УДК 519.713:517:338
DOI https://doi.org/10.32782/2663-5941/2025.2.2/27

Савченко І. О.
Національний університет харчових технологій

Мацько П. І.
Національний університет оборони України

СИСТЕМНИЙ ПІДХІД ДО ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ЗАГРОЗ КРИТИЧНІЙ ІНФРАСТРУКТУРІ З ВИКОРИСТАННЯМ МЕТОДІВ ЕКСПЕРТНОГО ОЦІНЮВАННЯ

У даній роботі розглядається проблема оцінки загроз критичній інфраструктурі в умовах війни та їх вплив на національну безпеку. Важливість прийняття рішень у умовах невизначеності підкреслюється як ключовий аспект управління ризиками для критичної інфраструктури.

Також автори провели аналіз раніше опублікованих наукових матеріалів, що стосуються застосування різноманітних експертних методів для оцінювання небезпек та потенційних негативних наслідків надзвичайних ситуацій, що можуть виникнути на об'єктах критичної інфраструктури України в умовах триваючої збройної агресії з боку Російської Федерації.

Для аналітичного зважування потенційних небезпек для критичної інфраструктури в контексті сучасної російсько-української війни, розглянуто перспективу застосування методів експертного оцінювання. Сформульовано необхідні рекомендації та висновки щодо його ефективності та доцільності в цьому випадку. З використанням власного програмного забезпечення, розробленого авторами на Python, проведено практичні розрахунки, підкріплені науковими обґрунтуванням висновків щодо потенційних загроз. Завдяки цій програмі було реалізовано процедуру підтримки прийняття рішень щодо визначення пріоритетності загроз для об'єктів критичної інфраструктури, зважаючи на ступінь ризиків, ймовірність та можливі збитки від пошкодження.

На підставі даних, отриманих внаслідок функціонування програмного забезпечення, стає очевидним, що використання методів експертного оцінювання забезпечує можливість дослідження ризиків для критичної інфраструктури в умовах апріорної невизначеності, враховуючи ймовірнісний характер воєнних дій та стохастичність ракетно-дронових атак.

Програма надає можливість створити ранжований список потенційних загроз, провести процеуру відсіювання тих загроз, що не мають першочергового значення. Це робиться задля ефективного розподілу обмежених сил та ресурсів для зменшення ймовірного негативного впливу надзвичайних ситуацій природного, техногенного та воєнно-техногенного характеру.

Ключові слова: *критична інфраструктура, загрози, ракетно-дронові удари, експертна оцінка, Python, процедура оцінювання, мінімізація ризиків, надзвичайні ситуації, цивільний захист.*

Постановка проблеми. У воєнний час, критична інфраструктура є фундаментальною складовою національної безпеки держави. Порушення її роботи, або ж повне знищення, призводить до важких наслідків, які відчуватимуться на місцевому або загальнодержавному рівні. Саме об'єкти критичної інфраструктури (ОКІ) стають ціллю для ракетних та дронових атак ворога. Основна мета цих ударів – досягти рівня руйнувань, здатного спричинити екологічну, техногенну та гуманітарну катастрофу, враховуючи обмежене використання ядерної зброї та застосування звичайної.

Відтак, сьогодні надзвичайно важливим є всебічний аналіз та оцінка загроз, яким піддається критична інфраструктура. Це потрібно для превентивного реагування, уникнення надзвичайних ситуацій, як воєнного, так і техногенного характеру. У випадку їх виникнення, першочерговим завданням стає мінімізація наслідків та швидке реагування для їх ліквідації.

Аналіз останніх досліджень і публікацій. Проведемо аналіз низки наукових публікацій щодо систем підтримки прийняття рішень (СППР), що застосовуються для підвищення рівня еколого-техногенної безпеки.

