УДОСКОНАЛЕННЯ МЕТОДОЛОГІЇ РАНЖУВАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ЇХ ВІДНЕСЕННЯ ДО КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація

Проаналізовано сучасні методологічні підходи до оцінки критичності об'єктів інфраструктури. Показано, що зважаючи на невизначеності, зокрема, неточність та неповноту інформації, необхідної для коректної оцінки загроз та ризиків критичній інфраструктурі, багатовимірність та незіставність можливих наслідків, необхідність врахування численних взаємозв'язків та взаємозалежностей об'єктів критичної інфраструктури, універсальність оцінки критичності може забезпечити застосування методів нечіткої логіки та експертних оцінок.

Запропонована 3-рівнева ієрархічна модель критеріїв визначення критичності інфраструктури та надані пропозиції щодо дальших кроків з розбудови в Україні державної системи захисту критичної інфраструктури.

Наведено приклад визначення критичності об'єктів інфраструктури, заснований на використанні методів експертних оцінок та нечіткої логіки.

УДОСКОНАЛЕННЯ МЕТОДОЛОГІЇ РАНЖУВАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ЇХ ВІДНЕСЕННЯ ДО КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Усвідомлення світової тенденції до посилення негативних процесів природного та техногенного характеру, зростання терористичних загроз, кількості та витонченості кібер-атак, драматичні події на Сході та Півдні Україні 2014-2016 років актуалізували для країни питання захисту інфраструктури, життєво важливої для безпеки людини, суспільства і держави – інфраструктури, яка в світовій практиці визначається як критична.

У країнах світу, які в рамках забезпечення національної безпеки використовують поняття «Критична інфраструктура» (КІ), під такою інфраструктурою розуміють об'єкти і системи, настільки важливі для забезпечення життєдіяльності людей і держави, дестабілізація роботи яких, не говорячи вже про колапс, призведе до тяжких негативних або навіть катастрофічних наслідків. При цьому, особливу небезпеку несуть каскадні ефекти, коли порушення в роботі одного об'єкту КІ приводять до порушень в роботі інших об'єктів і систем унаслідок їх взаємозалежності («ефект доміно») [1]. З іншої сторони, до КІ відносять і особливо небезпечні виробництва, аварії на яких, викликані будь-якими причинами (природними або техногенними надзвичайними ситуаціями, зловмисними діями), також можуть обернутися катастрофічними наслідками.

Спираючись на досвід ЄС, США, країн-членів НАТО в Національному інституті стратегічних досліджень в 2015 році була підготовлена Зелена книга з питань захисту критичної інфраструктури в Україні [2]. У цьому документі були систематизовані підходи до розуміння і визначення самого поняття «Критична інфраструктура», яка 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, у т.ч., людськими помилками; природні лиха та небезпечні природні явища; зловмисні дії), представлені пропозиції щодо переліку секторів КІ (галузей народного господарства) і основних принципів, на яких має здійснюватися дальша розбудова в Україні системи захисту критичної інфраструктури. Метою цієї системи повинне стати гарантування спроможності критичної інфраструктури виконувати (чи у найкоротші терміни відновлювати) свої функції з життєзабезпечення людей, суспільства, бізнесу і держави.

Слід зазначити, що у провідних країнах світу виходять із необхідності забезпечення захисту критичної інфраструктури від усіх видів загроз (all hazards approach). Водночас, розуміння неможливості забезпечити однаково високий рівень захисту всієї критичної інфраструктури від всіх можливих загроз призвів до розвитку підходу до захисту, який зосереджений на вибірковому захисті конкретного об’єкту КІ від обмеженого набору відомих та відносно прогнозованих загроз, віддаючи пріоритет тій або іншій інфраструктурі залежно від ступеня її «критичності», головною мірою якої виступає *ризик* [3].

Існують різні підходи до визначення ризику[1]. Втім, узагальнений підхід до оцінки ризиків КІ включає:

– 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 обґрунтованого найгіршого сценарію розвитку подій).

