УДК 355.58.0001, 351.862.001, 621.396.61, 621.396.62 **https://doi.org/10.37700/enm.2020.4(18).114 - 123**

Застосування експертно-аналітичних методів для оцінювання загроз об'єктам критичної інфраструктури оборонно-промислового комплексу на сході України

С.М. Чумаченко [1], О.П.Кутовий [2], А.В. Михайлова [3]

[1] Національний університет харчових технологій (м. Київ, Україна),
[2] Національний університет оборони України
ім. Івана Черняховського (м. Київ, Україна),
[3] Інститут державного управління та наукових досліджень
з цивільного захисту (м. Київ, Україна)
email: [1] sergiy23.chumachenko@gmail.com; [3] mihajlova-a-v@ukr.net
ORCID: [1] 0000-0002-8894-4262; [2] 0000-0003-3168-5105; [3] 0000-0001-9440-4417

Автори статті пропонують методичний підхід до оцінювання загроз для об'єктів критичної інфраструктури оборонно-промислового комплексу держави в умовах ведення гібридної війни. Актуальність роботи обумовлена процесами протидії загрозам техногенного характеру на території Донбасу, які існують в Україні, а також відсутністю методичних розробок, за допомогою яких можливо оцінити рівень загроз критичній інфраструктурі оборонно-промислового комплексу. Автори публікації визначають фактори, які суттєво впливають на воєнно-техногенні загрози об'єктам критичної інфраструктури оборонно-промислового комплексу неї. У відповідності з цими факторами у роботі наводиться ієрархічна система показників, яка складається з трьох груп. Ці групи характеризують фактори оцінки воєнно-техногенних та природно-техногенних загроз, а також містять часткові критерії, які дозволяють оцінити ймовірні загрози.

Доведено працездатність цього методичного підходу на прикладі боєприпасної галузі України. Для проведення розрахунків з оцінки найбільш небезпечних об'єктів оборонно-промислового комплексу використано метод аналізу ієрархій з використання розробленої інформаційно-аналітичної системи. Розрахунки були спрямовані на оцінювання пріоритетності захисту арсеналів, баз, складів і підприємств оборонно-промислового комплексу, які у випадку їх ураження становлять найбільшу загрозу для держави в цілому, у відповідності з відповідними критеріями, визначеними у проєкті закону України «Про критичну інфраструктуру та її захист».

У статті наводяться результати чисельного експерименту, який підтвердив працездатність науково-методичного підходу, його достатньо високу точність та наочність отриманих результатів.

Проведене експертне оцінювання дозволило встановити рівні загроз для об'єктів критичної інфраструктури оборонно-промислового комплексу, до яких відносяться підприємства оборонно-промислового комплексу боєприпасної галузі (інтегральний індекс загрози становить 0,472), арсенали (інтегральний індекс загрози становить 0,259), склади (інтегральний індекс загрози становить 0,147), бази зберігання (інтегральний індекс загрози становить 0,122).

Ключові слова*: ризик, загроза, снаряди, боєприпаси, метод аналізу ієрархій, метод контрольних списків.*

Постановка проблеми та її актуальність. Одним із чинників забезпечення національної безпеки України є захищеність та безпечна робота об'єктів оборонно-промислового комплексу (ОПК), які функціонують в мирний час та особливий період. Зважаючи на реалії сьогодення, виникає необхідність створення дієвої системи підтримки прийняття рішень шляхом здійснення ретельного аналізу реальних та потенційних загроз і ризиків, що дасть можливість надійно функціонувати об'єктам критичної інфраструктури (ОКІ) ОПК.

Важливість цієї проблеми підтверджується тим, що забезпечення безпеки й захищеності державних ОКІ ОПК [1] є особливо актуальним у період проведення самостійного розвитку військової науки і техніки, зважаючи на зміну масштабів розробок і виробництв військової техніки, що пов'язано з веденням збройного конфлікту на території Сходу України, а також адаптацією до стандартів НАТО, формуванням самодостатнього ОПК, органів його управління та створенням якісної системи логістичного забезпечення.

Зосередження уваги на ОКІ ОПК зумовлене й зі значною кількістю пожеж на військових складах України, які сталися останніми роками, зокрема у м. Бахмут, м. Лозова, м. Сватове, м. Балаклея, м. Ічні, с. Новобогданівка тощо [2].

Аналіз останніх досліджень та публікацій щодо оцінки забезпечення захисту ОКІ ОПК свідчить, що проблематика у сфері військової діяль-

ності є специфічною, тому потребує застосування сучасного математичного апарату, об'єктивних висновків і узагальнень експертів.

Варто зазначити, що захист ОКІ ОПК регламентується державними нормативно-правовими актами для внутрішньовідомчого використання. Наразі визначено ряд категорій об'єктів, для яких визначено особливі умови забезпечення захисту [4-7], зокрема на сайті Мінекономрозвитку у 2019 році оприлюднено проєкт Закону «Про критичну інфраструктуру та її захист» [3].

Так, до ОКІ віднесені підприємства, установи, організації незалежно від форми власності, які, згідно з [3]:
– провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, ОПК, транспорту, інформаційно-телекомунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;
– надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, централізованого водовідведення, постачання теплової енергії, гарячої води, електричної енергії і газу, виробництва харчових продуктів, охорони здоров'я;
– включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;
– підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду;
– є об'єктами підвищеної небезпеки;
– є об'єктами, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру;
– є об'єктами, порушення функціонування яких призведе до кризової ситуації регіонального значення.

В той же час, наразі у ході проведення експертної оцінки чинників воєнно-техногенного впливу на ОКІ ОПК недостатньо уваги приділяється застосуванню сучасних методів моделювання, експертного оцінювання та застосуванню інформаційних технологій. Це не дає можливості в достатній мірі забезпечувати особу, яка приймає рішення, точною, оперативною та достовірною інформацією. Така ситуація може призвести до унеможливлення прийняття обґрунтованих управлінських рішень. У зв'язку з цим розвиток і практичне застосування методів математичного моделювання, комплексного експертного оцінювання особливостей впливу чинників воєнно-техногенного впливу на ОКІ ОПК, а також їх загроз і управління ними набувають особливої важливості та актуальності.