У статті Якуба Л., Хана Н. А., Субхана Ф. [9] (2024) «Огляд існуючих систем підтримки рішень для управління лихами» проаналізовано існуючі СППР для управління надзвичайними ситуаціями. Автори аналізують різні підходи до використання інформаційних технологій у кризових ситуаціях та визначають їхню ефективність у зниженні ризиків

та підвищенні ефективності реагування. У статті Попова А. (2024) [10] «Архітектура регіонального моніторингу навколишнього середовища» проаналізовано регіональні архітектури екологічного моніторингу на основі Інтернету речей та хмарних обчислень. Проаналізовано рівень інтегрованих інформаційних систем, які дозволяють збирати, обробляти та управляти екологічними даними для підвищення ефективності моніторингу та управління природними ресурсами.

Робота Пеанковського С. [11] (2023) «Інформаційне забезпечення прийняття рішень система в надзвичайних ситуаціях» присвячена інформаційній підтримці систем прийняття рішень в умовах надзвичайних ситуацій. Автор аналізує шляхи оптимізації процесів управління, скорочення часу реагування та використання інформаційних технологій для підвищення ефективності прийняття рішень у кризових ситуаціях. У статті Ванґа, В.-Ц. [12] (2020) «Багатофункціональна система підтримки прийняття рішень у разі лиха на основі динамічних даних із багатьох джерел» обговорюється розробка багатоджерельної СППР з управління катастрофами на основі інтеграції декількох джерел інформації. Автор підтримує важливість ефективної комунікації та швидкого доступу до актуальних даних для оптимізації процесу реагування на катастрофи, включаючи готовність, реагування та відновлення.

У статті Лавала Б. Н. Дж., О. Дж.-Й., Гікса Д., Кумар В. [13] (2024) «Система підтримки прийняття рішень для відновлення після катастроф» обговорюється розробка СППР для управління надзвичайними ситуаціями на основі інтеграції динамічних даних з різних джерел. Автори підтримують важливість ефективної комунікації та швидкого доступу до актуальних даних для оптимізації процесу реагування на катастрофи, включаючи готовність, швидке реагування та відновлення. Система включає функції моделювання та навчання для різних сценаріїв катастроф, які можуть підвищити ефективність готовності та реагування.

Раніше згадані дослідження акцентують увагу на існуванні численних загроз (збройні конфлікти, катастрофи, кібернетичні атаки) та небезпек (екологічні, техногенні, гуманітарні) для критичної інфраструктури, зокрема, в умовах військових конфліктів. Для ефективного контролю над цими загрозами та ризиками необхідно не тільки збирати й аналізувати інформацію, але й ухвалювати обґрунтовані рішення, що, своєю чергою, базуються на результатах прогнозних методів.

Постановка завдання. У світовій практиці оцінювання небезпек для життя людей та функціонування критичної інфраструктури традиційно використовуються терміни «загроза» та «ризик». Загроза визначається як природне або техногенне явище, яке потенційно може призвести до виникнення подій чи процесів, здатних завдати шкоди здоров'ю людей, спричинити матеріальні збитки та негативно вплинути на навколишнє середовище.

Проте, стосовно умов бойових дій в Україні, пристосований термін «загроза» окреслює ймовірність появи певних обставин воєнно-техногенного плану, за яких можуть виникнути негативні екологічні процеси, зумовлені воєнно-техногенними чинниками ураження компонентів навколишнього природного середовища.

За визначенням В. Маршалла, «ризик – це частота реалізації загрози», а загроза – природне чи техногенне явище, що може призвести до виникнення подій або процесів, здатних нашкодити людям, завдати матеріальних збитків, знищити довкілля. Саме таке трактування ризику одержало найбільше розповсюдження у науково-технічній літературі з промислової безпеки. Небезпека виникнення аварій на об'єктах підвищеної небезпеки обумовлена можливістю руйнування будівель або технічних пристроїв, вибухами та викидами небезпечних речовин з ураженням людей, спричиненням майнових втрат і забрудненням навколишнього природного середовища.

Зазвичай, у теоретичному плані термін «ризик» інтерпретують по-різному, проте в кожному з пояснень присутній елемент «невідомості»: чи станеться щось небажане, чи ні; чи виникне через це небажаний (небезпечний) стан, чи ні. Така обмеженість інформації при вивченні явищ, процесів та ситуацій зближує концепцію «ризику» з процесом «прийняття рішень» за наявності недетермінованих чинників.