Слід зазначити, що хоча зазначений ризик-орієнтований підхід і використовується в управлінні техногенно-екологічною безпекою, проте кількісно оцінити та адекватно зіставити ризики КІ не завжди можливо. Це

[1] Згідно з ДСТУ 2293-99 «ризик – це ймовірність заподіяння шкоди з урахуванням її тяжкості». Державний російський стандарт ГОСТ Р 52448-2005 дає наступне визначення ризику: «поєднання ймовірності нанесення шкоди внаслідок того, що визначена загроза реалізована через наявність вразливості».

пов’язано як із невизначеністю, зокрема, неточністю та неповністю інформації, необхідної для коректної оцінки частості загроз (найбільше це позначається на невизначеності терористичних загроз), так і з багатовимірністю та незіставністю можливих наслідків [4]. Окрім того, ключовою особливістю оцінки ризиків для КІ є необхідність врахування 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 іншої сторони, говорячи 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 направлений, у першу чергу, на зниження рівня загроз та вразливості об’єктів, мінімізацію наслідків, а щодо функцій – на безперервність їх надання та скоріше відновлення у разі переривання [6, 7].

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 сторін. 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 наступних 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’єкту 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 у бюджет);
- 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 використовується й в РФ [8]; при цьому показники розподілені на два рівня:

– 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 ж виду, що випускається в державі %.

– Нанесення 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) значимість об’єктів;

– залежність основних процесів життєзабезпечення суспільства від інфраструктури;

– наявність складних взаємозв’язків та залежностей між об’єктами інфраструктури.

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

В США в загальнонаціональну базу для аналізу критичності включено близько 33 тис. об’єктів інфраструктури, з яких близько 2 тис. було віднесено

до критичної інфраструктури [9]. Ці об’єкти були 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 (крупні системи енергозабезпечення, метрополітен, мережі водопостачання та каналізації, магістральні трубопроводи); важливі (морські порти, очисні споруди, магістральні автомобільні та залізничні дороги, крупні аеропорти, центри зв’язку тощо). Загалом, при оцінці критичності об’єктів у США її ступінь зазвичай ділиться на три категорії: висока, середня, низька.

Слід зазначити, що в США також використовуються 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 5-и ступенів готовності: червона (вища), помаранчева (висока), жовта (підвищена), голуба (можлива) та зелена (низька) [9,10].

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

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

Окрім того, враховується символічна значимість об’єктів, шкода національній обороні та можливі вторинні проблеми національній безпеці.

Інтересним є й підхід для ранжування об’єктів військово-промислового комплексу у 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 розраховується сумарний індекс «ризикованості» об’єкта. Ці фактори враховують вплив на великосерійні програми виробництва, на бойові можливості (значущість продукції), фінансові можливості компанії, економічну живучість, можливості відновлення, кількість населення, що проживає поряд, супутні втрати від враження хімічними / біологічними / радіаційними та вибуховими речовинами, які використовувалися при атаці, та інші. Цікавим є й те, що у 2007 році найбільш критичними визнані об’єкти, на яких виконуються великосерійні програми виробництва для ВПК, в той час як раніше такими об’єктами вважалися ті, які мають найбільший вплив на сучасні бойові можливості.

Враховуючи наведене можна побудувати наступну ієрархічну модель критеріїв визначення критичності інфраструктури – див. Табл. 1.

Таблиця 1

Ієрархічна модель критеріїв визначення критичності інфраструктури

1 рівень	2 рівень	3 рівень
взаємозв’язок між елементами критичної інфраструктури	каскадні ефекти	зниження 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, тижнів, місяців
	тривалість впливу	до кількох годин, діб, тижнів, місяців, років
	час на відновлення	кілька годин, діб, тижнів, місяців, років
важкість можливих наслідків	збиток 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

Слід зазначити, що коректно оцінити кількісно більшість наведених вище параметрів вкрай складно, а то і неможливо. Використання ж методів експертної оцінки (оцінки поточного рівня параметрів шляхом віднесення до певної підгрупи значень показника цих параметрів), 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 наведений у Додатку 1.

Проблематика дальшої розбудови державної системи захисту критичної інфраструктури

Що роблять держави світу на цьому напрямі?

1. Розробляють нормативну базу та регулярно її переглядають.

2. Визначають координуючий орган (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]).

