Математична модель оцінювання ризиків функціонування об’єктів критичної інфраструктури на основі теорії нечіткої логіки

Mathematical model of risk assessment of the operation of critical infrastructure objects based on the theory of fuzzy logic

Рустам Мурасов [A]
Corresponding author: кан. техн. наук, професор кафедри, e-mail: rustamm@ukr.net, ORCID:0000-0003-0800-2062
Анатолій Нікітін [A]
Доктор філософії, професор кафедри, e-mail: tolik-nikitin@ukr.net, ORCID: 0000-0003-1487-0616
Іван Мещеряков [A]
Доктор філософії, доцент кафедри, e-mail: shulyk3004@ukr.net, ORCID: 0000-0001-5797-0735

Rustam Murasov [A]
Corresponding author: Candidate of Technology Sciences, Professor of the Department, e-mail: rustamm@ukr.net, ORCID: 0000-0003-0800-206
Anatolii Nikitin [A]
Doctor of Philosophy, Professor of the Department, e-mail: tolik-nikitin@ukr.net, ORCID: 0000-0003-1487-0616
Ivan Meshcheriakov [A]
Doctor of Philosophy, associate professor of the department, e-mail: shulyk3004@ukr.net, ORCID: 0000-0001-5797-0735

[A] Національний університет оборони України, м. Київ, Україна
[A]National Defense University of Ukraine, Kyiv, Ukraine

Received: October 4, 2024 | Revised: October 20, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.17

Мета роботи: розробка математичної моделі оцінювання ризиків функціонування об’єктів критичної інфраструктури на основі теорії нечіткої логіки.
Метод: теорія ймовірності, теорія нечіткої логіки, метод центру ваги, моделювання.
Результати дослідження: розроблена математична модель оцінювання ризиків функціонування об’єктів критичної інфраструктури на основі теорії нечіткої логіки. На практичному прикладі обчислення нечітких та невизначених даних перевірена її адекватність.
Теоретична цінність дослідження: процес оцінювання ризиків в наслідок ударів противника став більш адаптивним і точним для подальших досліджень.
Тип статті: дослідницька.

Purpose: development of a mathematical model for assessing the risks of the operation of critical infrastructure objects based on the theory of fuzzy logic
Method: theory of probability, fuzzy logic theory, center of gravity method, modeling.
Findings: a mathematical model was developed for assessing the risks of the operation of critical infrastructure objects based on fuzzy logic theory. Its adequacy is verified on a practical example of calculating fuzzy and uncertain data.
Theoretical implications: the process of assessing risks as a result of enemy strikes has become more adaptive and accurate for further research.
Papertype: research.

Ключові слова: критична інфраструктура, надзвичайна ситуація, нечітка логіка, ймовірність, загроза, захист, ризик.

Key words: critical infrastructure, emergency, fuzzy logic, probability, threat, protection, risk.

Вступ

Оцінювання ризиків функціонування об’єктів критичної інфраструктури є ключовим елементом забезпечення національної безпеки, оскільки дозволяє ідентифікувати можливі загрози та приймати рішення щодо їхнього усунення чи мінімізації. Традиційні методи оцінювання ризиків часто виявляються недостатньо ефективними через високу невизначеність і складність даних, що надходять з існуючих систем захисту критичної інфраструктури. В умовах постійно змінюваних загроз, таких як природні катаклізми, техногенні аварії або цілеспрямовані ракетно-дронові атаки рф, особливо актуальним є використання методів, які дозволяють працювати з нечіткими, неповними або непередбачуваними даними.

Використання теорії нечіткої логіки є одним із найбільш перспективних підходів для ідентифікації можливих загроз та оцінювання відповідних ризиків їх реалізації, оскільки вона дозволяє працювати з інформацією, яка не може бути точно виміряною або яка має значну невизначеність. Відповідно, застосування нечітких множин дозволяє ефективніше

моделювати реалізацію загроз для об’єктів критичної інфраструктури та оцінювати ризик їх функціонуванню на основі змінних, що не мають чітких границь або однозначних значень.