З метою проведення аналізу можливих загроз, надзвичайних ситуацій (НС) та наслідків їх виникнення, а також застосування превентивних заходів, оператори ОКІ повинні подавати на погодження до відповідальних за сектори суб'єктів захисту критичної інформації (КІ), Служби безпеки України та суб'єктів із забезпечення фізичної охорони паспорт безпеки на кожен ОКІ.

Для оцінювання можливих загроз і ризиків існує ряд підходів. Наприклад, у країнах Євросоюзу активно впроваджується системний підхід, що базується на оцінюванні загроз і ризиків з використанням декількох критеріїв [8, 9].

Так, за результатами числового визначення ризику людських втрат та економічних збитків, завданими ОКІ ОПК, прогнозні експертні оцінки відображають індивідуальне судження фахівців про можливий розвиток небезпечних подій. Методи експертних оцінок засновані на мобілізації професійного досвіду та інтуїції експертів. Такі методи оцінювання загроз і ризику використовують формальну теорію ухвалення рішень в умовах невизначеності. У разі виникнення НС центральною фігурою і суб'єктом ухвалення рішення є особа, що приймає рішення (ОПР). Це може бути як одна особа, так і група осіб, котрі опрацьовують колективне рішення. Зазвичай, ОПР – це керівник або керівний орган, який формулює проблему, відіграє вирішальну роль у виборі вирішення проблеми і несе відповідальність за прийняте рішення. В той же час, експерти й консультанти несуть відповідальність за обґрунтованість рекомендацій, які вони готують для ОПР. Остаточне ж рішення завжди приймає ОПР, відповідно до власної системи переваг, а також несе повну відповідальність за свій вибір та його наслідки [8, 10].

Метою даної роботи є аналіз та обґрунтування застосування можливих підходів експертного оцінювання небезпек та загроз для ОКІ ОПК. Останні оцінюються із застосуванням різноманітних математичних методів та прикладного програмного забезпечення, в основі яких лежить загальна методологія оцінінювання ризиків, при чому ключовою особливістю оцінінювання загроз для ОКІ ОПК є врахування численних взаємозв'язків та взаємозалежностей критеріїв і чинників експертної оцінки.

Результати досліджень. Віднесення об'єктів до ОКІ визначається сукупністю критеріїв [3], що враховують їх життєво важливі функції з надання послуг, та свідчать про існування загроз для них. Виникнення небажаних подій на таких об'єктах унаслідок несанкціонованого втручання в їх роботу може призвести до порушення режиму функціонування, причиною яких є людський фактор, природне лихо чи аварії. Тривалістю робіт для усунення таких наслідків є період до повного відновлення штатного режиму.

Таким чином, об'єкти ОПК, арсенали, бази і склади зберігання військової техніки та боєприпасів відносяться до ОКІ, а тому потребують оцінювання всіх можливих ризиків й загроз їх функціонування, а

також визначення необхідних превентивних заходів забезпечення їх безперебійної і роботи.

Проведення такого оцінювання варто проводити із використанням методу аналізу ієрархій (МАІ) запропонованого Т. Сааті, який є одним із методів підтримки прийняття рішень. МАІ є загальним методом розв'язання широкого класу слабко структурованих задач прийняття рішень, що дозволяє поєднати відносно простий математичний апарат з досвідом та інтуїцією особи, яка приймає рішення і передбачає послідовне виконання наступних етапів:

– структурування задачі та виявлення зв'язків між її складовими (побудова багаторівневої ієрархії);
– визначення критеріїв оцінювання та порівняння;
– синтез пріоритетів та вибір пріоритетної альтернативи.

МАІ є замкнутою логічною конструкцією, що забезпечується простими правилами аналізу складних проблем, які приводять до оптимальної відповіді Цей метод є найбільш обґрунтованим для розв'язання багатокритеріальних завдань при складних обставинах з ієрархічними структурами, що містять як помітні, так і непомітні фактори, у порівнянні з методами, що базуються на лінійній логіці. До того ж застосування МАІ дозволяє включати в ієрархії усі наявні у дослідника даної проблеми знання та факти [8, 12].

Детальний опис та роз'яснення використання МАІ, тлумачення результатів, отриманих при застосуванні цього методу, тощо описано у [13].

Для здійснення експертного оцінювання пріоритетності захисту найбільш вразливих об'єктів ОПК (арсеналів, складів, баз та підприємств) було застосовано метод аналізу ієрархій у вигляді відповідного програмного додатку. Критеріями для визначення пріоритетності були обрані ті, які визначено в проєкті закону України «Про критичну інфраструктуру та її захист» [3], а саме:

– існування викликів і загроз, що можуть виникати щодо ОКІ;
– завдання значної шкоди нормальним умовам життєдіяльності населення;
– уразливість цих об'єктів, тяжкість можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода: здоров'ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення); соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства); економіці (вплив на внутрішній валовий продукт, розмір економічних втрат, як прямих, так і непрямих); природним ресурсам загальнодержавного значення; обороноздатності; іміджу країни;
– масштабність негативних наслідків для держави, які: вплинуть на діяльність стратегічно важливих об'єктів для кількох секторів життєзабезпечення або призведуть до втрати унікальних національно значущих активів, систем і ресурсів, матимуть тривалі наслідки для держави і позначаються на діяльності ряду інших секторів;
– тривалість ліквідації таких наслідків та дія подальшого негативного впливу на інші сектори держави;
– вплив на функціонування суміжних секторів КІ.

На думку авторів, методичний підхід, який викладено нижче, дає можливість працювати з неповною інформацією водночас із значною кількістю якісних та кількісних характеристик військової, техногенної та природної небезпеки. Це полегшує здійснення обчислень вагових коефіцієнтів окремих чинників, які впливають на воєнно-техногенну безпеку ЗС України, ОПК та безпеку життєдіяльності населення, яке проживає на прилеглих територіях.

