DOI 10.37491/UNZ.87.6
УДК 351.86:323

Олександр ЯРЕМЕНКО[1],
Ярослав СТРАХНІЦЬКИЙ[2]

ВИЗНАЧЕННЯ ТА УПРАВЛІННЯ ЗАГРОЗАМИ У СТРУКТУРІ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Проаналізовано теоретичні підходи до змістовного наповнення поняття «захист критичної інфраструктури». Визначено, що ключові акценти в більшості підходів робляться на проблеми загроз і ризиків їхнього виникнення для критичних об'єктів. Відзначається, що фундамент наукового обґрунтування державної політики у сфері захисту критичної інфраструктури варто формувати на основі теоретико-методичних підходів до визначення та управління саме цими категоріями, як детермінантами безпеки. Найбільшою небезпекою для функціонування критичної інфраструктури на сьогодні в Україні визнано воєнні загрози, які загострюють ризики виникнення надзвичайних ситуацій на критичних об'єктах. Проведено аналіз наукових напрацювань з ідентифікації дефінітиву «ризик безпеки критичної інфраструктури» в державній політиці захисту. Його розкрито як імовірність виникнення нещасного випадку, небезпеки, аварії або катастрофи в роботі об'єктів критичної інфраструктури за певних обставин, управління якими відбувається в умовах невизначеності та необхідності прогнозування множини альтернативних варіантів ситуації. Наголошується, що багатоаспектність

[1] кандидат наук з державного управління, доцент, доцент кафедри публічного управління та адміністрування, декан факультету права, публічного управління та адміністрування, Вінницький державний педагогічний університет імені Михайла Коцюбинського, *oleksandr.yaremenko@vspu.edu.ua*, https://orcid.org/0000-0002-3053-2257.
[2] аспірант, Вінницький державний педагогічний університет імені Михайла Коцюбинського, *strahnitskiy@gmail.com*, https://orcid.org/0000-0002-3066-0961.

Університетські наукові записки, 2022, № 3 (87), С. 73-82. unz.univer.km.ua

проблем захисту критичної інфраструктури детермінує необхідність систематичного аналізу ризиків в управлінні безпекою (ризик-аналізу). Особливість критичного ризик-аналізу визначено в тому, що розглядаються потенційно негативні наслідки, які можуть виникнути у результаті відмови в роботі технічних систем, збоїв або помилок з боку персоналу об'єкта та ін. Акцентовано увагу на складнику «управління критичними ризиками» як головному складнику державної політики забезпечення безпеки критичної інфраструктури. Цю категорію проаналізовано із позиції адміністрування й менеджменту та зроблено висновок про необхідність її доповнення «критичним ризик-менеджментом». Результатом вбачається посилення складника захисту як державних, так і приватних критичних об'єктів. Визначено, що прийняття управлінських рішень у межах запропонованого критичного ризик-менеджменту здійснюється в умовах невизначеності. Для вирішення таких завдань пропонується використовувати теорію нечіткої логіки як засобу моделювання.

Ключові слова: критична інфраструктура, захист критичної інфраструктури, державна політика, ризики, загрози, ризик-менеджмент, теорія нечіткої логіки.

unz.univer.km.ua Університетські наукові записки, 2022, № 3 (87), С. 73-82

Структурованість державної політики у сфері захисту критичної інфраструктури відіграє ключове значення в сучасних умовах військового стану та збройної агресії ворога на території України. Значимість цього процесу вчені пояснюють суттєвими наслідками для національної безпеки [1]. Як відомо, саме об'єкти критичної інфраструктури становлять визначальний потенціал для забезпечення комфортного та безперебійного функціонування в мирний час та життедіяльності суспільства і держави у військовий час. Своєчасне виявлення та профілактику загроз об'єктам критичної інфраструктури доцільно сприймати як невід'ємний складник державної політики у сфері її захисту. Злагоджена діяльність відповідних державних органів із прогнозування та протидії ризикам і загрозам сприятиме надійній захищеності критичних об'єктів та стане ключовою перевагою в геополітичній боротьбі. Необхідність інтеграції названих процедур у структуру державної політики захисту об'єктів критичної інфраструктури аргументують учені Д. Г. Бобро, С. П. Іванюта, С. І. Кондратов та О. М. Суходоля [2], акцентуючи увагу на важливості раннього виявлення та попередження ризиків в управлінні безпекою критичної інфраструктури, наголошуючи, що окремі її елементи — це об'єкти підвищеної небезпеки, які належать як до національного, так і міжнародного рівня. Загалом, цей підхід передбачає реалізацію на рівні державних інститутів відповідних заходів стратегічного планування, серед яких особливого значення набуває необхідність наукового обґрунтування сучасних теоретико-методичних підходів до визначення ризиків для об'єктів критичної інфраструктури та заходів протидії.