Сучасні виклики, зокрема пов’язані з військовими загрозами, кібератаками, природними катастрофами, потребують створення математичних моделей, здатних швидко реагувати на зміни та враховувати комплексність процесів. Особливо це актуально в умовах агресивних ракетно-дронових атак на об’єкти критичної інфраструктури, що може призвести до каскадних деструктивних наслідків. Знищення ключових об’єктів атомної енергетики, гідросистем, водопостачання, зв’язку чи транспорту може викликати великомасштабні аварії, що впливають на економіку, екологію та населення.

Теоретичні основи дослідження

Аналіз останніх публікацій [1-4] стосовно підходів до ідентифікації загроз і оцінювання ризиків на основі теорії нечіткої логіки свідчить, що застосування нечіткої логіки для оцінювання ризиків функціонування критичної інфраструктури є актуальним напрямком дослідження через високу невизначеність даних і складність системи. Методи, які запропоновані у попередніх дослідженнях, демонструють, що нечітка логіка є ефективним інструментом для моделювання надзвичайних ситуацій та ідентифікації загроз і оцінювання ризиків.

На думку багатьох провідних фахівців [5-12], які досліджували питання захисту об’єктів критичної інфраструктури (ОКІ), на сьогодні не існує загальноприйнятої методики для ідентифікації загроз і оцінювання ризиків функціонування ОКІ, особливо в умовах ракетно-дронових атак. Існують тільки часткові рішення для окремих об'єктів або конкретних надзвичайних ситуацій. Основним пріоритетом ставиться мінімізація наслідків надзвичайних ситуацій на ОКІ. Крім того, підходи до оцінювання ризиків функціонування ОКІ здебільшого фокусуються на проведенні аварійно-рятувальних заходів, спрямованих на усунення наслідків, а не на проактивні стратегії попередження можливих загроз. В умовах сучасних викликів, таких як масовані ракетно-дронові атаки рф, ці методи залишаються недостатньо ефективними. Існуючі методики не враховують комплексний характер взаємодії різних типів загроз і обмежуються аналізом ризиків на локальному рівні, не забезпечуючи системного підходу до управління ризиками. Світовий досвід також вказує на те, що основна увага зосереджується на відновленні після події, але не на попередженні або мінімізації реалізації загрози.

Загалом, аналіз зазначених джерел свідчить про активне використання нечіткої логіки та інших математичних методів для оцінювання ризиків функціонування ОКІ. Ці методи дозволяють працювати з невизначеністю та складністю таких систем, що робить їх незамінними інструментами для ідентифікації загроз і оцінювання ризиків функціонування ОКІ під час виникнення надзвичайних ситуацій та в разі вчинення терористичних актів.

Постановка проблеми

Зважаючи на важливість захисту об’єктів критичної інфраструктури, розробка математичних моделей для оцінювання ризиків функціонування ОКІ на основі нечіткої логіки стає вкрай необхідною. Такі моделі дозволяють формалізувати взаємозв’язки між ймовірністю реалізації загроз, ступенем їх впливу на функціонування ОКІ та ефективністю засобів захисту ОКІ. Вони також дають змогу враховувати широкий спектр можливих сценаріїв, роблячи процес оцінювання ризиків більш адаптивним і точним.

Таким чином, метою цієї роботи є розробка математичної моделі оцінювання ризиків функціонування ОКІ на основі теорії нечіткої логіки, яка дозволить працювати з невизначеними даними та забезпечить точнішу оцінку можливих загроз.

Результати

Актуальні виклики сьогодення, такі як військові загрози, вторинні деструктивні впливи та природні катаклізми, потребують створення математичних моделей, здатних швидко адаптуватися до змін і враховувати багатофакторність процесів. Це особливо актуально при захисті від ракетно-дронових атак на ОКІ, оскільки вони можуть спровокувати ланцюгові руйнівні аварії та катастрофи, що матимуть значний вплив на економічний стан країни, стан довкілля та добробут населення.

Із найперспективніших підходів до вирішення цієї проблеми є теорія нечіткої логіки, яка дає можливість аналізувати інформацію, яка не піддається точному вимірюванню або має значний рівень невизначеності. Застосування нечітких множин забезпечує більш ефективну ідентифікацію і моделювання загроз для функціонування ОКІ та дозволяє оцінювати ризик на основі даних, які не мають чітких меж.

