

Мурасов Рустам Камілович (кандидат технічних наук)¹
Нікітін Анатолій Анатолійович (доктор філософії)¹
Мещеряков Іван Сергійович (доктор філософії)¹
Підгородецький Микола Миколайович (кандидат військових наук)¹
Поплавець Сергій Іванович (доктор філософії)²

¹ *Національний університет оборони України, Київ, Україна*

² *Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна*

МЕТОДИКА ОЦІНЮВАННЯ ЗАГРОЗ І РИЗИКІВ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА СЦЕНАРІЯМИ РОЗВИТКУ НАДЗВИЧАЙНИХ СИТУАЦІЙ

В умовах широкомасштабного вторгнення російської федерації в Україну на рівні відсічі збройної агресії ворога виникла нагальна потреба захисту не тільки сил оборони держави, а й цивільних об'єктів, які не мають жодного відношення до військового сектора. Для країни-агресора цілями для ураження стали як місця проживання населення, так і об'єкти критичної інфраструктури, що забезпечують життєдіяльність на всій території України. Внаслідок одностороннього виходу російської федерації із зернової угоди, під ураження потрапили зерносховища та навколишня інфраструктура. Таким чином росія тероризує не лише Україну, але й призводить до нестачі харчових продуктів у багатьох країнах світу. Метою статті є удосконалення методики оцінювання загроз і ризиків для об'єктів критичної інфраструктури за сценаріями розвитку надзвичайних ситуацій для запобігання втрат населення та особового складу сил оборони. Під час проведення дослідження застосовано аналітичний метод для аналізу останніх досліджень і публікацій, метод оптимізації (за мінімальним і максимальним критеріями) та метод мінімаксу для вибору кращого варіанту дій та синтезу для досягнення мети дослідження. Зазначений методичний підхід дає змогу провести аналіз і декомпозицію існуючих методик оцінювання загроз для об'єктів критичної інфраструктури в зоні ведення бойових дій та оцінювання ризиків для об'єктів критичної інфраструктури внаслідок бойових дій. Удосконалено методика оцінювання загроз і ризиків для об'єктів критичної інфраструктури за сценаріями розвитку надзвичайних ситуацій. Зазначена методика включає п'ять послідовних блоків, що дають змогу приймати раціональні управлінські рішення для впровадження відповідних заходів безпеки і оборони, здійснення оптимального розподілу сил і засобів та мінімізації наслідків надзвичайних ситуацій, застосовуючи інформаційні технології. Теоретичною значущістю методики є те, що дає змогу оцінювати можливі ризики та визначати стратегії захисту об'єктів критичної інфраструктури. Удосконалена методика дає змогу практично визначати варіанти сценаріїв надзвичайних подій, оцінювати збитки та вибирати найгірші сценарії з метою їх запобігання та локалізації. Це мінімізує наслідки виникнення надзвичайних ситуацій в умовах обмеженості сил і засобів оборони об'єктів критичної інфраструктури.

Ключові слова: об'єкт критичної інфраструктури, загроза, ризик, надзвичайна ситуація, катастрофа, ліквідація наслідків надзвичайної ситуації, мінімізація наслідків надзвичайної ситуації, інформаційні технології.

Вступ

Постановка проблеми. Економічне зростання України залежить від технологічного розвитку та виконання промислових завдань багатьма різномісними об'єктами критичної інфраструктури (далі – ОКІ), що розміщені на всій території нашої країни. Такі об'єкти мають великі розміри та займають великі території, що підвищує загрозу їх ураження. За таких умов ОКІ стали ціллю номер один для ракетно-дронових ударів противника, а засоби протиповітряної оборони не спроможні забезпечити їх повний захист у повітрі в повному обсязі.

У разі зруйнування (пошкодження) будь якого ОКІ виникають загрози для цивільного населення та особового складу сил оборони, що потрапляють в зону їх ураження (впливу). Одним із основних стратегічних завдань противника є порушення енергетичної системи держави, особливо у осінньо-зимовий період, з метою підризу її внутрішнього устрою, про що свідчать масовані ракетно-дронові атаки минулого року. Ракетно-дроновими атаками впродовж 10–20 жовтня 2022 року було виведено з ладу 30% об'єктів електроенергетики. На території всієї України почалися віялові відключення

електроенергії. Подальші подібні атаки ставлять під загрозу існування цілісності електричної системи України. Також потенційними цілями ракетних ударів є великі транспортні комунікації – мости, дамби, вузли автомобільних та залізничних сполучень, які також є об'єктами критичної інфраструктури.

Цілеспрямований вогневий вплив противника на критичну інфраструктуру держави призводить до створення масштабних надзвичайних ситуацій з подальшим розвитком каскадних деструктивних подій, що завдасть суттєвих збитків економіці держави, економо-, соціо-, гуманітарних катастроф та змушення до послаблення військово-політичної позиції.

Тому удосконалення методичного апарату оцінювання загроз і ризиків втрат населення та особового складу підрозділів в умовах руйнування об'єктів критичної інфраструктури за сценаріями розвитку надзвичайних ситуацій, що дає можливість використовувати інформаційні технології та сучасного наукового потенціалу є важливим науковим завданням.

Аналіз останніх досліджень і публікацій.