Зазначений методичний підхід складається із трьох основних етапів:

1. Системний аналіз та структуризація проблеми захисту ОКІ ОПК;
2. Визначення комплексних показників загроз для ОКІ ОПК;
3. Розрахунок інтегральних показників загроз для ОКІ ОПК на основі комплексних показників потенційної небезпеки.

Огляд сучасних підходів до системного аналізу складних систем і процесів та аналіз математичного апарату, який застосовується при цьому, дозволяють зробити висновок, що аналіз і оцінювання загроз для ОКІ ОПК повинні бути багатофакторними, а порівняльний аналіз сукупності їх джерел варто здійснювати з урахуванням ряду показників, які є визначальними під час формування цільових функцій для відповідних часткових та інтегрального критеріїв.

Серед процедур, які використовуються під час вирішення багатокритеріальних задач та дають можливість вибрати з них допустимі для використання під час проведення системного аналізу загроз і ризиків для ОКІ ОПК, є:

– використання цільової функції;
– використання функції переваги при згортанні багатокритеріальної задачі до однокритеріальної, що ґрунтується на згортанні багатьох критеріїв в один;
– використання функції переваги й виділення пріоритетного критерію.

Структура інформаційної моделі, яка обґрунтовано використовується для оцінювання загроз і ризиків [14], зображена на рис. 1.

У зв'язку з тим, що кожен елемент моделі загрози є складним організаційно-технічним заходом з багатофакторним комплексним впливом, необхідно провести його декомпозицію на послідовність окремих елементів.

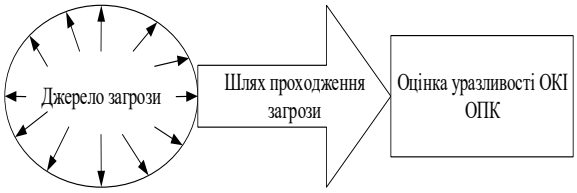

Рис. 1. Структура інформаційної моделі для оцінювання загроз і ризиків для ОКІ ОПК

Так, для формування логіко-інформаційної моделі авторами публікації застосовано метод декомпозиції, який дозволяє виділити його окремі типові складові та зобразити їх у вигляді ієрархічного дерева. Логіко-інформаційна модель ієрархічного дерева елементарних подій може бути представлена у вигляді орієнтованого графа (орграфа), який зображує їх послідовність і склад (рис. 2).

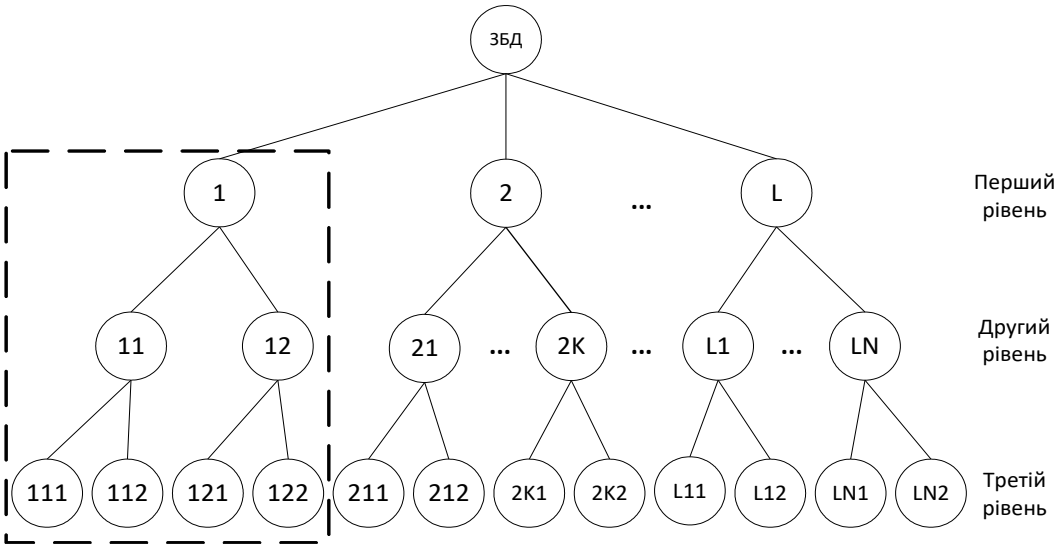

Рис. 2. Орграф формування загрози

Склад вузлів орграфу характеризує ієрархічну підпорядкованість та їх декомпозицію на елементарні події, вклад яких у загальну оцінку загрози можна визначити за допомогою кваліфікованих експертів. Після цього оцінювання складного елементу здійснюється за елементами вузлів орграфу.

Для загальної оцінки загрози показник обчислюється за такими формулами

$$O_{\text{БД}} = k_1 \cdot O^1_{\text{БД}} + k_2 \cdot O^2_{\text{БД}} + \ldots + k_L \cdot O^L_{\text{БД}}, \qquad (1)$$

$$\begin{cases} O^1_{\text{БД}} = k_{11} \cdot O^{11}_{\text{БД}} + k_{12} \cdot O^{12}_{\text{БД}}, \\ O^2_{\text{БД}} = k_{21} \cdot O^{21}_{\text{БД}} + \ldots + k_{2K} \cdot O^{2K}_{\text{БД}}, \\ \ldots \\ O^L_{\text{БД}} = k_{L1} \cdot O^{L1}_{\text{БД}} + \ldots + k_{LN} \cdot O^{LN}_{\text{БД}}, \end{cases} \qquad (2)$$

$$\begin{cases} O^{11}_{\text{БД}} = k_{111} \cdot O^{111}_{\text{БД}} + k_{112} \cdot O^{112}_{\text{БД}}, \\ O^{12}_{\text{БД}} = k_{121} \cdot O^{121}_{\text{БД}} + k_{122} \cdot O^{122}_{\text{БД}}, \\ \ldots, \\ O^{LN}_{\text{БД}} = k_{LN1} \cdot O^{LN1}_{\text{БД}} + k_{LN2} \cdot O^{LN2}_{\text{БД}}, \end{cases} \qquad (3)$$

де $0 < k_i < 1$ − вагові коефіцієнти, для яких виконується правило нормування.

