз слід сформувати критерії не тільки в значенні "критеріальна функція", а в ширшому значенні - як спосіб оцінки і порівняння загроз.

Випадки, коли єдиний критерій вдало відображає мету оцінки загрози, швидше виключення, ніж правило. Один критерій лише приблизно (як і всяка модель) відображає мету оцінки і його адекватність може виявитися недостатньою. Вирішення задачі підвищення адекватності полягає не тільки в пошуку

адекватнішого критерію (можливо, він і не існує), але й у використанні декількох критеріїв, що описують різносторонньо мету оцінки загрози і доповнюють один одного.

Об’єктивність вирішення задачі оцінки і ранжування обумовлюється забезпеченням критеріями достатньо повного ланцюга оцінки ознак загроз. Це означає, що критерії описують всі важливі аспекти мети оцінки, але при цьому доцільно мінімізувати їх число. Остання вимога задовольняється, якщо критерії є незалежними, не пов'язані між собою (наприклад, бажано не використовувати в різних складових критеріях однакові вимірювані величини або величини, які виводяться одна з одної тощо).

Огляд сучасних підходів до системного аналізу складних природно-техногенних систем та аналіз математичного апарату, що застосовується при цьому, дозволяють зробити висновок: аналіз і оцінка загроз повинні бути багатофакторними, а порівняльний аналіз сукупності їх джерел доцільно проводити з урахуванням ряду показників, що є визначальними при формуванні цільових функцій для відповідних критеріїв.

Аналіз процедур, які використовуються при вирішенні багатокритеріальних задач, дає можливість вибрати ті з них, якими можна було б скористатися при системному аналізі загроз.

До числа цих способів можна віднести [55-59]:

- використання цільової функції;

- використання функції переваги при згортанні багатокритеріальної задачі до однокритеріальної, що ґрунтується на згортанні багатьох критеріїв в один;

- використання функції переваги й виділення пріоритетного критерію.

Структура інформаційної моделі, що обґрунтовано використовується в процедурах екологічної експертизи та аудиту для оцінки ризиків і загроз [54], зображена на рис. 2.2.

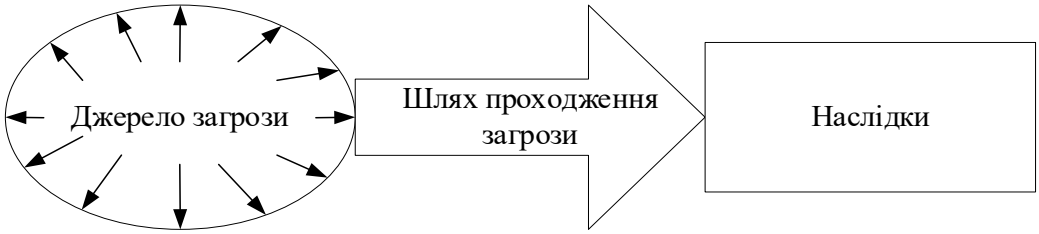


Рисунок 2.2 - Ключові елементи для оцінки загроз

Для оцінки загроз пропонується застосувати наступні складові критерії, які органічно витікають із цієї моделі:

критерій оцінки джерела загрози;

критерій оцінки шляху проходження загрози;

критерій оцінки наслідків впливу загрози.

Для формування інтегральної оцінки слід сформувати узагальнену цільову функцію, яка за умови експертної оцінки є інструментом приведення багатокритеріальної задачі до однокритеріальної. Вона представляє собою певну функцію векторного аргументу, так званий інтегральний критерій:

$$J_{\Sigma}(e) = f(J_1(e_1), J_2(e_2), \ldots, J_n(e_n)), \tag{2.9}$$

де $J_{\Sigma}(e)$ - цільова інтегральна функція інтегрального критерію оцінки загроз, $J_i(e_i), i = \overline{1,3}$- цільові функції часткових критеріїв оцінки загроз.

Вид функції (2.9) визначається внеском кожного часткового критерію в комплексний критерій та можливим видом згортки, який при цьому використовується. При згортці багатокритеріальних задач оцінки загроз до однокритеріальних, коли часткові критерії є різноваговими, зазвичай використовують адитивні чи мультиплікативні функції згортки [57, 58].

Аналіз результатів оцінки загроз за інтегральним критерієм чи за частковими критеріями дає можливість виділення інтервалів оціночних значень та проведення ранжувань ОКІ за рівнем загроз.

Можлива ієрархічна структура критеріїв і факторів для оцінки загроз наведена на рис. 2.3.

Рисунок 2.3 - Ієрархічне дерево критеріїв оцінки і ранжування загроз

Керуючись підходами наведеними у публікаціях [55-58], узагальнену цільову функцію можна представити у вигляді:

$$J_{\Sigma}(e) = \sum_{i=1}^{n} \frac{\alpha_i}{s_i} J_i(e_i), \tag{2.10}$$

де α_i і s_i - вагові коефіцієнти, що можуть бути визначені експертним шляхом (через процедури методу аналізу ієрархій) [60].

Аргументи цільової функції e_i, які є ознаками факторами в оцінках загроз за відповідними складовими критеріями.

Із зазначеного випливає, що для моделювання загроз виникнення надзвичайних ситуацій на об’єктах критичної інфраструктури найбільш підходять

методи, пов’язані з експертно-аналітичними процедурами, оскільки розроблення майбутніх можливих сценаріїв реалізації загроз передбачає якісний аналіз варіантів з можливими розрахунковими додатками, якими будуть виступати геоінформаційні технології.

Кожен частковий критерій J_i складається з множини підкритеріїв f_{ij}. Для отримання експертних оцінок експерти заповнюють анкети, в яких присвоюють відповідні оцінки ознакам факторів e_i, значення яких фіксуються в деякій шкалі.

Дія факторів ВТН веде до забруднення складових геосфер ВПТГС. Під забрудненням ВПТГС слід розуміти зміну властивостей його складових геосфер (хімічних, механічних, фізичних, біологічних і пов'язаних з ними інформаційних), яка відбувається внаслідок дії факторів воєнно-техногенного навантаження, що спричиняють погіршення функцій екосистем стосовно живих об'єктів біосфери (людей, біологічних організмів, біоценозів тощо). Джерело забруднення ВПТГС (джерело факторів воєнно-техногенного навантаження) − це військовий об'єкт (функціональний елемент ВПТГС за термінологією функціонального зонування), від якого забруднення надходить у складові геосфери (атмосфера, літосфера, гідросфера, біосфера).

Порівняльний аналіз існуючих класифікацій техногенного навантаження та узагальнення досвіду в цій галузі воєнної екології дозволяють сформувати наступні класифікаційні ознаки воєнно-техногенного навантаження [61-65]:

- характер походження; природа походження;
- сфера поширення; масштаби поширення;
- тип джерела;
- режим функціонування джерела.

Відповідно до цього пропонується наступна класифікація джерел воєнно-техногенних загроз, що наведена в таблиці 2.1.

Таблиця 2.1 - Класифікація джерел воєнно-техногенних загроз

1. Характер походження забруднення						
Безпосереднє	Вторинне		Ланцюжкове		Фактороформуюче	
2. Природа походження факторів впливу забруднення						
Механічне	Хімічне	Фізичне	Біологічне	Інформаційне		
3. Сфера поширення забруднення						
Атмосферне повітря	Ґрунти	Ґрунтові води		Поверхневі води		
4. Масштаб поширення забруднення						
Глобальне	Регіональне	Місцеве		Локальне		
5. Тип джерел забруднення:						
Точкові	Площинні	Одиночні	Групові	Організовані	Неорганізовані	
6. Режим функціонування джерел забруднення:						
Рухомі	Нерухомі	Постійно діючі	Періодично діючі	Разові	Штатні	Аварійні

До джерел воєнно-техногенних загроз для ОКІ при веденні БД в операційних зонах та районах відносяться:

- системи зброї і військова техніка;

- райони і місця ведення БД.

Ці об'єкти мають значну специфіку в залежності від їхньої приналежності до видів збройних сил і родів військ. Вони є безпосередніми джерелами впливу факторів ВТН на екологічні процеси, явища чи стан ОКІ.

2.3. Алгоритм оцінювання ризиків і загроз на об’єктах критичної інфраструктури

Алгоритмізація моделей оцінки воєнно-техногенних загроз виникнення надзвичайних ситуацій на об’єктах критичної інфраструктури повинна ґрунтуватися на універсальних та специфічних методах, що дозволяють проводити оцінювання, виходячи із умов виникнення надзвичайних ситуацій.

Для оцінки загрози виникнення НС можуть бути застосовані універсальні підходи (здебільшого експертно орієнтовані), то для оцінки ризику доцільно використовувати більш специфічні підходи, оскільки поняття ризику містить в собі ймовірнісну складову.

На рис. 2.4 показано розроблений алгоритм оцінки ризику виникнення надзвичайної ситуації на окремо взятому ОКІ в районі ведення БД з використанням геоінформаційних технологій (ГІС).

Коли ризик переростає в загрозу виникнення надзвичайної ситуації, для оцінювання рівня загрози може бути використаний більш універсальний підхід із яких на сьогодні найбільш поширеним і системно довершеним є метод аналізу мереж (ANP-process).

На рис. 2.5 показана блок-схема розробленого алгоритму оцінювання загроз на об’єкті критичної інфраструктури з використанням ГІС-технологій.

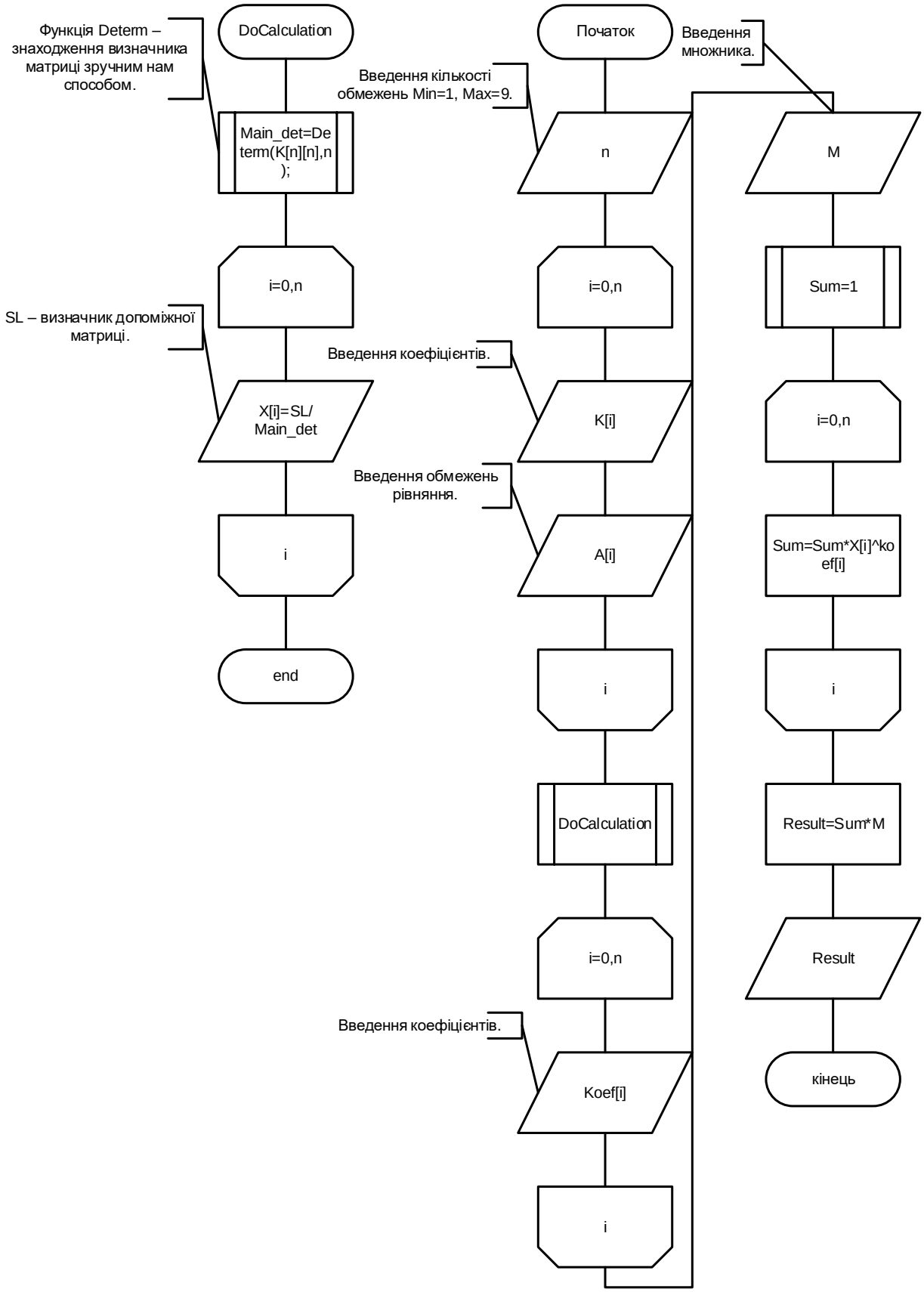
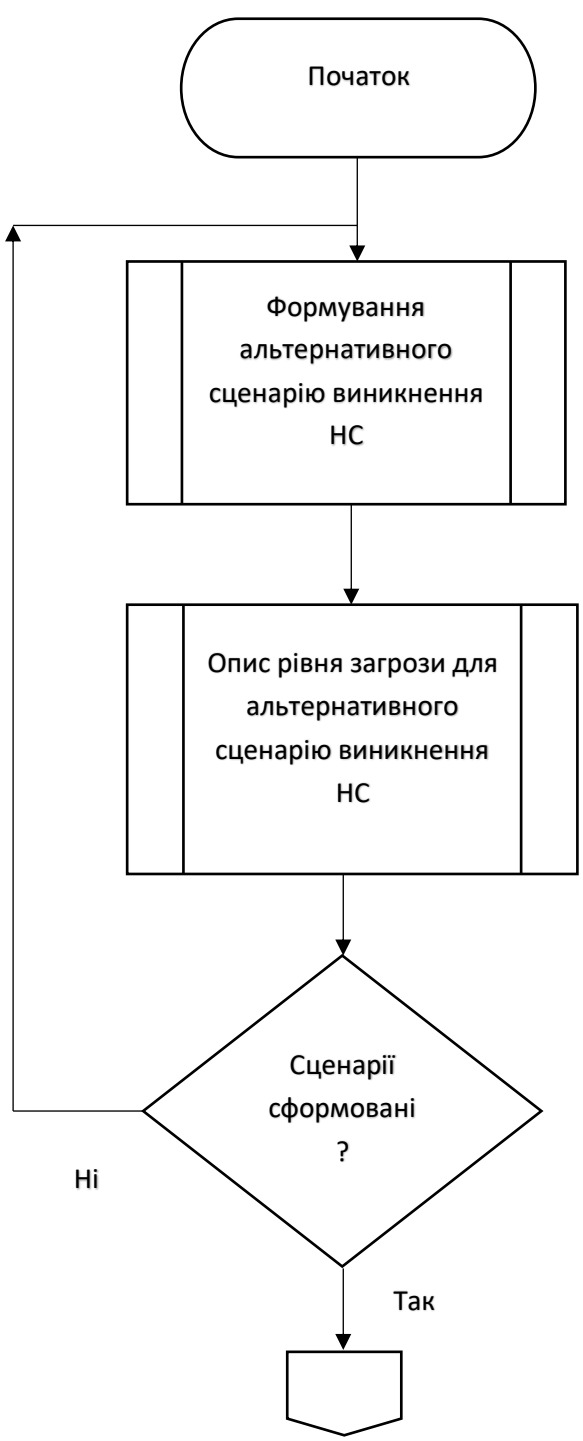
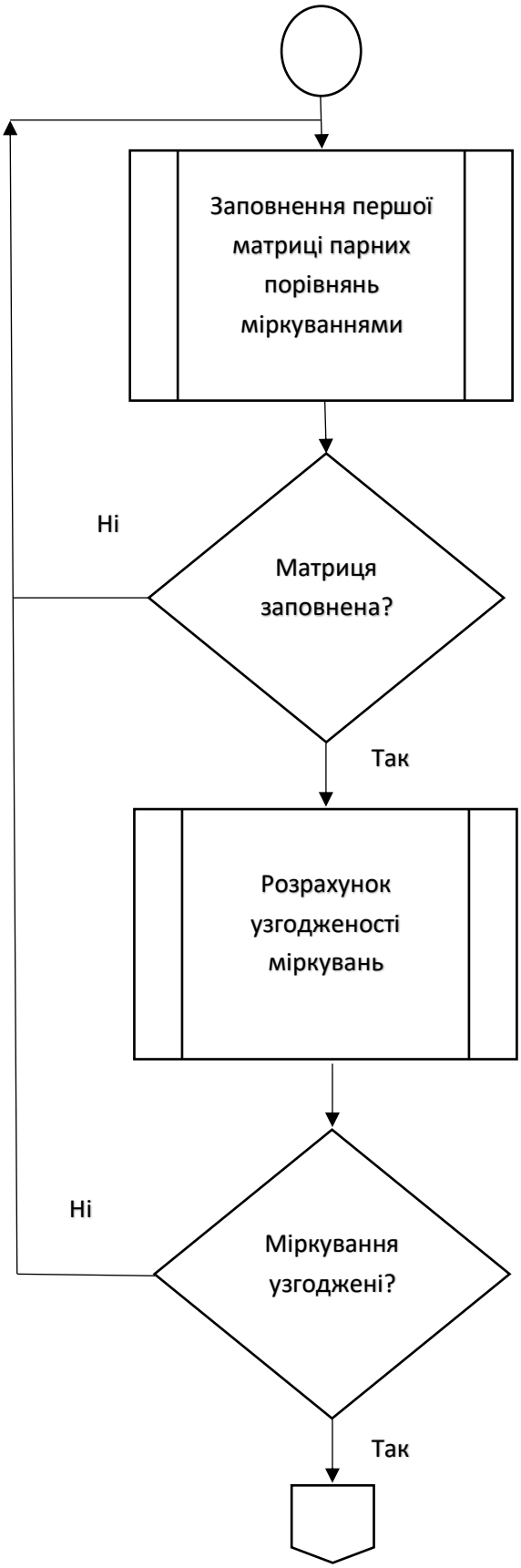


Рисунок 2.5 - Алгоритм оцінки ризику виникнення надзвичайної ситуації на окремо взятому ОКІ з використанням ГІС технологій


Початок
Формування альтернативного сценарію виникнення НС
Опис рівня загрози для альтернативного сценарію виникнення НС
Сценарії сформовані ?
Ні
Так


Створення кластеру
Додавання елементу до кластеру
Елементів більше немає?
Ні
Так
Кластери створені?
Ні
Так


Заповнення першої матриці парних порівнянь міркуваннями
Матриця заповнена?
Ні
Так
Розрахунок узгодженості міркувань
Міркування узгоджені?
Ні
Так


Заповнення наступної матриці парних порівнянь міркуваннями
Матриця заповнена?
Ні
Так
Розрахунок узгодженості міркувань
Міркування узгоджені?
Ні
Так

