УДК 323:005:330.131.7

МЕТОДОЛОГІЯ ОЦІНКИ РІВНЯ КРИТИЧНОСТІ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ

Бобро Дмитро Геннадійович

У статті проаналізовано сучасні методологічні підходи до оцінки критичності об'єктів інфраструктури. Продемонстровано, що, зважаючи на невизначеність, зокрема неточність та неповноту інформації, необхідної для коректної оцінки загроз та ризиків критичній інфраструктурі, багатовимірність та незіставність можливих наслідків, необхідність урахування численних взаємозв'язків та взаємозалежностей об'єктів критичної інфраструктури, універсальність оцінки критичності може забезпечити застосування методів нечіткої логіки та експертних оцінок. Запропонована трирівнева ієрархічна модель критеріїв визначення критичності інфраструктури та надані пропозиції щодо подальших кроків з розбудови в Україні державної системи захисту критичної інфраструктури. Наведено приклад визначення критичності об'єктів інфраструктури, який ґрунтується на використанні методів експертних оцінок та нечіткої логіки.

Ключові слова: критична інфраструктура, загроза, вразливість, ризик, стійкість, надзвичайна ситуація, тероризм, нечітка логіка.

Bobro Dmytro

METHODOLOGY OF ESTIMATION OF INFRASTRUCTURE OBJECTS CRITICALITY LEVEL

The modern methodological approaches are analyzed for the estimation of criticality of infrastructure objects. It is rotined that because of vaguenesses, in particular, inaccuracy and incompleteness of information, that are necessary for the correct estimation of threats and risks to the critical infrastructure, because of multidimensionalness and uncomparableness of possible consequences, because of necessity to account numerous relationship and interdependencies of critical infrastructure objects, universality of estimation of criticality can provide application of methods of fuzzy logic and expert estimations. The 3-level hierarchical criteria model of criticality determination of infrastructure objects is offered. Suggestions are given to concerning further steps to build in Ukraine the state system of critical infrastructure protection.The example how to determinate the criticality of infrastructure objects was cite an instance, that based on the use of methods of expert estimations and fuzzy logic.

Keywords: critical infrastructure, threat, vulnerability, risk, resilience, emergency situation, terrorism, fuzzy logic.

Проблеми забезпечення безпеки критичної інфраструктури

Світові тенденції до посилення негативних процесів природного та техногенного характеру, зростання терористичних загроз, кількості та витонченості кібератак, драматичні події на сході та півдні України 2014–2016 років актуалізували для країни питання захисту інфраструктури, життєво важливої для безпеки людини, суспільства і держави, яка в світовій практиці визначається як критична.

У країнах світу, які для гарантування національної безпеки використовують поняття «критична інфраструктура» (*далі* – КІ), розуміють під нею

об'єкти і системи, настільки важливі для забезпечення життєдіяльності людей і держави, що дестабілізація їхньої роботи, не кажучи вже про колапс, призведе до тяжких негативних або навіть катастрофічних наслідків. При цьому особливу небезпеку становлять каскадні ефекти, коли порушення в роботі одного об'єкта КІ призводять до порушень у роботі інших об'єктів і систем унаслідок їх взаємозалежності («ефект доміно») [1]. З іншого боку, до КІ відносять і особливо небезпечні виробництва, аварії на яких, викликані будь-якими причинами (природними або техногенними надзвичайними ситуаціями, кризовими ситуаціями, пов'язаними зі зловмисними діями), також можуть обернутися катастрофічними наслідками.

Спираючись на досвід ЄС, США, країн – членів НАТО, в Національному інституті стратегічних досліджень у 2015 р. підготовлена Зелена книга з питань захисту критичної інфраструктури в Україні [2]. У цьому документі систематизовано підходи до визначення поняття «критична інфраструктура», що розуміється як «системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку та забезпечення національної безпеки». Визначені основні групи загроз КІ (техногенні аварії та технічні збої, викликані, зокрема, людськими помилками; природні лиха та небезпечні природні явища; зловмисні дії), подані пропозиції щодо переліку секторів КІ (галузей господарства, державних органів та систем) і основних принципів, на яких має здійснюватися подальша розбудова в Україні системи захисту критичної інфраструктури. Метою цієї системи має стати гарантування спроможності критичної інфраструктури виконувати та, у разі переривання, в найкоротші терміни відновлювати функції із життєзабезпечення людей, суспільства, бізнесу і держави.

Слід зазначити, що у провідних країнах світу розуміють необхідність забезпечення захисту критичної інфраструктури від усіх видів загроз (*all hazards approach*). Водночас усвідомлення неможливості забезпечити однаково високий рівень захисту всієї критичної інфраструктури від усіх можливих загроз призвело до розвитку підходу, зосередженого на вибірковому захисті конкретного об'єкта КІ від обмеженого набору відомих та відносно прогнозованих загроз, надаючи пріоритет тій або іншій інфраструктурі залежно від ступеня її «критичності», головною мірою якої є ризик [3].