Інтегральна бальна оцінка отримується методом кумулятивного накопичення оцінок складових елементів загрози із врахуванням ваги кожного компоненту на певному рівні орграфу

$$\begin{gathered} O_{\text{БД}} = k_1 \cdot (k_{11} \cdot (k_{111} \cdot O^{111}_{\text{БД}} + \\ + k_{112} \cdot O^{112}_{\text{БД}}) + k_{12} \cdot (k_{121} \cdot O^{121}_{\text{БД}} + \\ + k_{122} \cdot O^{122}_{\text{БД}})) + \cdots + \\ + k_L \cdot (k_{L1} \cdot (k_{L11} \cdot O^{L11}_{\text{БД}} + \\ + k_{L12} \cdot O^{L12}_{\text{БД}}) + \cdots + \\ + k_{LN} \cdot (k_{LN1} \cdot O^{LN1}_{\text{БД}} + k_{LN2} \cdot O^{LN2}_{\text{БД}})) \end{gathered} \qquad (4)$$

Задача оцінювання та ранжування загроз і ризиків для ОКІ ОПК в умовах невизначеності розв'язується методами системного аналізу з використанням багатокритеріальної оцінки [12, 15]. Для оцінки і ранжування загроз та ризиків слід сформувати критерії не лише в значенні «критеріальна функція», а в ширшому значенні – як спосіб оцінки і порівняння загроз та ризиків.

Для оцінювання можливих загроз і ризиків існує ряд підходів. Наприклад, в країнах Євросоюзу активно впроваджується системний підхід. Він грунтується на оцінюванні природно-техногенних загроз і ризиків з використанням декількох критеріїв, оскільки випадки, коли єдиний критерій вдало відображає мету оцінювання загроз та ризиків, швидше виключення, ніж правило. Один критерій лише приблизно (як і всяка модель) відображає мету оцінювання, тому його адекватність може виявитися недостатньою. Вирішення задачі підвищення адекватності полягає не лише в пошуку

більш адекватного критерію (можливо, його і немає), але й у використанні декількох критеріїв, які описують різносторонньо мету оцінювання загроз і ризиків для ОКІ ОПК та доповнюють один одного.

Об'єктивність вирішення задачі оцінювання і ранжування обумовлюється забезпеченням критеріями достатньо повної послідовності оцінювання ознак для загроз та ризиків. Тобто критерії визначають всі важливі аспекти мети оцінювання, але при цьому варто мінімізувати їх кількість. Остання вимога задовольняється, якщо критерії є незалежними та не пов'язані між собою.

З метою оцінювання і ранжування загроз та ризиків для ОКІ ОПК застосовуються методи обчислення бальних оцінок різних чинників, які характеризують окремі складові конкретних критеріїв. Ієрархічну структуру чинників, а також часткового та інтегрального критеріїв наведено на рис. 3.

Процедура комплексного оцінювання базується на підходах багатокритеріальної оцінки загроз для ОКІ ОПК з подальшою згорткою її до інтегрального індексу. Як правило, вона набуває практичного сенсу лише в тому випадку, коли використовується такий метод, за якого багатокритеріальна задача зводиться до однокритеріальної. Проте, очевидні переваги об'єднання декількох критеріїв в один інтегральний (суперкритерій) супроводжуються деякими труднощами і недоліками, які необхідно враховувати при використанні цієї методики.

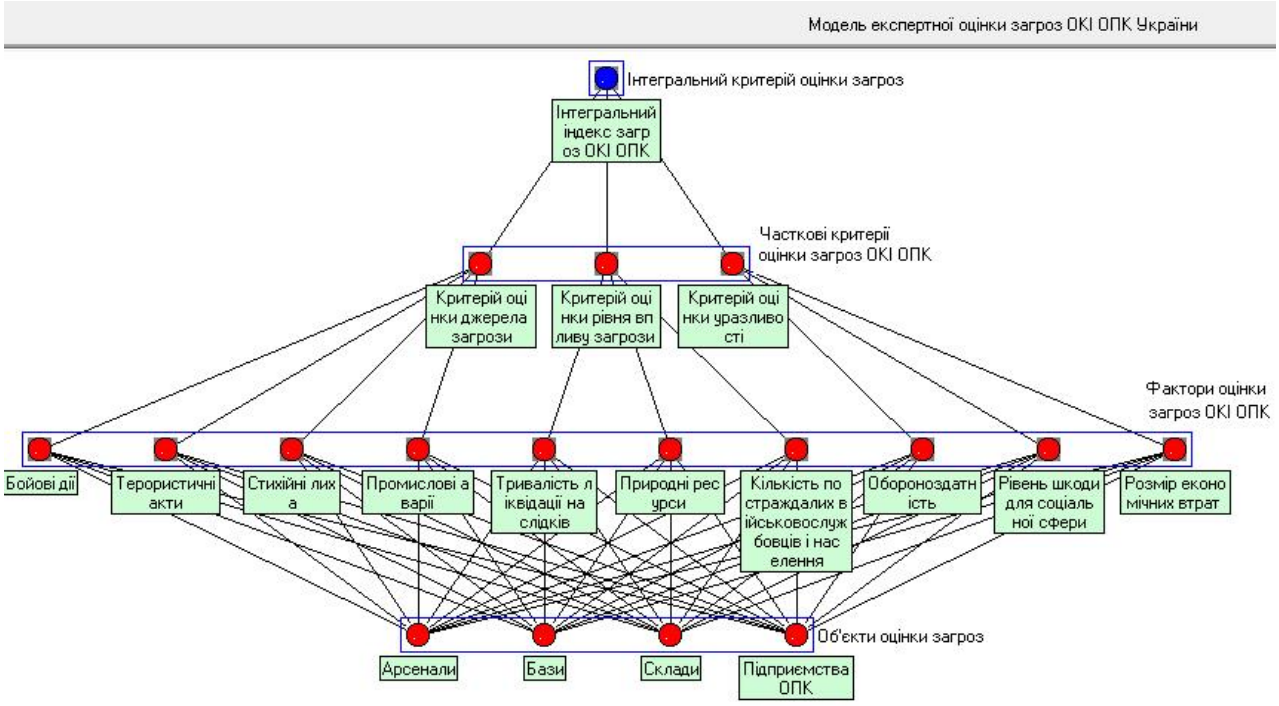

Рис. 3. Ієрархічне дерево критеріїв і чинників для оцінки загроз ОКІ ОПК

Керуючись теретичною інформацією, наведеною у [16], узагальнено адитивну та мультиплікативну цільові функції, які можна представити у такому вигляді:

$$J_\Sigma(e) = \sum_{i=1}^{n} \frac{\alpha_i}{s_i} J_i(e_i), \qquad (5)$$

де α_i і s_i − вагові коефіцієнти, які можуть визначатися експертним шляхом, наприклад, за допомогою процедур МАІ.