Тому виникає необхідність, щодо розробки та опису математичної моделі оцінювання ризиків функціонування ОКІ на основі теорії нечіткої логіки яка представлена на рис. 1.

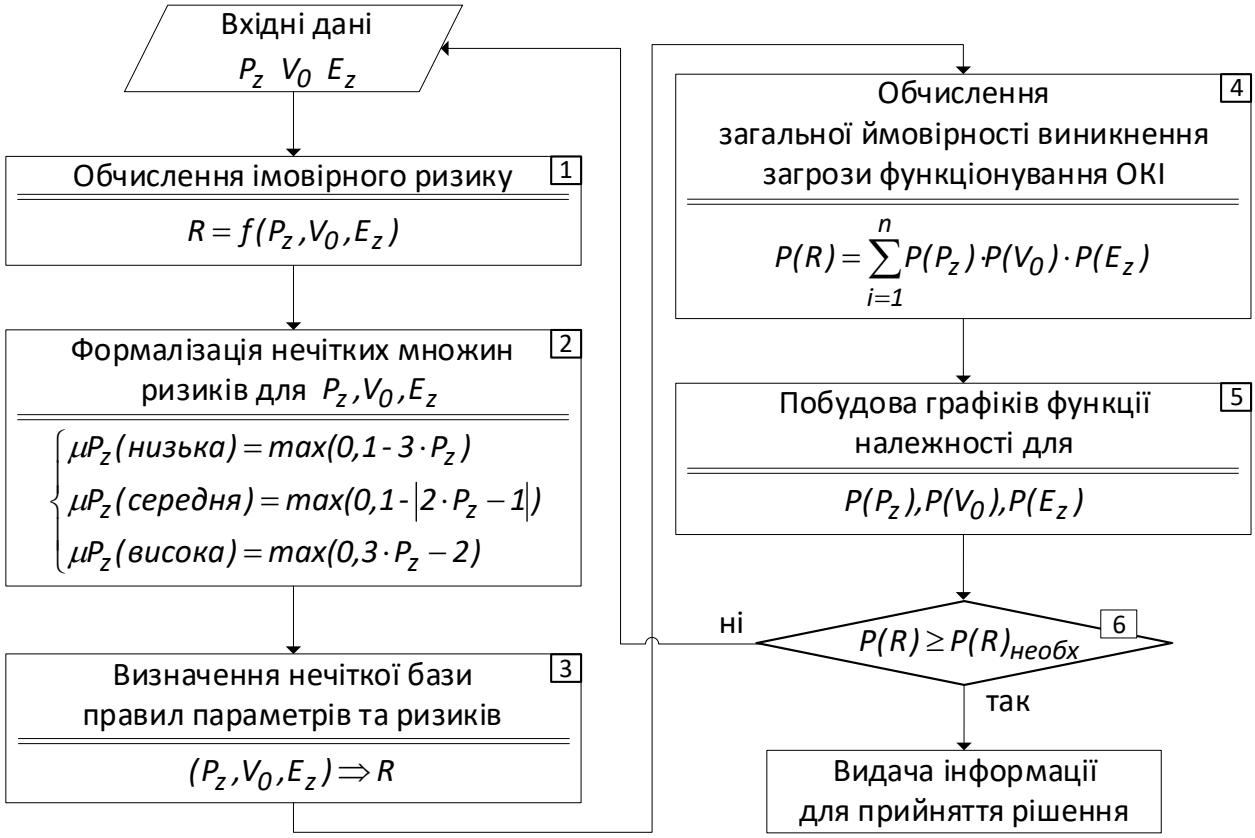

Рисунок 1 – Структурно-логічна схема математичної моделі оцінювання ризиків критичної інфраструктури на основі теорії нечіткої логіки

Блок 1. Обчислення імовірного ризику.

Метою є оцінювання ризику функціонування ОКІ з урахуванням таких основних параметрів:

P_z – ймовірність виникнення загрози;

V_0 – рівень впливу загрози на об’єкт;

E_z – ефективність засобів захисту.

Рівень ризику R розраховується на основі трьох змінних і визначається як:

$$R = f(P_z, V_0, E_z). \quad (1)$$

Кожен із цих параметрів є нечітким, тому їх необхідно моделювати за допомогою функцій належності.

