УДК 621.396.4
DOI https://doi.org/10.32782/2663-5941/2025.2.2/13

Кисельов В. Б.
Таврійський національний університет імені В. І. Вернадського

Морщ Є. В.
Державний науково-дослідний інститут
технологій кібербезпеки та захисту інформації

Чумаченко С. М.
Державний науково-дослідний інститут авіації
Міністерства оборони України

Гуйда О. Г.
Таврійський національний університет імені В. І. Вернадського

Ромащенко Р. А.
компанія Рінвік

МОДЕЛЬ ПОПЕРЕДЖЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ В СИСТЕМІ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТУКТУРИ

У статті розглянуто актуальні питання розробки моделей попередження надзвичайних ситуацій (НС) в рамках функціонування системи підтримки прийняття рішень (СППР) на об'єктах критичної інфраструктури (ОКІ) в умовах зростаючих загроз техногенного, природного та воєнного походження. На основі положень чинного законодавства України, обґрунтовано необхідність впровадження ефективних механізмів оцінки ризиків та прийняття управлінських рішень для запобігання НС, особливо в умовах ведення бойових дій.

Автори аналізують вітчизняний та міжнародний досвід щодо організації систем захисту критичної інфраструктури, зокрема в США та ЄС, де впроваджено системні підходи до зменшення вразливості національних інфраструктур до терористичних, техногенних і природних загроз. Розглянуто специфіку ідентифікації ризиків для ОКІ, де враховуються сценарії розвитку подій, імовірності їх виникнення та масштаби потенційних наслідків.

Запропонована СППР базується на застосуванні методів аналізу ієрархій та аналітичних мереж, які дозволяють ураховувати багатоаспектність загроз, а також невизначеність і неповноту вихідної інформації. У статті наведено принципову схему функціонування СППР, а також детально описано алгоритм її роботи. Окрема увага приділена розмежуванню понять «загроза» та «ризик», які розглядаються як основа для формалізованої моделі аналізу.

Також проаналізовано типові причини виникнення НС – технічні, людський фактор та бойові дії – із наголосом на необхідність всебічного підходу до оцінювання. Запропоновано використання концепції «джерело – шлях – наслідки» для побудови якісної та кількісної моделі загроз. Представлена модель дозволяє здійснювати ранжування загроз за ступенем їх критичності, сприяє підвищенню обґрунтованості управлінських рішень та є дієвим інструментом забезпечення безпеки об'єктів критичної інфраструктури України.

Ключові слова: *критична інфраструктура, надзвичайна ситуація, загроза, ризик, система підтримки прийняття рішень, аналіз ієрархій, воєнно-техногенні загрози, оцінка ризику.*

Постановка завдання. 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» [1] та Указу Президента України від 16 лютого 2017 року № 37/2017 Про рішення Ради національної безпеки і оборони України від від 16 лютого 2017 року «Про невідкладні заходи з нейтралізації загроз енергетичній безпеці України та посилення захисту критичної інфраструктури» [2] питання що стосуються

захисту об'єктів енергетичної інфраструктури в Україні є пріоритетними в державі.

Визначення основних питань щодо безпеки і організації захисту критичної інфраструктури наведені в Законі України «Про критичну інфраструктуру» [3]. 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 та природної небезпеки для ЗС України і життєдіяльності населення на відповідних територіях.

Рівні небезпеки для окремих територій 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 об'єктах критичної інфраструктури (ОКІ).

На сьогоднішній день, порушення в роботі критичних об'єктів енергопостачання призвели до надзвичайних ситуацій (НС), що за своїми наслідками впливають на рівень безпеки життєдіяльності населення, економіки та обороноздатності держави [4, 5]. Тому, розробка системи підтримки прийняття рішень в умовах постійних ракетно-дронових ударів по об'єктах енергетичної інфраструктури держави є актуальною.

Аналіз останніх досліджень і публікацій. Досвід досліджень з питань оцінки й управління воєнно-техногенними загрозами та ризиками в ЗС провідних країнах світу [6–9] свідчить про те, що їх організація стикається з рядом нових проблем. Для ЗС України ці проблеми пов'язані з постійно діючими техногенними чинниками військової та промислової діяльності, що можуть призвести на ОКІ, що знаходяться на територіях ведення БД, до НС воєнно-техногенного походження.

Згідно із Законом США «Про патріотизм» (USA Patriot Act), ухваленим Конгресом 26 жовтня 2001 року, критична інфраструктура визначається як сукупність фізичних або віртуальних систем і ресурсів, які мають таке значення для функціонування Сполучених Штатів, що їх виведення з ладу або знищення може мати серйозні наслідки для національної оборони, економіки, систем охорони здоров'я та загальної безпеки держави. [4].