Є різні підходи до визначення ризику. Узагальнений підхід до оцінки ризиків КІ вміщує:

- ідентифікацію та класифікацію загроз, оцінку ймовірності (чи, точніше, частості) кожної загрози;
- оцінку вразливостей до кожного типу подій/атак (що з урахуванням частості загрози визначає ймовірність нанесення шкоди);
- оцінку наслідків (для різних сценаріїв розвитку подій).

Питання захисту критичної інфраструктури за останні роки розглядалося у низці робіт, зокрема, А.О. Мороза, О.М. Євдіна, В.А. Заславського, В.Ф. Гречанінова, В.В. Бєгуна, С.І. Кондратова, Д.С. Бірюкова, О.М. Суходолі. Більшість цих робіт так чи інше стосувалася запровадження в управління безпекою ризик-орієнтованого підходу, що, безумовно, слід вважати кроком уперед у розбудові в Україні сучасної системи забезпечення національної безпеки. Хоча зазначений ризик-орієнтований підхід і використовується в управлінні техногенно-екологічною безпекою, слід зазначити, що кількісно оцінити та адекватно зіставити ризики КІ не завжди можливо. Це пов'язано як із невизначеністю, зокрема, неточністю та неповнотою інформації, необхідної для коректної оцінки частості загроз (найбільше пов'язано із невизначеністю терористичних загроз), так і з багатовимірністю та незіставністю можливих наслідків [4]. Окрім того, ключовою особливістю оцінки ризиків для КІ є необхідність урахування численних взаємозв'язків та взаємозалежностей [5], які можуть бути як очевидними (функціональна залежність), так і розмитими (наприклад, коли інформаційний стан однієї системи визначає функціональний стан іншої). Зазначене потребує застосування інших методів, зокрема, методів нечіткої логіки та експертних оцінок [6].

З іншого боку, коли йдеться про захист КІ, постає питання не лише «від чого захищатись», але й «що захищати»: об'єкт чи функцію? Слід зазначити, що захист цих елементів КІ має відмінності, оскільки щодо об'єктів він спрямований передусім на зниження рівня загроз та вразливості об'єктів, мінімізацію наслідків, а щодо функцій – на безперервність їх надання та швидше відновлення у разі переривання. В цьому аспекті у пригоді можуть стати сучасні технології управління кризовими ситуаціями, побудовані на концепції управління безперервністю бізнесу [6, 7].

Мета статті – опрацювання підходів до визначення міри «критичності» об'єктів інфраструктури та

можливості забезпечення адекватного захисту КІ від усіх видів загроз, надання пропозицій щодо подальшої розбудови системи захисту КІ в Україні.

Визначення параметрів (критеріїв) оцінки критичності елементів інфраструктури

Параметри оцінки рівня критичності мають різну природу та характеризують вплив кризової ситуації на об'єкті КІ (її наслідки) з різних боків. Вони можуть бути представлені в якісному або кількісному вигляді [6].

Для визначення множини параметрів оцінки рівня критичності розглянемо фактори та характеристики, які згадані у Зеленій книзі [2], використовуються в РФ [1, 8], Ізраїлі [1] та США [9, 10].

Так, при визначенні потенційних елементів КІ Зелена книга [2] з урахуванням Директиви 2008/114/ЄС визначає необхідність аналізу таких характеристик:

- масштаб (географічне охоплення території, для якої втрата елементу критичної інфраструктури викликає значну шкоду);
- взаємозв'язок між елементами критичної інфраструктури;
- тривалість впливу (як саме і коли проявлятимуться шкода, пов'язана із втратою чи відмовою, виходом з ладу або порушенням функціонування об'єктів критичної інфраструктури);
- вразливість об'єкта до впливу небезпечних чинників;
- важкість можливих наслідків за показниками в таких основних групах:
  - економічна безпека (вплив на ВВП, розмір економічних втрат, як прямих, так і непрямих, частки продукції на ринку, чисельності зайнятих співробітників, податкових надходжень до бюджету);
  - безпека життєдіяльності та здоров'я населення (число постраждалих, загиблих, осіб, які отримали серйозні травми, а також чисельність евакуйованого населення, забезпечення роботи аварійно-рятувальних служб, екстреної допомоги населенню);
  - внутрішньополітична й державна безпека (втрата впевненості в дієздатності влади, авторитету держави, порушення управління державою);
  - обороноздатність (зниження боєздатності збройних сил, розголошення таємної інформації);
  - екологічна безпека (вплив на навколишнє природне середовище).