Попередніми дослідженнями створені передумови для розробки методики оцінювання загроз і ризиків для об'єктів критичної інфраструктури за сценаріями розвитку надзвичайних ситуацій. Лисиченко Г. В., Забулоновим Ю. Л. та Хміль Г. А. [1] було запропоновано основні поняття ризиків та загроз ОКІ. Їх порядок обчислення у загальному вигляді та викладенні основних наукових підходів щодо принципів оцінювання ризиків та загроз. Мурасов Р. К., Мельник Я. В., Куртсеїтов Т. Л., Чумаченко С. М., Мещеряков І. С., Романюк В. П., Нікітін А. А. [2–8] досліджували окремі питання щодо наслідків від ураження ОКІ різних типів та видів надзвичайних ситуацій (далі – НС), що дає широкі можливості для комплексного оцінювання каскадних НС та їх наслідків різної природи. У статті [9] автори описують інновації для захисту критичної інфраструктури від природних катастроф.

Методик оцінювання загроз для ОКІ в зоні ведення бойових дій [10; 11] та оцінювання ризиків для ОКІ внаслідок бойових дій [12; 13], що були створені для вирішення конкретних завдань стосовно захисту ОКІ. Перевагою цих методик є наявність у кожній з них чітко визначених функцій та послідовності дій. Недоліком цих методик є те, що вони потребують великого ресурсу для обчислень і вироблення окремих рекомендацій та не забезпечують оперативного прийняття єдиного управлінського рішення.

Незважаючи на розглянуті питання стосовно методики оцінювання загроз і ризиків для об'єктів критичної інфраструктури питання захисту населення та особового складу сил оборони за сценаріями розвитку надзвичайних ситуацій потребують подальшого опрацювання.

Метою статті є удосконалення методики оцінювання загроз і ризиків для об'єктів критичної інфраструктури за сценаріями розвитку надзвичайних ситуацій для запобігання втрат населення та особового складу сил оборони.

Виклад основного матеріалу дослідження

За результатами досліджень удосконалена методика отримала таку назву «Методика оцінювання загроз і ризиків для об'єктів критичної інфраструктури за сценаріями розвитку надзвичайних ситуацій».

Запропонована методика створена завдяки декомпозиції методик оцінювання загроз для ОКІ в зоні ведення бойових дій та оцінювання ризиків для ОКІ внаслідок бойових дій та враховує їх недоліки стосовно виникнення НС в умовах обмеженості сил і засобів оборони ОКІ.

Передумовами створення методики було наявність завдання щодо комплексного застосування попередніх методик. Бо за умови ураження ОКІ, надзвичайні ситуації будуть мати складний технічний та багатовекторний характер. Для повного врахування комплексних складових векторного стану та взаємопов'язаних подій надзвичайних ситуацій необхідно зазначені методики застосувати в комплексі для реалізації їх повного потенціалу та врахування сценаріїв розвитку надзвичайних ситуацій.

Удосконалення зазначених методик дасть змогу здійснити аналіз, моделювання, оптимальний розподіл оцінок за загрозами і ризиками, які дозволять цілеспрямовано застосовувати сили і засоби та запобігати глобальним катастрофам, що можуть призвести до вагомих втрат населення та особового складу сил оборони. Крім того, безпосереднє знищення ключових ОКІ здатне суттєво ускладнити соціо-економічну сферу в державному масштабі.

Об'єктом дослідження методики є захист населення та особового складу сил оборони в умовах зруйнування ОКІ.

Методика призначена для проведення розрахунків стосовно оцінювання втрат населення та особового складу підрозділів в умовах зруйнування ОКІ за сценаріями розвитку надзвичайних ситуацій.

Запропонована *методика відрізняється від попередніх* тим, що дає змогу розраховувати варіанти сценаріїв надзвичайних подій, оцінювати збитки та вибирати найгірші сценарії з метою їх запобігання та локалізації. Це дозволить мінімізувати наслідки виникнення надзвичайних ситуацій в умовах обмеженості сил і засобів оборони об'єктів критичної інфраструктури.

Припущення. Під час оцінювання загроз і ризиків для об'єктів критичної інфраструктури використовуються сценарії розвитку надзвичайних ситуацій для запобігання втрат населення та особового складу сил оборони.

Основними *обмеженнями* є те, що

деструктивної дії в умовах ведення бойових дій. Оскільки перелік таких об'єктів залежить від конкретної обстановки, то він формується на основі даних про зони ведення бойових дій, райони вогневого впливу противника та інші фактори. Серед основних об'єктів критичної інфраструктури зазвичай виокремлюють об'єкти енергетики, нафтопереробної та хімічної промисловості, систему логістики, мости, дамби (рис. 2), системи та об'єкти зв'язку, об'єкти соціально-побутової сфери. Також слід враховувати можливі комплексні дії ОКІ, які взаємодіючи між собою, можуть мати високий потенціал загроз та катастрофічних наслідків. Важливо враховувати особливості кожного об'єкту та його взаємодії з іншими об'єктами, щоб забезпечити належний рівень безпеки та захисту в умовах конфлікту.

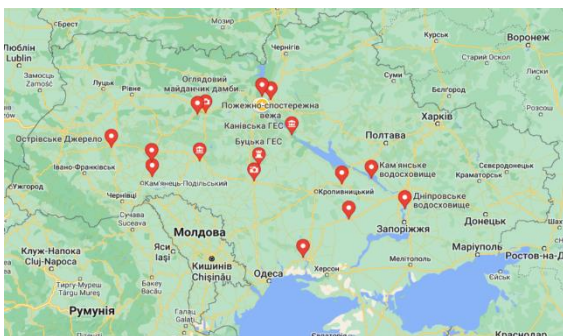


Рисунок 2 – Схема розташування дамб (частина)

У другому блоці здійснюється оцінювання загроз та ризиків для ОКІ в зоні ведення бойових дій. Детально ці питання розглянуті у [9–12].