У цій формулі коефіцієнти відображають відносний внесок складових критеріїв в інтегральний, а коефіцієнти забезпечують оцінку інформативності складових критеріїв. Узагальнені вагові коефіцієнти можуть бути визначені експертним шляхом із застосуванням МАІ.

Так, кожен частковий критерій складається з множини чинників. З метою отримання експертних оцінок експерти заповнюють анкети, в яких присвоюють відповідні оцінки ознакам чинників, значення яких можна зафіксувати в бальній шкалі, що відповідає бальній шкалі Сааті.

Для оцінки загроз ОКІ ОПК пропонується застосувати наступні критерії:

– критерій оцінки джерела загрози;
– критерій оцінки рівня впливу загрози;
– критерій оцінки уразливості.

Для формування інтегральної оцінки необхідно сформулювати узагальнену цільову функцію, яка, за умови бальної оцінки, є інструментом приведення багатокритеріальної задачі до однокритеріальної. Вона є скалярною функцією векторного аргументу (інтегральний критерій або суперкритерій):

$$J_\Sigma(e) = f\big(J_1(e_1), J_2(e_2), J_3(e_3), J_4(e_4)\big), \qquad (6)$$

де $J_\Sigma(e)$ – цільова інтегральна функція критерію оцінки загроз, $J_i(e_i), i = \overline{1,4}$ – цільові функції складових критеріїв оцінки загроз.

Вигляд функції (6) визначається внеском кожного складового критерію в інтегральний критерій та видом згортки, який при цьому використовується. При згортці багатокритеріальних задач оцінки загроз до однокритеріальних, коли складові критерії є різноваговими, зазвичай, використовують адитивні (інколи мультиплікативні) функції згортки.

Як вже зазначалося, з метою оцінювання загроз ОКІ ОПК було розроблено відповідну інформаційно-аналітичну систему та спільно з представниками Міністерства оборони України здійснено експертну оцінку за ієрархічним деревом, що наведене на рис. 3.

Алгоритм цієї методики полягає у виконанні таких етапів [18]:

1. Визначення цілі (фокусу) проблеми оцінювання загроз ОКІ ОПК.

2. Системний аналіз та структуризація проблеми оцінювання загроз ОКІ ОПК у вигляді ієрархічної моделі, що включає критерії, чинники оцінки та об'єкти оцінки загроз ОКІ ОПК.

3. Формування бази даних характеристик критеріїв, чинників та об'єктів оцінки загроз ОКІ ОПК.

4. Заповнення матриць попарних порівнянь елементів кожного рівня групою експертів, до складу якої входить системний аналітик.

5. Визначення власних векторів матриць попарних порівнянь та їх нормування. Середня оцінка балів, дисперсія цієї оцінки та інші показники визначаються за формулами, які використовуються для методу шкальних оцінок.

6. Оцінка узгодженості суджень експертів на основі відношення узгодженості. Після проведення всіх попарних порівнянь визначається індекс узгодженості і відношення узгодженості. Індекс узгодженості, який дає інформацію про порушення числової та транзитивної матриці порівнянь, є важливим елементом моделі визначення вагових коефіцієнтів. Тому цей індекс можна розглядати як показник «близькості до узгодженості». Тобто похибки співвідношень $a_{ik} = a_{ij} \cdot a_{jk}, k = \overline{1,n}, i = \overline{1,n}, j = \overline{1,n}$.

7. Якщо матриці узгоджені, то виконують п. 8, якщо ні – то переходять до п. 4.

8. Визначення локальних і глобальних пріоритетів (вагових коефіцієнтів) кожного з елементів ієрархії. Пріоритети синтезуються, починаючи з другого рівня до низу. Локальні пріоритети перемножують на пріоритет відповідного елементу на вищому рівні і підсумовують за кожним елементом відповідно до значень коефіцієнтів важливості чи пріоритетності кожного з елементів, на які він впливає у кожному рівні ієрархії.

9. Визначення пріоритетних загроз ОКІ ОПК та їх ранжування.

10. Створення бази даних ОКІ ОПК за відповідними кластерами.

11. Створення відповідної форми в Microsoft Excel 2010 для проведення експертного оцінювання за відповідними кластерами.

12. Узагальнення та аналіз експертних оцінок загроз ОКІ ОПК.

Експертні оцінки приймаються як групові. Під час проведення процедури комплексного оцінювання значення якісних і кількісних характеристик загроз ОКІ ОПК проєктуються на значення відповідних шкал − систем чисел визначеної послідовності чи інших елементів, прийнятих для виміру чи оцінювання яких-небудь величин, виявлення зв'язків і відносин між елементами. Аргументи цільової функції, які є ознаками-чинниками в оцінках загроз ОКІ ОПК за відповідними складовими критеріями, виражаються балами в безрозмірному вигляді за чотирибальною шкалою.