Блок 2. Формалізація нечітких множин.

Для кожної змінної ми використовуємо три рівні належності: “низька”, “середня”, “висока”. Ці рівні задаються трикутними функціями належності.

Функції належності для ймовірності виникнення загрози P_z визначаються таким чином:

$$\begin{cases} \mu P_z(низька) = max(0,1\text{-}3 \cdot P_z) \\ \mu P_z(середня) = max(0,1\text{-}|2 \cdot P_z - 1|), \\ \mu P_z(висока) = max(0,3 \cdot P_z - 2) \end{cases} \quad (2)$$

де, μP_z – функція належності для параметра P_z.

Функції належності для рівня впливу загрози на об’єкт V_0 визначаються таким чином:

$$\begin{cases} \mu V_0(низький) = max(\,0,1 - 3 \cdot V_0) \\ \mu V_0(середній) = max(\,0,1 - |2 \cdot V_0 - 1|). \\ \mu V_0(високий) = max(\,0,3 \cdot V_0 - 2) \end{cases} \quad (3)$$

Функції належності для ефективності засобів захисту E_z визначаються таким чином:

$$\begin{cases} \mu E_z(низький) = max(\,0,1\text{-}3 \cdot E_z) \\ \mu E_z(середній) = max(\,0,1\text{-}|2 \cdot E_z - 1|). \\ \mu E_z(високий) = max(\,0,3 \cdot E_z - 2) \end{cases} \quad (4)$$

Блок 3. Визначення нечіткої бази правил параметрів та ризику

Правила в нечіткій базі знань мають вигляд умов “якщо-то”, які визначають взаємозв’язок між параметрами P_z, V_0, E_z та ризиком R.

$$(P_z, V_0, E_z) \Rightarrow R. \quad (5)$$

Показник між параметрами та ризиком визначається за табл. 1.

Таблиця 1 – Нечітка база правил

Правило	P_z	V_0	E_z	R
1	Низька	Низький	Високий	Низький
2	Низька	Високий	Низький	Середній
3	Середня	Середній	Середній	Середній
4	Висока	Високий	Низький	Високий
5	Середня	Високий	Високий	Низький
6	Висока	Низький	Середній	Високий

Блок 4. Обчислення загальної ймовірності виникнення загрози функціонування ОКІ.

Для обчислення загальної ймовірності ризику ми можемо скористатися комбінованою оцінкою, яка враховує ймовірності різних загроз, їх впливу та ефективності захисту. Нехай $P(P_z), P(V_0), P(E_z)$ – ймовірності значень відповідних параметрів.

Сукупний рівень ризику можна виразити так:

$$P(R) = \sum_{i=1}^{n} P(P_z) \cdot P(V_0) \cdot P(E_z) \quad (6)$$

Блок 5. Побудова графіків функції належності.

Для кращого розуміння, як функції належності описують кожен параметр, побудуємо графіки для $P(P_z), P(V_0), P(E_z)$.