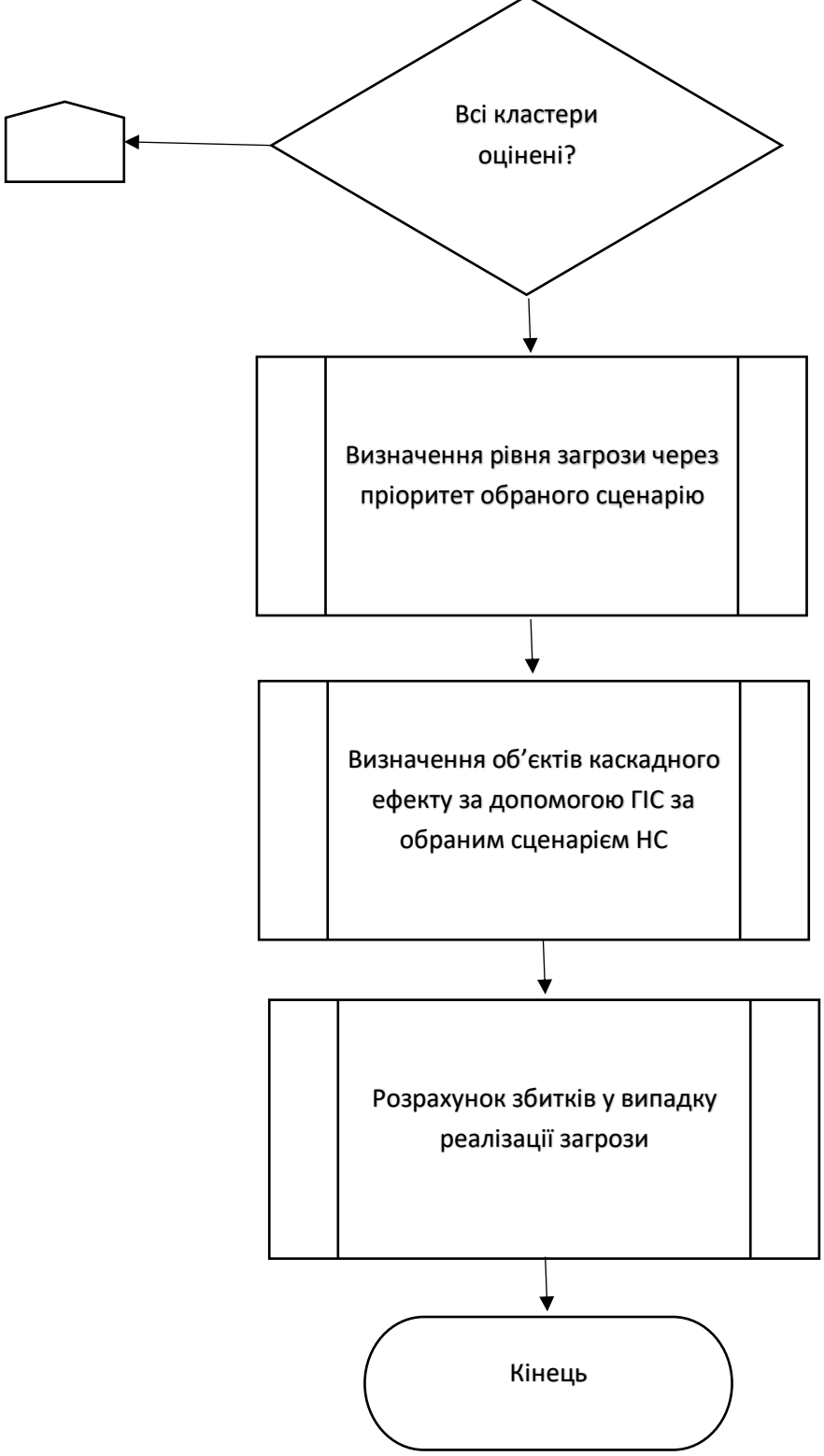


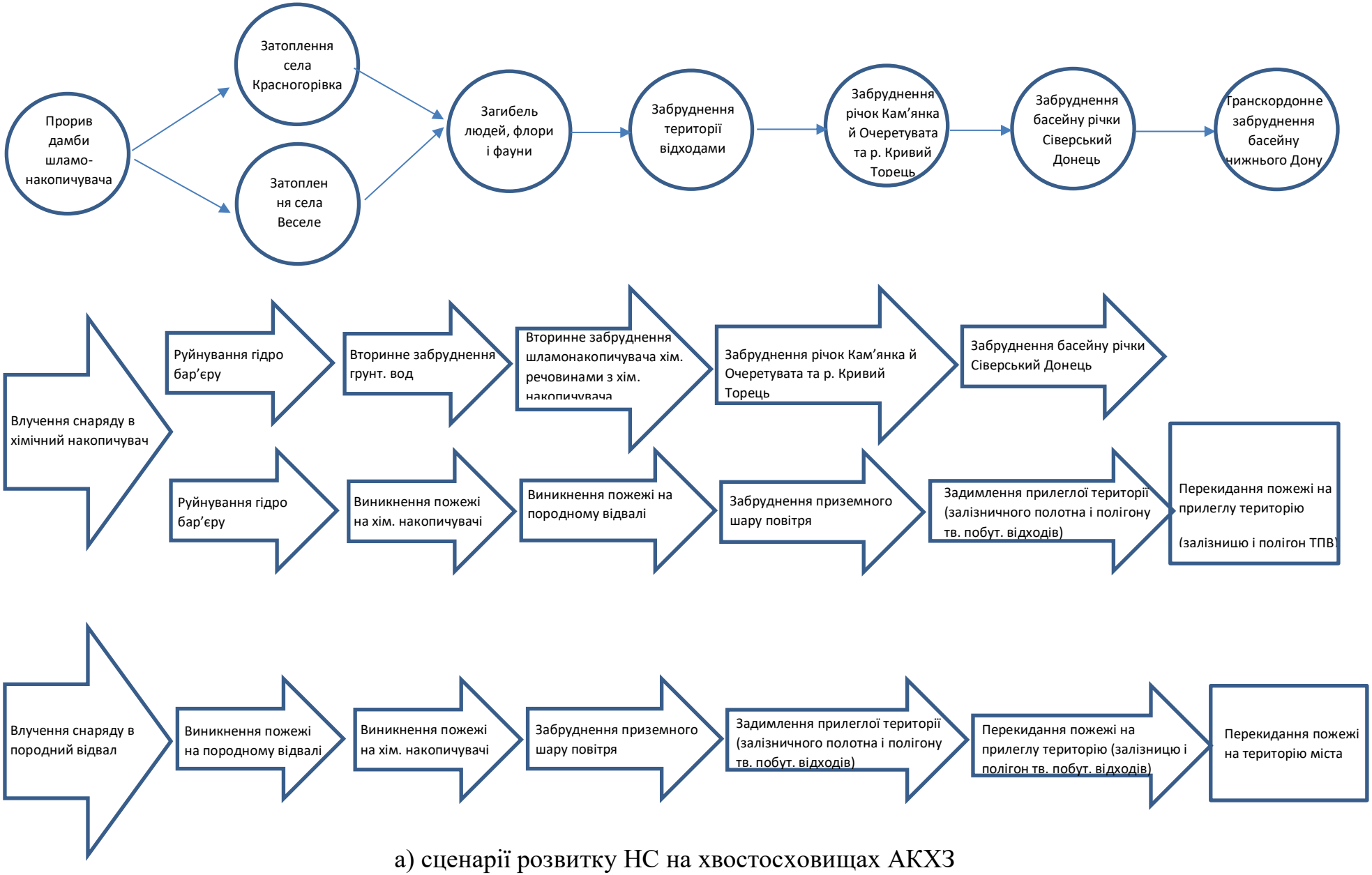
Рисунок 2.5 - Блок-схема алгоритму оцінювання загрози на об’єкті критичної інфраструктури з використанням ГІС-технологій

Для показу застосування ГІС технологій наведено приклад оцінювання воєнно-техногенних загроз для ОКІ (хвостосховищ) Авдіївського коксохімічного заводу (АКХЗ). Через розташування промислових потужностей ПРАТ «АКХЗ» неподалік лінії розмежування, завод неодноразово опинявся під обстрілами, а території промислових майданчиків було заміновано. Такі зовнішні чинники

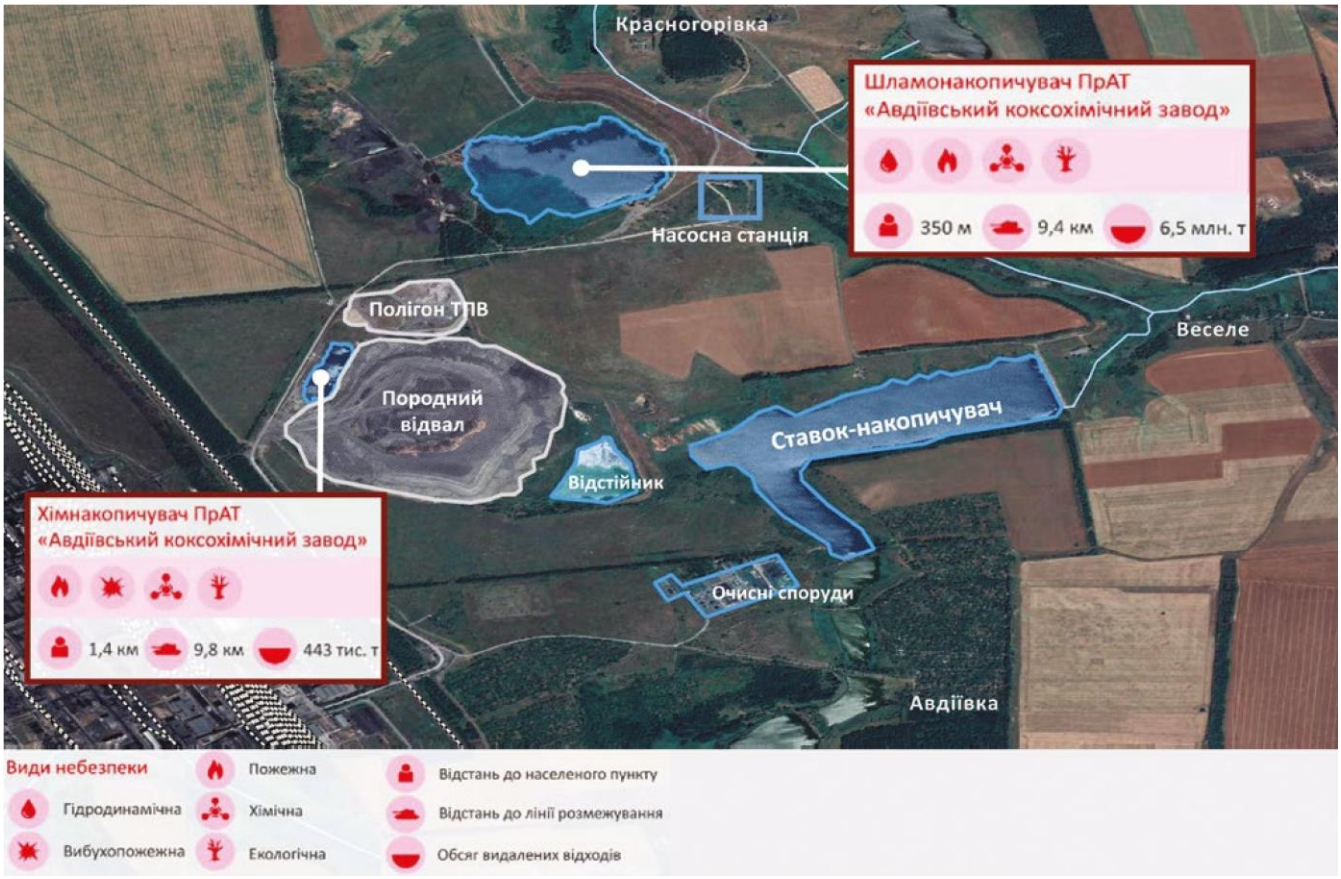
небезпеки військового характеру призвели до порушень в роботі підприємства та виникнення численних НС – за весь час збройного конфлікту на територію заводу впало сотні мін.

Було пошкоджено заводські будівлі та споруди, газові та паровідвідні трубопроводи, лінії електропередач. Крім того, істотної шкоди завдано рухомому залізничному складу і автопарку підприємства. АКХЗ зупинявся і запускався 15 разів, більше 200 разів було знеструмлено. Загинуло 12 працівників, і поранено більше 60 працівників заводу. В рамках дослідження виконано ідентифікацію та картування воєнно-техногенних загроз при ймовірних аварійних сценаріях на хвостосховищах з урахуванням розташування об’єктів у зоні ведення військових дій. Накопичувачі ПРАТ «АКХЗ» (хвостосховища), що містять вибухонебезпечні і токсичні речовини у складі відходів, та розташовані у зоні ведення БД, як джерело загрози становлять гідродинамічну, вибухопожежну, пожежну, хімічну та екологічну небезпеки з ефектом «доміно», особливо у зоні збройного конфлікту

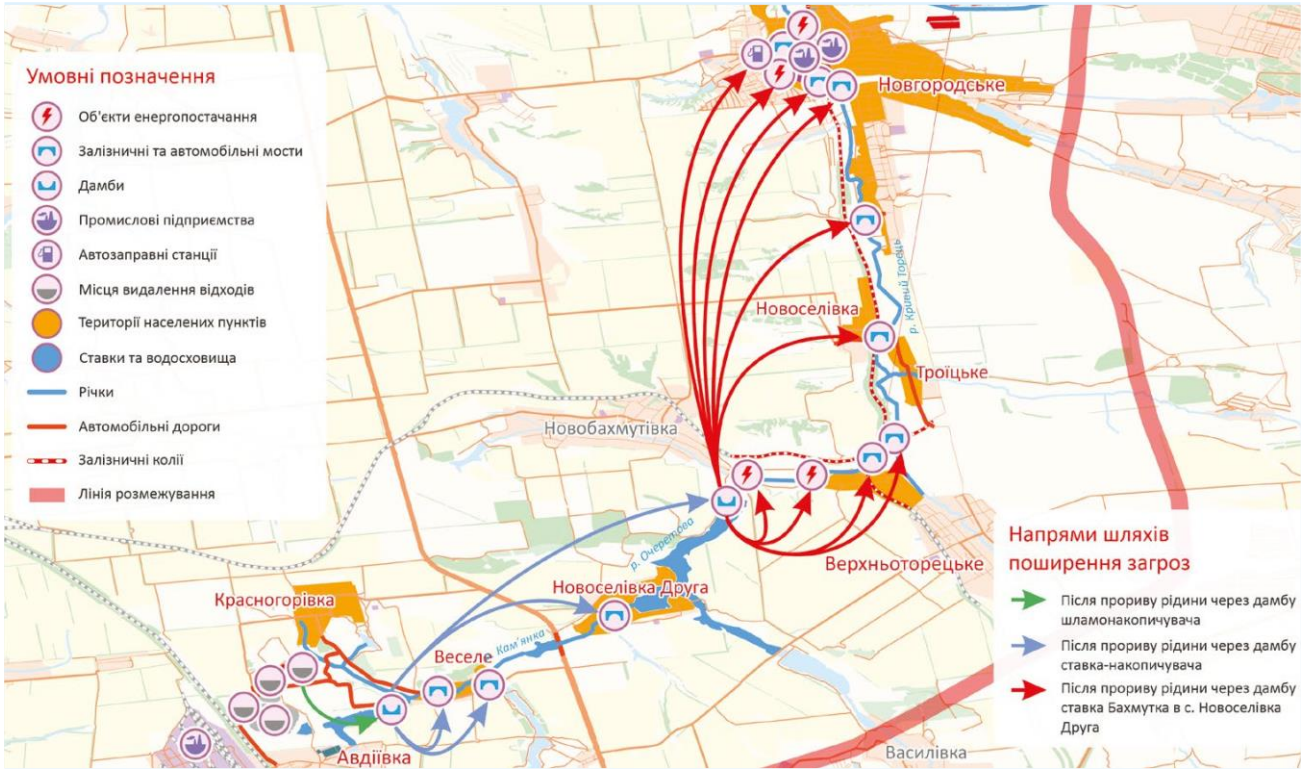
Результати оцінювання воєнно-техногенних загроз з визначенням каскадних доміно-ефектів для хвостосховищ АКХЗ наведено на рис. 2.6 (а, б, в).



а) сценарії розвитку НС на хвостосховищах АКХЗ



б) загальна обстановка та види небезпек на хвостосховищах АКХЗ;



в) сценарії розвитку ефектів «Доміно» у випадку ураження хвостосховищ АКХЗ

Рисунок 2.6 - Результати ГІС оцінювання загроз для ОКІ

Ці види небезпек можуть призвести до виникнення аварійних сценаріїв на накопичувачах, найбільш ймовірними серед яких є:

1) на шламонакопичувачі:

- виникнення пожежі;
- місцевий прорив рідини через дамбу;
- руйнування дамби з ефектом «доміно»;

2) на хімнакопичувачі:

- місцевий прорив або руйнування дамби;
- виникнення пожежі з ефектом «доміно».

Реалізація сценарію руйнування дамби шламонакопичувача може призвести до ефекту «доміно» – порушення цілісності споруд ставка-накопичувача, розташованого нижче за рельєфом, із подальшим забрудненням водних об'єктів (річки Скотовата (Кам'янка), Очеретова, Кривий Торець, Казенний Торець, Сіверський Донець), об'єктів ПЗФ (Балка «Кровецька»), пошкодженням елементів транспортних комунікацій (мостів, автомобільних доріг, залізничних колій), руйнуванням будівель житлового та виробничого призначення (с. Красногорівка, с. Веселе, с. Новоселівка Друга, смт. Верхньоторецьке, с. Троїцьке, с. Новоселівка, смт. Новгородське), виникненням аварій в електричних мережах (трансформаторні підстанції, ЛЕП).

Наявність біля хімнакопичувача породного відвалу та полігону ТПВ створює потенційну загрозу виникнення ефекту «доміно»: при загорянні рідини у хімнакопичувачі у тому числі через потрапляння снаряду, що зумовлено вогненебезпечними властивостями речовин у складі відходів, існує ймовірність перенесення аварійного сценарію «виникнення пожежі» на породний відвал та полігон ТПВ.

У разі настання вище перелічених аварій, поширення загроз через підземні та поверхневі води, ґрунти, атмосферне повітря призведе до отруєння компонентів природного середовища, затоплення територій, руйнування житлових і промислових будівель населених пунктів та елементів транспортної

інфраструктури. За розрахунками експертів Сіверсько-Донецького БУВР час добігання забруднюючих речовин від накопичувачів до питного водозабору складе 14-15 діб [66].

2.4. Процедура оцінювання ризиків і загроз на об’єктах критичної інфраструктури

Найбільш освоєні на сьогодні методи розв'язку прикладних задач спираються на добре формалізовані алгоритми, які отримані в результаті побудови математичних моделей окремих процесів. Але в практичній діяльності багато задач відносяться до таких, що важко формалізуються, для них невідомі аналітичні залежності або послідовність дій, що приводять до отримання результатів без інтелектуального втручання людини. Тому використання сукупності методів, зокрема системного аналізу, експертних оцінок для оцінки рівнів потенційної небезпеки виникнення надзвичайних ситуацій воєнно-техногенного характеру на окремих територіях Донецької та Луганської області, де ведуться БД, представляється перспективним.

Викладений нижче методичний підхід дає можливість працювати з неповною інформацією, разом з широким колом кількісних характеристик техногенної та природної небезпеки враховувати і якісні, тобто такі, що не мають безпосередньої числової оцінки, дозволяє легко реалізувати обчислення вагових коефіцієнтів окремих чинників, які впливають на воєнно-техногенну безпеку ЗС України та безпеку життєдіяльності населення, що проживає на цих територіях.

Він складається із трьох основних етапів:

1.Системний аналіз та структуризація проблеми техногенної та природної небезпеки;

2.Визначення комплексних показників потенційної небезпеки східних регіонів держави щодо виникнення техногенних та природних надзвичайних ситуацій;

3.Розрахунок інтегральних показників небезпеки виникнення надзвичайних ситуацій на основі комплексних показників потенційної небезпеки територій, індивідуального ризику смерті та матеріального збитку.

Виходячи з вищенаведеного визначення загрози, можна говорити, що кожна задача, яка виконується на тому чи іншому військовому об'єкті під час ведення БД, є різномасштабною техногенною загрозою для НПС, населення, особового складу ЗС України, ОКІ, ПНО й ОПН. В зв'язку з цим, процедуру екологічної оцінки БД на ОКІ можна побудувати як оцінку воєнно-техногенних загроз від ведення БД в районах проведення ООС.

Для виконання вимоги повноти і всебічності існує вже випробуваний спосіб: використання достатньо повної моделі воєнно-техногенної загрози від ведення БД в операційних зонах і районах. В зв'язку з тим, що кожен елемент БД представляє собою складний організаційно-технічний захід з багатофакторним комплексним впливом на довкілля необхідно провести його декомпозицію на послідовність окремих елементів, доступних для оцінки [67, 68].

Для формування логіко-інформаційної моделі БД застосуємо метод декомпозиції, який дозволяє виділити його окремі типові складові та зобразити їх у вигляді "ієрархічного дерева подій" [67-69]. Логіко-інформаційна модель ведення БД в операційних зонах та районах із використанням ієрархічного дерева елементарних подій може бути представлена у вигляді орієнтованого графа (орграфа), який зображує їх послідовність і склад.

Склад вузлів орграфу характеризує ієрархічну підпорядкованість певних завдань БД та їх декомпозицію на елементарні події, вклад яких в загальну оцінку воєнно-техногенної загрози можна оцінити за допомогою кваліфікованих експертів. Після цього оцінка елементу БД здійснюється за окремими елементами вузлів орграфу.

Для проведення оцінки елементу БД показник обчислюється за такою формулою

$$O_{БД} = k_1 \cdot O^1_{БД} + k_2 \cdot O^2_{БД} + ... + k_L \cdot O^L_{БД}, \qquad (2.11)$$

$$\begin{cases} O^{1}_{БД} = k_{11} \cdot O^{11}_{БД} + k_{12} \cdot O^{12}_{БД}, \\ O^{2}_{БД} = k_{21} \cdot O^{21}_{БД} + ... + k_{2K} \cdot O^{2K}_{БД}, \\ ... \\ O^{L}_{БД} = k_{L1} \cdot O^{L1}_{БД} + ... + k_{LN} \cdot O^{LN}_{БД}, \end{cases} \quad (2.12)$$

$$\begin{cases} O^{11}_{БД} = k_{111} \cdot O^{111}_{БД} + k_{112} \cdot O^{112}_{БД}, \\ O^{12}_{БД} = k_{121} \cdot O^{121}_{БД} + k_{122} \cdot O^{122}_{БД}, \\ ..., \\ O^{LN}_{БД} = k_{LN1} \cdot O^{LN1}_{БД} + k_{LN2} \cdot O^{LN2}_{БД}, \end{cases} \quad (2.13)$$

де $0 < k_i < 1$ − вагові коефіцієнти, для яких виконується правило нормування.

Задачу визначення вагових коефіцієнтів можна вирішити експертним шляхом (за рахунок використання процедур методу аналізу ієрархій чи ін.) [60, 69 - 72].

Інтегральна бальна оцінка отримується методом кумулятивного накопичення оцінок складових елементів БД із врахуванням ваги кожного компоненту на певному рівні орграфу

$$O_{БД} = k_1 \cdot (k_{11} \cdot (k_{111} \cdot O^{111}_{БД} + k_{112} \cdot O^{112}_{БД}) + k_{12} \cdot (k_{121} \cdot O^{121}_{БД} + k_{122} \cdot O^{122}_{БД})) + \\ + ... + k_L \cdot (k_{L1} \cdot (k_{L11} \cdot O^{L11}_{БД} + k_{L12} \cdot O^{L12}_{БД}) + ... + k_{LN} \cdot (k_{LN1} \cdot O^{LN1}_{БД} + k_{LN2} \cdot O^{LN2}_{БД})). \quad (2.14)$$

Задача оцінки та ранжування воєнно-техногенних загроз і ризиків в умовах невизначеності розв'язується методами системного аналізу з використанням багатокритеріальної оцінки воєнно-техногенних загроз і ризиків [73, 43]. Для оцінки і ранжування воєнно-техногенних загроз і ризиків слід сформувати критерії не тільки в значенні “критеріальна функція”, а в ширшому значенні - як спосіб оцінки і порівняння воєнно-техногенних загроз і ризиків .