3. Розробляють методологічні підходи, формують перелік КІ, оцінюють загрози та ризики КІ, розробляють плани реагування, регулярно

оцінюють їх ефективність (наприклад, у США цим опікується Національний центр аналізу та імітаційного моделювання інфраструктури МВБ).

4. Забезпечують підготовку кваліфікованих кадрів у сфері захисту КІ.
5. Організовують обмін інформацією та кращими практиками.
6. Розвивають державно-приватне партнерство.

Невірно було б заявляти, що в Україні не приділяється належної уваги захисту критичної інфраструктури. Навпаки, на сьогоднішній день діє ряд нормативно-правових актів (НПА), які визначають повноваження і компетенцію державних органів в цій та суміжних сферах, встановлюють особливості охорони і безпечного функціонування таких об’єктів. Проте більшість цих НПА відомчі, а цілісної національної системи з управління захистом і безпекою критичної інфраструктури немає.

Висновки та рекомендації

Фактично до цих пір під захистом критичної інфраструктури розумілося або забезпечення охорони (фізичної безпеки), чим займається ряд служб і відомчих підрозділів, або захист від надзвичайних ситуацій техногенного і природного характеру, чим займається Державна служба з надзвичайних ситуацій. Глобальнішими питаннями, які пов’язані із забезпеченням стійкості об’єктів КІ по відношенню до будь-яких загроз і можливістю на державному рівні забезпечити виконання функцій із життєзабезпечення людей, суспільства, бізнесу і держави у разі реалізації цих загроз, на системному рівні не займається 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 дальшої розбудови системи необхідно мати апарат, який координуватиме розробку правових, організаційних, методологічних, технологічних та інших інструментів захисту КІ, проводитиме оперативний аналіз існуючих загроз і ризиків,

розроблятиме рекомендації керівництву держави по режимах функціонування системи захисту КІ залежно від рівня загроз і правового стану.

Враховуючи комплексність питання це означає необхідність створення Національного центру з питань захисту критичної інфраструктури та мережі 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, Додаток 1), відповідальність за захист яких лежить, у т.ч., на державі, а відповідні галузеві (функціональні) центри за тією ж методологією та під методичним керівництвом Національного центру – сформувати перелік об'єктів КІ для груп 3 та 4 (див. Додаток 1), відповідальність за захист яких лежить, у першу чергу, на операторах (власниках) цих об'єктів.

Відділ енергетичної та техногенної безпеки

(*Д. Г. Бобро*)

№ 33, Серія « Національна безпека»

Список використаної літератури

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. 2015 р. [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/public/File/2015_nauk_an_rozrobku/Green%20Paper%20-%20dopovid.pdf
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. Стратегічні пріоритети, № 4 (37), 2015 р., Серія «Економіка», стор. 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. - Т1 - 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., Смолян Г.Л., Черешкин Д.С. «Обеспечение безопасности критических инфраструктур в США (аналитический обзор)». Труды ИСА РАН, 2006, т. 27.

10. Баранник А., Клементьев С., «Организация обеспечения безопасности критической инфраструктуры в США, Зарубежное военное обозрение. № 8, 2009, с.3-10.

Додаток 1. 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 (Табл. 1). Експертами для аналізу об’єктів інфраструктури використана множина з 16-и параметрів 2-го рівня (Табл. 1).

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).

3. **Визначення значень параметрів.**

За методом експертної оцінки Дельфі було визначено нечітке значення параметрів оцінюваного об’єкту інфраструктури (нафтобаза у м. Васильків Київської обл.). Була використана лінгвістична зміна з 5-и термів: несуттєвий (голубий), незначний (зелений), значимий (жовтий), значний (помаранчевий) та критичний (червоний).

4. **Візуалізація результату.**

Для візуалізації рівня критичності оцінюваного об’єкта побудована пелюсткова діаграма, де ширина пелюстка відповідає вазі (значимості) параметру, а його нечітке значення для цього об’єкта визначено експертами із використанням вищезгаданої лінгвістичної зміни з 5-и термів. Було обчислене значення агрегованого (інтегрального) показника критичності (відповідає площі пелюсткової діаграми), проведена його нормалізація (представлено у діапазоні 0-1,0).