На підставі отриманих даних першого етапу, будується орграф розвитку катастроф внаслідок зруйнування/руйнування ОКІ, здійснюються розрахунки оцінки чисельного значення імовірності ураження ОКІ ракетно-артилерійськими ударами. Визначається ступінь їх ураження. Будується схема орграфа розвитку катастроф з урахуванням імовірностей виникнення катастроф Р і деструктивних потенціалів D з урахуванням районів ведення бойових дій, районів розвитку катастроф, ступеню захисту ОКІ.

Третій блок відповідає за формування каталогу загроз та ризиків для ОКІ. Здійснюється аналіз отриманої інформації із заданих параметрів зброї противника щодо ураження певних ОКІ у визначених районах. В цілому на даному етапі буде сформовано основне інформаційне ядро за характером загроз і ризиків зруйнування ОКІ, їх способів ураження. Це дозволить визначити сили та засоби протидії атакам противника. Характер та стратегію захисту ОКІ, які ресурси необхідно буде застосовувати та їх можливості. За змістом, це буде відправною точкою побудови стратегії захисту ОКІ та протидії засобам ураження противника, характеру, фізичній та хімічній природі чинників ураження внаслідок зруйнування ОКІ. За досвідом агресії рф проти України, внаслідок широкого застосування ракет різного типу та, з вересня 2022 року, дронів-камікадзе, баражуючих боєприпасів

рис. 3, ОКІ були нанесені значні збитки на суму 143,8 млрд. дол. (рис. 4) [14]. Це відбувалося через відсутність, на той час, дієвої системи протиповітряної оборони.

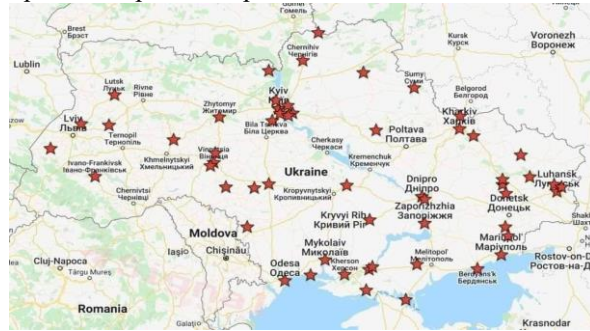


Рисунок 3 – Карта ударів по об'єктах критичної інфраструктури

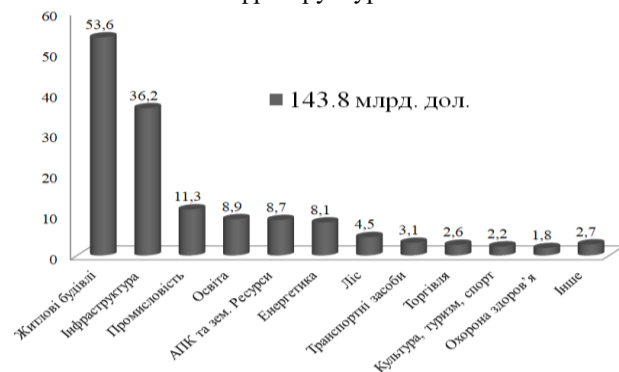


Рисунок 4 – Прямі втрати за типами майна

Четвертий блок дає змогу будувати та обчислювати сценарії розвитку подій у вигляді орграфів у випадку зруйнувань ОКІ. Такі схеми (орграфи) будується для усіх ОКІ, які об'єднуються в одну загальну схему. Вони мають відповідні сфери збитків (екологічні, енергетичні, соціальні, і т.д.) та розвитку подій, які корелюються між собою. Після побудови загальної схеми здійснюється обчислення деструктивних потенціалів та визначаються найбільш критичні сценарії та вузлові події. На схемі відображено шляхи розвитку деструктивних подій у різних сферах внаслідок надзвичайної ситуації, зокрема в: енергетичній, екологічній, логістичній сферах, що призводять до соціально-економічної кризи. Застосовуючи значення деструктивних потенціалів

D, можливо визначити ключові ОКІ та здійснити їх нормування та створення відповідного каталогу ОКІ. Внаслідок зруйнування ОКІ визначаються найбільш критичні за ступенем ризику сценарії розвитку надзвичайних ситуацій. Виходячи з характеру бойових дій та ракетно-авіаційних ударів, здійснюється розгляд варіанту раціонального перегрупування сил і засобів ППО, визначають райони надзвичайних ситуацій для своєчасної евакуації військ та цивільного населення. Це дає змогу зосередити основні зусилля на посиленні захисту та живучості визначених ОКІ.

Підсумковий п'ятий блок дозволяє обґрунтовано прийняти рішення із розподілу сил

засобів щодо охорони та оборони ОКІ їх пріоритет і розташування (переміщення) військ й населення в зоні ураження ОКІ. Визначення районів майбутніх надзвичайних ситуацій та вжиття запобіжних безпекових заходів.

Усі зазначені блоки мають зворотний зв'язок і за умови надходження оновлених даних або виникнення непередбачуваних подій можна здійснити відповідні обчислення на відповідних рівнях.