Кульмінацією законотворчої діяльності Конгресу США в сфері внутрішньої безпеки стало ухвалення 25 листопада 2002 року важливого нормативного акта – «Закону про внутрішню безпеку» (Homeland Security Act). В межах реалізації положень цього закону було створено спеціальний комітет Палати представників (House Homeland Security Committee), який здійснює постійний контроль за його виконанням. Відповідно до закону, для протидії загрозам міжнародного тероризму та з метою гарантування безпеки громадян було засновано Міністерство внутрішньої безпеки США (Department of Homeland Security, DHS). До основних завдань новоствореного відомства віднесено: запобігання терористичним актам, зменшення вразливості критичної інфраструктури, реагування на наслідки терористичних атак, а також координацію дій інших органів влади щодо ліквідації наслідків техногенних, антропогенних і природних катастроф на території країни [10].

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 [4].

Об'єднання 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 [11].

Постановка завдання. Метою публікації є розробка інформаційно-аналітичної системи для підтримки прийняття рішень щодо попередження надзвичайних ситуацій із застосуванням методів аналізу ієрархій і аналітичних мереж.

Виклад основного матеріалу. Під час кількісного оцінювання ризику виникнення техногенних аварій або надзвичайних ситуацій, що можуть спричинити людські жертви й завдати шкоди довкіллю, прогнозні експертні висновки відображають суб'єктивне бачення фахівців щодо можливого розвитку подій. Методи експертного аналізу базуються на використанні професійного досвіду та інтуїції експертів. Вони спираються на формальні підходи до прийняття рішень в умовах невизначеності.

У ситуаціях природного, техногенного або соціального характеру ключову роль у процесі прийняття рішень відіграє особа, відповідальна за вибір – так звана особа, яка приймає рішення (ОПР). Це може бути як окрема людина (індивідуальна ОПР), так і колектив осіб, що спільно ухвалюють рішення (групова ОПР). Варто зазначити, що індивідуальною ОПР не обов'язково є одна фізична особа – нею може виступати й група, яка представляє спільні інтереси, або юридична особа. У випадку групової ОПР, рішення можуть ухвалювати кілька груп, кожна з яких має власні погляди та пріоритети.

ОПР зазвичай є керівником або уповноваженим органом, який визначає проблему, обирає спосіб її розв'язання та несе відповідальність за прийняте рішення. Для пошуку оптимального варіанту ОПР залучає експертів і консультантів, які мають глибокі знання в конкретних галузях, зокрема в питаннях технологій та організації процесу прийняття й реалізації 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).

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.