Схожий набір параметрів використовують і в РФ [8]:

- значущість об'єкта для економіки держави:
  - вартість річного випуску товарної продукції (млн руб.);
  - загальна чисельність виробничого персоналу (тис. осіб);
  - балансова вартість основних виробничих фондів (млн руб.);
  - частка основної продукції об'єкта в продукції того самого виду, що випускається в державі (%);
- завдання шкоди престижу держави:
  - порушення керованості держави або регіону;
  - нанесення шкоди авторитету держави, у тому числі на міжнародній арені;
  - розкриття державних секретів, конфіденційної науково-технічної та комерційної інформації;
  - порушення боєготовності та боєздатності Збройних Сил;
  - порушення стабільності фінансової та банківської систем;
- можливі загрози населенню та територіям:
  - великомасштабне знищення національних ресурсів (природних, сільськогосподарських, продовольчих, виробничих, інформаційних);
  - територія зараження (забруднення) у разі аварії на об'єкті;
  - чисельність населення, яке може постраждати у разі надзвичайної ситуації на об'єкті;
  - порушення систем забезпечення життєдіяльності міст та населених пунктів;
  - масові порушення правопорядку;
  - зупинка безперервних виробництв;
  - аварії та катастрофи регіонального масштабу.

В Ізраїлі при ідентифікації об'єктів КІ враховуються три критерії [1]:

- символічна (ідеологічна, історична або культурна) значущість об'єктів;
- залежність основних процесів життєзабезпечення суспільства від інфраструктури;
- наявність складних взаємозв'язків та залежностей між об'єктами інфраструктури.

Цікаво, що об'єкти культурної спадщини Ізраїлю (музеї, архіви, культові споруди та інші пам'ятки) віднесені до об'єктів, які повинні бути захищені в першу чергу.

При визначенні потенційних елементів КІ у США використовують схожі характеристики [9]:

- масштаб;
- взаємовплив елементів інфраструктури;
- тривалість впливу;
- час на відновлення;
- важкість можливих наслідків у таких основних групах:
  - економіка;
  - фінанси;
  - навколишнє середовище;
  - безпека життєдіяльності та здоров'я людей;
  - технологічне середовище.

Окрім того, враховується символічна значущість об'єктів, шкода національній обороні та можливі вторинні проблеми для національної безпеки.

Так, у США в загальнонаціональну базу для аналізу критичності внесено приблизно 33 тис. об'єктів інфраструктури, з яких близько 2 тис. віднесено до критичної інфраструктури [9]. Ці об'єкти розділені на три категорії: життєво важливі (АЕС, великі гідроспоруди та ГЕС, сховища стратегічних запасів нафти та газу, небезпечні хімічні та нафтохімічні виробництва, сховища ядерних матеріалів та боєприпасів); вкрай важливі (великі системи енергозабезпечення, метрополітен, мережі водопостачання та каналізації, магістральні трубопроводи); важливі (морські порти, очисні споруди, магістральні автомобільні та залізничні дороги, великі аеропорти, центри зв'язку тощо). Загалом, при оцінці критичності об'єктів у США її ступінь зазвичай ділиться на три категорії: високий, середній, низький.

Слід зазначити, що в США також використовують ризик-орієнтовані підходи до управління безпекою, зокрема, ризики КІ оцінюються на основі експертних оцінок за п'ятибальною шкалою від низького рівня до катастрофічного. Схожий підхід використовується й для визначення п'яти ступенів готовності: червоний (вищий), помаранчевий (високий), жовтий (підвищений), голубий (можливий) та зелений (низький) [9, 10].

Як приклад використання методу експертних оцінок можна навести підхід для ранжування об'єктів військово-промислового комплексу США – модель визначення пріоритетності об'єктів ВПК (*The Asset Prioritization Model*) [10]. Усі об'єкти оцінюються за 16-ма факторами, яким присвоєні вагові коефіцієнти від 16 до 1, з діапазоном оцінок «важливості» об'єкта від 1 до 3 (інколи 5), та за якими розраховується сумарний індекс «ризикованості» об'єкта. Ці фактори враховують вплив на великосерійні програми виробництва, бойові можливості (значущість продукції), фінансові можливості компанії, економічну живучість, можливості відновлення, кількість населення, що проживає поряд, супутні втрати від ураження хімічними, біологічними, радіаційними та вибуховими речовинами, які використовувалися при атаці,тощо. Цікаво, що у 2007 р. найкритичнішими визнані об'єкти, на яких виконуються великосерійні програми виробництва для ВПК, тоді як раніше такими об'єктами вважалися ті, що мають найбільший вплив на сучасні бойові можливості.

Враховуючи вищенаведене, можна запропонувати таку ієрархічну модель критеріїв визначення критичності інфраструктури (табл. 1).