Виклад основного матеріалу. На теперішній час існує декілька математичних концепцій для фахової оцінки потенційних небезпек і ризиків у контексті критичної інфраструктури. У державах Європейського Союзу активно впроваджується систематичний підхід, котрий базується на оцінюванні загроз і ризиків з використанням низки критеріїв [1–5].

Встановлено, що методи експертного оцінювання спираються на акумуляцію професійного досвіду та інтуїції експертів. Ці методи оцінювання небезпек та ризиків застосовують формальну теорію ухвалення рішень в умовах неви-

значеності. У випадку виникнення надзвичайної ситуації (НС) ключовою постаттю та суб'єктом прийняття рішень є особа, що приймає рішення (ОПР). Це може бути як індивідуальна особа, так і група людей, які формують колективне рішення, зазвичай, ОПР – це керівник або керуючий орган, котрий формулює проблему, відіграє вирішальну роль у виборі рішення проблеми та несе відповідальність за прийняте рішення. При цьому експерти та консультанти відповідають за обґрунтованість рекомендацій, які вони готують для ОПР. Остаточне рішення завжди приймається ОПР, відповідно до власної системи пріоритетів, а також несе повну відповідальність за свій вибір та його наслідки [6, 7].

Існують різні підходи до оцінювання загроз критичній інфраструктурі:

1. Метод експертної оцінювання: Цей підхід передбачає залучення кількох спеціалістів, які на основі своїх знань та досвіду оцінюють потенційні загрози та їхню ймовірність.

2. Методи аналізу ризиків: включають такі методи, як аналіз потенційних втрат, аналіз вірогідності та наслідків, а також метод Монте-Карло та інші.

3. Методи математичного моделювання: За допомогою математичних моделей можна оцінювати загрози та аналізувати ризики.

4. Методи машинного навчання: Використання штучного інтелекту, глибокого навчання, а також машинного навчання, заснованого на даних.

Застосування комбінації різних методів також може бути корисним у процесі оцінювання загроз для критичної інфраструктури.

Враховуючи невизначеність, складність і різноманітність систем критичної інфраструктури, особливо актуальним є метод експертного оцінювання. Провідні наукові інститути, що спеціалізуються на питаннях енергетичної безпеки, також активно застосовують цей метод.

Переваги:

– Використання напрацювань: Фахівці здатні здійснювати оцінку небезпек з більшою точністю, спираючись на свій багатий досвід та глибокі знання.

– Поглиблений аналіз загроз: Експерти можуть ефективніше аналізувати складні, багатогранні загрози, які важко піддаються оцінці за допомогою автоматизованих систем.

Недоліки:

– Людський фактор: Експерти можуть припускатися помилок при оцінюванні небезпек, що може вплинути на достовірність результатів.

– Суб'єктивність: Експерти можуть бути під впливом конфлікту інтересів або мати обмежені знання та досвід у конкретній галузі.

Застосування експертного оцінювання загроз є доцільним сьогодні, з огляду на те, що:

1. Інформація, необхідна для аналізу та прийняття рішень, є неповна, частина даних відсутня.

2. Значна частина інформації має якісний, а не кількісний характер.

3. Складність поставленого завдання та обмежені ресурси не дозволяють зібрати та узагальнити всю необхідну інформацію.

4. Недостатність математичного інструментарію для оцінювання та оперування даними.

5. Обмежений розгляд кількох варіантів усунення ризиків через брак ресурсів та технічні складнощі.

6. Фактори різної природи, що вислизають з-під контролю прогнозування, але зумовлюють відчутний вплив на захищеність критичної інфраструктури.

Експертне оцінювання загроз для критичної інфраструктури полягає у встановленні їхнього рейтингу з огляду на рівень ризику (від можливих наслідків та кумулятивних руйнівних ефектів), щоб визначити найнебезпечніші та відрізнити ті, що спричинять незначні або прийнятні руйнівні наслідки. Основна мета такого пріоритезування – це ефективне застосування ресурсів для захисту об'єктів критичної інфраструктури, а також для усунення найбільш серйозних та ймовірних загроз.