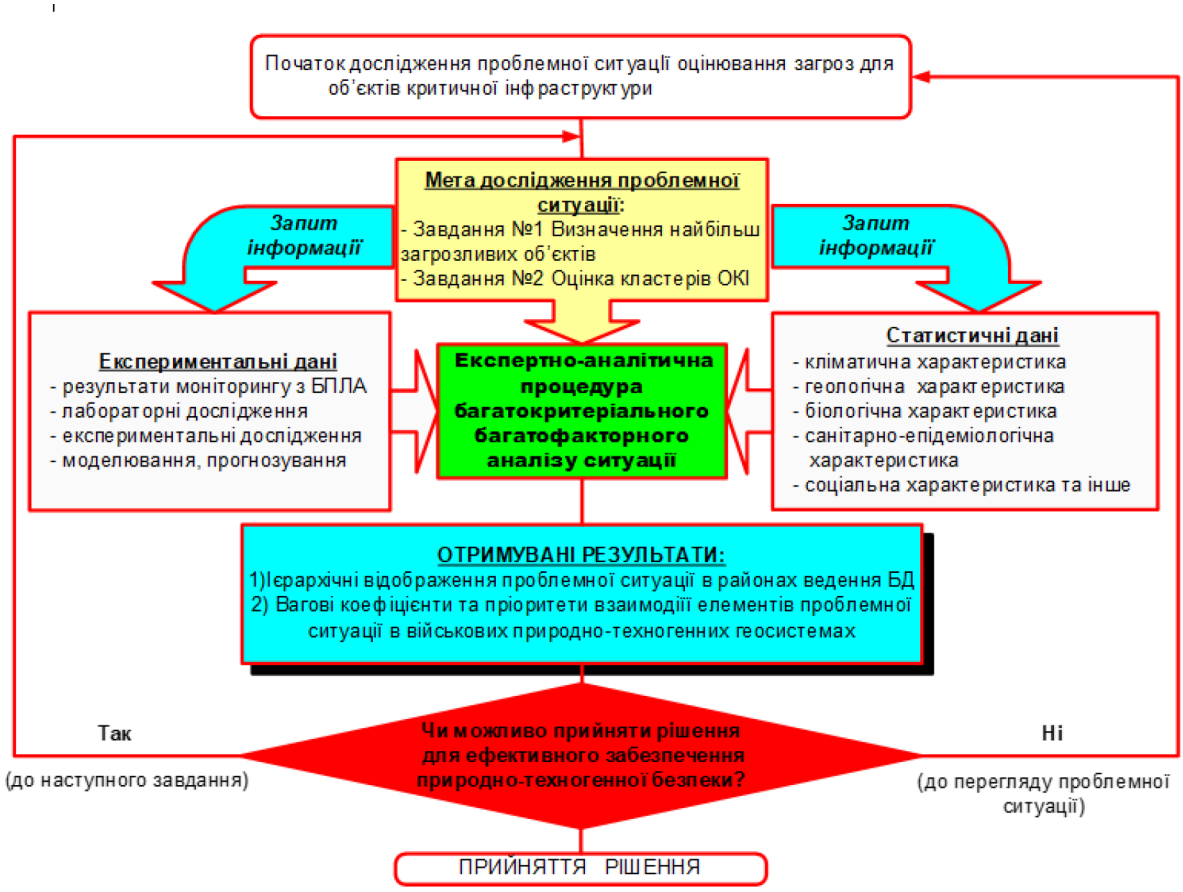


Рис. 1. Принципова схема роботи системи підтримки прийняття рішень (СППР)

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.

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 об'єкту критичної інфраструктури (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:

$$\text{Ризик} = \text{Загроза/Заходи запобігання},$$
$$\text{або } R = Z/S. \qquad (1)$$

Формула (1) – 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 [13]

$$Z = \{\langle s_j, p_j \rangle\} s, \qquad (2)$$

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) 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 систем-

ного аналізу з використанням багатокритеріальної оцінки загроз [13, 14, 15].

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.

Для ефективної оцінки та ранжування загроз доцільно формувати критерії не лише як «критеріальні функції» у вузькому сенсі, а в ширшому – як засоби оцінювання та порівняння загроз. У більшості випадків використання лише одного критерію для досягнення мети оцінювання є радше винятком, ніж правилом. Окремий критерій, як і будь-яка модель, може лише приблизно відображати ціль оцінки, і його адекватність часто виявляється недостатньою. Підвищення достовірності оцінювання загроз полягає не стільки в пошуку одного «ідеального» критерію (який може взагалі не існувати), скільки у використанні сукупності критеріїв, які з різних боків відображають ціль оцінки та взаємно доповнюють одне одного.

Об'єктивність процесу оцінювання та ранжування загроз значною мірою визначається здатністю обраної системи критеріїв охопити всі ключові ознаки загроз. Це означає, що критерії повинні відображати всі суттєві аспекти цілі оцінювання. Водночас важливо прагнути до мінімізації кількості таких критеріїв. Ця вимога може бути реалізована за умови, що критерії є незалежними, тобто не дублюють однакові показники або взаємопов'язані величини (наприклад, не слід включати до різних критеріїв одні й ті самі або похідні від них вимірювані характеристики).

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.

На рис. 2 показано алгоритм оцінки ризику виникнення надзвичайної ситуації на окремо взятому ОКІ в районі ведення БД з використанням ГІС технологій.

Коли ризик переростає в загрозу виникнення надзвичайної ситуації, для оцінювання рівня загрози може бути використаний більш універсальний підхід із яких насьогодні найбільш поширеними і системно довершеними є методи аналізу ієрархій і аналітичних мереж (ANP-process).

На рис. 2 представлено блок-схему алгоритму оцінювання загроз на об'єкті критичної інфраструктури з використанням ГІС-технологій. У рамках розробки було враховано європейські підходи до аналізу загроз та ризиків виникнення надзвичайних ситуацій на потенційно небезпечних об'єктах критичної інфраструктури. Запропоновано використання адитивної згортки зважених критеріїв, яка базується на методах підтримки прийняття рішень, зокрема методі аналізу ієрархій (AHP) та методі аналітичних мереж (ANP) [16, 17]. В якості критеріїв використано наступні:

1. Критерій оцінки джерела виникнення загроз.
2. Критерій оцінки рівня впливу загрози.
3. Критерій оцінки середовища поширення загрози.
4. Критерій оцінки можливого збитку.