Слід зазначити, що коректно оцінити кількісно більшість наведених вище параметрів украй складно, а то й неможливо. Використання ж методів експертної оцінки (оцінки поточного рівня параметра шляхом віднесення до певної підгрупи значень показника цього параметра), суб'єктивність рішень, невизначеність чітких критичних значень показників та різнорідність шкал для їх оцінювання вимагають використання апарату нечіткої логіки.

Приклад використання методів нечіткої логіки для визначення рівня критичності об'єкта/функції інфраструктури

1. Визначення параметрів оцінки критичності

Множина параметрів оцінки критичності об'єктів/функцій інфраструктури сформована на основі параметрів ієрархічної моделі критеріїв, наведених у табл.1. Експертами для аналізу використана множина з 16 параметрів ІІ рівня.

Таблиця 1. **Ієрархічна модель критеріїв визначення критичності інфраструктури**

I рівень	II рівень	III рівень
Взаємозв'язок між елементами критичної інфраструктури	Каскадні ефекти	Зменшення обсягу функцій залежних систем
		Настання важких негативних екологічних, економічних, соціально-політичних наслідків
		Унеможливлення ліквідації наслідків кризової ситуації (роботи аварійно-рятувальних служб, надання екстреної допомоги населенню тощо)
	Взаємозамінність (диверсифікованість)	Можливість постачання послуг/ресурсів з інших джерел (іншими шляхами)
	Резервування	Наявність резервних виробництв/ресурсів
Масштаб впливу	Територіальне поширення	Локальне, район, регіон, вся територія держави, глобальне
	Масштаб інциденту в організаційному аспекті	На рівні процесу, підприємства, галузі економіки, загальний для держави або групи держав
Часовий ефект впливу	Час, через який з'являються негативні наслідки	Негайно, через кілька годин, діб, тижнів, місяців
	Тривалість впливу	До кількох годин, діб, тижнів, місяців, років
	Час на відновлення	Кілька годин, діб, тижнів, місяців, років
Важкість можливих наслідків	Шкода здоров'ю і життю людей	Кількість постраждалих, травмованих, загиблих, евакуйованих
	Ступінь порушення нормальних умов життєдіяльності людей	Енергопостачання
		Водопостачання
		Каналізація та вивезення сміття
		Постачання товарів першої необхідності (продуктів харчування, засобів гігієни тощо)
		Послуги з охорони здоров'я
		Транспортне сполучення
	Економічна шкода	Вплив на ВВП
		Розмір економічних втрат, як прямих, так і непрямих
		Чисельність персоналу та населення, що пов'язано з діяльністю об'єкта
		Частка продукції об'єкта в загальнодержавному її випуску/споживанні
	Ступінь порушення безперервності надання функцій із забезпечення виробничої діяльності стратегічних підприємств	Зупинка безперервних виробництв
		Частка продукції об'єкта в загальнодержавному її випуску/споживанні
	Ступінь впливу на фінансову та банківську систему	Частка об'єкта в загальнодержавному обсязі банківських чи фінансових послуг
	Екологічна шкода	Вплив на населення (забрудненість повітря, води, продуктів харчування тощо)
		Вплив на навколишнє природне середовище
Соціально-політична шкода	Нанесення шкоди авторитету держави	Рівень панічних, протестних та антидержавних настроїв
		Суспільна тривога, втрата впевненості в дієздатності влади, розбрат
		Символічна значимість об'єктів (історичні та культурні цінності)
	Ступінь впливу на безпеку держави та обороноздатність	Порушення керованості держави або регіону
		Масові порушення правопорядку
		Зниження боєготовності та боєздатності збройних сил
		Вплив на бойові можливості (значущість продукції/послуг)
		Розкриття державних секретів, конфіденційної науково-технічної та комерційної інформації

2. Визначення ваги параметрів

Для кожного з параметрів за методом експертної оцінки Дельфі визначена вага (значимість) параметру від 0 до 100% (від 0 до 1,0); при цьому сума ваги всіх параметрів дорівнює 100% (1,0).

Так, одними з найвагоміших параметрів експерти цілком очікувано визнали каскадні ефекти, шкоду здоров'ю і життю людей, ступінь порушення нормальних умов життєдіяльності людей, ступінь впливу на безпеку держави та обороноздатність.

3. Визначення значень параметрів

За методом експертної оцінки Дельфі оцінювався потенційний вплив об'єкта на безпеку за кожним параметром. Визначені нечіткі значення параметрів оцінюваного об'єкта інфраструктури (нафтобаза у м. Васильків Київської обл.). Використана лінгвістична зміна з п'яти термів: несуттєвий (голубий), незначний (зелений), значущий (жовтий), значний (помаранчевий) та критичний (червоний).