Окремі загрози та їх кумулятивні руйнівні наслідки можуть мати незначний вплив при високій імовірності, або ж бути значними, але малоймовірними.

Експертна оцінка, що базується на якісному методі, передбачає встановлення рівня кожної визначеної загрози шляхом оцінювання сукупності наслідків та імовірності їхнього виникнення, з урахуванням їхньої значущості.

Для цілей даного аналізу зазвичай припускається, що кожна складова система, яка потенційно може постраждати від небезпеки h, взятої із переліку виявлених загроз $h = 1, \ldots, k$, демонструє найвищий рівень уразливості, що виражається у формулі:

$$\sum_{jj=1}^{mm} VV_{jj} LL_{jj} = 1, \qquad (1)$$

VV_{jj} – вразливість j зі списку вразливостей об'єкта управління $j = 1, \ldots, m$; LL_{jj} – ймовірність реалізації вразливості j.

Руйнівний наслідок реалізації загрози є

$$CC_{tt} = \sum_{ii=1}^{mm} CC_{ii} LL_{ii}. \qquad (2)$$

CC_{ii} – негативний наслідок реалізації загрози з множини можливих наслідків $i = 1, \ldots, n$; LL_{ii} – ймовірність настання наслідку та реалізації загрози.

Зважаючи на вищесказане, процес розстановки пріоритетів для загроз Rt базується на спрощеній процедурі. Він передбачає порівняння добутків усереднених оцінок експертів щодо загальної ймовірності Lt та сукупних негативних наслідків Ct, які виникають у разі реалізації кожної загрози з наперед визначеного переліку, пронумерованого від $t = 1$ до k.