Для оцінки можливих екологічних воєнно-техногенних загроз і ризиків існує ряд підходів. В країнах Євросоюзу активно впроваджується системний підхід , що спирається на оцінювання природно-техногенних загроз і ризиків з використанням декількох критеріїв [43, 74].

Випадки, коли єдиний критерій вдало відображає мету оцінки воєнно-техногенних загроз і ризиків, швидше виключення, ніж правило. Один критерій

лише приблизно (як і всяка модель) відображає мету оцінки і його адекватність. Вирішення задачі підвищення адекватності полягає не тільки в пошуку адекватнішого критерію (можливо, він і не існує), але й у використанні декількох критеріїв, що описують різносторонньо мету оцінки воєнно-техногенних загроз і ризиків і доповнюють один одного.

Об’єктивність вирішення задачі оцінки і ранжування обумовлюється забезпеченням критеріями достатньо повного ланцюга оцінки ознак воєнно-техногенних загроз і ризиків. Це означає, що критерії описують всі важливі аспекти мети оцінки, але при цьому доцільно мінімізувати їх число. Остання вимога задовольняється, якщо критерії є незалежними, не пов'язані між собою (наприклад, бажано не використовувати в різних складових критеріях однакові вимірювані величини або величини, які виводяться одна з одної тощо).

Метод оцінки і ранжування воєнно-техногенних загроз і ризиків використовує прийоми обчислення бальних оцінок різних чинників, що характеризують окремі складові конкретних критеріїв [73, 43].

Ієрархічна структура критеріїв і чинників наведені на рисунку 2.7.

Узагальнена процедура комплексної оцінки базується на підходах багатокритеріальної оцінки воєнно-техногенних загроз і ризиків з подальшою згорткою її до інтегрального індексу.

Як правило, вона набуває практичного сенсу лише в тому випадку, коли використовується такий метод, при якому багатокритеріальна задача зводиться до однокритеріальної. Проте очевидні переваги об'єднання декількох критеріїв в один суперкритерій супроводжуються деякими труднощами і недоліками, які необхідно враховувати при використанні цього методу.

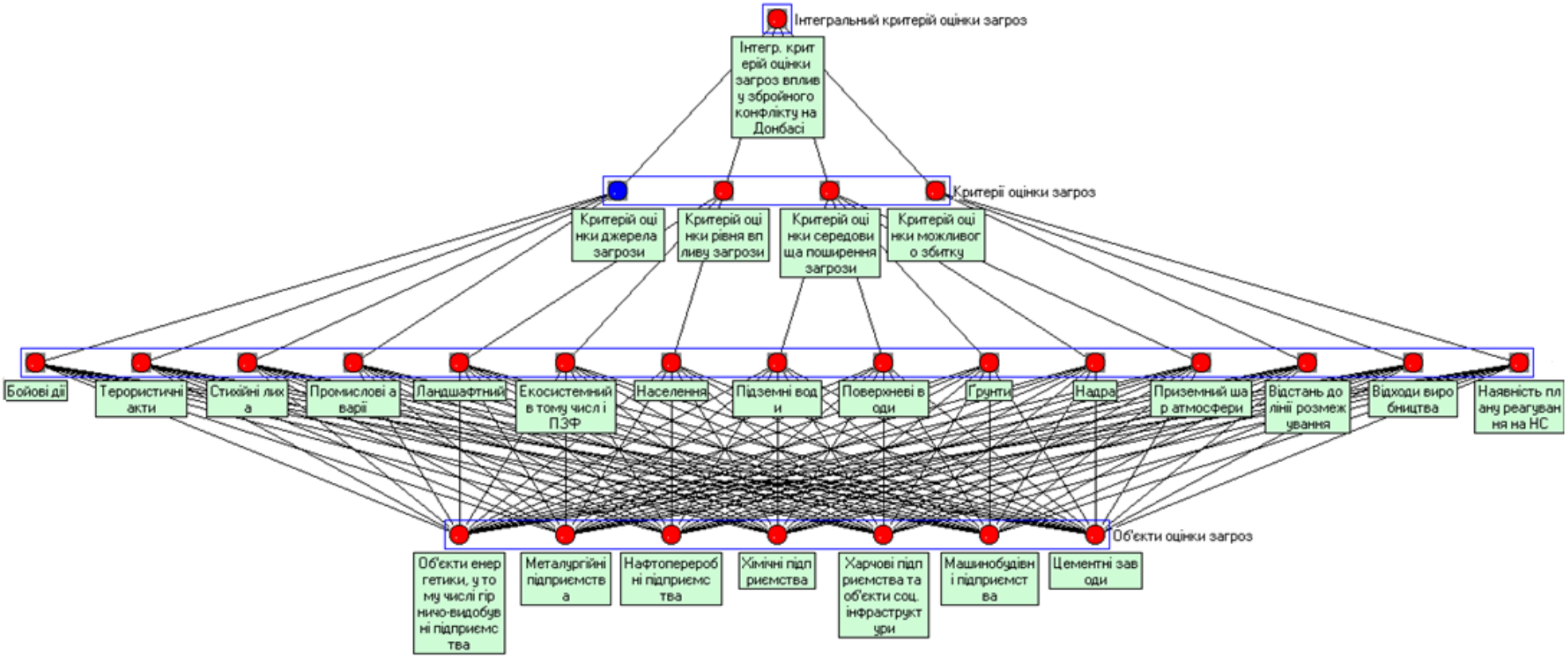


Рисунок 2.7- Ієрархічне дерево критеріїв і чинників оцінки і ранжування воєнно-техногенних загроз і ризиків

Керуючись підходом наведеним у публікації [75], узагальнені адитивну та мультиплікативні цільові функції можна представити у вигляді

$$J_{\Sigma}(e) = \sum_{i=1}^{n} \frac{\alpha_i}{s_i} J_i(e_i), \tag{2.15}$$

де α_i і s_i − вагові коефіцієнти, які можуть визначатися експертним шляхом, наприклад за допомогою процедур MAI.

У цих формулах коефіцієнти α_i відображають відносний внесок складових критеріїв в інтегральний, а коефіцієнти s_i забезпечують оцінку інформативності складових критеріїв. Узагальнені вагові коефіцієнти можуть бути визначені експертним шляхом (через процедури методу аналізу ієрархій тощо) [60, 70]. Кожен частковий критерій J_i складається з множини чинників f_{ij}. Для отримання експертних оцінок відповідних впливів ведення БД експерти заповнюють анкети, в яких присвоюють відповідні оцінки ознакам чинників e_i, значення яких можна зафіксувати в бальній шкалі, що відповідає бальній шкалі MAI.

Алгоритм цього методу стосовно оцінювання воєнно-техногенних загроз і ризиків в зоні збройного конфлікту на Донбасі складається з таких етапів.

1. Визначення цілі (фокусу) проблеми оцінювання екологічних воєнно-техногенних загроз і ризиків і ризиків в зоні збройного конфлікту на Донбасі.

2. Системний аналіз та структуризація проблеми оцінювання воєнно-техногенних загроз і ризиків в зоні збройного конфлікту на Донбасі у вигляді ієрархічної моделі, що включає критерії, чинники оцінки та об’єкти оцінки воєнно-техногенних загроз і ризиків .

3. Формування бази даних характеристик критеріїв, чинників та об’єктів оцінки воєнно-техногенних загроз і ризиків в зоні збройного конфлікту на Донбасі.

Складові елементи бази даних характеристик критеріїв, чинників та об’єктів оцінки наведено у таблиці 2.1.

4. Заповнення матриць попарних порівнянь елементів кожного рівня групою експертів, до складу якої входить системний аналітик, проводиться відповідно до таблиці 2.2.

Таблиця 2.2 – Узагальнена матриця попарних порівнянь елементів кожного рівня, відповідно до рисунку 2.2

Чинники	y_1	y_2	…	y_j	…	y_n
y_1	1	$a_1 : a_2$	…	$a_1 : a_j$	…	$a_1 : a_n$
y_2	$a_2 : a_1$	1	…	$a_2 : a_j$	…	$a_2 : a_n$
…	…	…	1	…	…	…
y_i	$a_i : a_1$	$a_i : a_2$	…	$a_i : a_j$	…	$a_i : a_n$
…	…	…	…	…	1	…
y_n	$a_n : a_1$	$a_n : a_2$	…	$a_n : a_j$	…	1

Експерт заповнює клітини таблиці 2.2. Порівняння фактору самого з собою дає одиницю. У першій клітині першого рядка експерт пише одиницю, в другій – результат порівняння першого фактору з другим (оцінку a_{12}), в третій – результат порівняння першого фактору з третім (оцінку a_{13}) тощо. переходячи до другого рядка, експерт записує в першій клітині результат порівняння другого фактору з першим (оцінку a_{21}), в другій – одиницю, в третій – результат порівняння другого фактору з третім (оцінку a_{23}) тощо.

5. Визначення власних векторів матриць попарних порівнянь та їх нормування. Дані таких таблиць, отриманих від m експертів, зводяться в одну загальну таблицю або матрицю порівнянь, у кожній клітинці якої *ij* стоїть число a_{ij}, яке дорівнює кількості оцінок переваги *i*-го фактору над *j*-м, отриманих від усіх *m* експертів.

Сума чисел a_{ij} по рядках з наступним діленням на *m* дає середню ранжировку фактору y_i, яка являє собою показник узагальненої думки щодо важливості чинників (чим більша сума *i*-го рядка, тим більш важливе значення має *i*-й фактор). Щодо суми по стовпцях має місце обернена картина. Послідовність рангів чинників

будується у порядку зменшення середніх сум по рядках $a_i = \frac{1}{m}\sum_{j=1}^{n} a_{ij}$ або у порядку середніх сум по стовпцях загальної матриці порівнянь $a_j = \frac{1}{m}\sum_{i=1}^{n} a_{ij}$. Ранг фактора, як і в методі шкальних оцінок, визначається його порядковим номером. Для цього порівнюються суми балів кожного рядка. Найбільшій сумі балів виставляється 1-й ранг (чинник найбільше впливає на розглядуваний процес). Далі виставляються ранги 2, 3, …, *n* у міру зменшення суми балів.

Середня оцінка балів, дисперсія цієї оцінки та інші показники визначаються за формулами, які використовуються для методу шкальних оцінок.

6. Оцінка узгодженості суджень експертів на основі відношення узгодженості. Після проведення всіх попарних порівнянь визначається індекс узгодженості (ІУ) і відношення узгодженості (ВУ). Індекс узгодженості (ІУ), який дає інформацію про порушення числової та транзитивної матриці порівнянь, є важливим елементом даної моделі визначення вагових коефіцієнтів. Тому цей індекс можна розглядати як показник “близькості до узгодженості”. Тобто похибки співвідношень $a_{ik} = a_{ij} \cdot a_{jk}$, $k = \overline{1,n}$, $i = \overline{1,n}$, $j = \overline{1,n}$.

Для ІУ має місце наступна формула:

$$IУ = \frac{\lambda_{\max} - n}{n-1}, \tag{2.16}$$

де n– число порівнюваних елементів.

Для обернено симетричної матриці завжди

$$\lambda_{\max} \geq n$$

Далі порівнюють отриману величину ІУ із тією, що утворилася б при випадковому виборі кількісних порівнянь із шкали 1/9, 1/8, …, 1, 2, …, 9 з утворенням обернено симетричної матриці.

Якщо розділити ІУ на число, що відповідає середній випадковій узгодженості (СУ) матриці того ж порядку, одержимо відношення узгодженості (ВУ):

$$ВУ = \frac{ІУ}{СУ} \tag{2.17}$$

Розмір ВУ повинний бути порядку 10% або менше, щоб бути прийнятним. У деяких випадках можна припустити 20%, але не більше. Якщо ВУ виходить із цих меж, то експертам потрібно переглянути задачу спочатку і перевірити свої міркування щодо вагових коефіцієнтів.

7. Якщо матриці узгоджені, то виконують п. 8, якщо ні – то переходять до п. 4.

8. Визначення локальних і глобальних пріоритетів (вагових коефіцієнтів) кожного з елементів ієрархії. Пріоритети синтезуються, починаючи з другого рівня до низу. Локальні пріоритети перемножують на пріоритет відповідного елементу на вищестоящому рівні і підсумовують за кожним елементом відповідно до значень коефіцієнтів важливості чи пріоритетності кожного з елементів, на які він впливає у кожному рівні ієрархії.

Вектор пріоритетів воєнно-техногенних загроз і ризиків $P_{vp} = \{P_{vp1}, \ldots, P_{vpn}\}$, який складається із компонентів P_{vpij} $(i = \overline{1,n},\ j = \overline{1,3})$, є інтегральною оцінкою відповідної i-ої воєнно-техногенної загрози за відповідним j-м критерієм. Наприклад для 1-ої воєнно-техногенної загрози:

$$\begin{aligned} P_{vp11} &= k_1 \cdot \overline{a_{11}} + k_2 \cdot \overline{a_{12}} + k_3 \cdot \overline{a_{13}}, \\ P_{vp12} &= k_1 \cdot \overline{a_{21}} + k_2 \cdot \overline{a_{22}} + k_3 \cdot \overline{a_{23}}, \\ &\ldots \\ P_{vp1n} &= k_1 \cdot \overline{a_{n1}} + k_2 \cdot \overline{a_{n2}} + k_3 \cdot \overline{a_{n3}}. \end{aligned} \tag{2.18}$$

На основі обчисленого вектору пріоритетів P_{vpij} можна провести ранжування воєнно-техногенних загроз і ризиків за вибраним критерієм оцінки і скласти матрицю пріоритетів

$$P = \left(\begin{array}{c|ccccc|c} & 1 & 2 & 3 & \dots & L & \\ \hline x_1 & P_{vp_{11}} & P_{vp12} & P_{vp13} & \dots & P_{vp1L} & \\ \dots & \dots & \dots & \dots & \dots & \dots & \\ x_i & P_{vp_{i1}} & P_{vp_{i2}} & P_{vp_{i3}} & \dots & P_{vp_{iL}} & \\ \dots & \dots & \dots & \dots & \dots & \dots & \\ x_n & P_{vp_{n1}} & P_{vp_{n2}} & P_{vp_{n3}} & \dots & P_{vp_{nL}} & \\ \hline & & & & & & \end{array}\right). \qquad (2.19)$$

Бальна шкала є проміжною між порядковою та інтервальною. Тому при обробці бальних оцінок поступають таким чином. Якщо є впевненість, що всі експерти користуються єдиною бальною шкалою (однаково розуміють “ціну балу”), як це буває, наприклад, за наявності спеціальних еталонів, то бальна шкала наближається до інтервальної, і бальні оцінки обробляють як кількісні (а сама бальна шкала має велике число градацій). Тоді, відповідно до початкового допущення про те, що різниця у відповідях експертів пояснюється випадковими незалежними флуктуаціями щодо деяких “істинних” величин, для обробки даних оцінок можна використовувати звичні статистичні методи точкового оцінювання. Кожному об'єкту слід приписати середній бал

$$x_j = \frac{1}{m} \cdot \sum_{i=1}^{m} x_{ij}, \quad j = 1,2,...,n \qquad (2.20)$$

Оцінки приймаються як групові. При проведенні процедури комплексного оцінювання значення якісних і кількісних характеристик воєнно-техногенних загроз і ризиків проектуються на значення відповідних шкал − систем чисел визначеної послідовності чи інших елементів, прийнятих для виміру чи оцінювання яких-небудь величин, виявлення зв'язків і відносин між елементами. Аргументи цільової функції e_i, які є ознаками-чинниками в оцінках воєнно-техногенних загроз і ризиків за відповідними складовими критеріями, виражаються балами в безрозмірному вигляді за чотирьохбальною шкалою.

Після оцінки чинників обчислюють значення часткових критеріїв. За умови застосування адитивної цільової функції часткові критерії обчислюють за формулами:

критерій оцінки джерела воєнно-техногенних загроз і ризиків

$$J_1(e^1) = 0{,}549 \cdot e^1{}_1 + 0{,}209 \cdot e^1{}_2 + 0{,}131 \cdot e^1{}_3 + 0{,}111 \cdot e^1{}_4 \quad (2.21)$$

критерій оцінки рівня впливу воєнно-техногенних загроз і ризиків

$$J_2(e^2) = 0{,}336 \cdot e^2{}_1 + 0{,}59 \cdot e^2{}_2 + 0{,}504 \cdot e^2{}_3 \quad (2.22)$$

критерій оцінки середовища поширення воєнно-техногенних загроз і ризиків

$$J_3(e^3) = 0{,}351 \cdot e^3{}_1 + 0{,}289 \cdot e^3{}_2 + 0{,}178 \cdot e^3{}_3 + 0{,}101 \cdot e^3{}_4 + 0{,}08 \cdot e^3{}_5 \quad (2.23)$$

критерій оцінки можливого збитку від воєнно-техногенних загроз і ризиків

$$J_4(e^4) = 0{,}692 \cdot e^4{}_1 + 0{,}231 \cdot e^4{}_2 + 0{,}077 \cdot e^4{}_3 \quad (2.24)$$

інтегральний критерій оцінки воєнно-техногенних загроз і ризиків

$$J_\Sigma(e) = 0{,}525 \cdot J_1(e^1) + 0{,}305 \cdot J_2(e^2) + 0{,}086 \cdot J_3(e^3) + 0{,}085 \cdot J4(e^4) \quad (2.25)$$

Отже, при цьому підході задача оцінки воєнно-техногенних загроз і ризиків зводиться до порівняння отриманих бальних оцінок і ранжування їх за сукупністю часткових критеріїв чи інтегральним критерієм.

9. Визначення пріоритетних воєнно-техногенних загроз і ризиків в зоні збройного конфлікту на Донбасі та їх ранжування. Проводиться з використанням Microsoft Excel 2010.

10. Створення бази даних промислових об’єктів та об’єктів критичної інфраструктури в зоні збройного конфлікту на Донбасі за відповідними кластерами проводиться в Microsoft Excel 2010.

11. Створення відповідної форми в Microsoft Excel 2010 для проведення експертного оцінювання за відповідними кластерами.

12. Узагальнення та аналіз експертних оцінок воєнно-техногенних загроз і ризиків в зоні збройного конфлікту на Донбасі у вигляді діаграм додаток А.

2.5 Висновки до розділу 2

В розділі обґрунтовані показники оцінювання впливу чинників воєнного і промислового техногенезу на об’єктах критичної інфраструктури.

Аналіз воєнно-техногенних загроз дозволив виділити основні чинники: виявлення елементів загрози; аналіз та кількісний вимір загрози; визначення допустимого рівня загрози; заходи щодо запобігання аварій та катастроф, управління в умовах аварійних ситуацій, зниження рівня загрози.

Аналіз результатів оцінки загроз за інтегральним критерієм дає можливість виділення інтервалів оціночних значень та проведення ранжувань ОКІ за рівнем загроз.

Розроблений алгоритм оцінки ризику та блок схема виникнення надзвичайної ситуації на окремо взятому ОКІ з використанням геоінформаційних технологій (ГІС). Практичне впровадження алгоритму оцінювалось для ОКІ (хвостосховищ) Авдіївського коксохімічного заводу (АКХЗ) відповідно до розробленого сценарію.

РОЗДІЛ 3 ІНФОРМАЦІЙНО-АНАЛІТИЧНА СИСТЕМА ОЦІНЮВАННЯ ВОЄННО-ТЕХНОГЕННИХ ЗАГРОЗ І РИЗИКІВ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА СХОДІ УКРАЇНИ

Аналіз значимих воєнно-техногенних чинників, що істотно впливають на територіальну організацію соціально-економічних процесів і ефективність виробництва, дозволяють виділити вплив БД, як складовий елемент безпеки для життєдіяльності населення в промислово розвинутих регіонах Сходу України.

Підвищення рівня воєнно-техногенної безпеки за допомогою впровадження інформаційно-аналітичної системи оцінювання воєнно-техногенних загроз і ризиків для ОКІ в зоні проведення ООС дозволить побудувати сценарій і стратегії реагування на можливі НС в умовах гібридного збройного конфлікту. Основними складовими розробки цієї інформаційно-аналітичної системи є розробка процедур оцінювання воєнно-техногенних ризиків та деталізація алгоритму для підтримки управлінських рішень, починаючи від забезпечення достовірності необхідної інформації до побудови програмних засобів для оцінювання загроз і ризиків, що базуються на сучасних моделях і засобах аналізу та візуалізації даних.

3.1 Структура і функції інформаційно-аналітичної системи оцінювання воєнно-техногенних загроз і ризиків в зоні проведення ООС на Сході України

Функціонування потенційно-небезпечних ОКІ призводить до погіршення екологічного стану навколишнього середовища та підвищення воєнно-техногенних загроз і ризиків для ПНО і ОПН, для здоров'я військовослужбовців і населення, що проживає на прилеглих територіях. У рамках виправлення даної ситуації важливу роль відіграють механізми екологічного регулювання, оцінювання воєнно-техногенних загроз і ризиків, що направлені на попередження надзвичайних ситуацій, зменшення негативних наслідків впливу збройного конфлікту в зоні ООС на ОКІ.