Після опрацювання усіх п'яти блоків методики буде отримано достатньо інформації для прийняття управлінських рішень, впровадження відповідних заходів безпеки і оборони, здійснення оптимального розподілу сил і засобів безпеки і оборони. Залежно від зміни оперативно-стратегічної обстановки будуть здійснені поточні уточнення та розрахунки. Такий циклічний порядок дій дасть змогу оперативно реагувати на зміни в обстановці та приймати управлінські рішення, здійснювати раціональне застосування ресурсів, що будуть у розпорядженні й запобігти надзвичайним ситуаціям техногенного характеру в районі бойових дій.

Теоретичною областю застосування методики слід зазначити таке. Методика дає можливість розраховувати варіанти сценаріїв надзвичайних подій, оцінювати збитки, здійснювати вибір найгірших сценаріїв з метою їх запобігання та локалізації. Це дає змогу в умовах обмежених сил і засобів оборони ОКІ мінімізувати наслідків надзвичайних ситуацій.

Для подальших досліджень здійснимо математичну формалізацію задачі, нехай:

A_1, A_2, \dots, A_i – множина ОКІ;

B_1, B_2, \dots, B_i – множина засобів захисту ОКІ;

S_1, S_2, \dots, S_i – сценарії розвитку деструктивних подій в системі критичної інфраструктури;

K_1, K_2, \dots, K_i – множина ключових елементів критичної інфраструктури, які переривають лінію розвитку деструктивних подій.

$f_{\text{захисту}}(A_i, B_i) \rightarrow \text{opt}$ – функція розподілу засобів захисту ОКІ;

$f_{\text{втрати}}(S_i, A_i, B_i) \rightarrow \text{min}$ – функція оцінювання сукупних втрат системи критичної інфраструктури за i -м сценарієм;

$f_{\text{захисту/ключ.елем.}}(A_i, B_i, K_i) \rightarrow \text{max}$ – функція захисту ключових елементів ОКІ K_j в умовах обмеженої кількості засобів захисту ОКІ B_i , множини ОКІ A_i .

Математична формалізація Методики може бути представлена так:

1. Визначення оптимального розподілу засобів захисту ОКІ: Знайти розподіл засобів захисту B_i для кожного об'єкта A_i , який максимізує функцію $f_{\text{захисту}}(A_i, B_i)$, тобто:

$$f_{\text{захисту}}(A_i, B_i) \rightarrow \text{max}, i = 1, 2, \dots, n. \quad (1)$$

2. Оцінювання сукупних втрат системи критичної інфраструктури за кожним сценарієм: для кожного сценарію S_i , обчислити втрати з урахуванням оптимального розподілу засобів захисту B_i для всіх об'єктів A_i :

$$f_{\text{втрати}}(S_i, A_i, B_i) \rightarrow \text{min}, i = 1, 2, \dots, k. \quad (2)$$

3. Знаходження оптимального захисту ключових елементів критичної інфраструктури: Визначення розподілу засобів захисту B_i для ключових елементів A_i які переривають лінію розвитку деструктивних подій K_j , таким чином, щоб максимізувати функцію

$$f_{\text{захисту/ключ.елем.}}(A_i, B_i, K_i) \rightarrow \text{max}, i = 1, 2, \dots, j. \quad (3)$$

Ці кроки спрямовані на забезпечення оптимального розподілу засобів захисту, мінімізацію загальних втрат від деструктивних подій та максимізацію захисту ключових елементів критичної інфраструктури. Таким чином, виходячи з цих розрахунків, можна оцінити втрати за сценаріями розвитку надзвичайних ситуацій і виробити раціональні рішення щодо захисту ОКІ наявними силами та засобами.

Метод мінімакс є стратегією оптимізації, яка використовується для мінімізації максимальних можливих втрат у ситуаціях прийняття рішень, зокрема в теорії ігор і аналізі ризиків. У контексті оцінювання загроз і ризиків, мінімакс може бути використаний для визначення оптимальної стратегії, яка забезпечує мінімальні можливі втрати навіть у найгірших умовах.

Для ілюстрації методу мінімакс, розглянемо матрицю рішень $A = [a_{ij}]$, де a_{ij} відображає втрати або ризики, пов'язані з вибором i -тої стратегії приймаючим рішенням і j -тої стратегії опонента. Для спрощення, припустимо, що обидва гравці мають однакову кількість стратегій n .

1. Знайдемо максимальні значення в кожному рядку матриці A :

$$\max(a_{ij}), \text{ для } i = 1, 2, \dots, n. \quad (4)$$

2. Знайдемо мінімальне значення серед знайдених максимальних значень:

$$\min[\max(a_{ij})]. \quad (5)$$

Це мінімальне значення з максимальних втрат (або ризиків) відображає оптимальний вибір стратегії з точки зору приймаючого рішення за допомогою методу мінімакса. Метод мінімакса може бути застосований для оцінювання загроз і ризиків у різних контекстах, таких як критична інфраструктура, фінанси, екологія та інші. У цьому випадку, матриця рішень A міститиме оцінки ризиків або втрат, пов'язаних із різними стратегіями управління та їх можливими наслідками, а метод мінімакса допоможе приймати рішення, які мінімізують найгірші можливі наслідки. Щоб застосувати метод мінімакса для даного графа розвитку надзвичайної ситуації критичної інфраструктури та значень збитків, спочатку потрібно визначити сценарії розвитку

надзвичайної ситуації та обчислити загальні збитки для кожного сценарію. Мінімакний принцип полягає в тому, щоб мінімізувати максимальні можливі збитки.

Для прикладу використання методики проведемо розрахунки для різних сценаріїв.