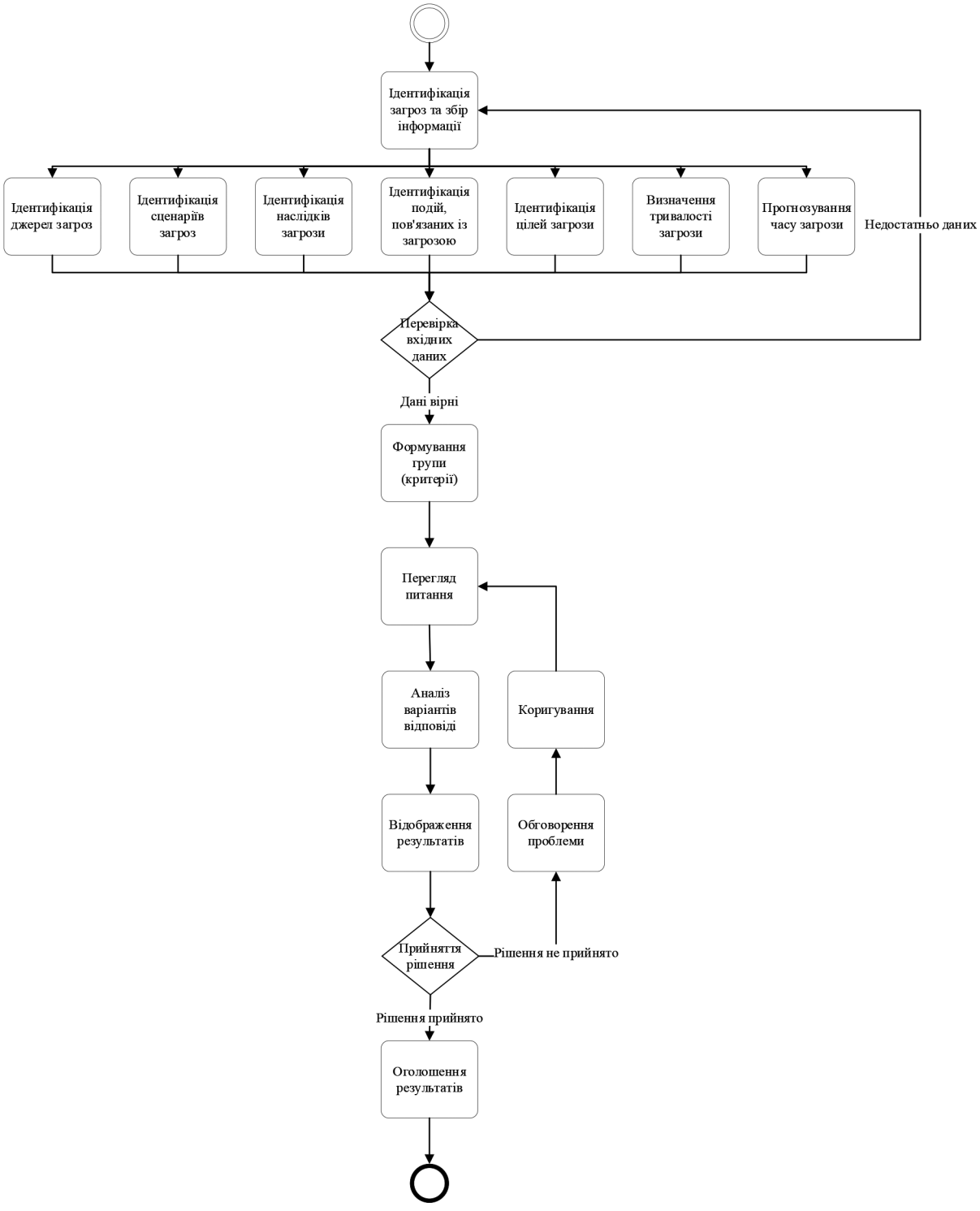

Рис. 1. Блок-схема виявлення загрози методом експертної оцінювання

$$RR_{tt} = LL_{tt}CC_{tt}. \quad (3)$$

Рекомендовано встановити такі дефініції шкали значущості та градації оцінювання значимості (у балах):

– для загальної ймовірності: «низька» (1), «відносно низька» (2), «середня» (3), «відносно висока» (4), «висока» (5);

– для сукупних негативних наслідків: «незначні» (1), «несуттєві» (2), «помірні» (3), «значні» (4), «катастрофічні» (5).

Схожі шкали застосовуються в матрицях впливу (Відносний Вплив) для оцінювання ризиків (Національна Оцінка Ризиків) у країнах-членах ЄС. Особлива увага приділяється загрозам, щодо яких спостерігається найбільший розкид експертних оцінок наслідків та/або ймовірностей (суперечливі оцінки). У таких випадках формулювання загрози та/або її опис потребують уточнення та/або додаткового роз'яснення координатором (модератором).

Загроза виключається з реєстру, якщо середньоарифметичне значення оцінки сукупних негативних наслідків або загальної ймовірності перевищує 2 бали. Для забезпечення об'єктивності, експерти не повинні мати доступу до відомостей про оцінки, зроблені іншими учасниками оцінювання.

Прикладом першочергового визначення важливості загроз для критичної інфраструктури може бути перелік, складений за допомогою методу Дельфі, до якого залучили 10 експертів.

Пріоритезація відбувалася згідно з рівнем небезпеки, що визначався як результат множення оцінок експертів сукупних негативних наслідків та загальної вірогідності втілення загрози. Виключення загрози зі списку відбувалося, якщо середнє арифметичне оцінок експертів наслідків та ймовірності було понад 2 бали. Оцінка небезпек, які постають перед критичною інфраструктурою, наведена у таблиці 1.