Оцінювання загроз і ризиків являє собою багатоплановий, формалізований процес, який допомагає здійснювати пошук і реалізацію нових можливостей при змінах навколишнього середовища, формулювати ефективні стратегії та сценарії

розвитку ситуації. На рисунку 3.1 наведено концептуальну схему оцінювання воєнно-техногенних загроз і ризиків на ОКІ.

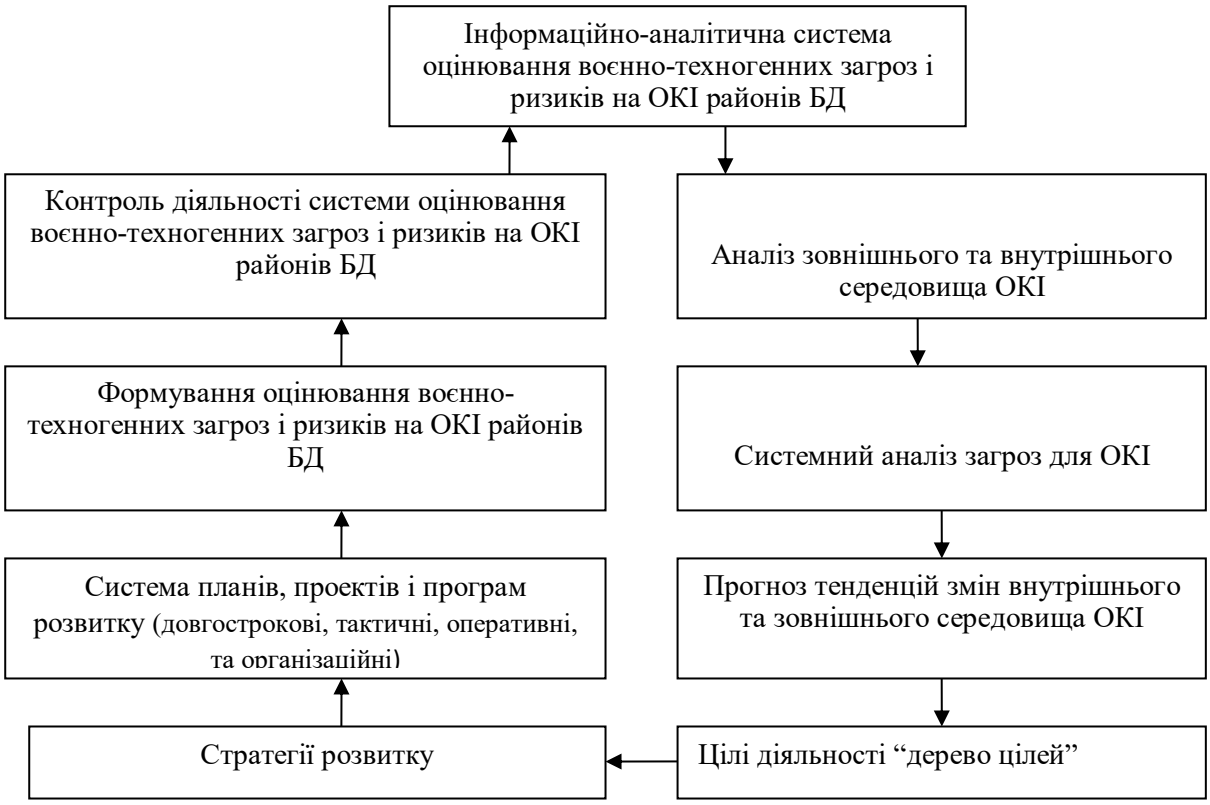


Рисунок 3.1 – Концептуальна схема оцінювання воєнно-техногенних загроз і ризиків на ОКІ районів БД

В основу експертних методів оцінювання покладено п’ять основних умов групового вибору рішень [76], а саме:

- універсальність, тобто наявність достатньої різноманітності можливостей вибору експертів та можливостей визначення для них індивідуальних профілів переваг;

- наявність позитивного зв’язку колективних та індивідуальних переваг, при якому відмова (або доповнення) від однієї альтернативи в індивідуальних перевагах окремого експерта не повинна змінити направленості переваги відносно колективної;

- незалежність непов’язаних альтернатив (якщо переваги кожного експерта однакові в кількох профілях, то й відповідні за альтернативами ступені переваг суспільства мають бути однакові для цих профілів);

- наявність суверенності експертів, тобто відсутність “нав’язаного” товариством ступеня переваг;

- відсутність диктаторства (як правило, з боку одного експерта, переваги якого визначають переваги товариства, а інші члени впливають на вибір альтернатив лише в тому разі, якщо ці альтернативи не мають ніякого значення для названого індивідуума).

Розробка сценаріїв може здійснюватися за допомогою наступних методів [77]:

1. Метод посилань. У цьому методі використовується система передумов, на базі яких створюються заключні висновки про можливості розвитку подій. Такими посиланнями (передумовами) можуть бути поточні тенденції, що поширюються на майбутнє. Недоліком цього підходу є те, що планове зменшення впливу негативних подій, яке потім відображується в стратегічних планах і програмах, призводить до надвитрат.

2. Метод системи діаграм. Цей метод був запропонований Акоффом Р. (1975 р.) як шлях визначення та формулювання стратегій. Використовуючи цей підхід, застосовують систему діаграм, які дають змогу описати стратегії координації та сценарії розвитку кожної з підсистем, що впливають на структуру та зміст стратегій.

3. Метод критичних полів (the critical site method), що базується на вивченні структури прийняття рішень у системі. Розробки сценаріїв ідентифікують ключові точки прийняття рішень, які допомагають у реструктуризації системи. Сценарії передбачають результати, яких треба очікувати та вплив цих результатів на майбутню систему загалом.

4. Метод “логіки можливого розвитку”. Цей метод використовується як додаток до інших методів. Згідно з ним розробник сценарію генерує різні альтернативи, базуючись на загальних чинниках розвитку.

5. Матриця перехресного впливу подій. Нерідко в сценарії треба передбачити розвиток взаємозалежних, але суперечливих подій, зв’язки між якими аналізуються в матричній формі, залучаючи експертні оцінки. Цей підхід дає змогу, виходячи з поглядів експертів, визначити ймовірність настання подій.

На практиці сценарії розвитку надзвичайної ситуації використовуються для формування попереджувальних заходів, розробки стратегічних планів і програм. Якість сценаріїв визначається за такими критеріями: змістовність, тобто показувати, як внутрішні суперечності процесів чи явищ впливають на формування прогресивних (негативних) тенденцій у системі (для якої сценарій складається), як можуть змінюватись кількісно та якісно характеристики цієї системи та результати її діяльності під впливом зовнішніх і внутрішніх чинників; достовірність, будь-який висновок мусить бути обґрунтований, побудований на достовірних припущеннях та інформації.

Для побудови інформаційно-аналітичної системи оцінювання воєнно-техногенних загроз і ризиків на Сході України згідно з обраними стратегіями необхідно: по-перше, визначити тип та обсяги необхідної інформації; по-друге, розробити ефективну систему збирання, обробки, використання та зберігання інформації; по-третє, вжити заходів для запобігання негативного ефекту використання недостовірної інформації; по-четверте, створити умови для ефективного використання необхідної інформації для прийняття рішень.

Обґрунтованість рішень, що приймаються, залежить від інформації, на якій вони базуються.

На рисунку 3.2 показано структурну схему інформаційно-аналітичної системи оцінювання воєнно-техногенних загроз і ризиків.

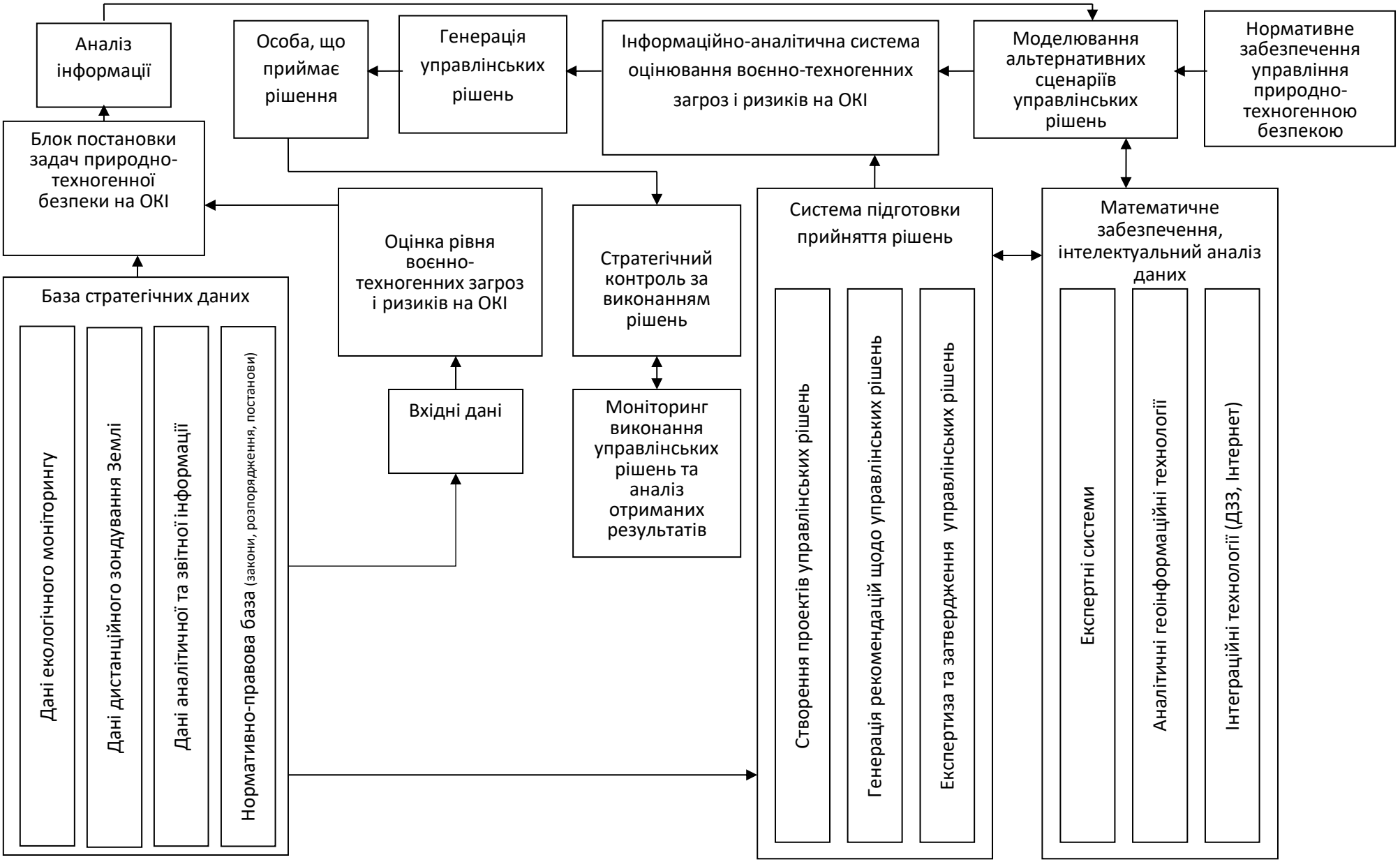


Рисунок 3.2 – Структурна схема ІАС оцінювання воєнно-техногенних загроз і ризиків на ОКІ

Діяльність в галузі природно-техногенної безпеки на Сході України потребує надійного інформаційного забезпечення у вигляді баз даних і прогнозів (БДП). Вони є основою для планування та управління і представляють стислий системний опис найсуттєвіших елементів. БДП використовуються для оцінки поточного стану природно-техногенної безпеки, для визначення прояву небезпечних процесів у майбутньому та для прийняття обґрунтованих управлінських рішень.

У БДП міститься інформація про вплив окремих складових і чинників процесу аналізу та управління на формування стратегічних альтернатив, а також інформація, що дозволяє обирати ті або інші рішення з визначених альтернативних варіантів, тобто БДП може трактуватись як підсистема підтримки прийняття рішень щодо оцінювання воєнно-техногенних загроз і ризиків. ІАС дає змогу:

- нагромаджувати інформацію про минуле й сучасне;

- складати прогнози розвитку подій;

- давати уявлення про реальний стан природно-техногенної безпеки в зоні проведення ООС за конкретний відрізок часу;

- відслідковувати події в навколишньому середовищі.

ІАС у стратегічному управлінні природно-техногенною безпекою може мати дворівневу ієрархічну структуру:

І рівень – підсистема стратегічної та прогнозної інформації, яка використовує текстову та кількісну інформацію, що надходить з усіх доступних джерел;

ІІ рівень – підсистема тактичної та оперативної інформації, що використовує дані аналізу оперативної обстановки в зоні ведення ООС, а також інформацію, отриману під час моніторингу із застосуванням БСМ, БПЛА та засобів ДЗЗ.

У межах ІАС можна досягти найбільшого поєднання контролю, координації, обліку та аналізу ОКІ, що дає можливість в ході виконання заходів попередження НС встановлювати та контролювати конкретні терміни стосовно робіт, які виконуються згідно них; постійно вирішувати питання щодо перерозподілу ресурсів, а також оцінювати результати ефективності прийнятих рішень. На основі результатів,

отриманих за допомогою обліку, можна приймати рішення про характер і напрямки змін, що здійснюються на ОКІ.

Головне призначення ІАС – за допомогою запровадження автоматизації і комп'ютерних технологій надати потрібну інформацію ОПР у необхідний термін.

3.2 Завдання, що вирішуються в сфері оцінювання воєнно-техногенних загроз і ризиків на ОКІ

В країнах, що входять до блоку НАТО, широке розповсюдження отримав системний підхід, який при оцінці життєвого циклу різного роду техноприродних систем спирається на поняття екологічного балансу [78].

На сьогоднішній день стан природно-техногенної безпеки в районі ведення БД [39], особливо в умовах військового конфлікту на Сході України, свідчить про наявність актуальної проблеми оцінювання воєнно-техногенних загроз і ризиків в місцях розташування ОКІ.

Це, в свою чергу, потребує створення інформаційно-аналітичних систем оцінювання воєнно-техногенних загроз і ризиків, що дозволить оперативно вирішувати питання в системі моніторингу та управління, зокрема, розвитку їх інформаційно-аналітичної складової. Комплексний підхід у вирішенні питань підвищення рівня природно-техногенної безпеки із застосуванням сучасних інформаційно-телекомунікаційних технологій в Збройних Силах України слід розглядати як необхідне підґрунтя для подальшого розвитку і удосконалення системи оцінювання екологічної обстановки в ЗС України.

Категорії серйозності загроз, представлені у табл. 3.1, встановлюють кількісне значення відносної серйозності ймовірних наслідків небезпечних надзвичайних ситуацій.

Таблиця 3.1 - Категорії серйозності загроз

Вид	Категорія	Опис нещасного випадку
Катастрофічна	I	Смерть або руйнування системи
Критична	II	Серйозна травма, стійке захворювання, суттєве пошкодження у системі

Гранична	III	Незначна травма, короткочасне захворювання, пошкодження у системі
Незначна	IV	Менш значні, ніж у категорії III, травми, захворювання, пошкодження у системі

Рівні ймовірності загрози, представлені у табл. 3.2, є якісним відображенням відносної ймовірності того, що відбудеться небажана надзвичайна ситуація, яка є наслідком неусуненої або непідконтрольної загрози для ОКІ. Звідси випливає, що коли потенційна загроза НС буде віднесена до категорії I (катастрофічна) з рівнем імовірності A (часта), то всі зусилля без сумнівів потрібно спрямовувати на виключення цієї загрози або забезпечити посилений контроль.

Таблиця 3.2 - Рівні ймовірності загрози

Вид	*Рівень*	*Опис наслідків*
Часта	A	Велика ймовірність того, що НС відбудеться
Можлива	B	НС може трапитися декілька разів за життєвий цикл
Випадкова	C	НС іноді може відбутися за життєвий цикл
Віддалена	D	Малоймовірна НС, але можлива подія протягом життєвого циклу
Неймовірна	E	Настільки малоймовірна НС, що можна припустити, що така загроза ніколи не відбудеться

Табл. 3.3 демонструє приклад матриці ризиків загрози, що включає елементи табл. 1 і 2 для того, щоб забезпечити ефективний інструмент для апроксимації припустимого та неприпустимого рівнів або ступенів ризику. Встановивши буквено-цифрову систему оцінки ризику, можна глибше класифікувати та оцінювати ризик за ступенем припустимості.

Таблиця 3.3 - Матриця оцінки ризику

Частота, з якою відбувається подія	*Категорія загрози*			
	I Катастрофічна	*II Критична*	*III Гранична*	*IV Незначна*
(A) Часта	1A	2A	3A	4A
(B) Можлива	1B	2B	3B	4B
(C) Випадкова	1C	2C	3C	4C
(D) Віддалена	1D	2D	3D	4D
(E) Неймовірна	1E	2E	3E	4E

3.3. Приклад експертної оцінки в інформаційно-аналітичній системі

можливих наслідків НС на об’єктах критичної інфраструктури життєзабезпечення внаслідок аварій в мережах енергопостачання на об’єктах ТОВ Луганського енергетичного об’єднання

На рис. 3.3 наведено приклад матриці ризиків виникнення НС за результатами проведеного експертного оцінювання воєнно-техногенних загроз для об’єктів критичної інфраструктури Луганської області внаслідок ураження системи електрозабезпечення в ОЗП.

Категорія загрози	Незначна	Гранична	Критична	Катастрофічна	Об'єкти ризик-аналізу
(A) Часта	4A	3A	2A	1A	ПНО та ОПН
					Безпека мереж енергопостачання
(B) Можлива	4B	3B	2B	1B	Безпека енергогенеруючих об'єктів (ТЕС, ТЕЦ)
					Забезпечення електроенергією та світлом населенни пунктів
(C) Випадкова	4C	3C	2C	1C	Комунальні об'єкти водопостачання та водовідведення
(D) Віддалена					Комунальні об'єкти теплопостачання
	4D	3D	2D	1D	Об'єкти забезпечення продовольчої безпеки
Очікувана ймовірність НС	0,252	0,408	0,698	0,966	

Рисунок 3.3 - Матриця ризиків виникнення НС на ОКІ в Луганській області в ОЗП

Відповідно до Указу Президента України від 16 січня №8/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» питання що стосуються захисту об’єктів енергетичної інфраструктури є пріоритетними в державі. Для проведення перевірки розробленого аналітичного

інструментарію було проведено експеримент з попередження НС на прикладі критичної інфраструктури електрозабезпечення ТОВ Луганського енергетичного об’єднання.

Як видно з рис. 3.3, за важливістю і значенням для держави, суспільства і національної безпеки одне з пріоритетних місць серед об’єктів критичної інфраструктури займають мережі електропостачання.

Аналіз цілого ряду публікацій [2,79]підтверджує, що в разі виходу з ладу мереж електропостачання виникають каскадні «доміно» - ефекти виходу з ладу інших, взаємозв’язаних з ними об’єктів критичної інфраструктури:

- системи водопостачання питної та технічної води;
- системи водовідведення;
- системи теплопостачання;
- системи транспортної інфраструктури;
- газотранспортної системи;
- системи забезпечення техногенної безпеки потенційно-небезпечних об’єктів (ПНО) та об’єктів підвищеної загрози (ОПН);
- системи електроживлення комунальних соціально-значимих об’єктів (школи, дитсадки, лікарні, бібліотеки, спорткомплекси);
- інформаційно-телекомунікаційної інфраструктури;
- системи цивільного захисту (ДСНС України).

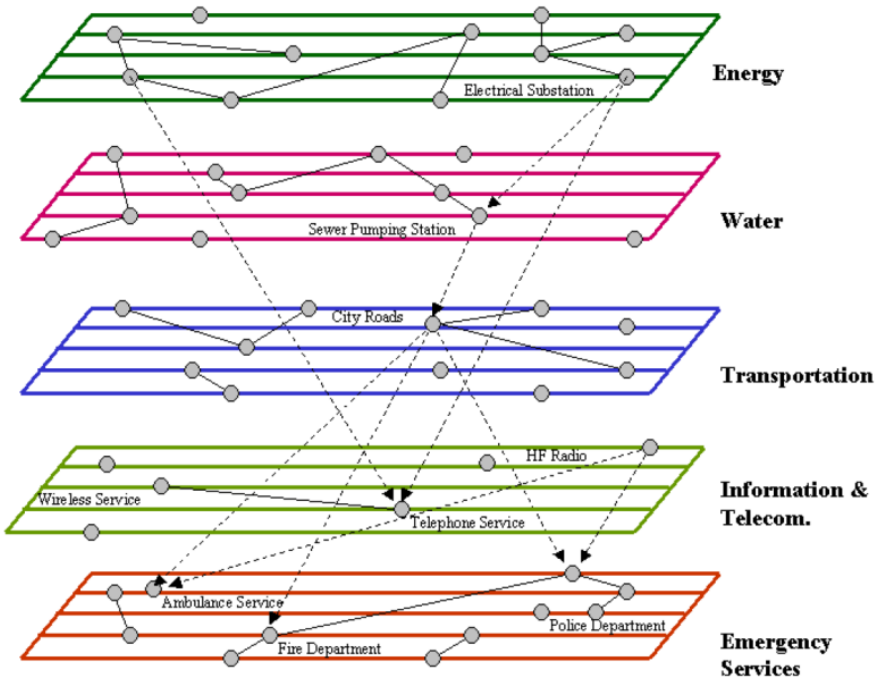


Рисунок 3.4 - Взаємозалежність елементів енергетичної, водопостачальної, транспортної, інформаційної та телекомунікаційної інфраструктури та екстрених служб [124].