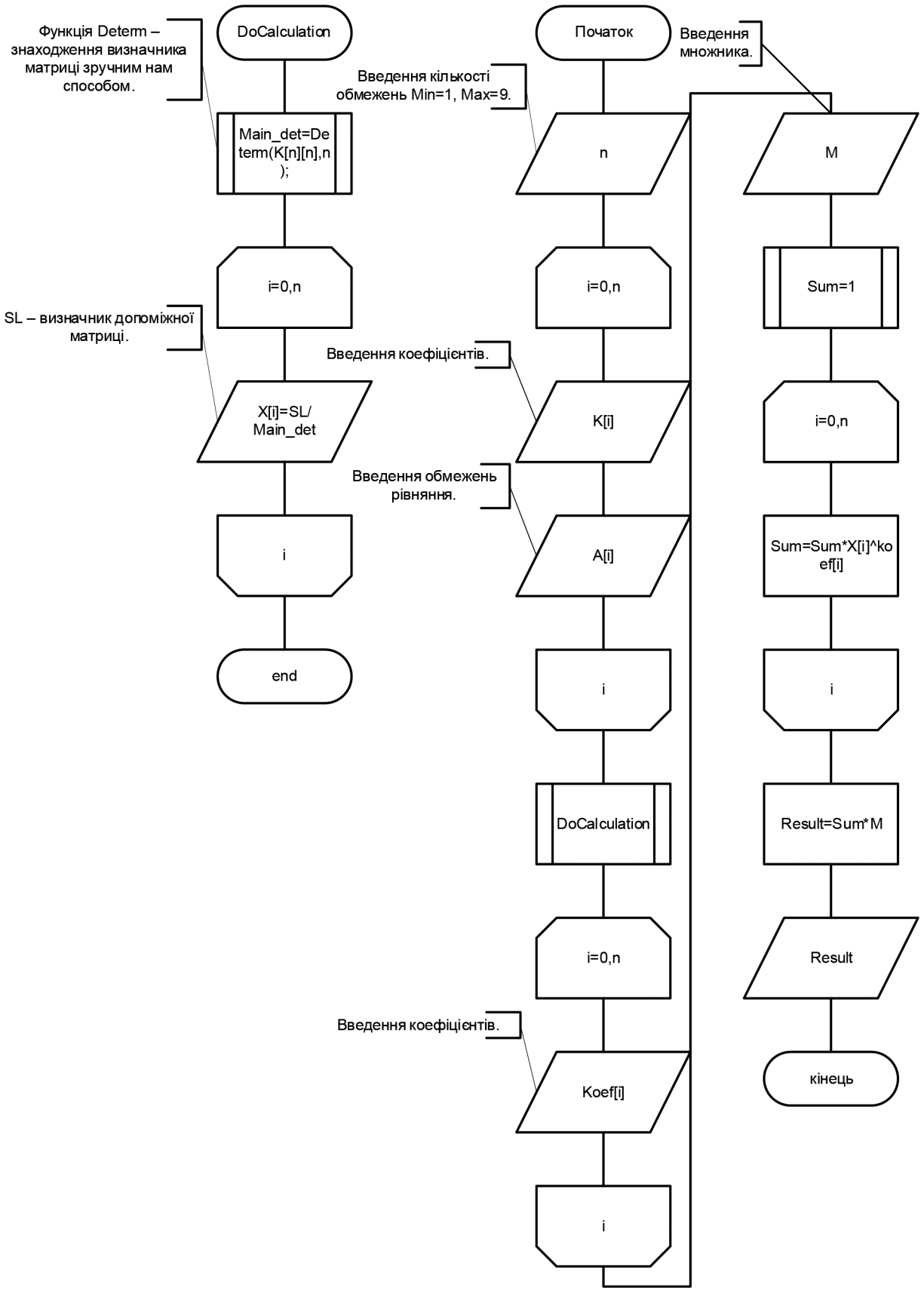


Рис. 2. Алгоритм оцінки ризику виникнення надзвичайної ситуації на окремо взятому ОКІ з використанням ГІС технологій

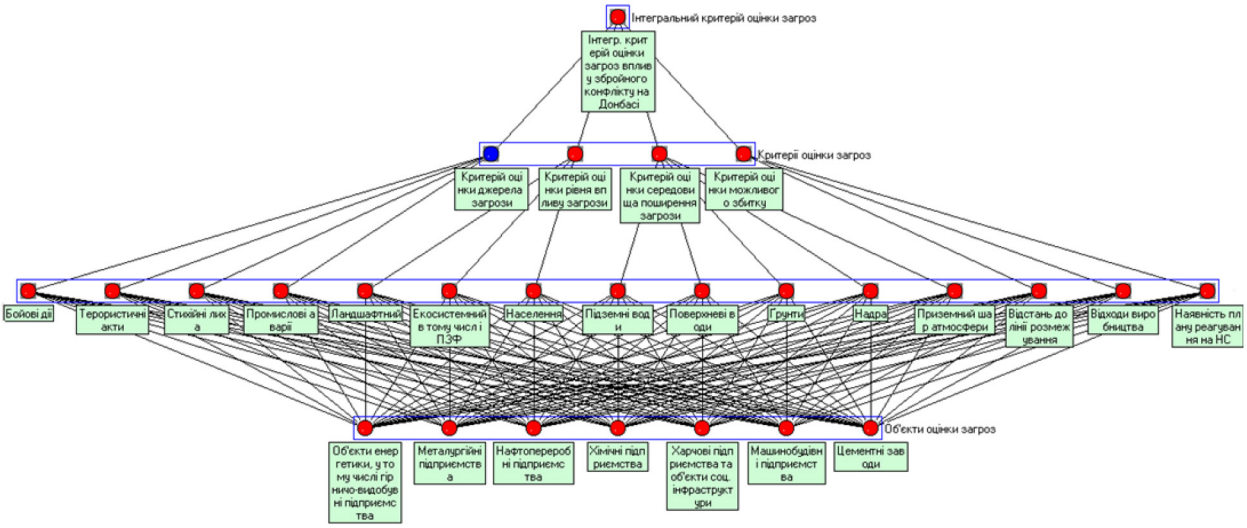


Рис. 3. Інформаційно-аналітична система оцінювання загроз для об'єктів критичної інфраструктури