Підсумки оцінювання загроз критичної інфраструктури були отримані завдяки роботі програмного забезпечення, що діє за конкретним сценарієм. Спочатку визначаються рамки параметрів об'єкта дослідження. Після цього створюються вхідні дані, які детально описують кожну потенційну загрозу критичній інфраструктурі. Вони заносяться до реєстру, представляючи собою опис загрози разом з набором експертних оцінок. Далі зі списку вилучаються ті загрози, що мають мінімальний сукупний негативний вплив або характеризуються як малоймовірні, після чого відбувається ранжування загроз за значимістю їхніх наслідків та імовірності виникнення. Виходячи з отриманих даних, система формулює висновки, які дають можливість корегувати експертні оцінки, тобто формуються домінуючі висновки, а оцінки – зменшуються. Процес корекції реєстру, ранжування, формування висновків та уточнення

Таблиця 1

Оцінка загроз критичній інфраструктурі

№	Загроза критичній інфраструктурі	Рівень	Ймовірність	Наслідки
1	Ракетні та дронові удари	**20,5**	5	4,1
2	Втрата контрольованого споживання енергії	**17,6**	4,4	4
3	Кібератаки	**15**	5	3
4	Технічна несправність	**14,35**	4,1	3,5
5	Аварії на прилеглих об'єктах	**13,86**	3,3	4,2
6	Стихійні лиха	**13,2**	3	4,4
7	Терористичні атаки	**12,3**	3	4,1
8	Наявність резервування критичних об'єктів	**12,3**	3	4,1
9	Відсутність системи стратегічного планування та координації	**12**	3	4
10	Недостатнє енергопостачання	**10**	4	2,5
11	Відсутність запасів палива	**10**	2	5
12	Захист потенційно небезпечних об'єктів критичної інфраструктури	**10**	2	5
13	Зношення основних засобів, збільшення аварійності	**9**	3	3
14	Брак енергетичних резервів	**9**	2	4,5
15	Штучні стихійні лиха	**8,8**	2,2	4
16	Технічне перевантаження об'єктів	**8**	4	2
17	Нечітке розмежування повноважень та відповідальності	**6**	2	3
18	Втрата кваліфікованого технічного персоналу	**5**	1	5
19	Нездатність реагувати на кризу	**5**	1	5
20	Блокування необхідних поставок	**5**	1	5