На сьогоднішній день, порушення в роботі об’єктів енергопостачання луганської області, до яких відносяться енергетичні мережі ТОВ Луганського енергетичного об’єднання в осінньо-зимовий період (ОЗП) можуть призвести до надзвичайних ситуацій (НС) регіонального, місцевого та об’єктового рівня, що за своїми наслідками можуть значно перевищити наслідки НС в Алчевську (2006 рік) [80].

Для оцінки можливих загроз і ризиків виникнення НС на об’єктах критичної інфраструктури існує ряд підходів. В країнах Євросоюзу активно впроваджується системний підхід [46,73], що спирається на оцінювання загроз і ризиків НС з використанням декількох критеріїв.

Використовуючи європейські підходи до оцінювання загроз і ризиків виникнення НС на потенційно небезпечних об’єктах було запропоновано адитивну згортку зважених критеріїв, що спирається на методи підтримки прийняття рішень (метод аналізу ієрархій та метод аналітичних мереж) [81].

За числового визначення ризику техногенної аварії чи надзвичайної ситуації,

пов'язаної з людськими жертвами і збитками, завданими навколишньому середовищу, прогнозні експертні оцінки відбивають індивідуальне судження фахівців про перспективи розвитку аварії. Методи експертних оцінок засновані на мобілізації професійного досвіду та інтуїції фахівців-експертів. Такі методи оцінювання ризику використовують формальну теорію ухвалення рішень в умовах невизначеності.

У разі природних, техногенних і соціальних надзвичайних ситуацій центральною фігурою і суб'єктом ухвалення рішення виступає особа, яка приймає рішення (ОПР). Це може бути одна особа – індивідуальна ОПР або кілька осіб, які виробляють колективне рішення – групова ОПР. Слід зауважити, що індивідуальна ОПР – це не завжди одна фізична особа, оскільки часто роль індивідуальної ОПР може відігравати й колектив, який обстоює певні спільні інтереси, або юридична особа. Груповою ОПР, у свою чергу, може бути кілька груп осіб, якщо кожна з груп має ті чи інші власні інтереси та переваги.

Вважають, що ОПР – це керівник або керівний орган, який формулює проблему, відіграє вирішальну роль у виборі розв'язку і несе відповідальність за обране рішення. Для допомоги у пошуку рішення ОПР залучає експертів і консультантів, які є фахівцями певних предметних галузей, у тому числі з питань технології й організації процесів прийняття і впровадження рішень. Експерти й консультанти відповідають за обґрунтованість рекомендацій, які вони готують для ОПР, проте вони не підміняють ОПР у виборі рішення. Остаточне рішення завжди обирає ОПР відповідно до власної системи переваг (пріоритетів). ОПР несе повну відповідальність за свій вибір та його наслідки.

Використовуючи європейські підходи до оцінювання загроз і ризиків виникнення НС на потенційно небезпечних ОКІ було запропоновано адитивну згортку зважених критеріїв, що спирається на методи підтримки прийняття рішень (метод аналізу ієрархій та метод аналітичних мереж) [81].

Алгоритм цього методу складається з таких етапів.

1. Визначення цілі (фокусу) проблеми оцінювання загрози виникнення НС на об’єктах критичної інфраструктури енергозабезпечення Луганської області.

2. Системний аналіз та структуризація проблеми у вигляді ієрархічної моделі.

3. Формування бази даних характеристик критеріїв, факторів та загроз.

5. Заповнення матриць попарних порівнянь елементів кожного рівня групою експертів, до складу якої входить системний аналітик.

6. Визначення власних векторів матриць попарних порівнянь та їх нормування.

7. Оцінка узгодженості суджень експерта на основі відношення узгодженості.

8. Перевірка узгодженості матриць порівнянь. Якщо матриці узгоджені, то виконують п. 9, якщо ні – то переходять до п. 5.

9. Визначення локальних і глобальних пріоритетів (вагових коефіцієнтів) кожного з елементів ієрархії.

10. Визначення пріоритетних загроз та їх ранжування.

В якості критеріїв використано наступні:

1. Джерело виникнення загроз.

   Фактори оцінювання:

   1. Кібератаки;
   2. Бойові дії;
   3. Терористичні акти;
   4. Стихійні лиха;
   5. Технологічні відмови;

2. Умови виникнення загрози.

   Фактори оцінювання:

   1. Електромагнітні;
   2. Механічні;
   3. Температурні;

3. Тривалість дії загрози.

   Фактори оцінювання:

   1. Постійно діюче;
   2. Періодично діюче;
   3. Одноразове;

4. Рівень впливу загрози.

   Фактори оцінювання:

   1. Ландшафтний;
   2. Флористичний;
   3. Фауністичний;
   4. Промислові об'єкти;
   5. Соціальні об'єкти;
   6. Населення;
   7. Персонал підприємств;

5. Ступінь важкості загрози.

   Фактори оцінювання:

   1. Фатальні;
   2. Середньої ваги;
   3. Незначні;

6. Ступінь поширення загрози.

   Фактори оцінювання:

   1. Регіональне;
   2. Глобальне;
   3. Локальне;

7. Середовище поширення загрози.

   Фактори оцінювання:

   1. Ґрунтові води;
   2. Поверхневі води;
   3. Ґрунти;
   4. Надра.

Для проведення оцінювання загроз виникнення НС було розроблено інформаційно-аналітичну систему та проведено експертну оцінку за наступним ієрархічним деревом критеріїв та факторів оцінювання, що наведене на рис. 3.5. Для проведення оцінювання загроз методом парних порівнянь використовувалась інтервальна шкала Сааті .

Таблиця 3.4 - Шкала відносної важливості елементів

Ступінь важливості	Визначення	Пояснення і рекомендації щодо використання
1	Об'єкти рівноцінні	Обидва об'єкти рівноцінні між собою
3	Один об'єкт дещо переважає інший	Є певні підстави вважати перший об'єкт дещо кращим за інший
5	Один об'єкт значно кращий за інший	Є підстави вважати один об'єкт значно кращим за інший
7	Один об'єкт набагато кращий за інший	Є вагомі підстави вважати перший об'єкт набагато кращим за інший
9	Дуже велика перевага одного об'єкта над іншим	Перевага одного об'єкта порівняно з іншим дуже велика
2, 4, 6, 8	Значення, що відбивають проміжні судження	Використовують у випадках, коли вибір між двома сусідніми непарними числами спричинює ускладнення

Результати отриманих експертних оцінок наведено у вигляді стовпчастих діаграм в додатку Б.

Аварійна ситуація, що склалася на сьогодні в електропостачанні Луганської області підтверджує, що в існуючих умовах, пов’язаних з проведенням ООС, стабільність та надійність енергетичного забезпечення регіону знаходиться на низькому рівні, що потребує термінових та невідкладних рішень.

Найбільшу тривогу викликає невиконання заходів з підготовки обладнання електричних мереж до роботи в умовах осінньо-зимового максимуму електричного навантаження періоду 2019-2020 рр., в тому числі капітальних ремонтів обладнання електричних мереж.

Внаслідок припинення різниці перетоків електричної енергії з територіями, де органи державної влади України не здійснюють свої повноваження, суттєво знижена надійність електропостачання значної частини відповідальних споживачів ТОВ «ЛЕО» (вугільні, хімічні підприємства, соціально важливі та військові об’єкти). Для відновлення обладнання, що пошкоджено внаслідок ведення БД та відновлення надійності електропостачання відповідальних споживачів необхідно щонайменше 1,5 млрд. грн.

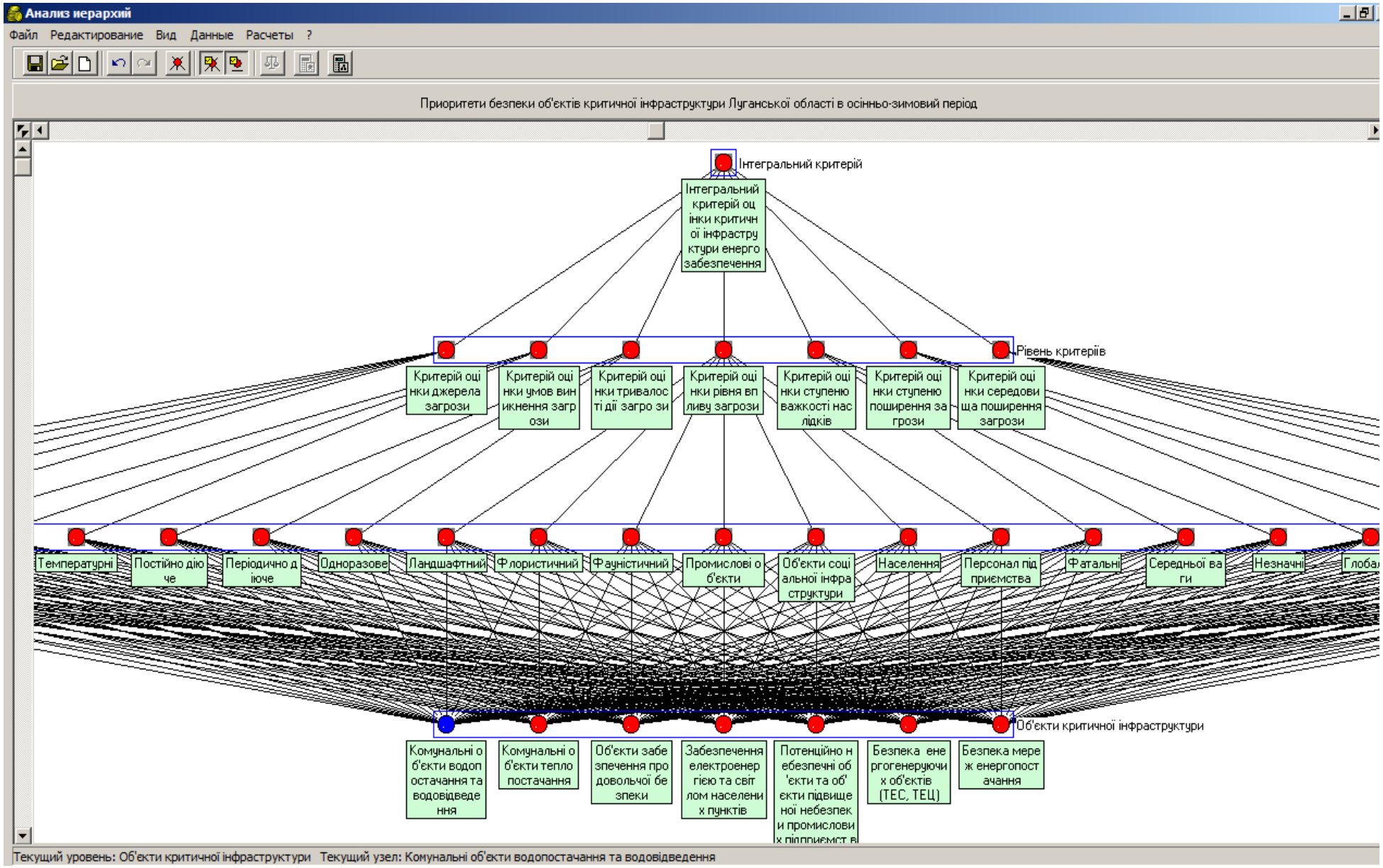


Рисунок 3.5 – Інформаційно-аналітична система оцінювання загроз для об’єктів критичної інфраструктури

Луганська область має критичну інфраструктуру життєзабезпечення населення, що включає до свого складу системи електро- і газопостачання, тепло- і електрогенеруючу мережу, транспортну інфраструктуру, інформаційно-телекомунікаційні мережі і т. ін. Однак за результатами експертно-аналітичного оцінювання стало ясно, що надійність даної системи не вище надійності самого ненадійного на сьогодні її елемента - системи електропостачання, ключовим вузлом якого в Луганській області є ТОВ «ЛЕО».

У якості прикладу можливих наслідків відключення енергопостачання на ключових об’єктах промислово-міських агломерацій (ПМА) слід навести наступні послідовності, що характерні для шахтарського регіону [82]: втрата енергопостачання – затоплення насосних установок шахт – некерований підйом рівня мінералізованих шахтних вод разом з вибухонебезпечними і токсичними газами до денної поверхні – підтоплення (затоплення) ПНО (ОКІ) - руйнування інженерно-технологічного комплексу шахти – розвиток небезпечних деформацій вуглепородного масиву (геологічного середовища) шахтного поля – – виникнення техногенних землетрусів, небезпечний вплив на прилеглі міста і селища внаслідок просідання земної поверхні - формування зсувів - руйнування інженерних, водопровідно-каналізаційних, газотранспортних та теплоенергетичних мереж - забруднення водозаборів для питно-господарчого водопостачання - заболочення місцевості - розвиток гострих і хронічних захворювань у місцевого населення та інші наслідки.

Систематизація наслідків цих НС для безпеки життєдіяльності населення має наступний вигляд [83]:

І. Психологічні наслідки

а) кризовий період:

1) стрес, шок;

2) неадекватна поведінка (паніка та інші поведінкові розлади);

3) співчуття;

4) альтруїстична взаємодопомога;

б) післякризовий період:

5) психічні розлади у постраждалих (тривожний стан, депресивні,

психовегетативні, астено-невротичні порушення);

6) “зациклення” постраждалих на власних проблемах;

7) розвиток комплексу жертви;

8) постійне співпереживання у колі постраждалих;

9) самозамикання соціумів потерпілих.

II. Медичні наслідки

а) кризовий період:

10) захворюваність виробничого персоналу, ліквідаторів і населення за рахунок травм, гострих отруєнь (у т.ч. сильно діючими отруйними речовинами - СДОР);

11) смертність персоналу, ліквідаторів і населення за рахунок травм, гострих отруєнь (у т.ч. СДОР);

б) післякризовий період:

12) зростання у постраждалих психосоматичних захворювань (виразки шлунку і 12-палої кишки, дискінезія жовчовивідних протоків, диспанкреатизм);

13) смертність опроміненого контингенту внаслідок радіогенних захворювань і передчасного старіння;

14) захворюваність постраждалих на хвороби, спричинені минулими травмами й отруєннями;

15) смертність постраждалих від віддалених наслідків травм і отруєнь;

16) захворюваність населення на інфекційні захворювання (у т.ч. на кишкові інфекції);

17) смертність населення від інфекційних захворювань (у т.ч. на кишкові інфекції).

III. Соціально-економічні наслідки

а) кризовий період:

18) втрата працездатності персоналом, ліквідаторами і населенням внаслідок аварії;

19) втрата роботи персоналом, ліквідаторами і населенням;

20) евакуація персоналу та населення з місць постійного проживання;

21) втрата майна й особистого господарства евакуйованими;

22) обмеження господарської діяльності на ураженій території;

23) дезорганізація місцевого господарства;

24) поширення мародерства;

25) пошкодження житла й інших споруд;

26) руйнування житла й інших споруд;

27) тимчасове припинення господарської діяльності на ураженій території;

28) знищення готової продукції;

29) забруднення джерел водопостачання;

30) тимчасове припинення теплопостачання під дією уражаючих чинників;

31) тимчасове припинення водопостачання;

32) забруднення водойм стічними водами;

33) тимчасове забруднення джерел водопостачання стічними водами;

б) післякризовий період:

34) зростання інвалідності серед ліквідаторів і постраждалого населення;

35) зростання безробіття серед ліквідаторів і постраждалого населення;

36) обмеження господарської та іншої діяльності на ураженій території;

37) зниження матеріального рівня життя й доходів колишніх ліквідаторів і постраждалого населення;

38) погіршення умов життєдіяльності ліквідаторів і постраждалого населення;

39) соціальна дизадаптація і маргіналізація постраждалих;

40) поширення безпритульних серед постраждалих;

41) зростання девіантної поведінки і злочинності серед постраждалих;

42) тривалі відновлювальні роботи;

43) значні витрати на відновлювальні роботи, реабілітацію ураженої території та поновлення виробництва.

За результатами експертного оцінювання із застосуванням методу аналізу ієрархій та матриці ризиків для випадку НС внаслідок відключення в електричних мережах ТОВ ЛЕО було розраховано ризики для Лисичансько-Сєвєродонецької ПМА, які наведено у табл. 3.5.

Аналізуючи схему електропостачання Луганської області слід зазначити, що

основними джерелами електропостачання Північної частини Луганської області були ЛуТЕС «ДТЕК Східенерго» і ПС 330 кВ Михайлівка, що забезпечує зв'язок з ПЛ-220 кВ з ПС: Ювілейна і Лисичанська Луганських МЕМ. ПС-330 кВ Михайлівка мала зв'язок з ПЛ-330 / 220кВ і вище з Вуглегірської ТЕС, Миронівської ТЕС, Луганської ТЕС, ПС Новодонбаська, Чайкіно, які забезпечували надійну схему мережі 220 кВ і вище, а також передачу необхідної потужності електроенергії по енерговузлах. ЛуТЕС «ДТЕК Східенерго» крім власної генерації мала зв'язок з ПЛ-220 кВ з ПС-330 Михайлівка, ПС-500 Перемога, що в свою чергу створювало надійну мережу для передачі потужностей електроенергії.

Станом на 09.10.2017 р. ПС-330 кВ Михайлівка не проводить електропостачання ПС-220 кВ: Ювілейна, Лисичанська (Бахмутські РЕЦ), ПС 35 / 110кВ Лисичанського РЕМ ТОВ «ЛЕО». ЛуТЕС «ДТЕК Східенерго» на даний момент часу забезпечує електропостачання Північної частини Луганської області по одній енерголінії - ПЛ-220 кВ ЛуТЕС -Лисичанська (навантаження літом до 200 МВт) до міст Сєвєродонецьк, Лисичанськ, Рубіжне, Гірське Лисичансько-Сєвєродонецької ПМА та міста Попасна, по мережі 110кВ по 5 приєднанням: Щастя, Петровська, Полив, Н.Айдарська, Н.Айдарська НПС (сумарна потужність до 40 МВт). Включені ВЛ-110 кВ Ювілейна-Бахмутська, Сватове-Курилівка забезпечують паралельну роботу ЛуТЕС «ДТЕК Східенерго», ТОВ «ЛЕО» з об’єднаною енергосистемою (ОЕС) України.

Таблиця 3.5 - Ризики виникнення НС на об’єктах критичної інфраструктури Лисичансько-Севєродонецької ПМА у одиницях уражених осіб на км^2

Об’єкти критичної інфраструктури	Кількість будинків	Кількість населення	Інтегральний ризик для населення ПМА, кількість уражених осіб/км^2
Електромережі	449275	485749	**188**
Комунальні водопроводи	53052	381231	106
Водопровідні мережі	52678	232775	66
Водопостачання загалом			**172**
Каналізаційна мережа	60493	259556	73
Насосні станції	45639	348802	97
Каналізаційна			**170**

система загалом			
ТЕЦ	1498	92155	15
Теплові мережі	2104	242524	40
Теплові пункти	198	65000	11
Котельні	2309	304900	50
Теплопостачання загалом			**116**

Факт відключення ПЛ-220кВ ЛуТЕС-Лисичанська під дією релейного захисту та автоматики призводить до відключення ПЛ-110кВ Ювілейна-Бахмутська, Сватове-Курилівка під дією ділильної автоматики. У разі виділення ЛуТЕС на збалансоване навантаження по мережі 110 кВ (по 5 вищевказаним приєднанням), що забезпечує електропостачання міст Щастя, Старобільськ і т.ін. північного регіону ТОВ «ЛЕО», для споживачів Лисичанського регіону повне знеструмлення міст Сєвєродонецьк, Лисичанськ, Рубіжне, Гірське, Попасна сумарно становить 141 населений пункт, 1656 ТП і 219125 кінцевих користувачів електроенергії. Під керівництвом диспетчера РДЦ Північного регіону НЕК Укренерго здійснюється подача напруги від ОЕС України по ВЛ-110 кВ Ювілейна-Бахмутська (Донецькобленерго (ДОЕ)) на шини 110 кВ ПС-220 кВ Ювілейна. Після синхронізації напруги ЛуТЕС з ОЕС України на ПС-220 кВ Ювілейна, під керівництвом диспетчера РДЦ Північного регіону НЕК «Укренерго» здійснюється відновлення електропостачання в першу чергу об'єктів соціального призначення, відповідно до дозволеної потужності.

У разі відключення турбогенераторів ЛуТЕС «ДТЕК Східенерго» при автоматичному відключенні вищевказаної ВЛ-220 кВ відбувається повне знеструмлення споживачів Північної частини Луганської області сумарно 531населенний пункт (4410 ТП-ЗТП). Диспетчер РДЦ Північного регіону НЕК «Укренерго» забезпечує подачу напруги на ЛуТЕС «ДТЕК Східенерго» для якнайшвидшого включення турбогенераторів, готує схему мережі 110 кВ для прийняття напруги, у міру появи генеруючих потужностей оперативний персонал ТОВ «ЛЕО» забезпечує відновлення електропостачання об'єктів соціального призначення, відповідно до наявних потужностей. При повному знеструмленими Північної частини Луганської області можливість і час подачі напруги на

першочергові об'єкти соціального призначення від ПС-110кВ Курилівка (Куп'янськ ЕС АК «Харківобленерго»), ПС-110 кВ Бахмутская (ДОЕ) буде задаватися в ході ліквідації аварійного режиму диспетчером РДЦ Північного регіону НЕК «Укренерго».