Після оцінки чинників розраховують значення часткових критеріїв. За умови застосування адитивної цільової функції часткові критерії обчислюють за формулами:

1. Критерій оцінки джерела загрози

$$J_1(e^1) = 0{,}549 \cdot {e^1}_1 + 0{,}209 \cdot {e^1}_2 + \\ +0{,}131 \cdot {e^1}_3 + 0{,}111 \cdot {e^1}_4 \qquad (7)$$

2. Критерій оцінки рівня впливу загрози

$$J_2(e^2) = 0{,}336 \cdot {e^2}_1 + 0{,}59 \cdot {e^2}_2 + 0{,}504 \cdot {e^2}_3 \qquad (8)$$

3. Критерій оцінки уразливості

$$J_3(e^3) = 0{,}351 \cdot {e^3}_1 + 0{,}289 \cdot {e^3}_2 + \\ +0{,}178 \cdot {e^3}_3 + 0{,}101 \cdot {e^3}_4 + 0{,}08 \cdot {e^3}_5 \qquad (9)$$

4. Інтегральний критерій оцінки загрози

$$J_\Sigma(e) = 0{,}525 \cdot J_1(e^1) + 0{,}305 \cdot J_2(e^2) + \\ +0{,}086 \cdot J_3(e^3) + 0{,}085 \cdot J4(e^4) \qquad (10)$$

Отже, у разі застосування такого підходу задача оцінки загроз ОКІ ОПК зводиться до порівняння отриманих бальних оцінок і ранжування їх за сукупністю часткових критеріїв чи інтегральним критерієм.

За результатами оцінювання було проведено ранжування ОКІ ОПК, яке наведено у вигляді графіку на рис. 4.

Висновки. В статті наведено підходи оцінювання загроз та ризиків на ОКІ ОПК із застосуванням методу аналізу ієрархій, запропонованого Т. Сааті. Доведено прийнятність застосування цього методичного підходу. З метою проведення розрахунків з оцінювання найбільш небезпечних ОКІ ОПК використано вищезазначений метод в комплексі із застосуванням відповідної інформаційно-аналітичної системи.

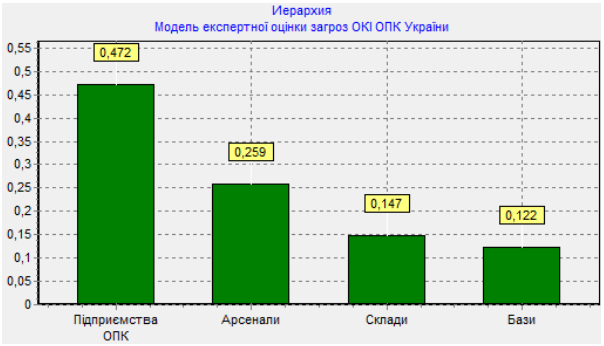

Рис. 4. Інтегральний індекс загроз ОКІ ОПК

Виконання розрахунків було спрямоване на оцінювання пріоритетності захисту підприємств ОПК, арсеналів, складів та баз боєприпасів, які, на випадок їх ураження, становлять найбільшу загрозу для держави вцілому, відповідно із критеріями, визначеними у проєкті закону України «Про критичну інфраструктуру».

Результати проведеного експертного оцінювання дають можливість встановити рівні загроз і ризиків для ОКІ ОПК та зробити наступні висновки: до загрозливих ОКІ ОПК відносяться підприємства ОПК, інтегральний індекс загрози для яких складає 0,472, арсенали, інтегральний індекс загрози для яких складає 0,259, склади боєприпасів, інтегральний індекс загрози для яких складає 0,147 та бази зберігання , інтегральний індекс загрози для яких складає 0,122. Ці чотири кластери підприємств ОПК відносяться до рівня катастрофічної загрози, порушення функціонування на яких може призвести до виникнення НС державного та регіонального значення.

Ураження цих об'єктів та можливі аварії на них можуть призвести до виникнення надзвичайних НС місцевого та локального рівня. Тому на останній, заключній стадії прийняття рішень щодо оцінювання і управління загрозами для ОКІ ОПК, необхідно звернути особливу увагу на ці об'єкти. Під час прийняття управлінських рішень щодо безпеки таких об'єктів необхідно розробити комплекс спеціальних заходів для її забезпечення.

Запропонований комплексний підхід може бути застосований в системах підтримки прийняття рішень щодо забезпечення захищенності ОКІ ОПК та Збройних Сил України.

Література:

1. Закон України «Про основи національної безпеки України» [Текст]: закон Украни // Відомості Верховної Ради України. – К., 2003. – № 39. – Ст. 351.

2. Бондаренко І. Самые масштабные взрывы на военных складах Украины: причины и хронология событий [Електронний ресурс] / Ігор Бондаренко // ТСН. – 2019. – Режим доступу до ресурсу: https://tsn.ua/ru/ukrayina/samye-masshtabnye-vzryvy-na-voennyh-skladah-ukrainy-prichiny-i-hronologiya-sobytiy-1444215.html.

3. Проєкт Закону «Про критичну інфраструктуру та її захист» реєстраційний № 10328 від 27.05.2019.

4. Кузнецов Д. Категорирование объектов критической информационной инфраструктуры (КИИ) [Електронний ресурс] / Дмитрий Кузнецов // Антифишинг. – 2019. – Режим доступу до ресурсу: https://www.anti-malware.ru/analytics/Threats_Analysis/categorize-critical-information-infrastructure-systems.

5. Мельничук О. Критическая инфраструктура государства как составляющая национальной безопасности: понятийно-категориальный аппарат / Олег Мельничук. // Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnic. – 2019. – №30. – С. 223–239.

6. Бірюков Д. С. «Про доцільність та особливості визначення критичної інфраструктури в Україні". Аналітична записка Читати більше - http://old2.niss.gov.ua/articles/1026/ Національний інститут стратегічних досліджень [Електронний ресурс]/Д. С. Бірюков – Режим доступу до ресурсу: http://old2.niss.gov.ua/articles/1026/.

7. Гриняев С. О взгляде на проблему безопасности критической инфраструктуры в государстве Израиль [Електронний ресурс] / Сергей Гриняев. – 2012. – Режим доступу до ресурсу: http://www.noravank.am/rus/issues/detail.php?ELEMENT_ID=6516.

8. Качинський А. Б. Безпека, загрози і ризик [Текст] : наукові концепції та математичні методи / А. Б. Качинський. – К.: 2003. – 472 с.

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

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

11. Синенко М. А. Метод Сааті при прийнятті управлінських рішень на прикладі підприємства малого бізнесу / М. А. Синенко // Інтелект XXI. – 2018. – № 1. – С. 235-238.

