DOI:**10.33099/2311-7249/2023-48-3-83-88**

УДК 355.45

Мурасов Рустам Камілович *(кандидат технічних наук)*
Мельник Ярослав Вячеславович

Національний університет оборони України, Київ, Україна

РЕЗУЛЬТАТИ ОЦІНЮВАННЯ ЗАГРОЗ КРИТИЧНІЙ ІНФРАСТРУКТУРІ МЕТОДОМ ЕКСПЕРТНОГО ОЦІНЮВАННЯ

Сьогодні досить часто використовуються методи експертного оцінювання, що базується на залученні експертів із різних областей знань, які надають свої фахові оцінки стосовно ймовірності виникнення загроз та характеру їх впливу на об'єкти критичної інфраструктури. Метою статті є оцінювання загроз критичної інфраструктури методом експертного оцінювання для запобігання виникнення надзвичайних ситуацій, а в разі неможливості їхнього запобігання – мінімізації їх наслідків та оперативного ліквідування. Під час проведення дослідження застосовано такі методи: методи аналізу під час аналізування існуючих джерел за напрямом досліджень, існуючих підходів оцінювання загроз, методи аналізу ризиків, методи математичного моделювання для оцінювання загроз та аналізу ризиків, методи машинного навчання такі як штучний інтелект, глибоке навчання та метод експертного оцінювання. Зазначений методологічний підхід дав змогу отримати результати оцінювання загроз критичної інфраструктури для раціонального розподілу засобів захисту, що використовуються складовими сил безпеки і оборони держави. У статті наведено існуючі підходи оцінювання загроз і розглянуто можливість використання методу експертного оцінювання для визначення загроз критичній інфраструктурі в сучасних умовах російсько-української війни. Також висвітлено методологію оцінювання загроз критичній інфраструктурі, засновану на методі експертного оцінювання. Наведено результати оцінювання загроз для об'єктів критичної інфраструктури. Запропоновано порядок оцінювання загроз критичній інфраструктурі з пріоритизацією загроз. Пояснена суть методу експертного оцінювання та удосконалення цього методу завдяки введенню ідентифікаторів загроз критичної інфраструктури та укладенню таких визначень: усереднена експертна імовірність, окремі та сукупні деструктивні наслідки, ймовірності загроз захисту критичної інфраструктури. Це дасть змогу зосередити зусилля на найбільш небезпечних загрозах і запобігти значним втратам критичної інфраструктури. Елементами наукової новизни статті є механізм пріоритизації ризиків (наслідків, сукупних деструктивних ефектів) з визначенням найнебезпечніших і відокремленні таких, що мають незначний ефект. Зроблено висновки стосовно можливостей і доцільності застосування методу експертного оцінювання з метою ідентифікації потенційних ризиків для об'єктів критичної інфраструктури та розроблення стратегій їх захисту. Проведено практичні розрахунки з висновками стосовно загроз і їх пріоритезації щодо критичної інфраструктури. До теоретичної значущості статті слід віднести вклад у розвиток методології оцінки загроз критичній інфраструктурі. Запропонований метод експертного оцінювання дозволяє отримати кількісні оцінки загроз, що є важливим для прийняття ефективних управлінських рішень та дозволяє враховувати різноманітні фактори, що впливають на рівень загрози в цілому. Практична значущість статті полягає в тому, що отримані результати дослідження можуть бути використані для: забезпечення безпеки критичної інфраструктури, формування пріоритетів захисту об'єктів критичної (військової) інфраструктури та розробки заходів щодо підвищення рівня безпеки критичної (військової) інфраструктури. Результати статті дають змогу здійснювати аналіз загроз критичної інфраструктури в умовах війни та ракетно-дронових ударів, формувати пріоритезований список загроз, відокремити незначні загрози з метою оптимального застосування наявних сил і засобів та мінімізації надзвичайних наслідків.

Ключові слова: *критична інфраструктура, ракетно-дронові удари, експертне оцінювання, мінімізація надзвичайних ситуацій, виникнення надзвичайних ситуацій, цивільний захист.*

Вступ

Оцінювання загроз критичній інфраструктурі держави є важливим завданням у сфері її безпеки та оборони. Така критична інфраструктура, як енергетика, транспорт, телекомунікації та інші об'єкти, забезпечує нормальне функціонування суспільства і є цілями для потенційних загроз. Адекватне оцінювання таких загроз допомагає виявити потенційні ризики для об'єктів критичної інфраструктури та розробити ефективні стратегії їх захисту.