Для проведення оцінювання загроз виникнення НС було розроблено інформаційно-аналітичну систему та спільно з представниками ГУ ДСНС у Донецькій області проведено експертне оцінювання за наступним ієрархічним деревом критеріїв та факторів оцінювання, що наведене на рис. 3. Для проведення оцінювання загроз методом парних порівнянь використовувалась інтервальна шкала Сааті.

Розроблювальна система націлена в першу чергу на полегшення роботи ОПР (Особи, що приймає рішення). Це може бути одна особа – індивідуальна ОПР або кілька осіб, які виробляють колективне рішення – групова ОПР. А також зменшує кількість роботи, необхідної для виконання аналітиками. А саме, дасть змогу швидко побудувати модель, необхідну для вирішення задачі прийняття рішення, наочно порівняти всі елементи моделі та отримати результати розрахунків.

Розроблювальна система повинна мати наступні функції:

1. Побудова моделі задачі;
2. Порівняння критеріїв та альтернатив;
3. Графічне зображення порівнянь;
4. Проведення розрахунків;
5. Графічне зображення розрахунків;
6. Можливість збереження і відкриття створюваних моделей.

Головною вимогою до інтерфейсу користувача є простота користування та мінімізація зусиль користувача при виконанні роботи.

Вхідні дані: об'єкти дослідження, критерії та альтернативи; файл збереженої моделі.

Вихідні дані: результати розрахунків; файл збереженої моделі.

Для оцінки ступеня екологічної загрози умовно шкалу оцінки від 0 до 3 було поділено на 4 інтервали:

коли рівень інтегрального критерію оцінки екологічних загроз змінюється від 0 до 1 – вважаємо, що рівень загрози малий;

коли рівень інтегрального критерію оцінки екологічних загроз змінюється від 1 до 1,5 – вважаємо, що рівень загрози середній;

коли рівень інтегрального критерію оцінки екологічних загроз змінюється від 1,5 до 2 – вважаємо, що рівень загрози високий;

коли рівень інтегрального критерію оцінки екологічних загроз змінюється від 2 до 3 – вважаємо, що рівень загрози катастрофічний.

Результати отриманих експертних оцінок загроз критичній інфраструктурі в районі ведення БД для Донецької області наведено у вигляді стовпчастих діаграм на рис. 4–6.

Висновки.

1. Сучасні системи підтримки прийняття рішення є системами, які максимально пристосовані до вирішення завдань повсякденної управлінської діяльності, є інструментом, покликаним надати допомогу ОПР. За допомогою СППР може проводитися вибір рішень деяких неструктурованих і слабо структурованих задач, в тому числі і багатокритеріальних.

2. За результатами проведеного експертного оцінювання можна зробити наступні висновки:

до найбільш загрозливих об'єктів відносяться хімічні підприємства індекс екологічної загрози яких складає більше 2,5 умовних одиниць, вторинні наслідки ураження яких призведуть до найбільш небезпечних екологічних