Для лінгвістичного розпізнання рівня критичності об’єкта інфраструктури за термами: життєво-важливий, вкрай важливий, важливий була використана наступна шкала:

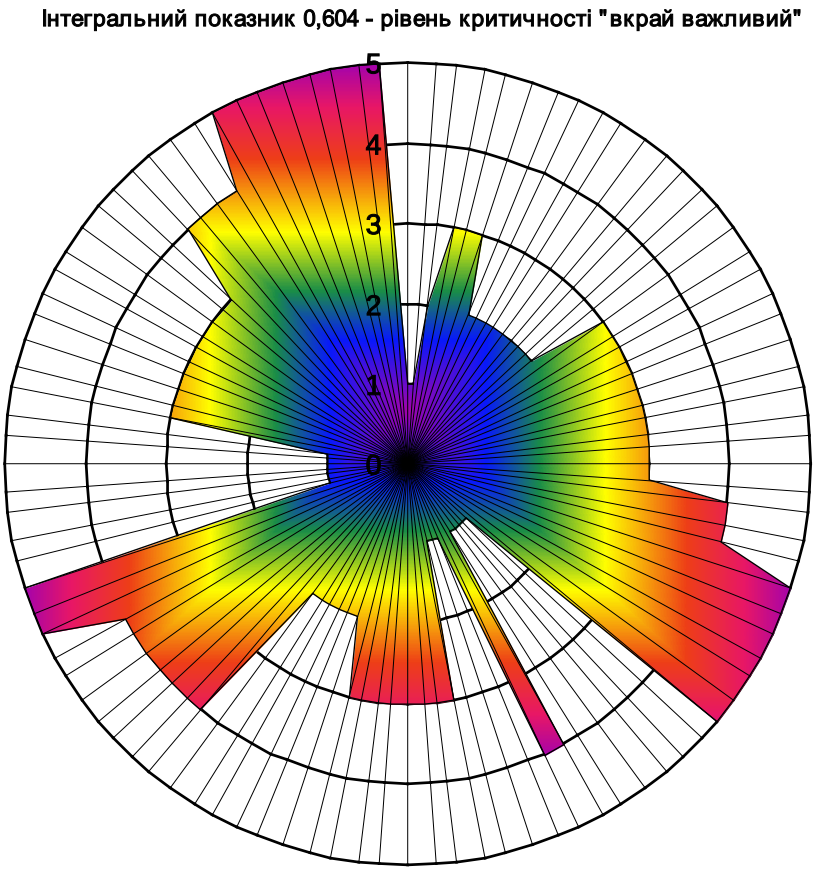
1) життєво-важливі об’єкти КІ – нормований коефіцієнт критичності понад 0,8;

2) вкрай важливі об’єкти КІ – нормований коефіцієнт критичності від 0,5 до 0,8;

3) важливі об’єкти КІ – нормований коефіцієнт критичності від 0,1 до 0,5.