Підходи до оцінювання використовуються залежно від конкретних потреб і характеристик критичної інфраструктури. Один із загальних підходів – це кваліативне оцінювання, де експерти

використовують свої знання і досвід для надання оцінки загрози на основі категорій, таких як імовірність загроз, вразливість об'єктів критичної інфраструктури, вплив на неї і можливі наслідки. Цей підхід може бути корисним для оцінювання загроз на початкових етапах аналізу. Інший підхід – кількісне оцінювання, під час якого експерти використовують статистичні методи та моделі для оцінювання загроз. Такий підхід використовує конкретні дані та показники для розрахунку ймовірності та впливу загрози. Він може бути корисним для більш точного оцінювання загроз у випадках, коли наявні статистичні дані. Також існує підхід, що комбінує як кваліативні, так і кількісні оцінювання. Експерти використовують як свої власні знання та досвід, так і конкретні дані для оцінювання загрози. Цей підхід може бути корисним для більш комплексного аналізу загроз та їхніх наслідків.

Один з методів, що доцільно використовувати для визначення загроз критичній інфраструктурі є метод експертного оцінювання. Цей підхід залучає експертів з різних областей знань для оцінювання ймовірності та впливу загроз. Експерти використовують свій професійний досвід і знання, для оцінювання потенційних ризиків.

Оцінювання загроз критичній інфраструктурі методом експертного оцінювання слід проводити за такою послідовністю [1]:

формування експертної групи;

визначення загроз;

встановлення критеріїв оцінювання;

проведення збору даних та їх аналіз;

інтерпретація результатів.

Постановка проблеми. Захист критичної інфраструктури є фундаментальною складовою національної безпеки. Виведення її з ладу або суттєве порушення функціонування матиме масштабні деструктивні наслідки регіонального або державного значення [8]. Ворог зосередив свої ракетно-дронові атаки саме на об'єктах критичної інфраструктури та має на меті досягнення такого деструктивного рівня своїх ударів, щоб створити еколого-техногенно-гуманітарну катастрофу в умовах обмеження застосування ядерної зброї. Отже, оцінювання загроз та захист на його основі критичної інфраструктурі є важливим завданням для забезпечення безпеки та стійкості критичних систем.

Аналіз останніх досліджень і публікацій. Оцінювання загроз критичній інфраструктурі методом експертного оцінювання є активним об'єктом досліджень і публікацій у галузі кібербезпеки, безпеки критичних систем та управління ризиками. Так, автор Єрменчук О. П. у роботі «Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України» [6] надає огляд загальних підходів до оцінювання ризиків критичної інфраструктури, включаючи методи експертного оцінювання загроз та розглядає проблемні питання ідентифікації загроз, визначення вразливостей та розрахунку наслідків. У публікації авторів Уряднікова І. В., Чумаченка С. М., Кармазіна С. В., Тесленко О. М. «Застосування експертно-аналітичних методів для оцінювання ризиків надзвичайних ситуацій на об'єктах критичної інфраструктури» [7] пропонується межі для експертного оцінювання ризиків та прийняття рішень. Вони розглядають питання залучення експертів, визначення вагомості їхніх оцінок і аналізу отриманих даних. Автор Цяпа С. М в статті «Правове та організаційне забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак» [8] розглядає правові та організаційні аспекти забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак. Використовує позитивний досвід США у забезпеченні стійкості об'єктів критичної інфраструктури та аналізує положення нової Стратегії кібербезпеки України.

Існує декілька методів оцінювання загроз критичної інфраструктури:

методи аналізу ризиків, такі як аналіз збитків, аналіз імовірності та впливу, метод Монте-Карло та інші [5];

методи математичного моделювання. Цей метод створює математичну модель, яка допомагає в оцінці загроз та аналізі ризиків [1];

методи машинного навчання такі як штучний інтелект, глибоке навчання та машинне навчання на основі даних [2];

метод експертної оцінки. У цьому методі кілька експертів оцінюють загрози та їх імовірність на основі свого досвіду та знань [7]. Саме цей метод був використаний для написання даної статті.