Так, експертами «червоні» оцінки були виставлені об'єкту за можливу шкоду здоров'ю і життю людей та потенційну екологічну шкоду, а, наприклад, вплив об'єкта на ступінь порушення безперервності надання функцій із забезпечення виробничої діяльності стратегічних підприємств був оцінений на рівні несуттєвого.

Примітка: слід зазначити, що при використанні цієї методики визначення *ваги* параметрів оцінки критичності потрібно робити лише у разі змін множини цих параметрів чи змін у соціально-політичній ситуації в країні, коли, наприклад, через зміни безпекової ситуації зростає вага оборонних заходів. Водночас зміни на об'єкті, зокрема зміни корпоративних зв'язків, як і зміни ситуації в регіоні чи країні, вимагають переоцінки *значень* параметрів.

4. Візуалізація результату

Для візуалізації рівня критичності оцінюваного об'єкта побудована «пелюсткова» діаграма, де ширина «пелюстки» відповідає вазі (значущості) параметра, а його нечітке значення для цього об'єкта визначено експертами із використанням вищезгаданої лінгвістичної зміни з п'яти термів. Було обчислене значення агрегованого (інтегрального) показника критичності (відповідає площі пелюсткової діаграми), проведена його нормалізація (представлено у діапазоні 0-1,0).

Результат оцінки критичності оцінюваного об'єкта наведено на рис. 1. Об'єкт за критичністю віднесений до 2-ї групи КІ – «вкрай важливий» (детальніше далі).

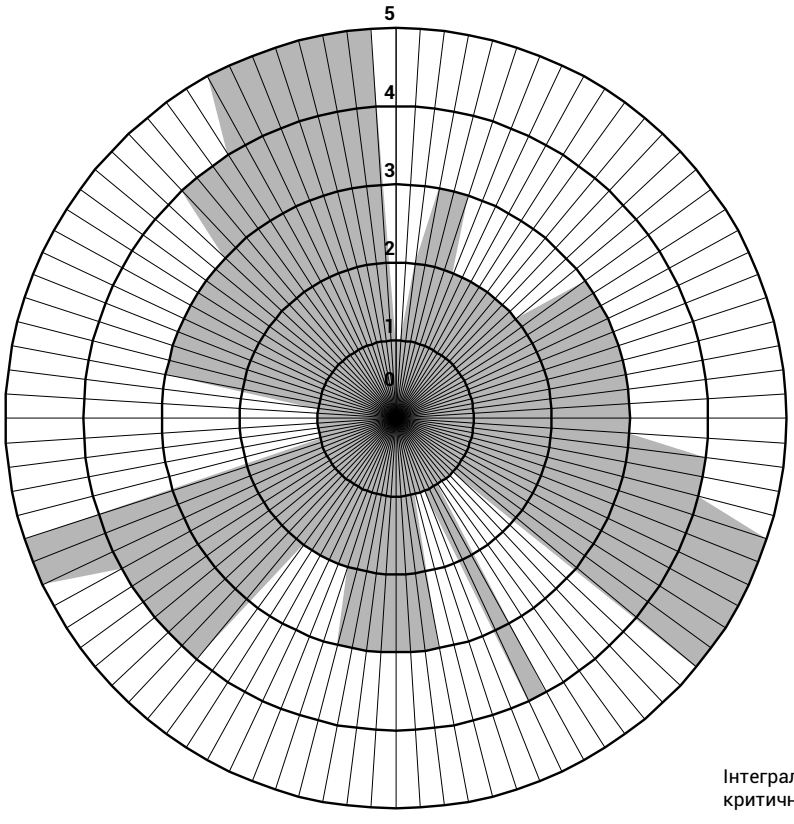
5. Ранжування об'єктів критичної інфраструктури

Ранжування всіх інфраструктурних об'єктів проведемо за обчисленими значеннями нормованого агрегованого (інтегрального) показника. Приклад такого ранжування, проведеного для мирного часу та особливого періоду (тобто двох рівнів загроз), наведено на рис. 2.

Для лінгвістичного розпізнання рівня критичності об'єкта інфраструктури за термами життєво важливий, вкрай важливий, важливий використано таку шкалу:

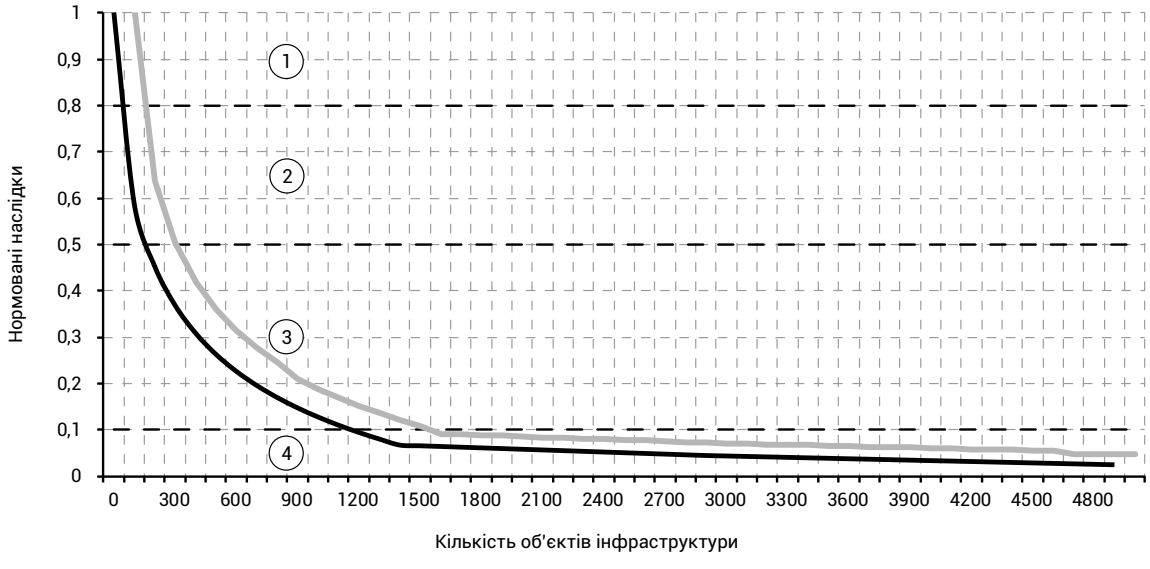
- *перша група*: життєво важливі об'єкти КІ – нормований коефіцієнт критичності понад 0,8. Це великі об'єкти інфраструктури загальнодержавного значення, які мають розгалужені зв'язки та значний вплив на іншу інфраструктуру, заходи з відновлення яких вимагають значних ресурсів та часу. На таких об'єктах з використанням державних сил та ресурсів має бути створена адекватна загрозам система фізичного захисту (наприклад, АЕС, нафтопереробні заводи, великі гідроспоруди тощо). Відповідальність за захист цієї КІ мають консолідовано нести держава та оператори (власники) з чітким регламентуванням відносин та взаємодії;
- *друга група*: вкрай важливі об'єкти КІ – нормований коефіцієнт критичності від 0,5 до 0,8. На таких об'єктах потрібно реалізувати як заходи з фізичного захисту, так і передбачити можливість швидшого відновлення функцій за допомогою диверсифікації та резервів (наприклад, великі нафтобази, підземні сховища газу, електричні підстанції, мостові переходи, великі елеватори, джерела питної води тощо). Відповідальність за захист цієї КІ мають нести оператори (власники) та держава на основі державно-приватного партнерства при жорсткому контролі з боку держави за дотриманням вимог та правил з безпеки.
- *третя група*: важливі об'єкти КІ – нормований коефіцієнт критичності від 0,1 до 0,5. Основним шляхом захисту такої інфраструктури є забезпечення швидшого відновлення функцій

Рис.1. **Приклад оцінки критичності об'єкта інфраструктури**



Інтегральний показник 0,604 – рівень критичності «вкрай важливий»

Рис.2. **Розподіл об'єктів інфраструктури за групами «критичності»**



завдяки диверсифікації та резервів (наприклад, теплові електростанції, автомагістралі тощо). Відповідальність за захист цієї КІ повинні нести оператори (власники), а держава має забезпечити наявність умов для диверсифікації та резервування;

- *четверта група*: об'єкти, що мають нормоване значення агрегованого (інтегрального) показника менше 0,1, до критичної інфраструктури не відносилися; безпосередній захист цих об'єктів є відповідальністю суто оператора (власника).

Слід зазначити, що прийняті у цьому прикладі граничні показники критичності (0,1, 0,5 та 0,8) визначені експертами попередньо та мають бути уточнені за результатами оцінки основної частини інфраструктурних об'єктів, зокрема відповідно до спроможності держави.

Проблематика дальшої розбудови державної системи захисту критичної інфраструктури

Враховуючи досвід провідних країн світу, а також роботи українських фахівців щодо захисту КІ [1, 2, 11], можна виділити *такі напрями подальшої розбудови в Україні державної системи захисту критичної інфраструктури*:

1. Розробка та регулярний перегляд нормативної бази, зокрема, прийняття Закону України про захист критичної інфраструктури, визначення головного державного координаційного органу у цій сфері (наприклад, у США –це Департамент (міністерство) внутрішньої безпеки (*The Department of Homeland Security* (МВБ), до складу якого увійшли 22 федеральних агентства та відомства із загальною чисельністю близько 170 тис. чол. [9]).

2. Розробка та впровадження єдиних методологічних підходів, на основі яких мають бути сформований перелік КІ, проводитися ранжування об'єктів за рівнем їх «критичності», розроблятися плани попередження загроз та реагування, оцінюватися їх ефективність (наприклад, у США цим опікується Національний центр аналізу та імітаційного моделювання інфраструктури МВБ).