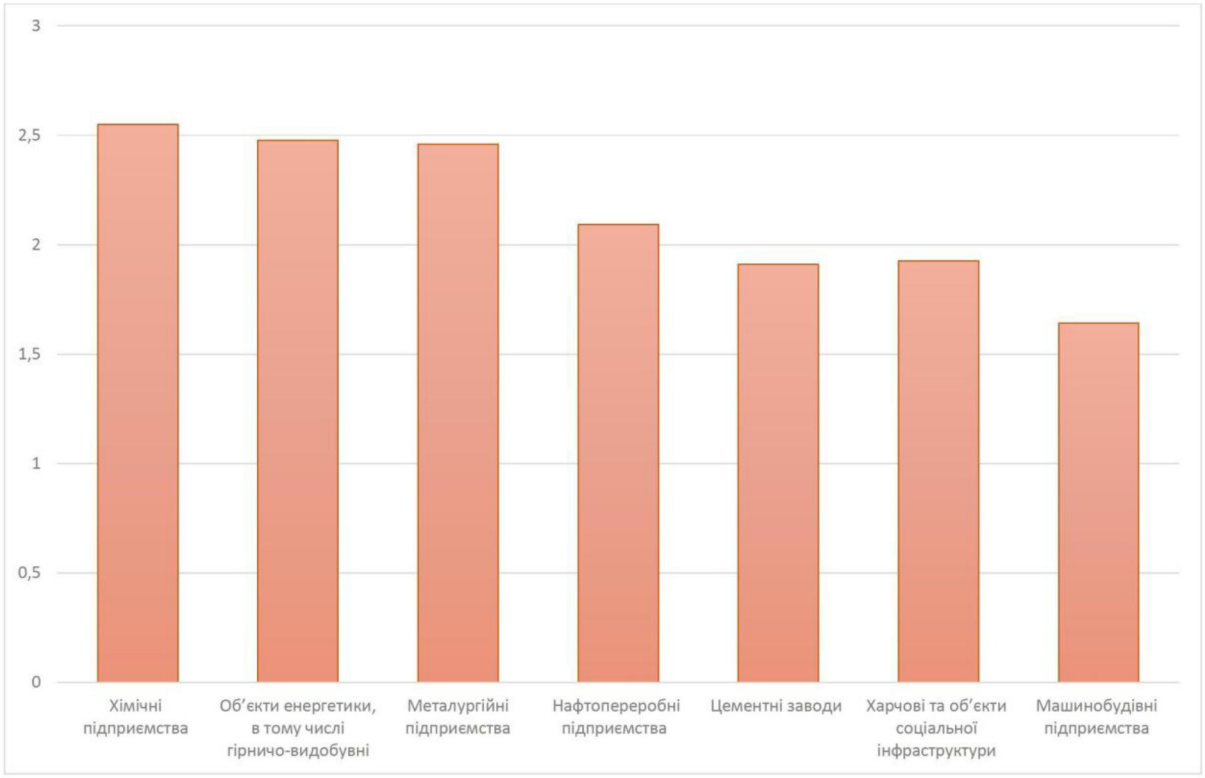


Рис. 4. Результати експертного оцінювання загроз для об'єктів критичної інфраструктури районів ведення бойових дій за інтегральним критерієм оцінки воєнно-техногенних загроз в зоні збройного конфлікту на Донбасі