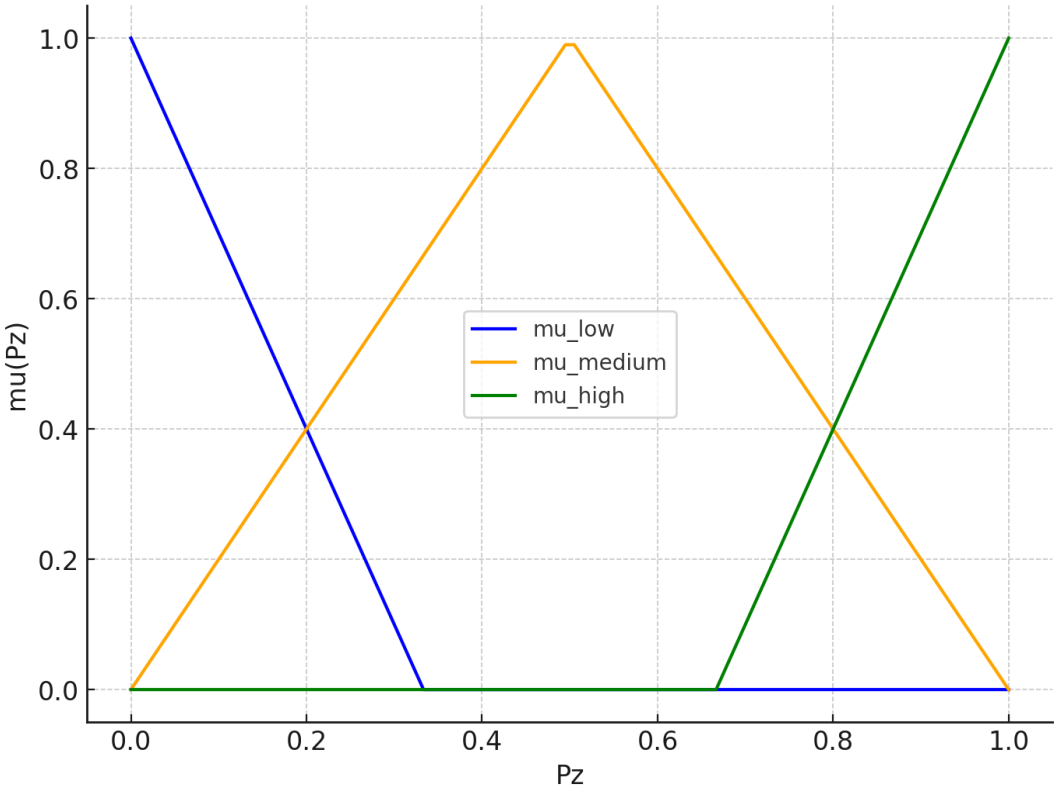

Рисунок 2 – Функція належності для параметра P_z

З цього графіка можна зрозуміти, як змінюються функції належності для різних значень параметра P_z. Він показує три функції належності – “низький”, “середній” і “високий” рівні значень P_z, які мають наступні властивості:

Низький рівень (mu_low) — функція належності має найбільші значення при малих значеннях P_z. Вона починається з максимальної належності (1) при P_z = 0 і лінійно зменшується до нуля при P_z=0,33.

Середній рівень (mu_medium) — ця функція має найбільшу належність при середніх значеннях P_z (близько 0,5). Вона є симетричною і досягає 1 при P_z = 0,5, а потім плавно зменшується до нуля при дуже малих або великих значеннях P_z.

Високий рівень (mu_high) — функція належності для високих значень P_z. Вона починається з нуля при P_z = 0,67, а потім лінійно зростає до 1 при P_z = 1.

Цей графік демонструє, що параметр P_z може належати до різних категорій (низький, середній, високий) з різним ступенем впевненості в залежності від свого значення.

Блок 6. Перевірка умов визначення показника ефективності запобігання реалізації ризику.

Для визначення показника ефективності пропонується використовувати наступний

критерій:

$$P(R) \geq P(R)_{\text{необх}} \quad (7)$$

Адекватність описано моделі оцінювання ризиків критичної інфраструктури на основі теорії нечіткої логіки перевіримо на практичному прикладі обчислення нечітких та невизначених даних.

Припустимо, що значення параметрів такі:

P_z = 0,6 – ймовірність виникнення загрози,

V_0 = 0,8 – рівень впливу загрози на об'єкт,

E_z = 0,4 – ефективність засобів захисту.

Для кожного параметра визначаємо відповідні значення функцій належності: "низька", "середня", "висока". Ці рівні задаються трикутними функціями належності.

Функції належності для параметра P_z:

низька: $\mu P_z(низька) = max(0,1 - 3P_z)$ для P_z = 0,6: $\mu P_z(низька) = max(0,1 - 3 \cdot 0,6) = 0$;

середня: $\mu P_z(середня) = max(0,1 - |2P_z - 1|)$ для P_z = 0,6: $\mu P_z(середня) = max(0,1 - |2 \cdot 0,6 - 1|) = 0,8$;

висока: $\mu P_z(висока) = max(0,3P_z - 2)$ для P_z = 0,6: $\mu P_z(висока) = max(0,3 \cdot 0,6 - 2) = 0,8$.