3. Підготовка кваліфікованих кадрів у сфері захисту КІ.

4. Організація обміну інформацією та кращими практиками.

5. Розвиток державно-приватного партнерства.

Висновки та рекомендації

Фактично до сьогодні під захистом критичної інфраструктури розумілося або забезпечення охорони (фізичної безпеки), чим займаються певні служби і відомчі підрозділи, або захист від надзвичайних ситуацій техногенного і природного характеру (сфера діяльності Державної служби з надзвичайних ситуацій). Над глобальнішими питаннями, пов'язаними із забезпеченням стійкості об'єктів КІ щодо будь-яких загроз і можливості на державному рівні забезпечити виконання функцій із життєзабезпечення людей, суспільства, бізнесу і держави у разі реалізації цих загроз, на системному рівні не працює жодне відомство.

У рекомендаціях Зеленої книги [2] говориться про необхідність розробки Закону України про захист критичної інфраструктури, в якому, зокрема, мають бути визначені суб'єкти та структура системи захисту критичної інфраструктури. При цьому для подальшої розбудови системи необхідно мати апарат, який координуватиме розробку правових, організаційних, методологічних, технологічних та інших інструментів захисту КІ, проводитиме оперативний аналіз наявних загроз і ризиків, розроблятиме рекомендації керівництву держави щодо режимів функціонування системи захисту КІ залежно від рівня загроз і правового стану.

З огляду на комплексність питання, це означає, що необхідно створити Національний центр з питань захисту критичної інфраструктури та мережу галузевих (територіальних) ситуаційних центрів, фахівці яких на єдиній методологічній основі мають оцінювати загрози та ризики КІ, формувати перелік та проводити ранжування об'єктів інфраструктури за їх критичністю, розробляти плани реагування та оцінювати ефективність їх виконання. На першому етапі роботи Національний центр має сформувати перелік об'єктів критичної інфраструктури державного рівня (групи 1 та 2), відповідальність за захист яких лежить, у т.ч., і на державі, а відповідні галузеві (функціональні) центри за тією самою методологією та під методичним керівництвом Національного центру – сформувати перелік об'єктів КІ для груп 3 та 4, відповідальність за захист яких покладено на операторів (власників) цих об'єктів.

Список використаних джерел

1. *Бірюков Д.С.* Про доцільність та особливості визначення критичної інфраструктури в Україні : Аналітична записка. [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/articles/1026/
2. *Зелена* книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / Упоряд. Д.С. Бірюков, С.І Кондратов ; за заг. ред. О.М. Суходолі. – К. : НІСД, 2016. – 176 с.

3. *Risk* assessment methodologies for critical infrastructure protection. Part I: a state of the art / G.Giannopoulos, R.Filippini, M. Schimmer. – Luxembourg: Joint Research Centre of Institute for the Protection and Security of the Citizen, 2012. – 70 p.
4. *Бобро Д.Г.* Визначення критеріїв оцінки та загрози критичній інфраструктурі / Д.Г. Бобро // Стратегічні пріоритети. – Серія «Економіка». – 2015. – № 4 (37). – С. 83-93. – Режим доступу : http://sp.niss.gov.ua/content/articles/files/10-1457002140.pdf
5. *Lewis T.G.,* Critical infrastructure protection in homeland security: defending a networked nation. – John Wiley & Sons, Inc., 2006. – 474 p.
6. *Корченко А.О.* Метод оцінки рівня критичності для систем управління кризовими ситуаціями / А.О. Корченко, В.А. Козачок, А.І. Гізун // Захист інформації. – 2015. – Т. 17, № 1. – С. 86-98. – Режим доступу : http://nbuv.gov.ua/UJRN/Zi_2015_17_1_14
7. *Гізун А.І.* Сучасні підходи до захисту інформаційних ресурсів для забезпечення безперервності бізнесу / А.І. Гізун, В.О. Гнатюк, О.П. Дуксенко, А.О. Корченко // Матеріали X Міжнародної науково-технічної конференції «АВІА-2011». – К. : НАУ, 2011. – Т. 1. – С. 2.5-2.9. – Режим доступу: http://avia.nau.edu.ua/doc/2011/2/avia2011_2_2.pdf
8. *Методика* отнесения объектов государственной и не государственной собственности к критически важным для национальной безопасности Российской Федерации : Нормативный документ МЧС России. – Режим доступу: http://central.mchs.ru/upload/site4/files/bea08465669b520c2603f73058fe188a.pdf
9. *Цыгичко В.Н.* Обеспечение безопасности критических инфраструктур в США (аналитический обзор) / В.Н. Цыгичко, Г.Л. Смолян, Д.С. Черешкин // Труды ИСА РАН. – 2006. – Т. 27.
10. *Баранник А.* Организация обеспечения безопасности критической инфраструктуры в США / А. Баранник, С. Клементьев, Зарубежное военное обозрение. – 2009. – № 8. – С. 3-10.
11. *Суходоля О.М.* Пріоритети формування державної політики захисту критичної енергетичної інфраструктури України / О.М. Суходоля // Стратегічні пріоритети. – 2015. – № 2. – С. 91-101.