1. Визначимо сценарії розвитку надзвичайної ситуації на основі графа (рис. 5):

- сценарій 1: 1 → 2 → 3 → 4 → 5 → 6;
- сценарій 2: 1 → 8 → 3 → 4 → 5 → 6;
- сценарій 3: 7 → 8 → 9 → 10 → 5 → 6;
- сценарій 4: 7 → 8 → 11 → 12 → 13;

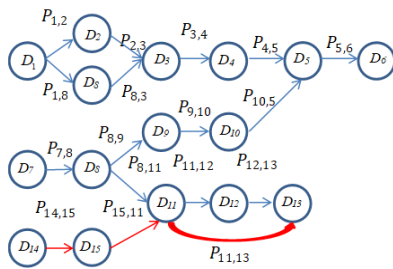


Рисунок 5 – Граф розвитку надзвичайної ситуації за сценаріями

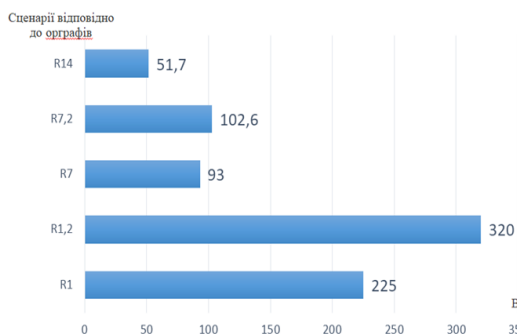
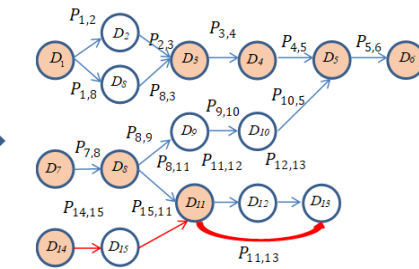


Рисунок 6 – Граф розвитку надзвичайної ситуації за сценаріями збитків

- сценарій 5: 14 → 15 → 11 → 13.
- 2. Обчислимо загальні збитки для кожного сценарію (рис. 6):
- сценарій 1: 10 + 50 + 100 + 500 + 100 + 100 = 860 млн. грн.;
- сценарій 2: 10 + 500 + 100 + 500 + 100 + 100 = 1310 млн. грн.;
- сценарій 3: 100 + 500 + 5 + 10 + 100 + 100 = 815 млн. грн.;
- сценарій 4: 100 + 500 + 100 + 1 + 1 = 702 млн. грн.;
- сценарій 5: 1 + 5 + 100 + 1 = 107 млн. грн.



3. Застосуємо метод мінімакса:
 Найгірший сценарій: сценарій 2 з максимальними збитками 1 410 млн. грн.;

Найкращий сценарій: сценарій 5 з мінімальними збитками 107 млн. грн.

4. Визначимо ключові деструктивні об'єкти для найгіршого сценарію: В даному випадку ключовими деструктивними об'єктами є ті, які призводять до найбільших збитків у найгіршому сценарії. У сценарії 2 ключовими деструктивними об'єктами є:

- об'єкт 1 (збитки: 10 млн. грн.);
- об'єкт 8 (збитки: 500 млн. грн.);
- об'єкт 3 (збитки: 100 млн. грн.);
- об'єкт 4 (збитки: 500 млн. грн.);
- об'єкт 5 (збитки: 100 млн. грн.);
- об'єкт 6 (збитки: 100 млн. грн.).

Загальні збитки в цьому сценарії становлять 1 310 млн. грн.

5. Визначимо ключові деструктивні об'єкти для найкращого сценарію: У сценарії 5 ключовими деструктивними об'єктами є:

- об'єкт 14 (збитки: 1 млн. грн.);
- об'єкт 15 (збитки: 5 млн. грн.);
- об'єкт 11 (збитки: 100 млн. грн.);
- об'єкт 13 (збитки: 1 млн. грн.).

Загальні збитки в цьому сценарії становлять 107 млн. грн.

Для оцінювання виграшу від використання методики доцільно визначити найгірший та найкращий сценарії розвитку надзвичайної ситуації, а також ключові деструктивні об'єкти. У цьому випадку найгірший сценарій передбачає збитки в 1 310 млн. грн., а найкращий сценарій – 107 млн. грн. Знання про ключові деструктивні об'єкти допоможе приймати ефективні рішення щодо зменшення потенційних збитків і забезпечення безпеки об'єктів критичної інфраструктури. Для даного орієнтовного графа ключові об'єкти, які припиняють подальший розвиток надзвичайної ситуації, можуть бути такі:

- об'єкт 2: забезпечення захисту або зниження ймовірності ураження об'єкта 2 може запобігти розвитку надзвичайної ситуації в напрямі 3 → 4 → 5 → 6;
- об'єкт 8: захист об'єкта 8 може також зупинити розвиток надзвичайної ситуації через 3 → 4 → 5 → 6;
- об'єкт 7: запобігання ураженню об'єкта 7 може зупинити розвиток надзвичайної ситуації через 8 → 9 → 10 → 5 → 6 та 8 → 11 → 12 → 13;

об'єкт 14: захист об'єкта 14 може зупинити розвиток надзвичайної ситуації через 15 → 11 → 13.

Ці об'єкти важливі, оскільки вони є відправними точками для подальшого розвитку ланцюга подій у графі. Забезпечення їхнього захисту або зниження ймовірності ураження може допомогти зупинити розвиток надзвичайної ситуації та зменшити потенційні збитки.

У результаті обчислень і визначення найбільш важливих ОКІ економія засобів оборони склала 43% у даному випадку та прийнятих умовах.