Метою статті є оцінювання загроз критичної інфраструктури методом експертного оцінювання для запобігання виникнення надзвичайних ситуацій, а в разі неможливості їхнього запобігання – мінімізації їх наслідків та оперативного ліквідування.

Виклад основного матеріалу дослідження

В умовах невизначеності, складності та неоднорідності систем (критичної інфраструктури) доцільно застосовувати метод експертного оцінювання групою експертів, що мають певні знання та досвід [3]. Провідні наукові установи у сфері енергетичної безпеки також широко застосовують такий метод.

Основними перевагами методу експертного оцінювання слід зазначити:

використання досвіду – експерти можуть точніше оцінювати загрози, використовуючи свій досвід та експертизу;

розширене оцінювання загроз – експерти здатні здійснити більш точне оцінювання складних загроз, що важко охарактеризувати за допомогою автоматизованих методів;

придатність при обмеженні ресурсів – у випадках, коли немає достатньої кількості даних для статистичного аналізу, експертне оцінювання є

доцільним і раціональним методом.

урахування впливу людського фактору на загрози.

Основними недоліками такого методу є:

поява людської помилки – експерти можуть допускати певні помилки під час оцінювання загроз, що можуть вплинути на точність результатів;

відсутність об'єктивності (суб'єктивність) – обмеженість знань та досвіду експертів в цій галузі, а також виникнення конфлікту інтересів;

неузгодженість думок – експерти можуть мати різні точки зору та оцінки, що призводить до труднощів у досягненні консенсусу;

незнання невідомого – експерти можуть бути непоінформованими або не мати достатньої інформації про певні аспекти загроз, що може призвести до неповної оцінки.

Використання експертного оцінювання загроз є актуальним, оскільки:

наявна інформація для аналізу та обробки може бути не повною, а частина спотворена;

певний обсяг інформації має якісний характер;

складність поставленого завдання оцінювання загроз та обмежені можливості математичного апарату не дають змогу зібрати й узагальнити всю потрібну інформацію для якісного оцінювання;

недостатність математичного апарату для аналізу й обробки інформації;

існує декілька можливих варіантів нейтралізації загроз, що не розглядаються через ресурсні та технічні обмеження;

виникають непередбачувані фактори різного походження, що не можливо спрогнозувати, але можуть мати суттєвий вплив на безпеку критичної (військової) інфраструктури.

Експертне оцінювання загроз критичній інфраструктурі полягає в їхній пріоритизації за ризиками (наслідками, сукупними деструктивними ефектами) з визначенням найнебезпечніших, і відокремленні таких, що мають незначний та допустимий деструктивний ефект. Основною метою такої пріоритизації є оптимальне використання наявних сил і засобів для захисту об'єктів критичної інфраструктури та нейтралізації найбільш значущих і найбільш імовірних загроз.

Відокремлюють загрози та сукупні деструктивні наслідки реалізації яких можуть бути незначними за високої ймовірності, або значними, проте малоймовірними. Експертне оцінювання з використанням якісного методу передбачає встановлення рівня кожної сформульованої загрози у спосіб поєднання її наслідків і ймовірностей їх настання, визначених у термінах значущості.

Для досягнення цілей такого дослідження, припускають, що всі складові частини об'єкта управління, на які може вплинути певна загроза h із переліку ідентифікованих загроз $h = 1…m$, є максимально уразливими, тобто в позначеннях у виразі:

$$\sum_{j=1}^{m} V_j L_j = 1, \qquad (1),$$

де V_j і L_j – коефіцієнти частини об'єкта управління.

У такому разі деструктивним наслідком реалізації загрози є:

$$C_t = \sum_{i=1}^{n} C_i L_i, \qquad (2)$$

де C_i – окремий деструктивний наслідок;

L_i – усереднена експертна імовірність;

C_t – сукупність деструктивних наслідків.

$t = 1…n$ – перелік загроз критичній інфраструктурі.