Функції належності для параметра V_0:

низька: $\mu V_0(низька) = max(0,1 - 3V_0)$ для V_0 = 0,8: $\mu V_0(низька) = max(0,1 - 3 \cdot 0,8) = 0$;

середня: $\mu V_0(середня) = max(0,1 - |2V_0 - 1|)$ для V_0 = 0,8: $\mu V_0(середня) = max(0,1 - |2 \cdot 0,8 - 1|) = 0,4$;

висока: $\mu V_0(висока) = max(0,3V_0 - 2)$ для V_0 = 0,8: $\mu V_0(висока) = 1$.

Функції належності для параметра E_z:

низька: $\mu E_z(низька) = max(0,1 - 3E_z)$ для E_z = 0,4: $\mu E_z(низька) = max(0,1 - 3 \cdot 0,4) = 0,8$;

середня: $\mu E_z(середня) = max(0,1 - |2E_z - 1|)$ для E_z = 0,4: $\mu E_z(середня) = 0,6$;

висока: $\mu E_z(висока) = max(0,3E_z - 2)$ для E_z = 0,4: $\mu E_z(висока) = 0$.

Згідно з нечітким правилом: "якщо P_z середня, V_0 середній, а E_z середня, то ризик середній", мінімальне значення належності для цього правила:

$$\mu R = min(\mu P_z(середня); \mu V_0(середня); \mu E_z(середня)) = min(0,8;0,4;0,6) = 0,4$$

Сукупний рівень ризику визначається за комбінованою оцінкою ймовірностей різних загроз, їх впливу та ефективності захисту:

$$P(R) = P(P_z) \cdot P(V_0) \cdot P(E_z) = 0,8 \cdot 0,4 \cdot 0,6 = 0,192.$$

Отже, сукупний рівень ризику становить $P(R)$ = 0,192.

Процес дефазифікації (розширений опис) дозволяє перетворити нечітке значення ризику R на чітке значення ризику R_{crips}. Для цього використовується метод центру ваги. Він визначає чітке значення R_{crips} на основі інтегралів площі функцій належності вихідної змінної.

Якщо нечітка множина для вихідного ризику описується функціями належності, побудованими для низького, середнього та високого ризиків, тоді формула виглядає так:

$$R_{crips} = \frac{\int_x \mu R(x) x dx}{\int_x \mu R(x) dx}. \quad (8)$$

Для нашого прикладу, після обчислення інтегралів ризик складає приблизно: $R_{\text{crips}} \approx 0{,}55$.

Висновки

У статті розроблена математична модель оцінювання ризиків функціонування ОКІ на основі теорії нечіткої логіки, яка є ефективним інструментом для обробки нечітких та невизначених даних з можливістю отримати чітке значення результату. Розроблена математична модель дозволяє:

використовувати невизначену інформацію для оцінки ризиків, що робить її придатною для застосування в умовах неповних даних;

побудувати нечітку базу правил, яка відображає складні взаємозв'язки між загрозами, рівнем впливу та ефективністю захисту;

включати в розрахунки ймовірнісні оцінки, що дозволяє більш точно прогнозувати ризики.

Застосування методів дефазифікації, зокрема методу центру ваги, дозволяє отримати чітке значення ризику, що є важливим для прийняття рішень в умовах реальних загроз. Модель є гнучкою і може бути адаптована для інших областей, таких як техногенна безпека та екологічний моніторинг.