У результаті обчислень та визначення найбільш критичних сценаріїв економія засобів оборони склала 56% у даному випадку та прийнятих умовах.

Практичними результатами застосування методики можна зазначити такі висновки:

1. Для кожного ОКІ необхідно проводити детальний аналіз потенційних загроз та сценаріїв розвитку можливих подій з метою визначення рівня ризику та розробки ефективних заходів безпеки.

2. Методика є ефективним інструментом для визначення рівня ризику та визначення необхідних заходів для забезпечення безпеки ОКІ.

3. Використання методу мінімакса дає змогу обрати можливий варіант дій, що мінімізує максимальні витрати на захист ОКІ.

4. Для ефективного використання Методики необхідно постійно моніторити потенційні загрози та проводити оновлення даних щодо їх характеру та ступеня ризику.

5. Розроблення на основі Методики спеціалізованого програмного забезпечення є важливим інструментом для визначення раціонального розподілу сил і засобів стосовно надійного захисту ОКІ від реалізації потенційних загроз.

Висновки й перспективи подальших досліджень

У статті викладено методику оцінювання загроз і ризиків для об'єктів критичної інфраструктури за

сценаріями розвитку надзвичайних ситуацій, що удосконалена шляхом декомпозиції методик оцінювання загроз для об'єктів критичної інфраструктури в зоні ведення бойових дій та оцінювання ризиків для об'єктів критичної інфраструктури внаслідок бойових дій, враховуючи виникнення надзвичайних ситуацій в умовах обмеженості сил і засобів оборони об'єктів критичної інфраструктури. Методика включає п'ять послідовних блоків, що дає змогу приймати раціональні управлінські рішення для впровадження відповідних заходів безпеки та оборони, здійснення оптимального розподілу сил і засобів і мінімізації наслідків надзвичайних ситуацій застосовуючи інформаційні технології. Методика дає змогу оцінювати можливі ризики та визначати стратегії захисту об'єктів критичної інфраструктури. Проведені розрахунки ймовірностей настання надзвичайних ситуацій та потенційних збитків з визначенням сценаріїв максимальних і мінімальних збитків та визначення ключових об'єктів критичної інфраструктури підтверджують адекватність розробленої методики.

Проте, слід відмітити, що Методика є лише одним інструментом для забезпечення безпеки ОКІ під час можливих бойових дій. Її використання має бути поєднане з іншими методами, такими як фізичний захист об'єктів критичної інфраструктури, контроль доступу, моніторинг та нагляд за цими об'єктами, а також ефективною системою реагування на небезпеку та ліквідації наслідків катастроф.

Перспективним напрямом подальших досліджень слід вважати розвиток методів і методик захисту критичної інфраструктури з урахуванням ризик-орієнтованого підходу, а також розроблення спеціалізованого програмного забезпечення для визначення раціонального розподілу сил і засобів стосовно надійного захисту об'єктів критичної інфраструктури від реалізації потенційних загроз.

Список бібліографічних посилань

- Лисиченко Г. В., Забулонов Ю. Л., Хміль Г. А. Природний, техногенний та екологічний ризики: аналіз, оцінка, управління : монографія. Київ : НАНУ, 2008. 542 с.
- Мурасов Р., Мельник Я., Марко В. Порівняння існуючих методик оцінювання загроз і ризиків для потенційно-небезпечних об'єктів критичної інфраструктури в зоні ведення бойових дій. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2022. № 3(45), С. 32–36. DOI: 10.33099/2311-7249/2022-45-3-32-36.
- Мурасов Р., Тертишний Б. Методика розрахунку наслідків пошкодження (руйнування) гідротехнічних споруд критичної інфраструктури. *Social Development and Security*. 2022. № 12(6). С. 140–152. DOI: 10.33445/sds.2022.12.6.12.
- Куртсеїтов Т., Мурасов Р., Мельник Ю. Обчислення надійності системи критичної інфраструктури шляхом декомпозиції її як складної системи. *Social Development and Security*. 2022. № 12(5). С. 84–92. DOI: 10.33445/sds.2022.12.5.8.
- Мещеряков І., Антонов А. Удосконалена методика оцінки ефективності хімічного, біологічного, радіологічного та ядерного захисту. *Social Development and Security*. 2023. № 13(1). С. 161–176. DOI: 10.33445/sds.2023.13.1.14.
- Мурасов Р., Мельник Я.

- Методика оцінювання захищеності кіберпростору об'єктів критичної інфраструктури України. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2023. № 1(46). С. 42–44. DOI: 10.33099/2311-7249/2023-46-1-41-44.
- Нікітін А., Воробйов О., Парталія А., Куртсеїтов Т., Романюк В., Івашук О. Обґрунтування раціонального розподілу пунктів спеціальної обробки на маршрутах руху в разі руйнування об'єкта ядерної енергетики. *Соціальний розвиток і безпека*. 2022. № 12(4). С. 129–137. DOI: 10.33445/sds.2022.12.4.12.
 - Чумаченко С., Кутвий О., Михайлова А. Застосування експертно-аналітичних методів для оцінювання загроз об'єктам критичної інфраструктури оборонно-промислового комплексу на сході України. *Інженерія природокористування*. 2020. № 4(18). С. 114–123. URL: <https://repo.btu.kharkov.ua/bitstream/123456789/1580/1/17.pdf> (дата звернення: 28.09.2023).
 - Mardirossian G., Rangelov B., Getsov P., Zabunov S. Two Innovations for Critical Infrastructure Protection from Natural Disasters. *Proceedings of the Bulgarian Academy of Sciences*. 2023. Vol. 76. № 10. Pp. 1554–1561. DOI: 10.7546/CRABS.2023.10.09.
 - Мурасов Р., Куртсеїтов Т., Чумаченко С., Лунова О., Піріков О.,

Луньов А., Чумаченко С. Математична модель оцінки загроз для об'єктів критичної інфраструктури в зоні ведення бойових дій. *Проблемне програмування*. 2022. № 3–4. С. 446–454. DOI: 10.15407/pp2022.03-04.446.