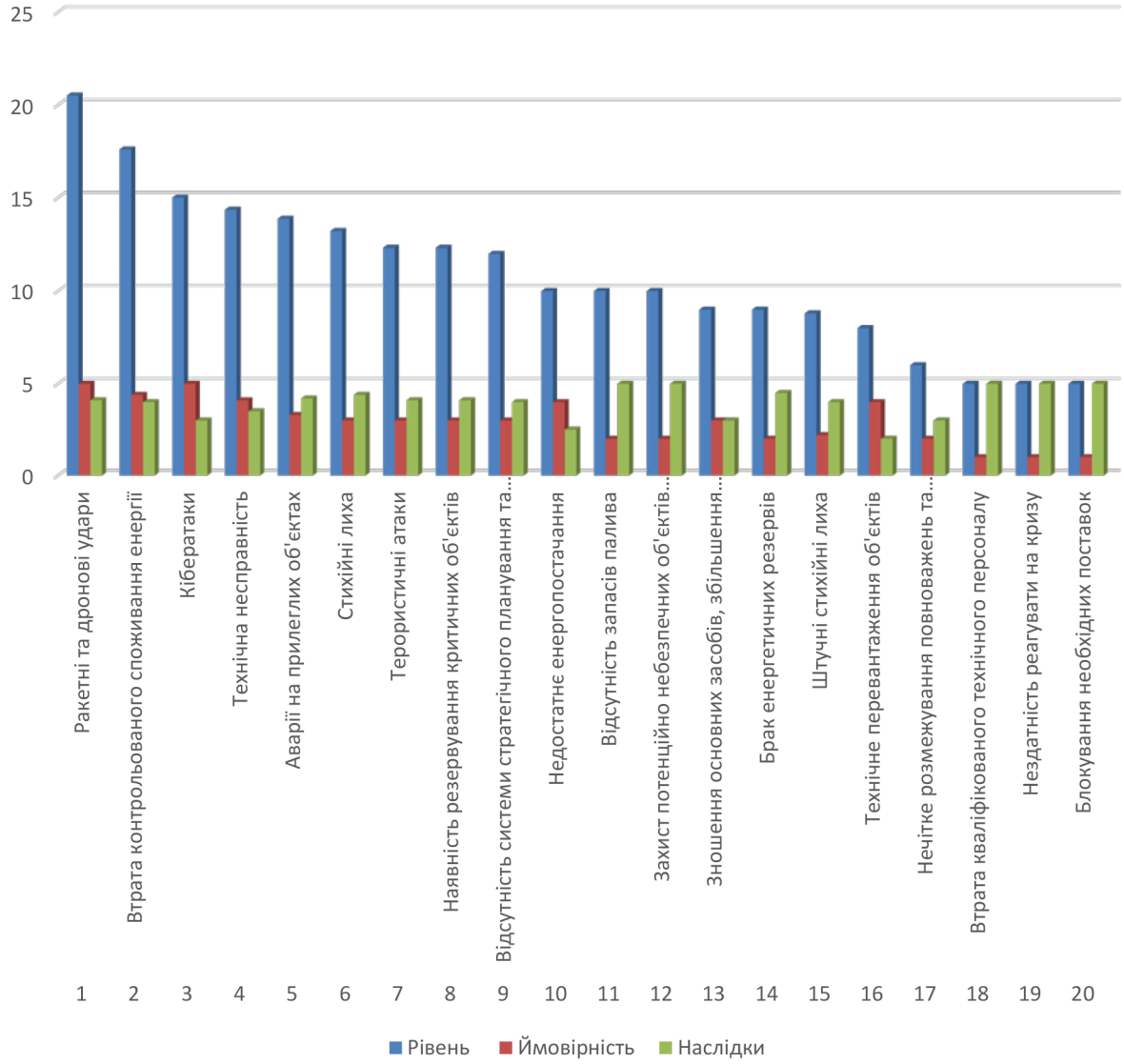

Рис. 1. Результати експертного оцінювання загроз критичній інфраструктурі

оцінок триває до досягнення одностайності думок між експертами щодо загроз, або до моменту, коли корекція оцінок припиняє змінювати пріоритетність. Після ухвалення остаточного рішення відбувається процедура оприлюднення результатів, що свідчить про завершення процесу оцінювання загроз методом експертного аналізу.

Результати аналізу загроз для критичної інфраструктури свідчать про таке.

Жодна з попередньо визначених загроз для енергетичної безпеки не отримала середнього арифметичного показника кумулятивних негативних наслідків чи загальної вірогідності нижче 2 балів. З цієї причини жодна з загроз не була виключена зі списку.

До п'ятірки найбільших викликів належать: атаки ракетами та безпілотниками, перебої з енергопостачанням, кібернетичні атаки, технічні збої та інциденти на суміжних підприємствах. Відповідно до зібраних даних, зосередження зусиль та ресурсів на протидії цим ризикам є найперспективнішим підходом для їхнього уникнення.

Висновки. Не варто перебільшувати значення отриманих результатів, або приписувати їм точність, більшу, ніж вимагають дані та використані підходи.

Отже, через застосування методу експертного оцінювання проведено практичний аналіз загроз для критичної інфраструктури з ранжуванням їх за важливістю. Це дозволяє спрямувати зусилля на найбільш серйозні загрози та мінімізувати можливі збитки для критично важливих об'єктів. Доведено, що використання експертних оцінок дає змогу здійснювати аналіз загроз у складних системах за умов невизначеності, що сприяє знаходженню оптимальних рішень для окреслених категорій. Ця робота буде корисною для експер-

тів з цивільного захисту, а також спеціалістів, що займаються профілактикою, локалізацією надзвичайних ситуацій та з'ясуванням їх причин на об'єктах критичної інфраструктури.

Список літератури:

1. Оцінювання загроз енергетичній безпеці / О. М. Суходоля та ін. Нац. ін-т стратег. дослідж., 2022. URL: https://doi.org/10.53679/niss-analytrep.2022.11

2. Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. 2015. URL: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96623/lbna27332enn.pdf

3. Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи. Київ, 2004. 472 с.