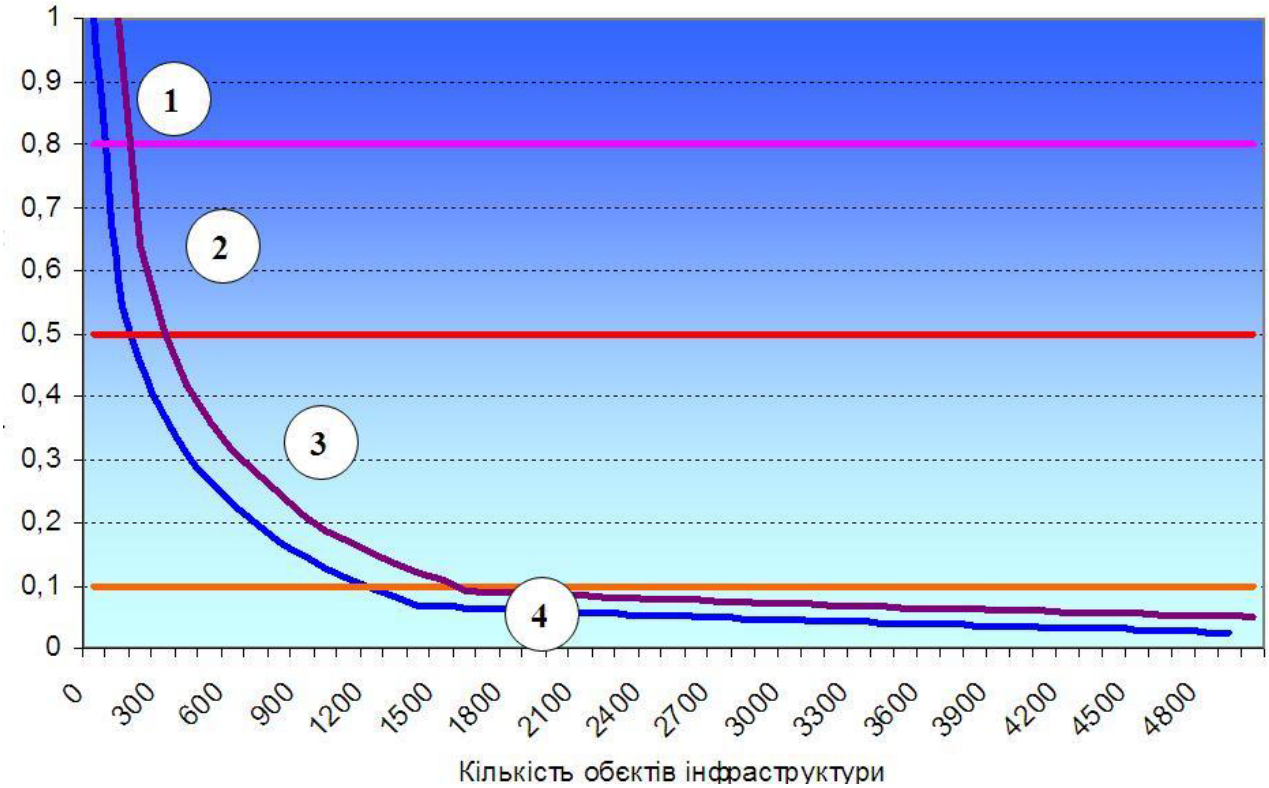
Об’єкти, що мають нормоване значення агрегованого (інтегрального) показника менше 0,1 до критичної інфраструктури не відносилися.

Результат оцінки критичності оцінюваного об’єкту наведений на наступному рисунку. Об’єкт за критичністю віднесений до 2 групи КІ – «вкрай важливий» (детальніше далі).



5. Ранжування об’єктів критичної інфраструктури.

Ранжування усіх інфраструктурних об’єктів проведемо за обчисленими значеннями нормованого агрегованого (інтегрального) показника. Приклад подібного ранжування наведений на наступному рисунку.



Розбивка об’єктів інфраструктури на групи проведена наступним чином:

1 група – життєво-важливі об’єкти КІ (нормований коефіцієнт критичності понад 0,8) – 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 має бути створена адекватна загрозам система фізичного захисту (наприклад, АЕС, нафтопереробні заводи, крупні гідроспоруди тощо). Відповідальність за захист цієї КІ має консолідовано нести держава та оператори (власники) з чітким регламентуванням відносин та взаємодії.

2 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 скорішого відновлення функцій за рахунок диверсифікації та резервів (наприклад, крупні нафтобази, підземні сховища газу, електричні підстанції, мостові переходи, крупні 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.

3 група – важливі об’єкти КІ (нормований коефіцієнт критичності від 0,1 до 0,5). Основним шляхом захисту такої інфраструктури є забезпечення скорішого відновлення функцій за рахунок диверсифікації та резервів (наприклад, теплові електростанції, автомагістралі тощо). Відповідальність за захист цієї КІ, в першу чергу, мають нести оператори (власники), а держава має забезпечити наявність умов для диверсифікації та резервування.

4 група – нормований коефіцієнт критичності до 0,1 – об’єкти інфраструктури, яка не відноситься до критичної, безпосередній захист якої є відповідальністю суто оператора (власника).

Слід зазначити, що прийняті у даному 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, у т.ч., виходячи зі спроможності держави.