Ми отримали змогу враховувати широкий спектр можливих сценаріїв, роблячи процес оцінювання ризиків більш адаптивним і точним для подальших досліджень.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Amini, A., Jamil, N., Ahmad, A.R. & Sulaiman, H. (2017). Підхід до оцінки ризиків на основі нечіткої логіки для оцінки та визначення пріоритетів ризиків у середовищі хмарних обчислень. – Recent Trends in Information and Communication Technology Lecture Notes on Data Engineering and Communications Technologies, 650-659. https://doi.org/10.1007/978-3-319-59427-9_67 [Дата звернення 1.10.2024].
2. Wang, Y.M., & Elhag, T.M.S. (2006). Метод нечіткої TOPSIS на основі наборів альфа-рівнів із застосуванням для поєднання оцінки ризику. – Expert Systems with Applications, 31(2), 309-319. https://doi.org/10.1016/j.eswa.2005.09.040 [Дата звернення 1.10.2024].
3. Haimes, Y.Y. (2004). Моделювання, оцінка та управління ризиками. – John Wiley & Sons. URL: https://onlinelibrary.wiley.com/doi/book/10.1002/0471723908 [Дата звернення 1.10.2024].
4. Фадєєва І.Г., Гринюк О.І. (2017). Нечітке моделювання в оцінці ризиків діяльності нафтогазовидобувних підприємств. – Балтійський журнал економічних досліджень, 3 (4), 256–264. https://doi.org/10.30525/2256-0742/2017-3-4-256-264 [Дата звернення 1.10.2024].
5. Мурасов Р., Нікітін А., Мещеряков І., Підгородецький М., Поплавець С. (2024). Удосконалення науково-методичного апарату для розрахунку ризиків виникнення та

аналізу сценаріїв надзвичайних ситуацій на об'єктах критичної інфраструктури. *Social Development and Security*, 14 (1), 205-217. https://doi.org/10.33445/sds.2024.14.1.17 [Дата звернення 1.10.2024].

6. Мурасов Р., Нікітін А., Мещеряков І., Підгородецький М., Поплавець С. (2024). Методика оцінювання загроз і ризиків для об'єктів критичної інфраструктури за сценаріями розвитку надзвичайних ситуацій. – Сучасні інформаційні технології у сфері безпеки та оборони, 3(48), 35-43. https://doi.org/10.33099/2311-7249/2023-48-3-35-43 [Дата звернення 1.10.2024].
7. Мурасов, Р., & Мещеряков, І. (2023). Інформаційно-технічний метод попередження надзвичайних ситуацій терористичного характеру шляхом оцінки можливості ступеневого росту деструктивних подій викликаних каскадними наслідками первинного терористичного впливу. *Social Development and Security*, *13*(5), 180-191. https://doi.org/10.33445/sds.2023.13.5.17 [Дата звернення 1.10.2024].
8. Фурсенко О.М., Чумаченко С.М. та Кармазин С.В. (2015) Експертна оцінка загроз для об'єктів критичної інфраструктури газотранспортної системи України з використанням методу аналізу ієрархій. – Техногенно-екологічна безпека та цивільний захист, 9, 68-77. URL: http://tes.igns.gov.ua/wp-content/uploads/2018/02/V9.pdf [Дата звернення 1.10.2024].
9. Wolbers J., Groenewegen P., Mollee J., & Bím J. (2013). Включення динаміки часу в аналіз соціальних мереж в управлінні надзвичайними ситуаціями. – Journal of Homeland Security and Emergency Management, 10(2), 555-585. https://doi.org/10.1515/jhsem-2013-0019 [Дата звернення 1.10.2024].
10. Яременко О.І., Страхніцький Я.О. (2022). Визначення та управління загрозами у структурі державної політики захисту критичної інфраструктури. – Університетські наукові записки, 3 (87), 73-82. https://doi.org/10.37491/UNZ.87.6 [Дата звернення 1.10.2024].
11. Ruban, I., Khudov, H., Makoveichuk, O., Khizhnyak, I., Khudov, V., Podlipaiev, V., Shumeiko, V., Atrasevych, O., Nikitin, A., & Khudov, R. (2019). Segmentation of opticalelectronic images from on-board systems of remote sensing of the earth by the artificial bee colony method. – Eastern-European Journal of Enterprise Technologies, 2 (9-98), 37-45. https://doi: 10.15587/1729-4061.2019.161860 [Дата звернення 1.10.2024].
12. Trysnyuk, V., Trysnyuk, T., Nikitin, A., Kurylo, A., & Demydenko, O. (2021). Geomodels of space monitoring of water bodies. – E3S Web of Conferences, 280, art. no. 09016. https://doi: 10.1051/e3sconf/202128009016 [Дата звернення 1.10.2024].

References

1 Amini, A., Jamil, N., Ahmad, A.R. & Sulaiman, H. (2017). A Fuzzy Logic Based Risk Assessment Approach for Evaluating and Prioritizing Risks in Cloud Computing Environment. *Recent Trends in Information and Communication Technology Lecture Notes on Data Engineering and Communications Technologies*, 650-659. https://doi.org/10.1007/978-3-319-59427-9_67 [Accessed date 1.10.2024].