У доповіді щодо ситуації з правами людини в Україні Управління Верховного комісара Організації Об'єднаних Націй з прав людини за період з 16 травня – 15 серпня 2017 року зазначено наступне [84]. У червні «Луганське енергетичне об'єднання» (ЛЕО) – єдине підприємство, що забезпечує електроенергією у Луганську область – повідомило УВКПЛ про те, що воно не може продовжувати постачати електроенергію чи підтримувати електромережу через затримки із оплатою за раніше здійснені поставки електроенергії по обидва боки від лінії зіткнення, та відповідно борг, який воно накопичило перед державним енергетичним підприємством «Енергоринок». Щонайменше чотири водоканали в Луганській області накопичили великі борги перед ЛЕО за поставлену їм електроенергію. Як повідомлялося, фінансове становище ЛЕО погіршилося й у зв'язку з несанкціонованим та неоплачуваним під'єднанням до електричних мереж військових позицій та об'єктів. Як наслідок, ЛЕО почало відключати електрику водоканалам. Ця криза, а також часті прориви старих труб, призводять до обмеженого доступу до чистої питної води для приблизно 220 тисяч осіб по обидва боки від лінії зіткнення.

Вивчення існуючої системи енергозабезпечення Луганської області ТОВ ЛЕО показало, що вона є вразливою під діями природно-техногенних факторів, як то військові дії, диверсії, природно-кліматичні умови, технічний стан енергогенеруючого та енергопостачального обладнання, технічний стан енергомереж та підстанцій, можливостей оперативного реагування на зміни роботи в системах енергопостачання, відсутності/наявності резервних джерел енергопостачання і потребує ретельного технічного та технологічного обслуговування, зведення до мінімуму часу на діагностику роботи мереж та проведення ремонтних робіт і створення належних умов для її надійної експлуатації, що знайшло відображення в додатку Б.

Зазначимо, що через технологічне порушення в магістральних електричних

мережах у вересні 2017 року на ПЛ 220 кВ ЛуТЕС - Лисичанська Бахмутських МЕМ, сталося знеструмлення великої кількості споживачів, які заживлені від електричних мереж ТОВ «ЛЕО». Так з причин недостатньої кількості резервних джерел живлення та заниженого рівня надійності енергопостачання відбулося знеструмлення 120 населених пунктів Лисичансько-Сєвєродонецької промислово-міської агломерації (ПМА) (рис. 3.4), відключена потужність становила 150 МВт.

На сьогоднішній день тут знаходиться значна частина потенційно-небезпечних ОКІ та найбільш енергоємних виробництв цієї ПМА. Враховуючи 1-годинну та 30-ти кілометрову доступність населених пунктів до центрів агломерації, до складу Лисичансько-Сєвєродонецької ПМА входять 47 населених пунктів, у т.ч. 8 міст, 10 селищ міського типу та 29 сільських поселень. Цей промисловий регіон є найбільш техногенно-насиченим на підконтрольній території порівняно із північною частиною Луганської області.

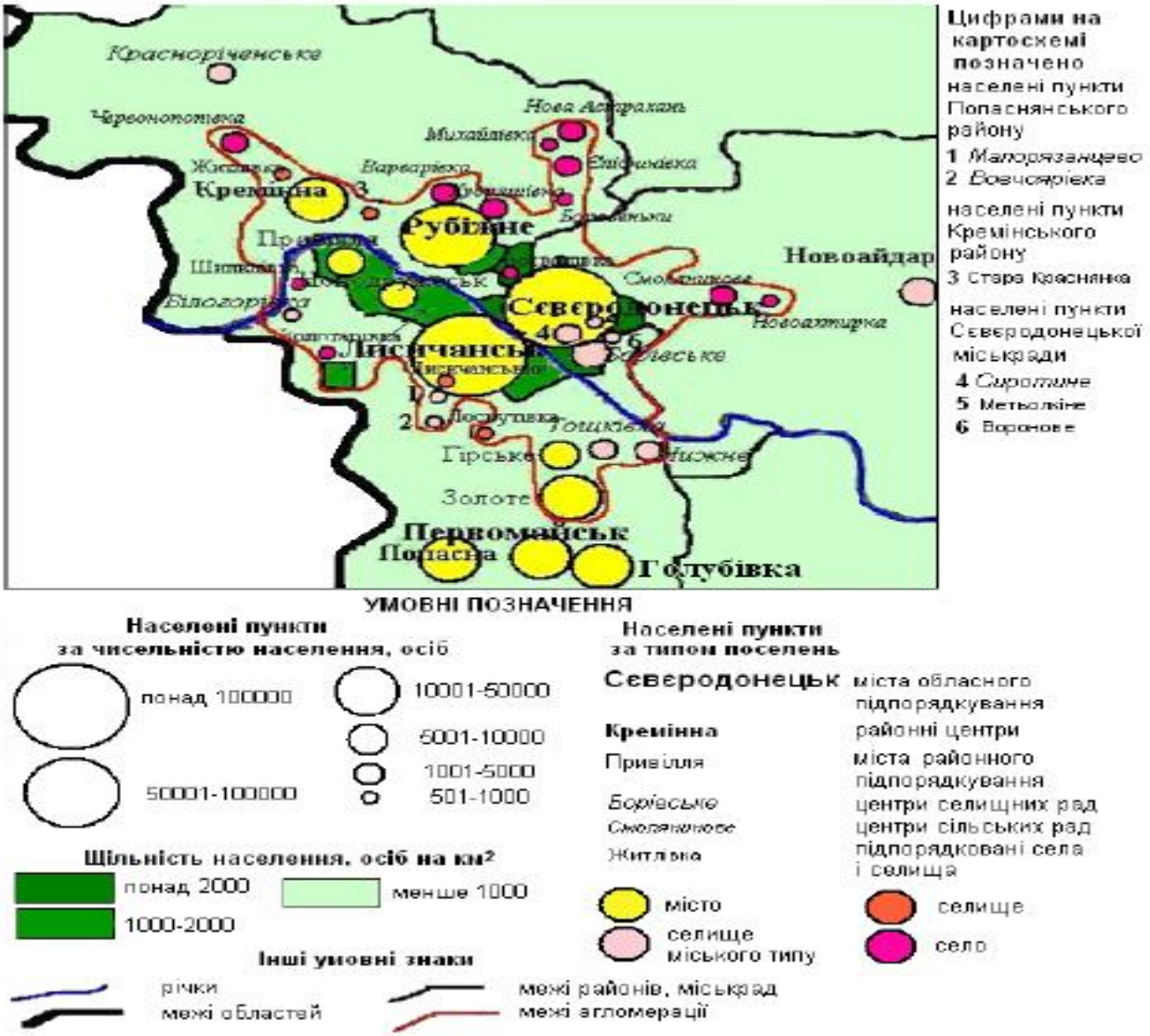


Рисунок 3.6 - Лисичансько-Сєвєродонецька міська агломерація

Лисичанський гірничо-промисловий район [6]

Ця частина Луганської області відноситься до Лисичанського гірничо-промислового району, в якому зосереджено 8 шахт: імені Д.Ф.Мельникова, імені Г.Г.Капустіна, «Привільнянська», «Новодружеська» ПАТ «Лисичанськвугілля»; «Золоте», «Карбоніт», «Тошківська», «Гірська» ДП «Первомайськвугілля»; водовідливні комплекси шахт «Кремінна», «Чорноморка» ДП «Укршахтгідрозахист».

Усі діючі шахти є небезпечними за викидами газовугільного пилу та метану. З метою контролю вмісту газу метану гірничі виробки обладнані спеціальними аналізаторами та вентиляційними установками, які забезпечують провітрювання горизонтів. Горизонти вугледобувних підприємств обладнані водовідливним комплексами, які забезпечують безпечне функціонування шахт та не допускають виходу шахтних вод на поверхню, перетікання на інші шахти.

Шахта «Привільнянська» ПАТ «Лисичанськвугілля»: 28.05.2016 на у магістральному уклоні пл. k_8 гор. 450 м сталася ендогенна пожежа, яку було локалізовано. Ведеться постійний моніторинг температури та вмісту повітря у виробках.

ВВК шахти «Чорноморка» обладнаний одним насосом. Існує заборгованість за спожиту електроенергію понад 6 млрд грн (постачальник Луганська філія ДП «Регіональні електричні мережі»). Виробки шахти пов’язані з виробками діючої шахти імені Д.Ф.Мельникова. У разі зупинки або поломки на ВВК існує загроза підтоплення шахти імені Д.Ф.Мельникова та території міста Лисичанська.

ВВК шахти «Кремінна» працює в штатному режимі. Існує заборгованість за спожиту електроенергію перед ТОВ «ЛЕО». 28.09.2016 припинено енергопостачання. На теперішній час на водовідливному комплексі шахти «Кремінна» перевищено критичний рівень затоплення, за інформацією райдержадміністрації підвальні приміщення домогосподарств та низини прилеглих

територій вже підтоплюються шахтними водами. Подальше обмеження енергопостачання може привести до підтоплення 212 га території, на яких розташовані житлові та адміністративні будівлі Кремінського району, а також перетікання шахтних вод до місцевого водозабору.

Шахта «Золоте» ДП «Первомайськвугілля». На початку 2015 року на шахті «Первомайська» (м. Первомайськ) виведений з роботи водовідливний комплекс (далі - ВВК), шахта повністю затоплена. Шахта гідрогеологічно зв'язана з шахтами С.М. Кірова, «Голубівська» (ОРЛО), «Родіна» (лінія розмежування) та діючою шахтою «Золоте», «Карбоніт», «Гірська» ДП «Первомайськвугілля» (контрольована територія). За підрахунками фахівців з 01.12.2016 вода почне перетікати на шахту «Родіна», а до 01.01.2017 – на горизонт 775 м шахти «Золоте», ВВК якої не розрахований на такий обсяг робіт. Для посилення ВВК необхідно за попередніми розрахунками 36-40 млн грн. (мінімальні обсяги).

Висновки до розділу 3

В розділі проведено аналіз значимих воєнно-техногенних чинників, що істотно впливають на територіальну організацію критичної інфраструктури. Це дозволило виділити вплив БД, як складовий елемент безпеки для життєдіяльності населення в східному регіоні України.

1. Для підвищення рівня техногенної безпеки запропоновано розробку і впровадження інформаційно-аналітичної системи оцінювання воєнно-техногенних загроз і ризиків для ОКІ в зоні проведення ООС. Основними складовими розробки цієї інформаційно-аналітичної системи є розробка процедур оцінювання техногенних загроз ризиків та деталізація алгоритму для підтримки управлінських рішень.

2. Проведено дослідження конкретних варіантів інформаційно-аналітичної системи на прикладі оцінювання воєнно-техногенних загроз і ризиків з використанням сучасних інформаційних технологій на прикладі критичної інфраструктури енергозабезпечення.

3. Проведено аналіз значимих воєнно-техногенних чинників, що істотно впливають на територіальну організацію критичної інфраструктури. Запропоновано ієрархічну систему критеріїв і факторів оцінювання. Це дозволило виділити вплив БД,

як складовий елемент техногенної безпеки для життєдіяльності населення в східному регіоні України.

3. Проведено перевірку роботи системи на прикладі критичної інфраструктури енергопостачання підконтрольних територій Луганської області і отримано конкретні результати для критичної інфраструктури енергозабезпечення.

4. Пріоритетним напрямком для техногенної безпеки критичної інфраструктури в Луганській області в ОЗП повинні стати заходи із забезпечення захисту енергетичної інфраструктури, а саме мереж енергопостачання для підтримки достатнього рівня техногенної безпеки ПНО і ОПН, забезпечення населення і соціально-значимих об'єктів, ЗС України в районах ведення бойових дій, систем водопостачання і водовідведення електроенергією та світлом;

5. На основі проведеного оцінювання загроз і ризиків для ОКІ енергозабезпечення зроблено висновок, що з огляду на високу протяжність ліній електропередачі по території Луганської області та їх повну доступність, а також те, що ведуться роботи по розвитку енергосистеми спрямовані на збільшення резервування без вирішення фундаментальних проблем, здатних призвести до надзвичайної ситуації в результаті технологічних відмов, природних або цілеспрямованих військових дій і терористичних впливів, наступне катастрофічне відключення та внаслідок цього НС державного рівня може статися взимку 2021 року.

6. Розробка концептуальних засад інформаційно-аналітичної системи оцінювання воєнно-техногенних загроз і ризиків для ОКІ на основі сучасних інформаційних технологій дозволить на новий рівень підняти екологічну безпеку та цивільний захист в районах ведення бойових дій.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

В кваліфікаційній роботі розроблено інформаційно-аналітичну систему, яка призначена для проведення комплексного оцінювання загроз і ризиків від чинників воєнного і промислового техногенезу для ОКІ на сході України.

Для підвищення рівня техногенної безпеки запропоновано розробку і впровадження інформаційно-аналітичної системи оцінювання загроз і ризиків від чинників воєнного і промислового техногенезу для ОКІ на сході України. Основними складовими розробки цієї інформаційно-аналітичної системи є розробка процедур оцінювання техногенних загроз ризиків. Проведені дослідження конкретних варіантів інформаційно-аналітичної системи на прикладі оцінювання воєнно-техногенних загроз і ризиків з використанням сучасних інформаційних технологій на прикладі критичної інфраструктури енергозабезпечення Луганської області.

Основними складовими розробки цієї інформаційно-аналітичної системи є розробка процедур оцінювання техногенних загроз ризиків. Проведено аналіз значимих чинників воєнного і промислового техногенезу, що істотно впливають на територіальну організацію критичної інфраструктури. Запропоновано ієрархічну систему критеріїв і факторів оцінювання. Це дозволило виділити вплив чинників воєнного і промислового техногенезу, як складовий елемент техногенної безпеки для життєдіяльності населення в східному регіоні України. Проведено перевірку роботи системи на прикладі критичної інфраструктури енергопостачання підконтрольних територій Луганської області і отримано конкретні результати для критичної інфраструктури енергозабезпечення.

На основі проведеного оцінювання загроз і ризиків для ОКІ енергозабезпечення зроблено висновок, що з огляду на високу протяжність ліній електропередачі по території Луганської області та їх повну доступність, а також те, що ведуться роботи по розвитку енергосистеми спрямовані на збільшення резервування без вирішення фундаментальних проблем, здатних призвести до надзвичайної ситуації в результаті технологічних відмов, природних або цілеспрямованих військових дій і терористичних впливів, наступне катастрофічне відключення та внаслідок цього НС державного рівня може статися взимку 2022 року.

Розробка концептуальних засад інформаційно-аналітичної системи оцінювання воєнно-техногенних загроз і ризиків для ОКІ на основі сучасних інформаційних технологій дозволить на новий рівень підняти еколого-техногенну безпеку на сході України.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ТА ІНТЕРНЕТ-РЕСУРСІВ

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

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

3. Critical infrastructure and key assets: definition and identification // Congressional research service, RL32631. – 2004. – October. – 19 p. 3. Green paper on a European programme for critical infrastructure protection (COM/2005/576 final) [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu.

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

5. Бірюков Д. С. Захист критичної інфраструктури в Україні: від наукового осмислення до розробки засад політики [Електронний ресурс] / Д. С. Бірюков // Наук.-інформ. вісн. Акад. нац. безпеки. – 2015. – № 3-4. – С. 155- 170.

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

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

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

9. Проект Закону України "Про критичну інфраструктуру та її захист" [Електронний ресурс]. – Режим доступу: https://www.me.gov.ua/Documents/ Detail?lang=uk-UA&id=a91bfd44-d9be-4a74-834f-feaf92bb886&title= Proekt_Zakonu

Ukraini pro KritichnuInfrastrukturuTaYiiZakhist

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

11. Постанова Кабінету Міністрів України від 29.08.2002 р. № 1288 «Про затвердження Положення про Державний реєстр потенційно небезпечних об'єктів»

12. Закон України від 18.01.2001 № 2245-III «Про об’єкти підвищеної небезпеки»

13. Перелік особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров'ю громадян, майну, спорудам, навколишньому природному середовищу / Затв. Постановою Кабінету Міністрів України від 06.05.2000 №765

14. Постанова Кабінету Міністрів України № 1051 від 15.08.2007 (для службового користування)

15. Постанова Кабінету Міністрів України від 10 серпня 1993 р. №615 «Про заходи щодо вдосконалення охорони об'єктів державної та інших форм власності» (із змінами)

16. Постанова Кабінету Міністрів України від 24.04.99 року №675-019 «Щодо затвердження Переліку об’єктів, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період»

17. Постанова Кабінету Міністрів України від 28.07.2003 № 1170 «Про затвердження переліку особливо важливих об'єктів електроенергетики, які підлягають охороні відомчою воєнізованою охороною у взаємодії із спеціалізованими підрозділами інших центральних органів виконавчої влади»

18. Розпорядження Кабінету Міністрів України від 27.05.2009 № 578-р «Про затвердження переліку особливо важливих об'єктів нафтогазової галузі»

19. Закон України від 10.01.2002 № 2919-III «Про Національну систему конфіденційного зв'язку» (із змінами)

20. Закон України від 05.04.2001 №2346-III «Про платіжні системи та переказ коштів в Україні»

21. Закон України від 13.03.2012 №4499-VI «Про систему екстреної допомоги населенню за єдиним телефонним номером 112»

22. Закон України від 08.06.2000 № 1805-III «Про охорону культурної спадщини»

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

24. Герасимов В.В. По опыту Сирии. Начальник Генерального штаба Валерий Герасимов: «Гибридная война требует высокотехнологичного оружия и научного обоснования» Военно-промышленный курьер 2016. https://www.vpk-news.ru/articles/29579.

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

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

27. Чумаченко С. М., Парталян А. С., Туровець Ю. С. Система підтримки прийняття рішень щодо управління станом навколишнього середовища на військових об’єктах у зоні збройного конфлікту // Форми та способи застосування військ (сил) за досвідом проведення антитерористичної операції на території Донецької та Луганської областей: зб. матер. наук.-практ. конф. (Київ, 15 листопада 2017 р.) / Київ: ЦНДІ ЗС України, 2017. С. 232–234. Інв. № 17806 (ЦНДІ ЗС України).

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

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

30. Закон України «Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій

та Луганській областях».

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

32. Сьогодні на Донбасі стартує операція Об'єднаних сил [Електронний ресурс] // Цензор.Нет. – 2018. – Режим доступу до ресурсу: https://ua.censor.net.ua/news/3063937/sogodni_na_donbasi_startuye_operatsiya_obyednanyh_syl.

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

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

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

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

37. Донбас стає непридатним для життя [Електронний ресурс]. Режим доступу: http://www.ekoinform.com.ua/index.php?option=com_content&view=article&id=140%3A2015-02-09-10-27-36&catid=7%3A2009-07-06-09-51 16&Itemid=41&lang=ru].

38. Донбас Треба рятувати від перетворення на пустелю [Електронний ресурс]. – Режим доступу: http://day.kyiv.ua/uk/article/cuspilstvo/donbastreba-ryatuvaty-vid-peretvorennya-na-pustelyu.

39. Полищук С.З., Рябко А.И. Системное моделирование и управление изменением состояния окружающей среды при разработке стратегии устойчивого развития на региональном уровне // Екологія і природокористування . — Дніпропетровськ: ІППЕ НАНУ, 2003. — №5. — С. 69 —76.

40.Майстренко В.Н. Эколого-аналитический мониторинг супертоксикантов. — М. : Химия, 1996. — 319 с.

41. Білявський Г.О. Основи екології: теорія та практикум: Навчальний посібник / Білявський, Г.О., Бутченко Л.І., Навроцький В.М. // — К.: Лібра, 2002. — 352 с.

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

43. Качинський А. Б. Безпека, загрози і ризик : наукові концепції та математичні методи / А. Б. Качинський// – К.: 2003. – 472 с.

44. Горелик В.А., Кононенко А.Ф. Теоретико-игровые модели принятия решений в эколого-экономических системах. — М.: Радио и связь, 1982. — 144с.

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

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

47. Морщ Є.В. Аналіз досвіду застосування принципів комплексності, виділення пріоритетів, ієрархічної організації в задачах екологічного моніторингу на об'єктах критичної інфраструктури / С.М. Чумаченко, Є.В. Морщ// Збірник наукових праць СНУЯЕтаП. – Севастополь: СНУЯЕтаП, 2011. – Вип. 20. – Инв. № 823. – С. 47-52.

48. Довгуша В. В. Введение в военную екологию / В. В. Довгуша, И. Д. Кудрин, М. Н. Тихонов. – М.: МО РФ, 1995. – 496 с.

49. Музалевский А. А. Индикаторы и индексы экодинамики. Методологические аспекты проблемы экологических индикаторов и индексов устойчивого развития / А. А. Музалевский // 3-я Межд. конф. по мягким

вычислениям и измерениям SCM-2000. — Т.1. — С.36–46.

50. Агробіорізноманіття України: Теорія, методологія, індикатори, приклади. Книга 1 / О. О. Созінов, В. І. Придатко, С. М. Чумаченко та ін. — К. : ЗАТ “Нічлава”, 2005. — 384 с.

51. Агробіорізноманіття України: Теорія, методологія, індикатори, приклади. Книга 2 / О. О. Созінов, В. І. Придатко, С.М. Чумаченко та ін. – К.: ЗАТ “Нічлава”, 2005. – 592 с.

52. Чумаченко, С. М. Методологічні особливості формування вектора екологічного стану військового полігону на основі застосування концепції екологічних індикаторів / С. М. Чумаченко, А. М. Турейчук // Збірник наукових праць. – Вип. 2(22). – К.: ННДЦ ОТ і ВБ України, 2004. – С. 57–68. − (Таємно; інв. 3398).

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

54. Дурдинець В.В. Соціальні ризики та соціальна безпека в умовах природних і техногенних надзвичайних ситуацій та катастроф / В.В. Дурдинець, Ю.І. Саєнко, Ю.О. Привалов. – К.: Стилос, 2001. – 497 с.

55. Моисеев Н.Н. Математические задачи системного анализа. - М.: Наука, 1981. - 487 с.