4. Novel methodologies for analysing critical infrastructure resilience / K. Storesund et al. Safety and Reliability – Safe Societies in a Changing World. 2018. P. 1221–1229. URL: https://doi.org/10.1201/9781351174664-154

5. Моделювання загроз виникнення надзвичайних ситуацій на об'єктах критичної інфраструктури з використанням методу системної динаміки / А. І. Невольніченко та ін. Таврійський науковий вісник. Серія: Технічні науки. 2022. № 3. С. 88–99. URL: https://doi.org/10.32851/tnv-tech.2022.3.10

6. Шаповалова О. О., Бурменський Р. В. Розробка програмного додатка для реалізації методу аналізу ієрархій. Системи обробки інформації. 2017. № 3(149). С. 45–48. URL: https://doi.org/10.30748/soi.2017.149.09

7. Куртсеітов Т., Мурасов Р., Мельник Я. Імовірнісний метод прогнозування надзвичайних подій на потенційно-небезпечних об'єктах критичної інфраструктури. Сучасні інформаційні технології у сфері безпеки та оборони. 2022. Т. 44, № 2. С. 60–63. URL: https://doi.org/10.33099/2311-7249/2022-44-2-60-63

8. Маршалл В. Основные опасности химических производств. М., 1989. 671 с.

9. Yaqoob L., Khan N. A., Subhan F. An overview of existing decision support systems for disasters management. Science International. 2014. URL: https://surl.li/klkmbz

10. Popov A. Architecture of regional environmental monitoring. Scientific-practical conference dedicated to World Meteorological Day «At the Frontline of Climate Action» and World Water Day "Water for a Peaceful and Sustainable Future". 2024. P. 211–212. URL: https://doi.org/10.15407/conf_uhmi_cgo_2024.073

11. Peancovschii S. Information support of the decision-making system in emergency situations. 2023. URL: https://surl.li/vwkjab

12. Wang W.-C. A Multi-Function Disaster Decision Support System Based on Multi-Source Dynamic Data. Environment and Natural Resources Research. 2020. Vol. 10, no. 1. P. 1. URL: https://doi.org/10.5539/enrr.v10n1p1

13. Decision support system for post-disaster resilience. Issues In Information Systems. 2024. URL: https://doi.org/10.48009/2_iis_2024_117.

Savchenko I. O., Matsko P. I. A SYSTEMATIC APPROACH TO SUPPORTING DECISION-MAKING ON THREATS TO THE CRITICAL INFRASTRUCTURE USING EXPERT ASSESSMENT METHODS

This work addresses the problem of assessing threats to critical infrastructure during wartime and their impact on national security. The importance of decision-making under uncertainty is emphasized as a key aspect of risk management for critical infrastructure.

The authors have also analyzed previously published scientific materials related to the application of various expert methods for evaluating hazards and potential negative consequences of emergency situations that may arise at critical infrastructure facilities in Ukraine during the ongoing armed aggression by the Russian Federation.

For analytical assessment of potential hazards to critical infrastructure in the context of the ongoing Russian-Ukrainian war, the perspective of applying expert evaluation methods is considered. Necessary recommendations and conclusions regarding their effectiveness and feasibility in this case are formulated. Using custom software developed by the authors in Python, practical calculations were performed, supported by scientific justification of conclusions regarding potential threats. This program implemented a decision-support procedure for determining the priority of threats to critical infrastructure objects, considering the degree of risk, probability, and potential damage from damage.

Based on the data obtained from the operation of the software, it becomes clear that the use of expert evaluation methods provides the opportunity to study risks to critical infrastructure under conditions of a priori uncertainty, taking into account the probabilistic nature of military actions and the stochasticity of missile-drone attacks.

The program allows creating a ranked list of potential threats, conducting a procedure for filtering out threats that are not of primary importance. This is done to effectively allocate limited forces and resources to reduce the likely negative impact of emergency situations of natural, technological, and military-technological nature.

Key words: *critical infrastructure, threats, missile-drone strikes, expert assessment, Python, evaluation procedure, risk minimization, emergency situations, civil defense.*