2. Wang, Y.M., & Elhag, T.M.S. (2006). Fuzzy TOPSIS method based on alpha level sets with an application to bridge risk assessment. *Expert Systems with Applications*, 31(2), 309-319. https://doi.org/10.1016/j.eswa.2005.09.040 [Accessed date 1.10.2024].
3. Haimes, Y.Y. (2004). Risk modeling, assessment, and management. – John Wiley & Sons. URL: https://onlinelibrary.wiley.com/doi/book/10.1002/0471723908 [Accessed date 1.10.2024].
4. Fadyeyeva, I., & Gryniuk, O. (2017). Fuzzy modelling in risk assessment of oil and gas production enterprises' activity. *Baltic Journal of Economic Studies*, 3 (4), 256–264. https://doi.org/10.30525/2256-0742/2017-3-4-256-264 [Accessed date 1.10.2024].
5. Murasov, R., Nikitin, A., Meshcheriakov, I., Pidhorodetskyi, M., & Poplavets, S. (2024).

Improvement of the scientific and methodological apparatus for calculating the risks of occurrence and analyzing scenarios of emergency situations at critical infrastructure facilities. *Social Development and Security*, 14(1), 205-217. https://doi.org/10.33445/sds.2024.14.1.17 [Accessed date 1.10.2024].

6. Murasov, R., Nikitin, A., Meshcheriakov, I., Pidhorodetskyi, M., & Poplavets, S. (2024). Methodology for assessing threats and risks for critical infrastructure objects under emergency development scenarios. *Modern Information Technologies in the Sphere of Security and Defence*, 3(48), 35-43. https://doi.org/10.33099/2311-7249/2023-48-3-35-43 [Accessed date 1.10.2024].
7. Murasov, R., & Meshcheriakov, I. (2023). The information and technical method of preventing emergency situations of a terrorist nature by assessing the possibility of gradual growth of destructive events caused by the cascading consequences of the primary terrorist impact. *Social Development and Security*, 13(5), 180-191. https://doi.org/10.33445/sds.2023.13.5.17 [Accessed date 1.10.2024].
8. Fursenko, O.M., Chumachenko, S.M., & Karmazyn, S.V. (2015). Expert assessment of threats to objects of critical infrastructure of the gas transportation system of Ukraine using the method of analysis of hierarchies. *Technogenic and ecological safety and civil protection*, 9, 68-77. Available from: http://tes.igns.gov.ua/wp-content/uploads/2018/02/V9.pdf [Accessed date 1.10.2024].
9. Wolbers J., Groenewegen P., Mollee J., & Bím J. (2013). Incorporating Time Dynamics in the Analysis of Social Networks in Emergency Management. *Journal of Homeland Security and Emergency Management*, 10(2), 555-585. https://doi.org/10.1515/jhsem-2013-0019 [Accessed date 1.10.2024].
10. Yaremenko, O., & Strahnitskyi, Y. (2022). Detection and Management of Threats in the Structure of State Policy for Critical Infrastructure Protection. *University Scientific Notes*, 3 (87), 73-82. https://doi.org/10.37491/UNZ.87.6 [Accessed date 1.10.2024].
11. Ruban, I., Khudov, H., Makoveichuk, O., Khizhnyak, I., Khudov, V., Podlipaiev, V., Shumeiko, V., Atrasevych, O., Nikitin, A., & Khudov, R. (2019). Segmentation of opticalelectronic images from on-board systems of remote sensing of the earth by the artificial bee colony method. *Eastern-European Journal of Enterprise Technologies*, 2 (9-98), 37-45. https://doi: 10.15587/1729-4061.2019.161860 [Accessed date 1.10.2024].
12. Trysnyuk, V., Trysnyuk, T., Nikitin, A., Kurylo, A., & Demydenko, O. (2021). Geomodels of space monitoring of water bodies. *E3S Web of Conferences*, 280, art. no. 09016. https://doi: 10.1051/e3sconf/202128009016 [Accessed date 1.10.2024].