Ураховуючи вирази (1, 2), пріоритизацію загроз R_t здійснюють за спрощеним варіантом, порівнюючи добутки усереднених експертних оцінок загальної імовірності L_t та сукупних деструктивних наслідків C_t реалізації кожної загрози з наперед установленого переліку t за виразом:

$$R_t = L_t C_t. \qquad (3)$$

Доцільно встановити такі дефініції шкали значущості та градацію виміру значущості (у балах):

для загальних імовірностей:

«низька» (1);

«відносно низька» (2);

«середня» (3);

«відносно висока» (4);

«висока» (5).

для сукупних негативних наслідків:

«незначні» (1);

«неістотні» (2);

«помірні» (3);

«істотні» (4);

«катастрофічні» (5).

Подібні шкали застосовують у матрицях впливу (Relative Impact) для оцінювання ризиків (National Risk Assessment) у державах – членах ЄС [2]. Окремо звертають увагу на загрози, для яких зафіксований максимальний розкид експертних оцінок наслідків та/чи імовірностей (контроверсійні). У таких випадках формулювання загрози та/чи її опису потребує уточнення та/чи додаткового роз'яснення з боку координатора (модератора) [8]. Загрозу вилучають із реєстру, якщо середня арифметична оцінка сукупних негативних наслідків чи загальної імовірності перевищує 2 бали. З метою збільшення об'єктивності експерти не повинні мати доступу до інформації про оцінки, виставлені іншими учасниками оцінювання.

Прикладом пріоритизації до оцінювання загроз критичній інфраструктурі є відповідний перелік, сформований методом Дельфі із залученням 10 експертів. Пріоритизацію виконано за рівнем загроз [1; 2], що визначали як добуток експертних оцінок її сукупних негативних наслідків і загальної ймовірності реалізації. Вилучення загрози з реєстру здійснювали, якщо середня арифметична експертна оцінка наслідків імовірності перевищувала 2 бали. Результати оцінювання загроз критичній інфраструктурі методом експертного оцінювання наведено в таблиці 1.

Результати оцінювання загроз критичній інфраструктурі свідчать про те, що жодна з

попередньо сформульованих загроз енергетичній безпеці не отримала середньої арифметичної оцінки сукупних негативних наслідків чи загальної імовірності, котра виявилася б меншою, аніж 2 [4]. Тому загрози з реєстру не вилучалися.

У першу п'ятірку загроз включено: ракетно-дронові удари, втрата контрольованого енергоспоживання, кібератаки, технічна несправність, аварії на суміжних об'єктах [5].

Таблиця 1

Результати оцінювання загроз критичній інфраструктурі

№ з/п	Назва загрози критичній інфраструктурі	Рівень Загроз R_t, бали	Імо-вірність загроз L_t, бали	Наслідки C_t, бали
1.	Ракетно-дронові удари	20,5	5	4,1
2.	Втрата контрольованого енергоспоживання	17,6	4,4	4
3.	Кібератаки	15	5	3
4.	Технічна несправність	14,35	4,1	3,5
5.	Аварії на суміжних об'єктах	13,86	3,3	4,2
6.	Природні катастрофи	13,2	3	4,4
7.	Теракти	12,3	3	4,1
8.	Наявність резервування критичних об'єктів	12,3	3	4,1
9.	Відсутність системи стратегічного планування та координування	12	3	4
10.	Недостатнє електропостачання	10	4	2,5
11.	Відсутність паливних резервів	10	2	5
12.	Захист потенційно-небезпечних об'єктів критичної інфраструктури	10	2	5
13.	Зношеність основних фондів, підвищення аварійності	9	3	3
14.	Відсутність енергетичних резервів	9	2	4,5
15.	Штучні природні катастрофи	8,8	2,2	4
16.	Технічне перевантаження об'єктів	8	4	2
17.	Нечітке розмежування повноважень і відповідальності	6	2	3
18.	Втрата кваліфікованого технічного персоналу	5	1	5
19.	Неспроможність до кризового реагування	5	1	5
20.	Блокування необхідних постачань	5	1	5

Саме на таких загрозах, відповідно до отриманих результатів, доцільно зосередити засоби захисту, що використовуються складовими сил безпеки і оборони держави для недопущення їх реалізації.

Отриманим результатам не доцільно надавати перебільшеної ваги або приписувати точність, вищу ніж у даних і методах, що використовуються.