11. Мурасов Р. Метод оцінювання ризиків для об'єктів критичної інфраструктури в умовах бойових дій з урахуванням їх деструктивно-кумулятивного потенціалу. *Social Development and Security*. 2023. № 13 (1). С. 152–160. DOI: 10.33445/sds.2023.13.1.13.

112. Чумаченко С., Мурасов Р., Мельник Я. Теоретико-методологічні основи інформаційного аналізу еколого-техногенних загроз для об'єктів критичної інфраструктури в умовах збройного конфлікту на сході України. *Сучасні інформаційні технології у сфері безпеки*

та оборони. 2021. № 1(40). С. 117–122. DOI: 10.33099/2311-7249/2021-40-1-117-122.

13. Мурасов Р., Чумаченко С., Пиріков О., Гуйда О., Ківа І. Особливості побудови математичної моделі оцінювання загроз для об'єктів критичної інфраструктури з використанням теорії графів. *Вчені записки ТНУ імені В.І. Вернадського серія "Технічні науки"*. 2021 № 6. С. 110–116. DOI: 10.32838/2663-5941/2021.6/18.

14. Звіт про прямі збитки інфраструктури від руйнувань внаслідок військової агресії росії проти України за рік від початку повномасштабного вторгнення. URL: https://kse.ua/wp-content/uploads/2023/03/UKR_Feb23_FINAL_Damages-Report-1.pdf (дата звернення: 28.09.2023).

METHODOLOGY FOR ASSESSING THREATS AND RISKS FOR CRITICAL INFRASTRUCTURE OBJECTS UNDER EMERGENCY DEVELOPMENT SCENARIOS

Murasov Rustam (Candidate of Technical Sciences)¹

Nikitin Anatolii (Doctor of Philosophy)¹

Meshcheriakov Ivan (Doctor of Philosophy)¹

Pidhorodetskyi Mykola (Candidate of Military Sciences)¹

Poplavets Serhii (Doctor of Philosophy)²

¹ *National Defence University of Ukraine, Kyiv, Ukraine*

² *Kharkiv National University of the Air Force named after Ivan Kozhedub, Kharkiv, Ukraine*

Formulation of the problem in general. *In the conditions of the large-scale invasion of the Russian Federation into Ukraine at the level of repelling the armed aggression of the enemy, there was an urgent need to protect not only the defense forces of the state, but also civilian objects that have nothing to do with the military sector. For the aggressor country, both the places of residence of the population and the objects of critical infrastructure that ensure life on the entire territory of Ukraine became targets for destruction. As a result of the unilateral withdrawal of the Russian Federation from the grain agreement, granaries and the surrounding infrastructure were affected. In this way, Russia terrorizes not only Ukraine, but also leads to food shortages in many countries of the world. The purpose of the article is to improve the methodology of threat and risk assessment for critical infrastructure objects under the scenarios of the development of emergency situations in order to prevent losses of the population and personnel of the defense forces. During the research, the analytical method was used to analyze the latest research and publications, the optimization method (based on minimum and maximum criteria) and the minimax method to choose the best option of actions and synthesis to achieve the research goal. The specified methodical approach makes it possible to analyze and decompose the existing methods of assessing threats to critical infrastructure objects in the area of hostilities and assessing risks to critical infrastructure objects as a result of hostilities.*

Analysis of recent researches and publications. *The analysis of recent research and publications showed that a large number of works were devoted to the issue of threat and risk assessment for critical infrastructure objects, in which the main concepts of risks and threats of critical infrastructure objects were proposed. Their order of calculation in a general form and presentation of the main scientific approaches to the principles of risk and threat assessment. Separate questions regarding the consequences of damage to critical infrastructure objects of various types and types of emergency situations were also investigated, which provides ample opportunities for a comprehensive assessment of cascading emergencies and their consequences of various nature. This is an extremely complex scientific problem, for the solution of which it is necessary to involve experienced specialists of various branches of science, where each one will solve a specialized scientific task. In these studies, the authors did not consider targeted attacks by the enemy on critical infrastructure objects, including for the creation of cascading emergency situations, which requires further research.*

Presenting the main material. *The developed methodology includes five consecutive blocks, which allows rational management decisions to be made with the aim of implementing appropriate security and defense measures, implementing the optimal distribution of forces and means, and minimizing the consequences of emergency situations, using information technologies.*

Elements of scientific novelty. *The methodology allows assessing possible risks and determining strategies for the protection of critical infrastructure objects, which confirms the adequacy of the obtained results.*

Practical significance of the article. *The method of assessing threats and risks for critical infrastructure objects based on scenarios of the development of emergency situations makes it possible to calculate options for scenarios of emergency events, assess damages, and choose the worst scenarios in order to prevent and localize them. This will allow to minimize the consequences of emergency situations in conditions of limited forces and means of defense of critical infrastructure objects.*