12. Информационно-коммуникационные технологии обеспечения безопасности жизнедеятельности: монография / под общ. ред. П.А. Попова, МЧС России. – М.: ФГУ ВНИИ ГОЧС (ФЦ), 2009. – 272 с.

13. Саати Т., Керне К. Аналитическое планирование. Организация систем: Пер. с англ. – М.: Радио и связь, 1991. – 224 с.

14. Измалков В. И. Техногенная и экологическая безопасность и управление риском [Текст] / В. И. Измалков, А. В. Измалков. – СПб.: НИЦЭБ РАН, 1998. – 482 с.

15. Коваленко Ю. Б. Системний аналіз проблеми багатокритеріального вибору варіанту удосконалення системи захисту інформації / Ю.Б. Коваленко // Захист інформації. - 2015. - Т. 17, № 1. - С. 38-43. - Режим доступу: http://nbuv.gov.ua/UJRN/Zi_2015_17_1_8.

16. Теслюк В.М., Загарюк Р.В. Методи багатокритеріальної оптимізації: Ч.1. Конспект лекцій з курсу — Методи багатокритеріальної оптимізації‖ для студентів спеціальності 8.05010103 — Системне проектування. – Львів: Видавництво Національного університету — Львівська політехніка‖, 2012. – 64 с.

17. Yevhenii Yakovliev, Sergiy Chumachenko Ecological Threats in Donbas, Ukraine Монографія. - Centre for Humanitarian Dialogue, Geneva, Switzerland, 2017.– 60 с.

18. Педченко Г.М., Лисиченко Г.В., Романченко І.С., Семенченко А.І., Лисенко О.І., Чумаченко С.М., Забулонов Ю.Л., Станкевич С.А., Бутенко С. Г., Борисюк С.Л. Система управління воєнно-техногенними ризиками при застосуванні Збройних Сил України. Монографія. – К.: ІГНС НАНУ та МНС, 2010.– 610 с.

References:

1. Zakon Ukrainy «Pro osnovy natsionalnoi bezpeky Ukrainy» [Law of Ukraine "On the foundations of national security of Ukraine"]. (2003). Vidomosti Verkhovnoi Rady Ukrainy – Bulletin of the Verkhovna Rada of Ukraine, 39. Art. 351 [in Ukrainian].

2. Bondarenko, I. (2019). Samye masshtabnye vzryvy na voennykh skladakh Ukrainy: prichiny i khronologiya sobytiy [The most large-scale explosions at military warehouses in Ukraine: causes and chronology of events]. tsn.ua. Retrieved from https://tsn.ua/ru/ukrayina/samye-masshtabnye-vzryvy-na-voennyh-skladah-ukrainy-prichiny-i-hronologiya-sobytiy-1444215.html [in Russian].

3. Proiekt Zakonu «Pro krytychnu infrastrukturu ta yii zakhyst» : vid 27.05.2019, № 10328 [Draft Law “On Critical Infrastructure and its Protection” from dated 27.05.2019, № 10328]. (n.d.). iportal.rada.gov.ua. Retrieved from http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996 [in Ukrainian].

4. Kuznetsov, D. (2019). Kategorirovanie obektov kriticheskoy informatsionnoy infrastruktury (KII) [Categorization of objects of critical information infrastructure (CII)]. www.anti-malware.ru. Retrieved from https://www.anti-malware.ru/analytics/Threats_Analysis/categorize-critical-information-infrastructure-systems [in Russian].

5. Melnichuk, O. (2019). Kriticheskaya infrastruktura gosudarstva kak sostavlyayushchaya natsionalnoy bezopasnosti: ponyatiyno-kategorialnyy apparat [Critical infrastructure of the state as a component of national security: conceptual and categorical apparatus]. Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnic, 30, 223–239 [in Russian].

6. Biriukov, D.S. (n.d.). Pro dotsilnist ta osoblyvosti vyznachennia krytychnoi infrastruktury v Ukraini [On the feasibility and features of determining the critical infrastructure in Ukraine]. old2.niss.gov.ua. Retrieved from http://old2.niss.gov.ua/articles/1026/ [in Ukrainian].

7. Grinyaev, S. (2012). O vzglyade na problemu bezopasnosti kriticheskoy infrastruktury v gosudarstve Izrail [On the view of the problem of the safety of critical infrastructure in the state of Israel]. www.noravank.am. Retrieved from http://www.noravank.am/rus/issues/detail.php?ELEMENT_ID=6516 [in Russian].

8. Kachynskyi, A.B. (2003). Bezpeka, zahrozy i ryzyk [Safety, threats and risk]. Kyiv [in Ukrainian].

9. Durdynets, V.V., Saienko, Yu.I., Pryvalov, Yu.O. (2001). Sotsialni ryzyky ta sotsialna bezpeka v umovakh pryrodnykh i tekhnohennykh nadzvychainykh sytuatsii ta katastrof [Social risks and social security in the conditions of natural and man-made emergencies and catastrophes]. Kyiv: Stylos [in Ukrainian].

10. Shapovalova, O.O., Burmenskyi, R.V. (2017). Rozrobka prohramnoho dodatka dlia realizatsii metodu analizu iierarkhii [Development of a software application for the implementation of the method of analysis of hierarchies]. Systemy obrobky informatsii – Information processing systems, 3(149), 45-48. https://doi.org/10.30748/soi.2017.149.09 [in Ukrainian].

11. Synenko, M.A. (2018). Metod Saati pry pryiniatti upravlinskykh rishen na prykladi pidpryiemstva maloho biznesu [Saaty method in making management decisions on the example of small business]. Intelekt XXI – Intellect XXI, 1, 235-238 [in Ukrainian].

12. Popov, P.A. (2009). Informatsionno-kommunikatsionnye tekhnologii obespecheniya bezopasnosti zhiznedeyatelnosti [Information and communication technologies for ensuring the safety of life]. Moscow: FGU VNII GOChS (FTs) [in Russian].

13. Saaty, T., Kearns, K. (1991). Analiticheskoe planirovanie. Orhanizatsiia sistem [Analytical Planning. The Organization of System]. Moscow: Radio i sviaz [in Russian].