Таким чином, застосовуючи метод експертних оцінок було здійснено практичне оцінювання загроз критичній інфраструктурі з пріоритизацією загроз, що дає змогу зосередити зусилля на найбільш небезпечних загрозах і запобігти значних втрат критичної інфраструктури.

Висновки й перспективи подальших досліджень

У результаті проведених досліджень було встановлено, що метод експертного оцінювання є ефективним інструментом для оцінювання загроз критичній інфраструктурі. Він дає змогу враховувати широкий спектр факторів, що впливають на рівень загрози, і отримати об'єктивну та достовірну оцінку. Застосування методу експертного оцінювання для оцінювання загроз критичній (військовій) інфраструктурі дає змогу: визначити пріоритетність об'єктів критичної інфраструктури для захисту; визначити найбільш значущі та найбільш імовірні загрози; розробити ефективні заходи захисту об'єктів критичної інфраструктури. Метод експертного оцінювання може бути ефективним інструментом для оцінювання загроз критичній інфраструктурі та використаний для пріоритизації та оптимального використання наявних сил і засобів для захисту об'єктів критичної інфраструктури та нейтралізації найбільш значущих і найбільш імовірних загроз. Результати дослідження мають теоретичну значущість, оскільки вони розширюють теоретичні знання про метод експертного оцінювання та його застосування для оцінювання загроз критичній інфраструктурі. Стаття має практичну цінність, оскільки результати можуть бути використані для підвищення ефективності заходів щодо захисту

критичної інфраструктури. Для підвищення ефективності застосування методу експертного оцінювання для оцінювання загроз критичній інфраструктурі рекомендується: використовувати експертів з відповідною кваліфікацією та досвідом; проводити експертизу в кілька етапів, що дасть змогу врахувати різні точки зору експертів; використовувати сучасні інформаційні технології для обробки експертних оцінок. Стаття буде корисною для експертів та фахівців цивільного захисту стосовно попередження та локалізації надзвичайних ситуацій, а також дослідження причин їх виникнення в критичній інфраструктурі. Отже, мета статті була досягнута.

Список бібліографічних посилань

1. Мурасов Р. К., Куртсеітов Т. Л., Мельник Я. В. Імовірнісний метод прогнозування надзвичайних подій на потенційно-небезпечних об'єктах критичної інфраструктури. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2022. № 2(44). С. 60–64. DOI: 10.33099/2311-7249/2022-44-2-60-63. **2. Мурасов Р. К., Невольніченко А. І., Чумаченко С. М., Пиріков О. В., Михайлова А. В.** Моделювання загроз виникнення надзвичайних ситуацій на об'єктах критичної інфраструктури з використанням методу системної динаміки. *Таврійський науковий вісник*. Серія: Технічні науки. 2022. № 3. С. 88–99. DOI: 10.32851/tnv-tech.2022.3.10. **3. Risk** assessment methodologies for critical infrastructure protection. Part II:A new approach. URL:http://publications.jrc.ec.europa.eu/repository/ bitstream/JRC96623/lbna27332enn.pdf (дата звернення: 13.06.2023). **4. Суходоля О. М., Харазішвілі Ю. М., Рябцев Г. Л., Бобро Д. Г., Завгородня С. П.** Оцінювання загроз енергетичній безпеці. Аналітична доповідь DOI: 10.53679/NISS-analytrep.2022.11. **5. Мурасов Р. К., Чумаченко С. М., Мельник Я. В.** Теоретико-методологічні основи інформаційного аналізу еколого-техногенних загроз для потенційно-небезпечних об'єктів критичної інфраструктури в умовах збройного конфлікту на сході України. Сучасні інформаційні технології у сфері безпеки та оборони. 2021. № 1 (40). С. 117–122. DOI: 10.33099/2311-7249/2021-40-1-117-122. **6. Єрменчук О. П.** Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монографія. Дніпропетровський державний університет внутрішніх справ : Дніпро, 2018. 180 с. **7. Уряднікова І. В., Чумаченко С. М., Кармазін С. В., Тесленко О. М.** Застосування експертно-аналітичних методів для оцінювання ризиків надзвичайних ситуацій на об'єктах критичної інфраструктури. *Науковий вісник Академії муніципального управління.* Серія : Техніка. 2015. Вип. 1. С. 206–218. URL: http://nbuv.gov.ua/UJRN/Nvamu_teh_ 2015_1_24 (дата звернення: 13.06.2023). **8. Цяпа С. М.** Правове та організаційне забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак. Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України. *Інформація і Право*. 2021. № 4(39). С. 121–128. DOI: 10.37750/2616-6798.2021.4(39).248832.