56. Перегудов Ф.И., Тарасенко Ф.П. Введение в системный анализ. - М.: Высшая школа, 1989, - 367 с.

57. Айдаров И.П., Алексеев Б.Н., Бударагин А.В. Военная экология: Учебник для высших военных учебных заведений / Под редакцией Н.В.Петрухина, А.В.Тарабары, И.А. Постовита. - М.: Издательство «Русь-СВ», 2000. - 360 с.

58. Катастрофы и безопасность: [науч.-метод. труд] / В.А. Акимов, В.А. Владимиров, В.И. Измалков; М-во Рос. Федерации по делам гражд. обороны, чрезвычайн. ситуациям и ликвидации последствий стихийн. бедствий. - Москва : Деловой экспресс, 2006. - 387 с.

59. Акимов В. А. Природные и техногенные чрезвычайные ситуации:

опасности, угрозы, риски / В. А. Акимов, В. Д. Новиков, Н. Н. Радаев. − М.: ЗАО ФИД “Деловой экспресс”, 2001. − 344 с.

60. Саати Т. Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. – 320 с.

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

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

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

64. Морщ Є.В. Математична модель інформаційно-технічного методу попередження надзвичайних ситуацій техногенного характеру на об’єктах критичної інфраструктури з використанням кластерних інформаційних портретів / С.М. Чумаченко, Є.В. Морщ // Збірник наукових праць СНУЯЕтаП. – Севастополь: СНУЯЕтаП, 2011. – Вип. 22. – Инв. № 829. – С. 75-81.

65. Морщ Є.В. Інформаційне забезпечення для методу попередження надзвичайних ситуацій техногенного характеру на об’єктах критичної інфраструктури з використанням кластерних інформаційних портретів / Є.В. Морщ // Збірник наукових праць СНУЯЕтаП. – Севастополь: СНУЯЕтаП, 2012. – Вип. 23. – Инв. № 838. – С. 73-78.

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

67. Чумаченко, С. М. Методологічні основи проведення екологічної оцінки впливу бойової підготовки на довкілля військових полігонів / С. М. Чумаченко // Зб. наук. пр. – К.: ННДЦ ОТ і ВБ України, 2003. – Вип. 20. – С. 105 – 115. − (Таємно. Інв. 3341).

68. Чумаченко, С. М. Методичні аспекти оцінки і ранжування загроз для

біорізноманіття в Україні / С. М. Чумаченко, О. В. Дудкін, М. М. Коржнєв, Є. О. Яковлєв // Екологія і ресурси. Зб. наук. пр. – Вип. 7. – К.: УІНСіР РНБОУ, 2003. – С. 77–86.

69. Романченко, І. С. Підходи до застосування методу аналізу ієрархій та нечітких множин для експертної оцінки впливу воєнно-техногенного навантаження на акваторіях і територіях приморських територій / І. С. Романченко, С. Л. Данилюк // Зб. наук. пр. ЦНДІ ЗС України. – К., 2014. – № 2 (68). – С. 5−22. – (Таємно; інв. № 44279).

70. Саати, Т. Аналитическое планирование. Организация систем / Т. Саати, К. Кернс. – М.: Радио и связь, 1991. – 224 с.

71. Подиновский В. В. Математическая теория выработки решений в сложных ситуациях / В. В. Подиновский. — М. : МО СССР, 1981. — 211 с.

72. Хемди, А. Т. Введение в исследование операций / А. Т. Хемди. – М.: Изд. дом “Вильямс”, 2005. – 912 с.

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

74. Лисиченко Г.В. Методологія оцінювання екологічних ризиків / Г. В. Лисиченко, Г. А. Хміль, С. В.Барбашев. – Одеса: Астропринт , 2011. – 368 с.

75. Измалков В. И. Техногенная и экологическая безопасность и управление риском / В. И. Измалков, А. В. Измалков// – СПб.: НИЦЭБ РАН, 1998. – 482 с.

76. Биченок М. М. Основи інформатизації управління регіональною безпекою / М. М. Биченок. – К.: ІПНБ, 2005. – 196 с.

77. Лысенко А. И. Математическая постановка задачи оптимального управления экологическим состоянием техногенно нагружаемых территорий / А. И. Лысенко, С. Н. Чумаченко, И. В. Чеканова, А. Н. Турейчук // Адаптивні системи автоматичного управління. – Вип.5(25). – 2002. – С.45–55.

78. Морщ Є.В. Інформаційно-технічний метод попередження надзвичайних ситуацій техногенного характеру на об’єктах критичної інфраструктури з

використанням кластерних інформаційних портретів / Є.В. Морщ // Збірник наукових праць СНУЯЕтаП. – Севастополь: СНУЯЕтаП, 2012. – Вип. 24. – Инв. № 839. – С. 56-63.

79. Суходоля О.М. Захист критичної інфраструктури: Сучасні виклики та пріоритетні завдання сектору безпеки [Електронний ресурс]/О.М. Суходоля. Режим доступу: file:///C:/Users/Student/Desktop/nivanb_2017_12_7.pdf.

80. Аварія на об'єктах ЖКГ в Алчевську взимку 2006 Електронний ресурс: tps://uk.wikipedia.org/wiki/Аварія_на_об%27єктах_ЖКГ_в_Алчевську_взимку_2006.

81. Війна в Перській затоці [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/ Війна в Перській затоці.

82. Кириченко І. О. Підбір вихідних даних для визначення пріоритетних напрямів взаємодії між формуваннями сил цивільного захисту МНС України та підрозділами внутрішніх військ МВС України у разі виникнення надзвичайних ситуацій / Кириченко І.О., Неклонський І.М. // Проблеми надзвичайних ситуацій. Зб. наук. пр. УЦЗ України. 2011. - Вип. 13 С. 77-84.

83. Морщ Є.В. Розробка структурно-функціональної моделі управління надзвичайними ситуаціями техногенного характеру на об’єктах критичної інфраструктури / С.М. Чумаченко, Є.В. Морщ// Збірник наукових праць СНУЯЕтаП. – Севастополь: СНУЯЕтаП, 2011. – Вип. 19. – Инв. № 822. – С. 66-71.

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

ДОДАТКИ

Додаток А

Результати розрахунку загроз для ОКІ

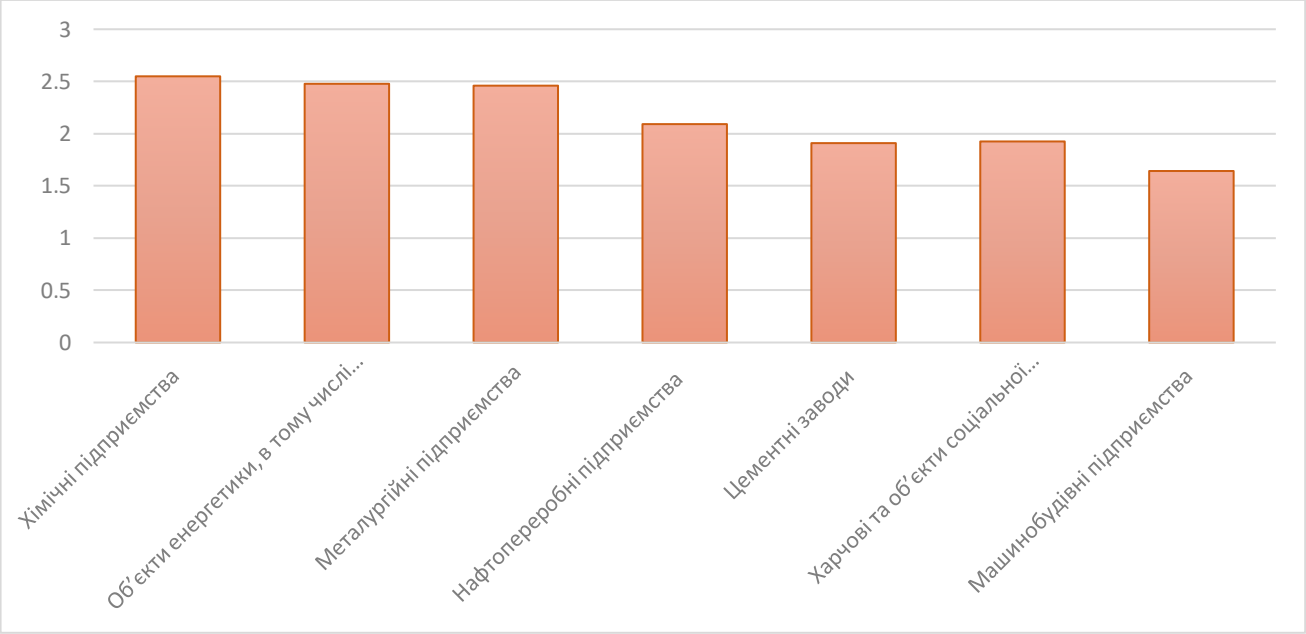


Рисунок А.1 – Результати експертного оцінювання загроз для об’єктів критичної інфраструктури районів ведення бойових дій за інтегральним критерієм оцінки воєнно-техногенних загроз в зоні збройного конфлікту на Донбасі

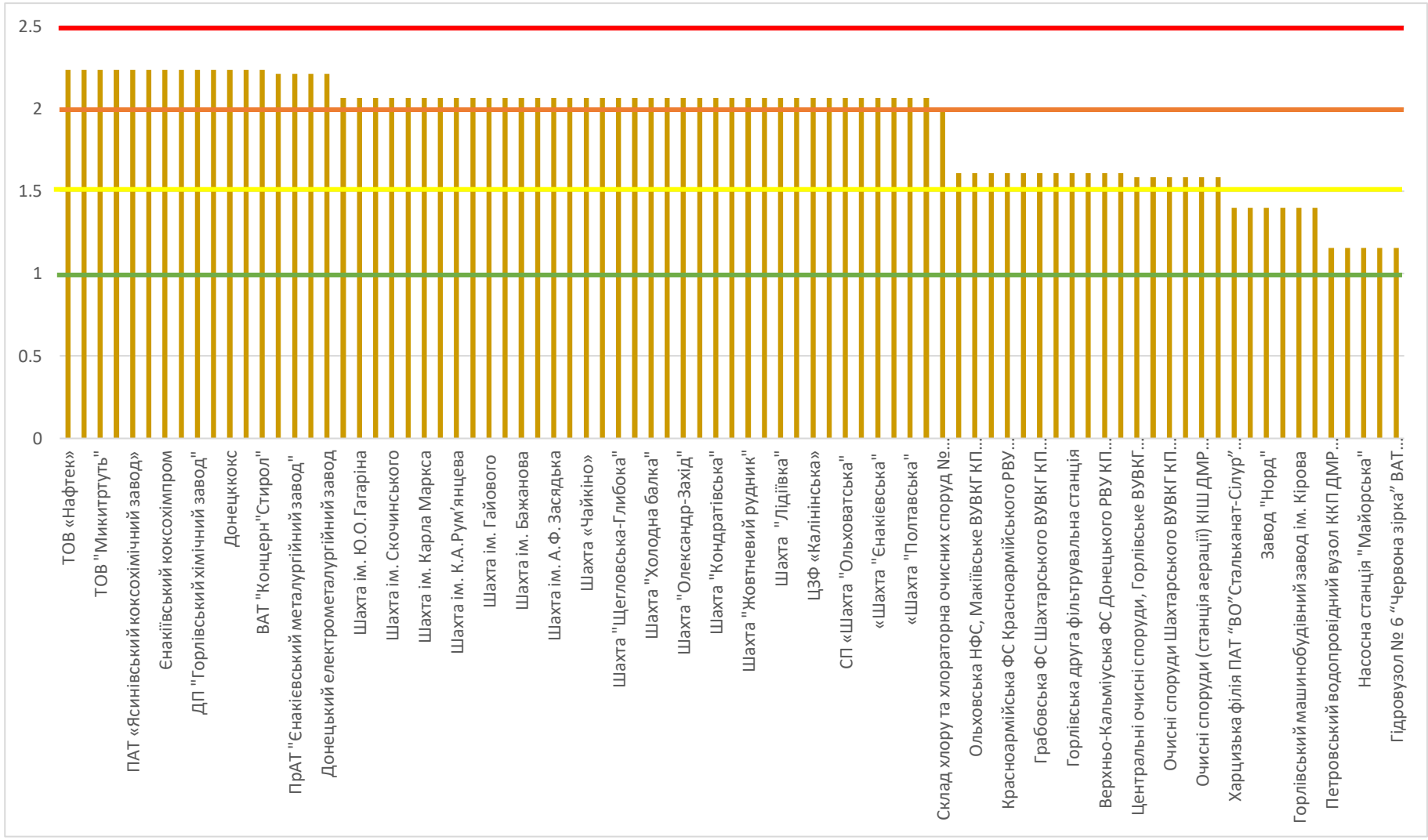


Рисунок А.2 - Інтегральний індекс загроз для об'єктів критичної інфраструктури (непідконтрольна території Донецької області)

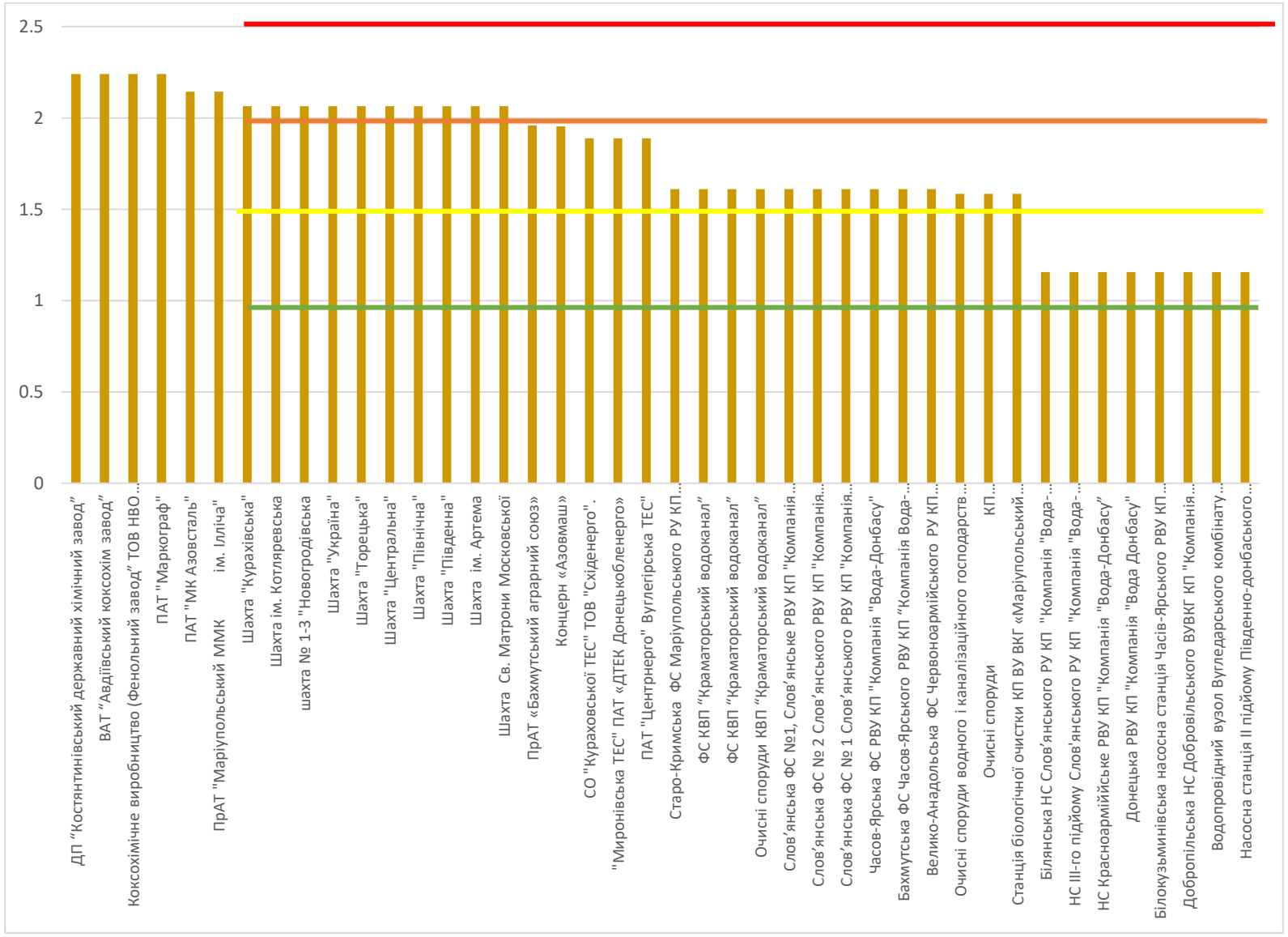


Рисунок А.3 - Інтегральний індекс загроз для об'єктів критичної інфраструктури (підконтрольна територія Донецької області)

Додаток Б

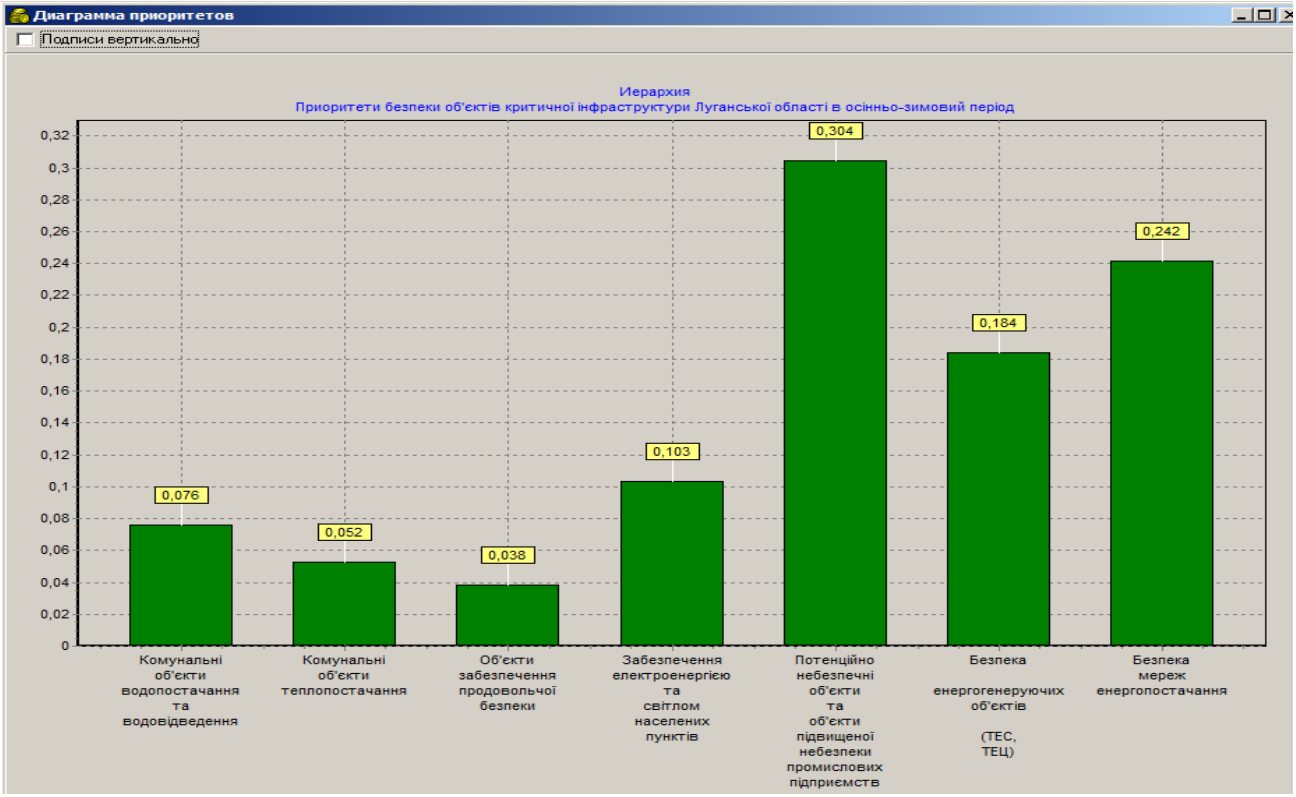


Рисунок Б.1 – Пріоритети безпеки об’єктів критичної інфраструктури Луганської області в осінньо-зимовий період