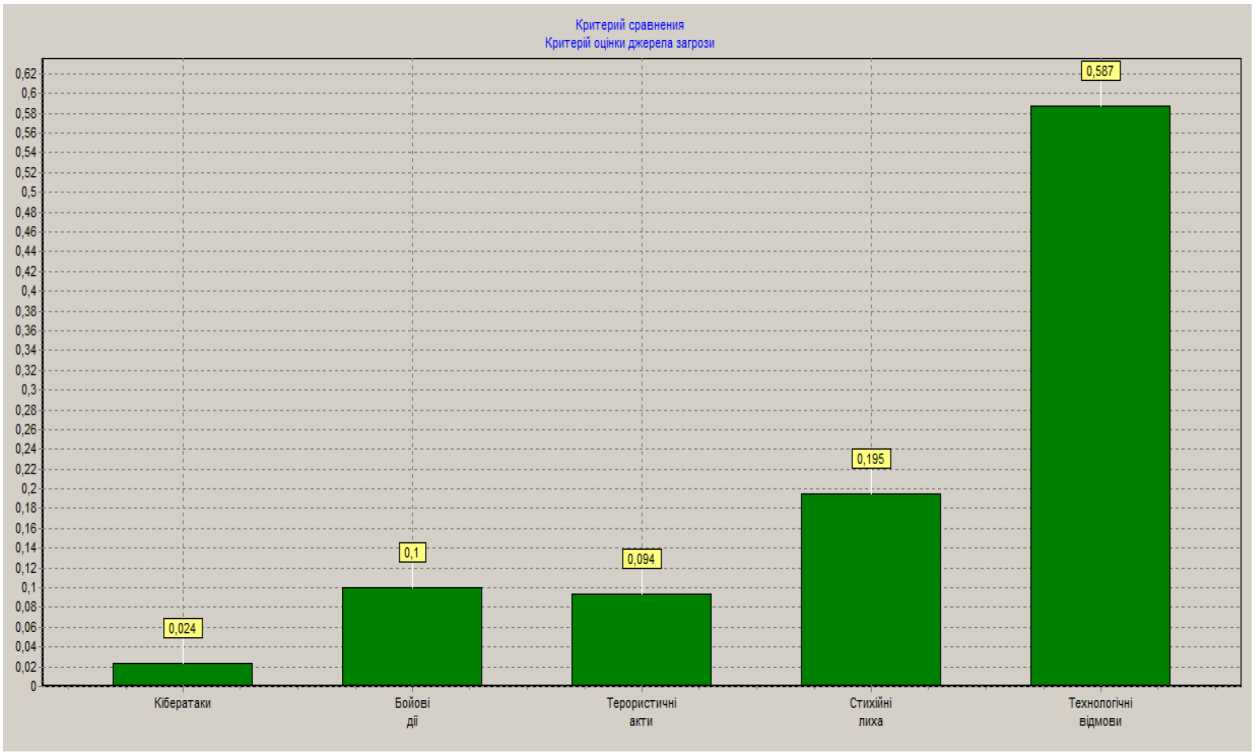


Рис. 5. Критерій оцінювання джерела загроз для об'єктів критичної інфраструктури

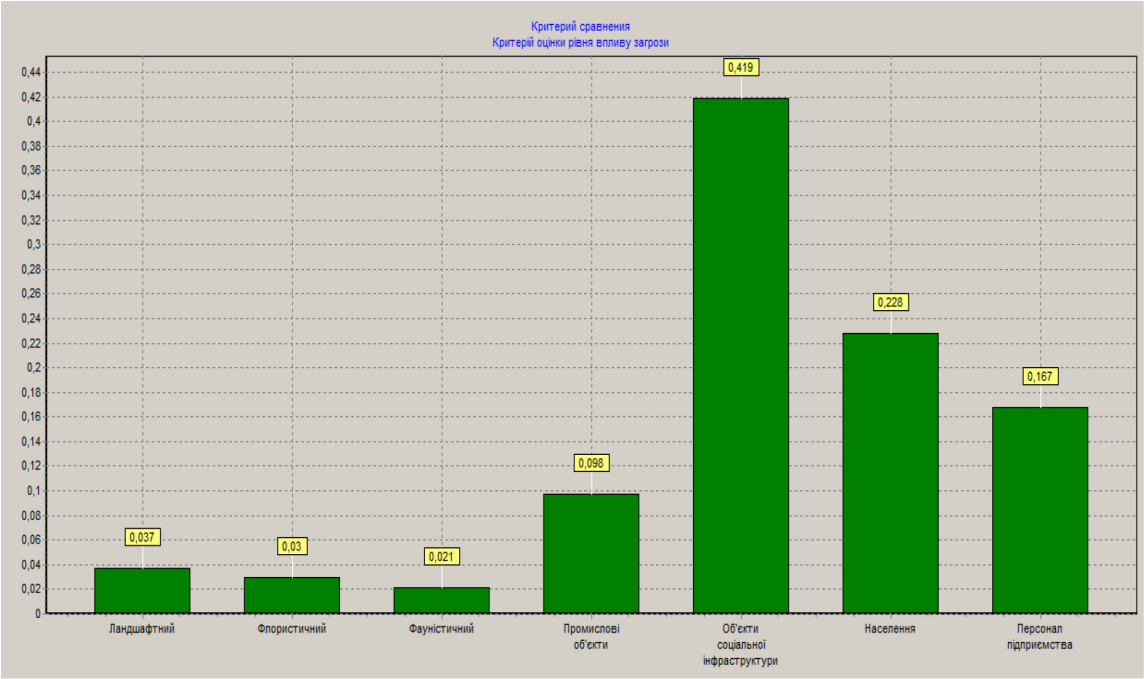


Рис. 6. Критерій оцінювання рівня впливу загрози для об'єктів критичної інфраструктури

наслідків для довкілля в зоні збройного конфлікту;

на другому місці стоять об'єкти енергетики та гірничо-видобувної промисловості індекс екологічної загрози яких складає трохи менше 2,5 умовних одиниць;

на третьому місці стоять металургійні підприємства індекс екологічної загрози яких складає трохи менше 2,5 умовних одиниць;

на четвертому місці стоять нафтопереробні підприємства індекс екологічної загрози яких складає трохи більше 2 умовних одиниць.

3. Ці чотири кластери підприємств відносяться до рівня катастрофічної екологічної загрози, що призведе до виникнення надзвичайної ситуації державного та регіонального значення.

4. На наступному місці стоять 3 кластери підприємств, що відносяться до високого рівня екологічної загрози:

на першому місці ідуть цементні заводи індекс екологічної загрози яких складає трохи менше 2-х умовних одиниць;

на другому місці ідуть харчові підприємства та об'єкти соціальної інфраструктури індекс екологічної загрози яких складає трохи менше 2-х умовних одиниць;

на третьому місці ідуть машинобудівні підприємства індекс екологічної загрози яких складає трохи менше 1,5 умовних одиниць.

5. Ураження цих об'єктів та можливі аварії можуть призвести до виникнення надзвичайних ситуацій місцевого та локального рівня.

Список літератури:

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» : Указ Президента України від 16.01.2017 № 8/2017. URL: https://zakon.rada.gov.ua/laws/show/8/2017#Text (дата звернення: 15.03.2025).