14. Izmalkov, V.I., Izmalkov, A.V. (1998). Tekhnogennaya i ekologicheskaya bezopasnost i upravlenie riskom [Technogenic and environmental safety and risk management]. Saint Petersburg: NITsEB RAN [in Russian].

15. Kovalenko, Yu.B. (2015). Systemnyi analiz problemy bahatokryterialnoho vyboru variantu

udoskonalennia systemy zakhystu informatsii [Information protection]. Zakhyst informatsii – Information protection, 17(1), 38-43. Retrieved from http://nbuv.gov.ua/UJRN/Zi_2015_17_1_8 [in Ukrainian].

16. Tesliuk, V.M., Zahariuk, R.V. (2012). Metody bahatokryterialnoi optymizatsii [Methods of multicriteria optimization]. (Vol. 1). Lviv: Vydavnytstvo Natsionalnoho universytetu [in Ukrainian].

17. Yakovliev, Ye., Chumachenko, S. (2017). Ecological Threats in Donbas, Ukraine. Geneva: Centre for Humanitarian Dialogue [in English].

18. Pedchenko, H.M., et al. (2010). Systema upravlinnia voienno-tekhnohennymy ryzykamy pry zastosuvanni Zbroinykh Syl Ukrainy [Military man-caused risk management system in the use of the Armed Forces of Ukraine]. Kyiv: IHNS NANU ta MNS.

Аннотация

Применение экспертно-аналитических методов для оценивания угроз объектам критической инфраструктуры оборонно-промышленного комплекса на Востоке Украины

С.Н. Чумаченко, О.П.Кутовий, А.В. Михайлова

Авторы статьи предлагают методический подход к оцениванию угроз для объектов критической инфраструктуры оборонно-промышленного комплекса государства в условиях ведения гибридной войны. Актуальность работы обусловлена процессами противодействия угрозам техногенного характера на территории Донбасса, которые существуют в Украине, а также отсутствием методических разработок, с помощью которых возможно оценить уровень угроз критической инфраструктуре оборонно-промышленного комплекса. Авторы публикации опереляют факторы, которые существенно влияют на военно-техногенные угрозы обьектам критической инфраструктуры оборонно-промышленного комплекса. В соответствии с этими факторами в статье приводится иерархическая система показателей, которая состоит из трех групп. Эти группы характеризуют факторы оценки военно-техногенных и природно-техногенных угроз, а также содержат частные критерии, которые позволяют оценить возможные угрозы.

Доказано работоспособность этого методического подхода на примере боеприпасной отрасли Украины. Для проведения расчетов по оценке наиболее опасных объектов ОПК использован метод анализа иерархий с использованием разработанной информационно-аналитической системы. Расчеты были направлены на оценивание приоритетности защиты арсеналов, баз, складов и предприятий оборонно-промышленного комплекса, которые в случае их поражения представляют наибольшую угрозу для государства в целом, по соответствующим критериям определенным в проекте закона Украины «О критической инфраструктуре и ее защите».

В статье приводятся результаты числового эксперимента, который подтвердил работоспособность научно-методического подхода, его достаточно высокую точность и наглядность получаемых результатов.

Проведенное экспертное оценивание позволило установить уровни угроз для объектов критической инфраструктуры оборонно-промышленного комплекса, к которым относятся предприятия оборонно-промышленного комплекса боеприпасной отрасли (интегральный индекс угрозы составляет 0,472), арсеналы (интегральный индекс угрозы составляет 0,259), склады (интегральный индекс угрозы составляет 0,147), базы хранения (интегральный индекс угрозы составляет 0,122).

Ключевые слова*: риск, угроза, снаряды, боеприпасы, метод анализа иерархий, критической инфраструктуре, оборонно-промышленный комплекс.*

Abstract

Application of expert-analytical methods for threat assessment of critical infrastructure objects of the defense and industrial complex in the East of Ukraine

S.M. Chumachenko, O.P. Kutovoy, AV. Mykhailova

The authors propose a methodological approach to assessing threats to critical infrastructure of the state's military-industrial complex in the context of a hybrid war. The relevance of the work is due to the processes of counteracting man-made threats in the territory of Donbass, which exist in Ukraine in Ukraine, as well as the lack of methodological developments with which is possible to assess the level of threats to the critical infrastructure of the defense industry. The authors of the publication identify the factors that significantly affect the military-man-made threats to the critical infrastructure of the defense-industrial complex. In accordance with these factors, the article gives a hierarchical system of indicators, which consists of three groups.

These groups characterize factors for assessing military-technological and natural-technological threats, and also contain particular criteria that allow us to assess possible threats.

The efficiency of this methodological approach is proved by the example of the ammunition industry in Ukraine. To carry out calculations to assess the most dangerous objects of the defense industry complex, the method of «hierarchy analysis» using the developed information-analytical system were used. The calculations were aimed at assessing the priority of protecting arsenals, bases, warehouses and defense industry enterprises, which, if they are defeated, pose the greatest threat to the state as a whole, according to the relevant criteria defined in the draft law of Ukraine «On critical infrastructure and its protection».

The article presents the results of a numerical experiment, which confirmed the efficiency of the scientific and methodological approach, its rather high accuracy and the visibility of the results.

The expert assessment made it possible to establish threat levels for the critical infrastructure of the defense industry complex, which include enterprises of the military-industrial complex of the ammunition industry (the integral threat index is 0.472), arsenals (the integral threat index is 0.259), warehouses (the integral threat index is 0.147), and the storage base (integral the threat index is 0.122).

Keywords*: risk, threat, munitions targets, shells, ammunition, hierarchy analysis method, critical infrastructure, defense-industrial complex.*

Бібліографічне посилання/ Bibliography citation: Harvard
Chumachenko, S. M., Kutovoy, O. P. and Mykhailova, A. (2020) 'Application of expert-analytical methods for threat assessment of critical infrastructure objects of the defense and industrial complex in the East of Ukraine', *Engineering of nature management*, (4(18), pp. 114 - 123.

Подано до редакції / Received: 02.11.2020