Conclusion and the perspectives of future researches. The article describes the Methodology for assessing threats and risks to critical infrastructure objects under emergency development scenarios through the decomposition and synthesis of the method for assessing threats to critical infrastructure objects in the area of hostilities and risk assessment methods. for critical infrastructure objects as a result of hostilities. The methodology includes five consecutive blocks, which allows you to make rational management decisions with the aim of implementing appropriate security and defense measures, implementing the optimal distribution of forces and means, minimizing the consequences of emergency situations using information technologies. The methodology makes it possible to assess possible risks and determine strategies for the protection of critical infrastructure objects, which confirms the adequacy of the obtained results. Calculations of the probabilities of the emergency system and potential losses with the determination of scenarios of maximum and minimum losses and the determination of key objects of critical infrastructure confirm the adequacy of the developed methodology. The developed Methodology requires further development, taking into account the risk-oriented approach, at the current stage for the prevention of armed aggression and remains a promising direction for further research and development of methods and techniques for the protection of critical infrastructure.

Key words: critical infrastructure facility, threat, risk, emergency situation, catastrophe, liquidation of the consequences of an emergency situation, minimization of the consequences of an emergency situation, information technologies.

References

1. **Lysychnenko, G., Zabulonov, Yu., Khmil, G.,** (2008). Natural, man-made and ecological risks: analysis, assessment, management. *Monograph*. Kyiv: Scientific thought, 542.
2. **Murasov, R., Melnyk, Y., Marko, V.,** (2022). Comparison of existing threat and risk assessment methods for potentially dangerous critical infrastructure facilities in the war zone. *Modern information technologies in the field of security and defense*. 3 (45), 32-36. DOI: 10.33099/2311-7249/2022-45-3-32-36.
3. **Murasov, R., Tertyshnyi, B.,** (2022). Methodology for calculating the consequences of failure (destruction) of hydrotechnical structures of critical infrastructure. *Social Development and Security*. 12 (6), 140-152. DOI: 10.33445/sds.2022.12.6.12.
4. **Kurtseitov, T., Murasov, R., Melnyk, Yu.,** (2022). Calculating the reliability of a critical infrastructure system by decomposing it as a complex system. *Social Development and Security*. 12 (5), 84-92. DOI:10.33445/sds.2022.12.5.8.
5. **Meshcheryakov, I., Antonov, A.,** (2023). An improved method of assessing the effectiveness of chemical, biological, radiological and nuclear protection. *Social Development and Security*. 13 (1), 161-176. DOI: 10.33445/sds.2023.13.1.14.
6. **Murasov, R. and Melnyk, Ya.,** (2023). Methodology for assessing cyberspace security of critical infrastructure objects of Ukraine. *Modern information technologies in the field of security and defense*. 1 (46), 42-44. DOI: 10.33099/2311-7249/2023-46-1-41-44.
7. **Nikitin, A., Vorobyov, O., Partalyan, A., Kurtseitov, T., Romanyuk, V., Ivashchuk, O.,** (2022). Justification of the rational distribution of special treatment points on traffic routes in the event of the destruction of a nuclear power facility. *Social development and security*. 12 (4), 129-137. DOI: 10.33445/sds.2022.12.4.12.
8. **Chumachenko, S., Kutovyi, O., Mykhaylova, A.,** (2020). Application of expert analytical methods to assess threats to critical infrastructure objects of the defense-industrial complex in eastern Ukraine. *Environmental engineering*. 4(18), 114-123. Available at: <https://repo.btu.kharkov.ua/bitstream/123456789/1580/1/17.pdf> [Accessed: 28 September 2023].
9. **Mardirossian, G., Rangelov, B., Getsov, P., Zabunov, S.,** (2023). Two Innovations for Critical Infrastructure Protection from Natural Disasters. *Proceedings of the Bulgarian Academy of Sciences*. 76, 10, 1554-1561. DOI: 10.7546/CRABS.2023.10.09.
10. **Murasov, R., Kurtseitov, T., Chumachenko, S., Lunyova, O., Pyrikov, O., Lunyov, A., Chumachenko, S.,** (2022). Mathematical model of threat assessment for critical infrastructure facilities in the war zone. *Problem Programming*. 3-4, 446-454. DOI: 10.15407/pp2022.03-04.446.
11. **Murasov R.,** (2023). The method of risk assessment for critical infrastructure objects in the conditions of hostilities, taking into account their destructive and cumulative potential. *Social Development and Security*. 13 (1), 152-160. DOI: 10.33445/sds.2023.13.1.13.
12. **Chumachenko, S., Murasov, R., Melnyk, Ya.,** (2021). Theoretical and methodological bases of information analysis of ecological and man-made threats to critical infrastructure facilities in the conditions of armed conflict in eastern Ukraine. *Modern information technologies in the field of security and defense*. 1 (40), 117-122. DOI: 10.33099/2311-7249/2021-40-1-117-122.
13. **Murasov, R., Chumachenko, S., Pyrikov, O., Guida, O., Kiva, I.,** (2021). Peculiarities of building a mathematical model of threat assessment for critical infrastructure objects using graph theory. *Academic notes of TNU named after V.I. Vernadsky series "Technical Sciences"*. 6, 110-116. DOI: 10.32838/2663-5941/2021.6/18.
14. **Report** on direct damage to infrastructure from the destruction caused by Russia's military aggression against Ukraine a year after the start of the full-scale invasion [online]. Available at: https://kse.ua/wp-content/uploads/2023/03/UKR_Feb23_FINAL_Damages-Report-1.pdf [Accessed : 28 September 2023].