2. Про рішення Ради національної безпеки і оборони України від 16 лютого 2017 року «Про невідкладні заходи з нейтралізації загроз енергетичній безпеці України та посилення захисту критичної інфраструктури» : Указ Президента України від 16.02.2017 № 37/2017. URL: https://zakon.rada.gov.ua/laws/show/37/2017#Text (дата звернення: 15.03.2025).

3. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : станом на 21 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 15.03.2025).

4. 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. Київ : НІСД, 2015. 176 с.

5. Попель В. А. Інформаційна технологія підвищення живучості об'єктів критичної енергетичної інфраструктури за фактором управління системою інформаційної безпеки. Дисертація на здобуття ступеню доктора філософії. НУХТ, 2023, 182 с.

6. Суходоля О. М. Державно-приватне партнерство в системі забезпечення безпеки та стійкості критичної інфраструктури. URL: https://niss.gov.ua/sites/default/files/2019-04/SukhodolyaPresentation.pdf (дата звернення: 15.03.2025).

7. Євсєєв В. О. Можливі шляхи удосконалення захисту критичної інфраструктури України з урахуванням світового досвіду. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2016. № 4(49). С. 168–172.

8. О. І. Лисенко, І. В. Чеканова, О. П. Кутовий, В. А. Нікітін. Стратегії управління ризиками на об'єктах критичної інфраструктури в умовах невизначеності. Науковий вісник УкрНДІПБ. 2015. № 1. С. 134–139. URL: http://nbuv.gov.ua/UJRN/Nvundipb_2015_1_18

9. Денісов Н., Аверін Д.; Ющук А., Чумаченко С., Єрмаков В., Улицький О., Бистров П., Зібцев С., Набиванець Ю. Оцінка екологічної шкоди та пріоритети відновлення довкілля на сході України. К. : ВАІТЕ, 2017. 88 с.

10. 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

11. 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) URL: http://eur-lex.europa.eu (дата звернення: 15.03.2025).

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

13. 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.

14. Чумаченко С. М. Метод оцінки екологічних загроз від заходів бойової підготовки на військовому полігоні. Зб. наук. пр. Вип. 4 (29). К. : ННДЦ ОТ і ВБ України, 2005. – С. 93–103.

15. Морщ Є. В. Процедура попередження надзвичайних ситуацій техногенного характеру на об'єктах критичної інфраструктури в районах ведення бойових дій з використанням кластерних інформаційних портретів. *Техногенно-екологічна безпека та цивільний захист*. – Київ : ДУ «ІГНС НАНУ», 2019. Вип. 3 (17). С. 50–56.

16. Чумаченко С. М., Валуйський С. В., Тесленко О. М., Лисенко О. І. Концепція автоматизованої краудсорсингової системи моніторингу надзвичайних ситуацій на об'єктах критичної інфраструктури міста. Науковий вісник Академії муніципального управління. Серія : Техніка. 2014. Вип. 2. С. 157–163. URL: http://nbuv.gov.ua/UJRN/Nvamu_teh_2014_2_20. (дата звернення: 15.03.2025).

Kyselov V. B., Morshch Ye. V., Chumachenko S. M., Guida O. H., Romashchenko R. A.

A MODEL FOR EMERGENCY PREVENTION IN THE DECISION SUPPORT SYSTEM FOR CRITICAL INFRASTRUCTURE FACILITIES

The article addresses current issues in the development of models for preventing emergencies (EEs) within the framework of Decision Support Systems (DSS) operating at critical infrastructure facilities (CIFs) amid growing threats of technological, natural, and military origin. Based on the provisions of current Ukrainian legislation, the necessity of implementing effective mechanisms for risk assessment and decision-making to prevent emergencies – especially under conditions of armed conflict – is substantiated.

The authors analyze both domestic and international experience regarding the organization of critical infrastructure protection systems, particularly in the USA and the EU, where systemic approaches have been adopted to reduce the vulnerability of national infrastructures to terrorist, technological, and natural threats. The specifics of risk identification for CIFs are considered, taking into account event development scenarios, their likelihood, and the scale of potential consequences.

The proposed DSS is based on the use of analytic hierarchy and network analysis methods, which allow for consideration of the multifaceted nature of threats, as well as the uncertainty and incompleteness of input data. The article presents a conceptual diagram of DSS operation and provides a detailed description of its algorithm. Special attention is given to distinguishing between the concepts of "threat" and "risk," which are viewed as the foundation for a formalized analytical model.

Typical causes of emergencies – technical failures, human factors, and military actions – are analyzed with an emphasis on the need for a comprehensive approach to evaluation. The article proposes the use of the «source–path–consequences» concept to construct both qualitative and quantitative threat models. The presented model enables the ranking of threats by their criticality level, supports more substantiated managerial decisions, and serves as an effective tool for ensuring the security of Ukraine's critical infrastructure facilities.

Key words: *critical infrastructure, emergency situation, threat, risk, decision support system, hierarchy analysis, military-technological threats, risk assessment.*