GENERAL APPROACHES TO THE ASSESSMENT OF THREATS TO CRITICAL INFRASTRUCTURE USING THE METHOD OF EXPERT ASSESSMENT

Murasov Rustam ***(Candidate of Technical Sciences)***
Melnyk Yaroslav

National Defence University of Ukraine, Kyiv, Ukraine

Formulation of the problem in general. *Critical infrastructure is the basis of the vital activities of society and the state. In case of its damage or destruction, emergency situations may arise, which will lead to significant economic losses, human casualties and disruption of the normal functioning of the state. There are many methods of assessing threats to critical infrastructure. Among them, the following can be distinguished: Quantitative assessment methods used to calculate risks arising from exposure to threats. Qualitative assessment methods that allow describing threats and their consequences. Expert assessment is one of the methods of qualitative assessment of threats. It allows you to use the knowledge and experience of experts to assess threats, which cannot be calculated using mathematical methods.*

Analysis of recent researches and publications *Evaluation of threats to critical infrastructure by the method of expert evaluation is an active object of research and publications in the field of cyber security, security of critical systems and risk management. Thus, the author O. P Yermenchuk in the work "Basic approaches to the organization of critical infrastructure protection in European countries: experience for Ukraine" provides an overview of general approaches to critical infrastructure risk assessment, including methods of expert threat assessment and considers problematic issues of threat identification, identification of vulnerabilities and calculation of consequences. In the authors' publication Uryadnikova I. V., Chumachenko S. M., Karmazina S. V., Teslenko O. M. "Application of expert-analytical methods for assessing the risks of emergency situations at critical infrastructure facilities" limits for expert risk assessment are proposed and decision-making. They consider the issue of attracting experts, determining the weight of their assessments and analyzing the received data. Author S. M. Tsyapa in the article «Legal and organizational protection of critical information infrastructure objects from cyber-attacks» considers the legal and organizational aspects of protection of critical information infrastructure objects from cyber-attacks. Uses the positive experience of the USA in ensuring the stability of critical infrastructure objects and analyzes the provisions of the new Cybersecurity Strategy of Ukraine.*

Presenting the main material *During the research, the following methods are used: analysis methods during the analysis of existing sources by research direction, existing threat assessment approaches, risk analysis methods, mathematical modeling methods for threat assessment and risk analysis, machine learning methods such as artificial intelligence, deep learning and method. expert assessment. The specified methodological approach makes it possible to obtain the results of the assessment of threats to critical infrastructure for the rational distribution of means of protection, which are created by the constituent forces of security and defense of the state. The article presents existing threat assessment approaches and considers*

the possibility of using the expert assessment method to determine threats to critical infrastructure in the modern conditions of the russian-ukrainian war. A methodology for assessing threats to critical infrastructure, based on the method of expert assessment, has also been created. The results of threat assessment for critical infrastructure objects are given. A methodology for assessing threats to critical infrastructure with threat prioritization is proposed. The essence of the method of expert assessment and improvement of this method by introducing identifiers of threats to critical infrastructure is explained, and the following definitions are formulated: averaged expert probability, separate and cumulative destructive consequences, probabilities of threats to the protection of critical infrastructure, which makes it possible to focus efforts on the most dangerous threats and prevent significant losses of critical infrastructure infrastructure

Elements of scientific novelty. *Elements of the article's scientific novelty are the mechanism of risk prioritization (consequences, cumulative destructive effects) with the definition of the most dangerous, and the separation of those that have an insignificant effect. Conclusions were made regarding the possibilities and expediency of using the expert assessment method to identify potential risks for critical infrastructure objects and develop strategies for their protection. Practical calculations were carried out with conclusions regarding threats and their prioritization in relation to critical infrastructure*