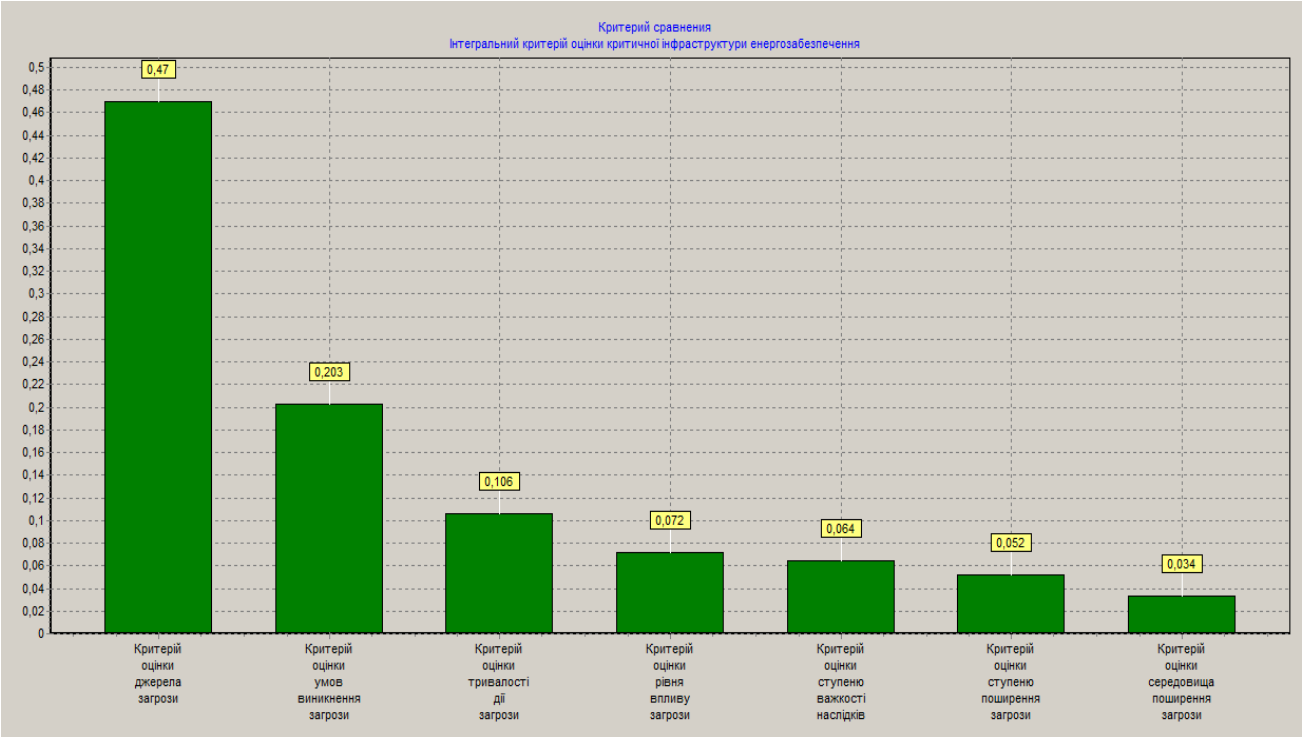


Рисунок Б.2 – Критерії оцінювання загроз для об’єктів критичної інфраструктури Луганської області

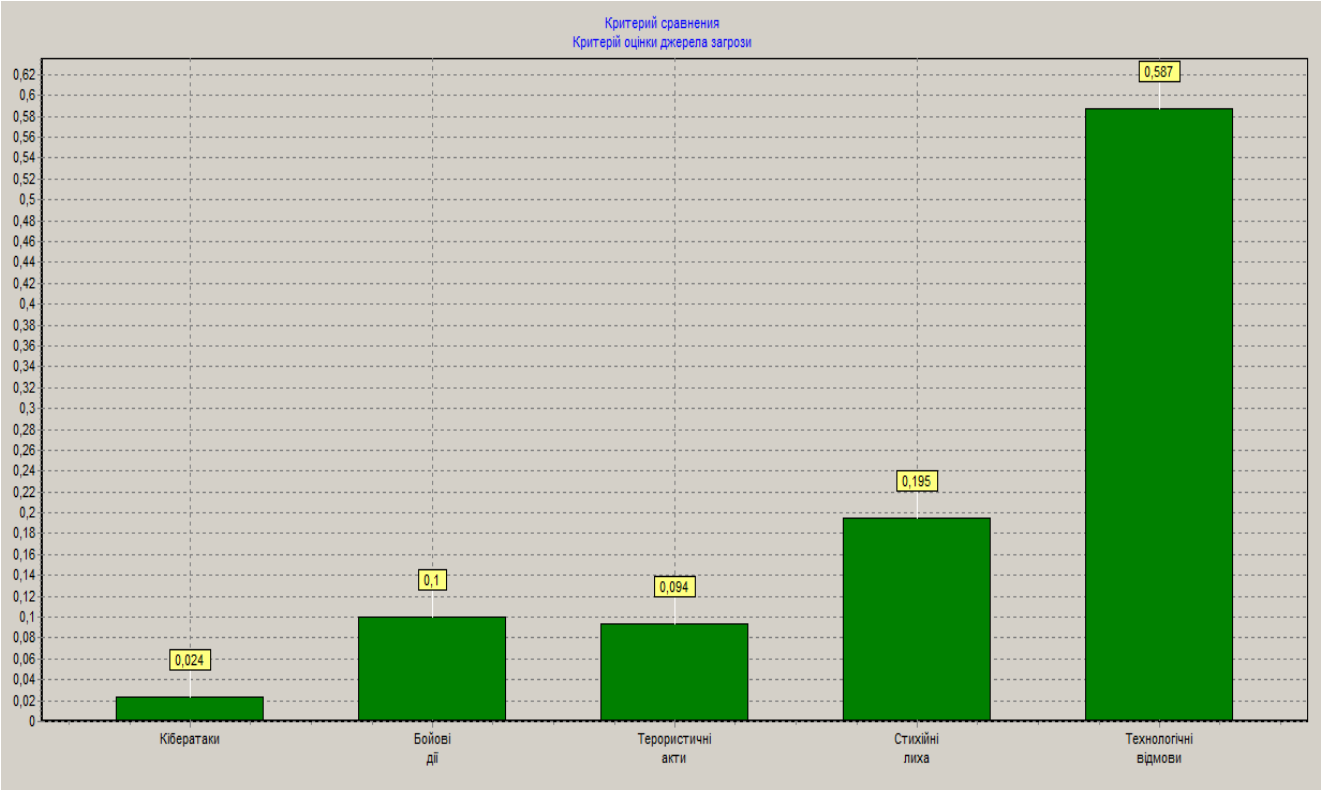


Рисунок Б.3 – Критерій оцінювання джерела загроз для об’єктів критичної інфраструктури

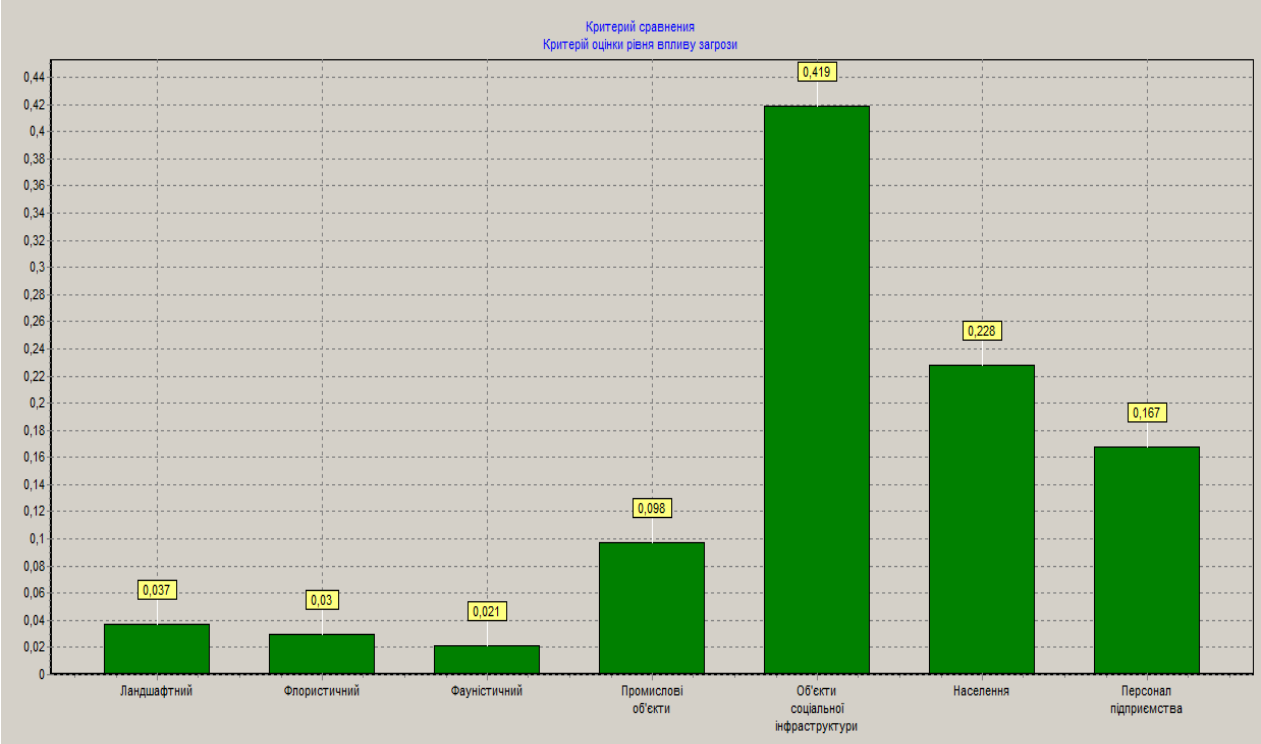


Рисунок Б.4 – Критерій оцінювання рівня впливу загрози для об’єктів критичної інфраструктури

Додаток В

УДК 519.713:517:338

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕКОЛОГО-ТЕХНОГЕННИХ ЗАГРОЗ ДЛЯ ПОТЕНЦІЙНО-НЕБЕЗПЕЧНИХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯМ ЕКСПЕРТНИХ ПІДХОДІВ

С.М.Чумаченко[1], Р.К.Мурасов[2], Савченко І.О. [1], Сорока Р.С.[1]
[1]Національний університет харчових технологій, Київ, Україна
[2]Національний університет оборони України імені Івана Черняховського
E-mail:s_chum@ukr.net

Comparative analysis of environmental and technogenic threats for potentialy hazardous critical infrastructure objects using experts

The report considers the development of theoretical and methodological foundations of information analysis of environmental and man-made threats to potentially dangerous critical infrastructure. Potentially dangerous objects of critical infrastructure in the east of Ukraine, which can become a source of emergency factors of military-technogenic origin, are considered. A model for classifying potential threats to critical infrastructure has been developed.

В зв'язку з тим що об'єкти критичної інфраструктури є найбільш уразливими при зростанні рівня інтенсивності бойових дій виникає завдання обґрунтування критеріїв оцінювання та розробка теоретико-методологічних основ інформаційного аналізу еколого-техногенних загроз для класифікації потенційно-небезпечних об'єктів критичної інфраструктури (ПНО КІ).

Розглянемо ПНО КІ на сході України, руйнування яких може призвести до катастрофічних наслідків (загибелі мирного населення, політичної та економічної дестабілізації, техногенних аварій і екологічних катастроф, евакуації населення та масової появи біженців). Масштаби збитків та наслідки в цьому випадку можна порівняти хіба що із наслідками від застосовування зброї масового ураження або тривалого ведення бойових дій на техногенно перевантаженій території.

Для проведення досліджень та оцінювання загроз розроблено модель класифікації та оцінювання загроз для ПНО КІ, основні елементи якої наведено на Рис.1.

Першим етапом є ідентифікація небезпек. Покажемо її на прикладі Авдіївського коксохімічного заводу та його шламонакопичувачів на Рис.2. Другий етап представляє собою експертний аналіз розвитку ситуації у випадку ураження шламонакопичувача та формування можливих сценаріїв [1-3], у яких розгорнуто послідовність розвитку техногенних аварій і екологічних катастроф при руйнуванні ПНО КІ (див. Рис.3)

Розглянемо детально склад зазначених ПНО КІ: 1) хвостосховища і шламонакопичувачі; 2) об'єкти хімічної промисловості; 3) шахти; 4) об'єкти водопостачання; 5) об'єкти електрозабезпечення; 6) газотранспортна система [4].

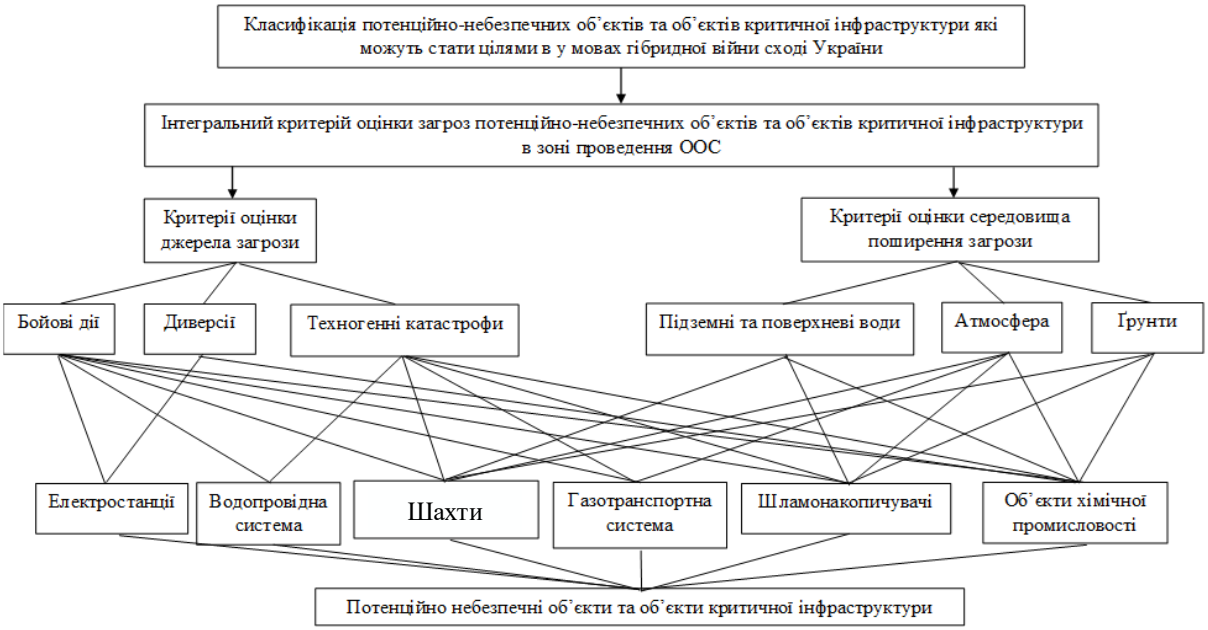


Рис.1. Модель класифікації та оцінки загроз об'єктів критичної інфраструктури

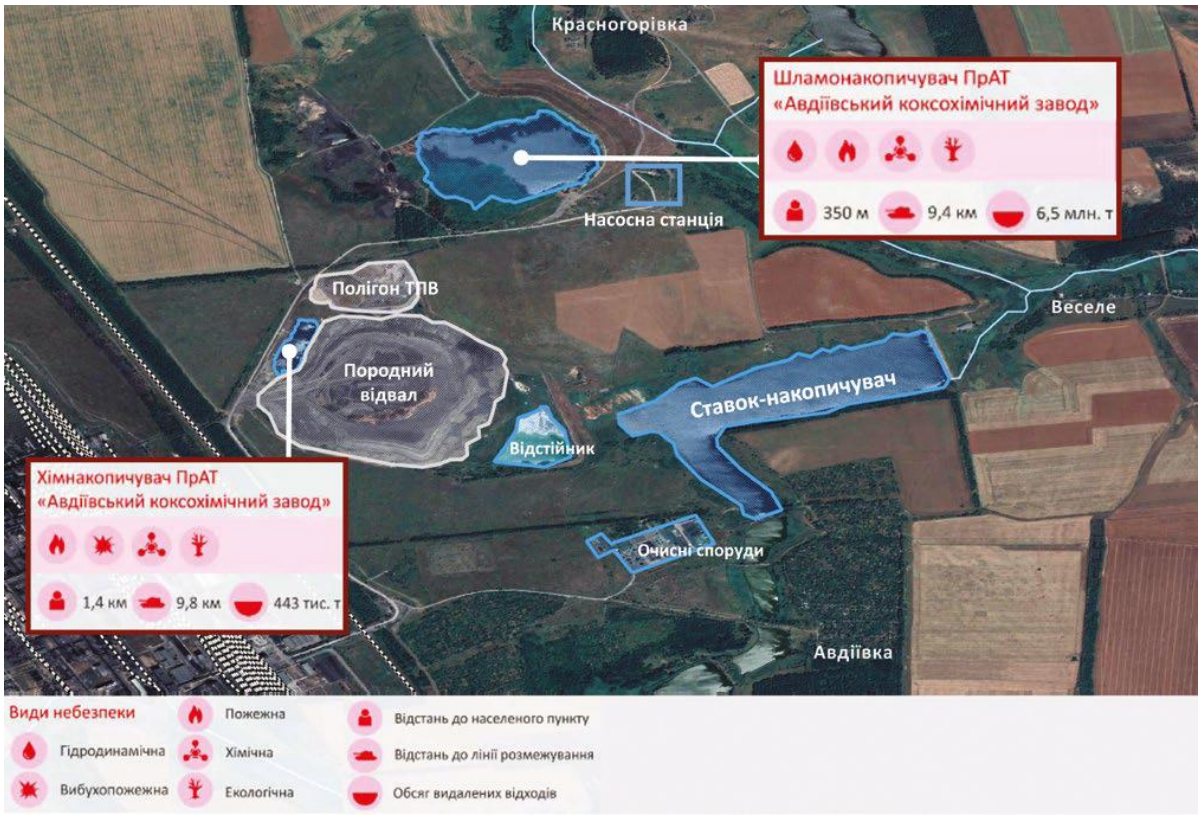


Рис. 2. Види небезпек від шламонакопичувачів ПрАТ АКХЗ [3]

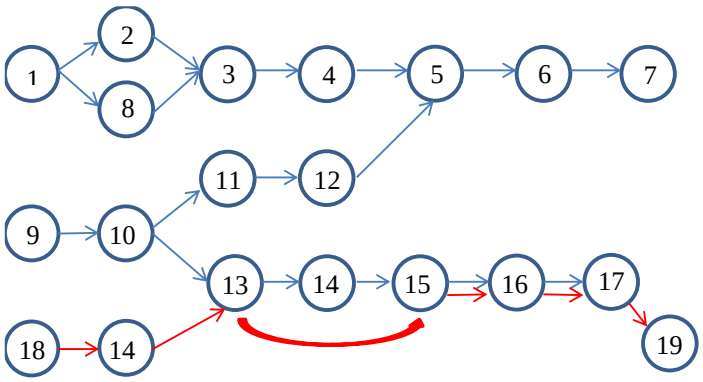


Рис.3. Послідовний розвиток екологічних катастроф при руйнуванні об’єктів критичної інфраструктури.

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

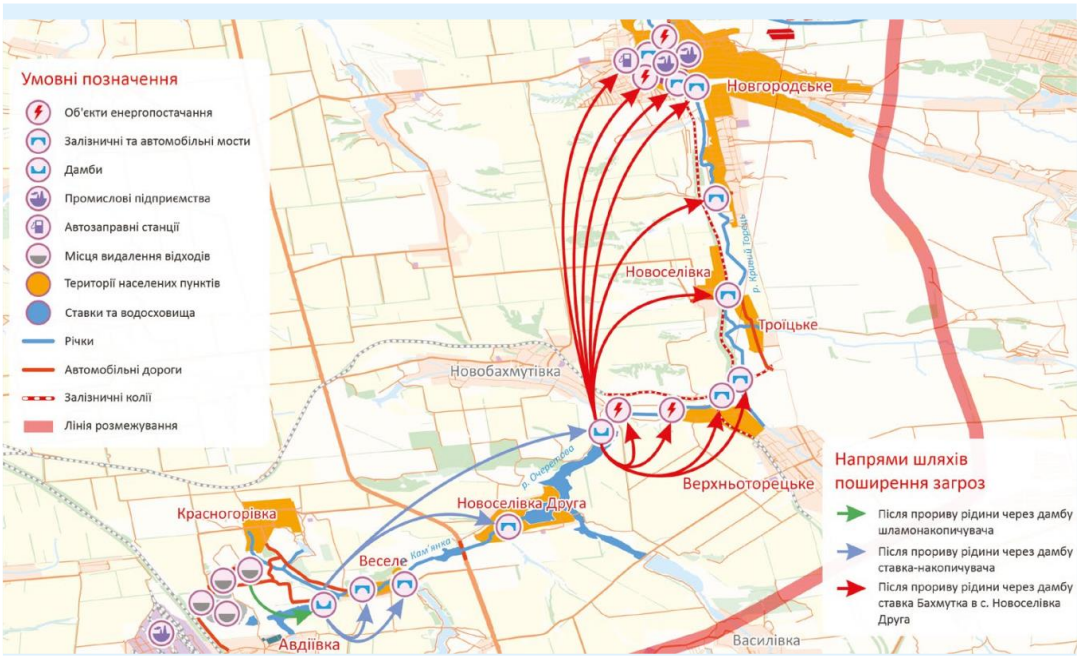


Рис. 4. Графічне представлення ефекту доміно [3]

Висновки

Таким чином, на Донбасі визначено 6 основних видів потенційно-небезпечних об'єктів критичної інфраструктури. Руйнування даних об'єктів призведе до масових жертв серед цивільного населення України. Для визначення шляхів запобігання техногенних аварій і екологічної катастрофи та оптимального розподілу ресурсів для їх усунення виникає необхідність в науковому дослідженні рівнів загроз та створенні науково-методологічного апарату оцінки загроз і ризиків для потенційно-небезпечних об'єктів критичної інфраструктури в зоні проведення операції Об'єднаних сил.

Література

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

2. Парталян А.С., Чумаченко С.М. Інформаційні технології в задачах управління екологічною безпекою військових об'єктів // Інформатика, обчислювальна техніка та автоматизація. Вчені записки Таврійського національного університету імені В.І.Вернадського. Том 29 (68) №1 2018 С.15-20

3. Хвостосховища Донбасу. Звіт по проекту ОБСЄ. 2019. - 50 с.

4. 15. С.М. Чумаченко, Р.К. Мурасов, Я.В. Мельник Теоретико-методологічні основи інформаційного аналізу еколого-техногенних загроз для потенційно-небезпечних об'єктів критичної інфраструктури в умовах збройного конфлікту на Сході України // Сучасні інформаційні технології у сфері безпеки та оборони 118 № 1 (40)/2021, с. 117-122