References

1. *Biriukov, D.S.* Pro dotcilnist ta osoblyvosti vyznachennia krytychnoi infrastruktury v Ukraini. Analitychna zapyska [About expedience and features of determination of critical infrastructure in Ukraine. Analytical Report]. Retrieved from http://www.niss.gov.ua/articles/1026/ [in Ukrainian].
2. *Sukhodolia, O.,* Biriukov, D., Kondratov, S. (Eds.) (2015). Zelena knyga z pytan zahystu crytychnoi infrastructury v Ukraini [The Green Book on Critical Infrastructure Protection]. Kyiv: NISS [in Ukrainian].
3. *Risk* assessment methodologies for critical infrastructure protection. Part I: a state of the art / G.Giannopoulos, R.Filippini, M. Schimmer. – Luxembourg: Joint Research Centre of Institute for the Protection and Security of the Citizen, 2012. – 70 p.
4. *Bobro, D.G.* (2015). Vyznachennia kryteriiv otsinky ta zahrozy krytychnii infrastrukturi. [Definition of Evaluation Criteria and Threats to Critical Infrastructure] *Stratehichni priorytety, Seriia «Ekonomika» – Strategic Priorities, Economics series,* 4 (37), 83-93. Retrieved from http://sp.niss.gov.ua/content/articles/files/10-1457002140.pdf [in Ukrainian].
5. *Lewis T.G.* Critical infrastructure protection in homeland security: defending a networked nation. – John Wiley & Sons, Inc., 2006. – 474 p.
6. *Korchenko, A.O.,* Kozachok, V. A., Hizun, A. I. (2015). Metod otsinky rivnia krytychnosti dlia system upravlinnia kryzovymy sytuatsiiamy [Method of estimation of criticality level for crisis situation control systems]. *Zakhyst informatsii – Protection of Information*, Vol. 17, 1, 86-98. Retrieved from http://nbuv.gov.ua/UJRN/Zi_2015_17_1_14 [in Ukrainian].
7. *Hizun A.I.,* Hnatiuk, V.O., Duksenko, O.P., Korchenko, A.O. (2011). Suchasni pidkhody do zakhystu informatsiinykh resursiv dlia zabezpechennia bezperervnosti biznesu [Modern approaches for information resources protection to provide business continuity]. Materialy X Mizhnarodnoi naukovo-tekhnichnoi konferentsii «AVIA-2011» – Materials of the X International scientific and technical conference «AVIA-2011». Kiev, National Aviation University, Vol. 1, 2.5-2.9. Retrieved from http://avia.nau.edu.ua/doc/2011/2/avia2011_2_2.pdf [in Ukrainian].
8. *Metodika* otneseniya obektov gosudarstvennoy i ne gosudarstvennoy sobstvennosti k kriticheski vazhnyim dlya natsionalnoy bezopasnosti Rossiyskoy Federatsii. Normativnyiy dokument MChS Rossii [Method of taking state and not state objects to critically important objects for national security of Russian Federation. Normative document of Ministry of emergency situations of Russia.] (n.d.). central.mchs.ru. Retrieved from http://central.mchs.ru/upload/site4/files/bea08465669b520c2603f73058fe188a.pdf [in Russian].
9. *Tsygichko, V.N.,* Smolyan, G.L., Chereshkin D.S. (2006). Obespecheniye bezopasnosti kriticheskikh infrastruktur v SShA (analiticheskiy obzor) [Providing of critical infrastructure security in the USA (Analytical review).]. *Trudy ISA RAN – Proceedings of Institute of System Analyses of Russian Academy of Science*. Vol. 27. [in Russian].
10. *Barannik, A.,* Klementyev, S. (2009). Organizatsiya obespecheniya bezopasnosti kriticheskoy infrastruktury v SShA [Organization of providing of critical infrastructure security in the USA]. *Zarubezhnoye voyennoye obozreniye – Foreign military review*, 8, 3-10 [in Russian].
11. *Sukhodolia, O* (2015). Priorytety phormuvannia derzhavnoi polityky zakhusty krytychoi infrastructury Ukrainy [The priorities of the state policy of Ukraine on critical energy infrastructure protection]. *Stratehichni priorytety – Strategic Priorities*, 2, 91-101 [in Ukrainian].