Practical significance of the article. *The contribution to the development of the methodology for assessing threats to critical infrastructure should be attributed to the theoretical significance of the article. The proposed method of expert assessment allows obtaining quantitative assessments of threats, which is important for making effective management decisions and allows taking into account various factors affecting the level of threat as a whole. The practical significance of the article is that the obtained research results can be used for: ensuring the safety of critical infrastructure, forming priorities for the protection of critical (military) infrastructure objects and developing measures to increase the level of security of critical (military) infrastructure.*

Conclusion and the perspectives of future researches. *As a result of the research, it was established that the expert assessment method is an effective tool for assessing the threat to critical infrastructure. It allows you to get a wide range of factors affecting the level of threat and makes it possible to get an objective and reliable assessment. The application of the expert assessment method for assessing threats to critical infrastructure allows: the strategicness of critical infrastructure objects for protection; the most significant option and the most probable threat; develop effective measures to protect critical infrastructure objects. The expert assessment method is an effective tool for assessing threats to critical infrastructure and can be used to prioritize and optimally use available forces and means to protect critical infrastructure objects and neutralize the most significant and most likely threats. The results of the study have theoretical significance, as they expand the theoretical knowledge about the method of expert evaluation and its application to the assessment of threats to critical infrastructure. The article has practical value, as the results can be used to improve the effectiveness of measures to protect critical infrastructure. To increase the efficiency of the application of the expert assessment method for assessing threats to critical infrastructure, it is recommended to: use experts with appropriate qualifications and experience; carry out an examination in several stages, which will allow taking into account different points of view of experts; use modern information technologies to process expert assessments.*

Key words: *critical infrastructure, missile and drone strikes, expert assessment, minimization of emergency situations, emergence of emergency situations, civil protection.*

References

1. Murasov, R., Kurtseitov, T., Melnyk, Y., (2022). A probabilistic method of forecasting emergency events at potentially dangerous objects of critical infrastructure. Modern information technologies in the sphere of security and defense, 2(44), 60–64. DOI: 10.33099/2311-7249/2022-44-2-60-63. **2. Murasov, R., Nevolnichenko, A., Chumachenko, S., Mykhailova, A., Pyrikov, O.,** (2022). Modeling threats of emergency situations at critical infrastructure facilities using the method of system dynamics. Taurian Scientific Bulletin. Series: Technical Sciences, 3, 88-99. DOI: 10.32851/tnv-tech.2022.3.10. **3. Risk** assessment methodologies for critical infrastructure protection. Part II: (2015). A new approach [on line]. Available at: http://publications.jrc.ec.europa.eu/repository/bitstream/ JRC96623/lbna27332enn.pdf [Accessed : 13 June 2023]. **4. Sukhodolya, O., Kharazishvili, Y., Ryabtsev, G., Bobro D., Zavhorodnia, S.** (2022). Assessment of threats to energy security. Analytical report. DOI: 10.53679/NISS-analytrep.2022.11. **5. Murasov, R., Chumachenko, S., Melnyk, Y.,** (2021). Modern information technologies in the field of security and defense, theoretical and methodological bases of information analysis of ecological and man-made threats to potentially dangerous objects of critical infrastructure in conditions of armed conflict in the east of Ukraine. Modern information technologies in the sphere of security and defense, 1(40), 117-122. DOI: 10.33099/2311-7249/2021-40-1-117-122. **6. Ermenchuk, O.,** (2018). Basic approaches to the organization of critical infrastructure protection in European countries: experience for Ukraine. Dnipropetrovsk State University of Internal Affairs, Dnipro, 180. **7. Uryadnikova, I., Chumachenko, S., Karmazin, S., Teslenko, O.,** (2015). Application of expert analytical methods for assessing the risks of emergency situations at critical infrastructure facilities. Scientific Bulletin of the Academy of Municipal Administration. Series: Technology. Issue 1, 206-218 [on line]. Available at: http://nbuv.gov.ua/UJRN/Nvamu_teh_2015_1_24 [Accessed : 13 June 2023]. **8. Tyapa, S.,** (2021). Legal and organizational support for the protection of critical information infrastructure objects from cyberattacks. Ukrainian Research Institute of Special Equipment and Forensic Examinations of the Security Service of Ukraine. Information and Law, 4(39), 121-128. DOI: 10.37750/2616-6798.2021.4(39).248832.