Питанням теоретичного осмислення загроз та ризиків для об'єктів критичної інфраструктури, теоретико-методичних підходів до їх керованості, а також вивченню питань інтеграції цих заходів у державну політику сфери захисту критичної інфраструктури в Україні присвятили свої наукові праці такі вчені: С. І. Азаров, Д. С. Бірюков, А. М. Демків, О. П. Єрменчук, С. А. Єременко, С. І. Кондратов, А. В. Пруський, В. Л. Сидоренко. Питання моделювання управлінських процесів в умовах невизначеності досліджували С. В. Козловський [14], В. А. Капранов, С. А. Олизаренко, А. В. Перепелица та ін.

Мета статті — здійснити обґрунтування теоретико-методичних підходів до ідентифікації та управління ризиками у структурі державної політики у сфері захисту критичної інфраструктури.

У сучасних наукових дослідженнях триває полеміка щодо визначення безпеки, яке б задовольнило як вітчизняних, так і зарубіжних науковців. Сучасна проекція національної безпеки знаходить відображення серед більшості наукових трактувань як стан захищеності національних інтересів від потенційних чи реальних загроз і ризиків їхнього виникнення на основі комплексу безпекових заходів. Згідно із Законом «Про критичну інфраструктуру» [3], захист критичної інфраструктури — це всі види діяльності, що виконуються перед або під час створення, функціонування, відновлення й реорганізації об'єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх виникнення. Відзначимо, що ключові акценти в більшості підходів ставляться на проблеми загроз і ризиків їх виникнення для об'єктів критичної інфраструктури. Отже, дійдемо висновку, що фундамент наукового обґрунтування державної політики у сфері захисту критичної інфраструктури мають становити теоретико-методичні підходи до визначення та управління саме цими категоріями як детермінантами безпеки.

Розпочнемо із ідентифікації дефінітиву «загрози» в контексті захисту критичної інфраструктури. Погодимось із думкою О. П. Єременчука, який пропонує розуміти їх як «наявні або потенційно можливі явища і чинники, що можуть нанести шкоду об'єкту критичної інфраструктури (фізичному або у кіберпросторі), вивести його з ладу або порушити функціонування відповідно до призначення, чим створюють небезпеку життєво важливим національним інтересам України» [4]. Звернемо увагу, що на сьогодні найбільші загрози для функціонування критичної інфраструктури в Україні створюють військові дії, загострюючи ризики виникнення надзвичайних ситуацій та нанесення ударів по критичних об'єктах. Відтак забезпечення захисту критичної інфраструктури у складі комплексу національної безпеки постає першочерговим завданням у реалізації функцій державної політики та вимагає активної і консолідованої участі усього суспільства.

Зазначимо, що кожний державний інститут або відомство, забезпечуючи розробку та реалізацію політики захисту критичної інфраструктури, має чітко визначити спектр потенційних загроз для підпорядкованих йому критичних об'єктів, оперуючи відповідним набором інструментів та ресур-

Університетські наукові записки, 2022, № 3 (87), С. 73-82. unz.univer.km.ua

сів. Погоджуємось із твердженням вчених Д. С. Бірюкова та С. І. Кондратова [5], що інститути державної політики захисту повинні враховувати розгалуженість світоглядних наукових досліджень, які мають передувати практичній частині реалізації державної політики захисту. До них науковці пропонують включити:

— секторальний поділ критичної інфраструктури на національному, регіональному та місцевому рівнях;

— ідентифікацію секторальних релевантних ризиків та загроз для об'єктів критичної інфраструктури;

— оцінку вразливості окремих секторів критичної інфраструктури до визначених ризиків та загроз;

— оцінку ризиків та загроз порушення або знищення секторів критичної інфраструктури;

— прийняття відповідних запобіжних заходів на основі створення системи захисту критичної інфраструктури.

Загалом, можна стверджувати, що в основі цього підходу лежить виконання на рівні державних інститутів заходів стратегічного планування, кінцевою метою яких повинна стати профілактика виникнення нових і зниження відомих ризиків виникнення загроз об'єктам критичної інфраструктури. Кінцевим продуктом цього процесу мають стати управлінські рішення на місцевому, регіональному і загальнодержавному рівнях, орієнтовані на реалізацію комплексу заходів із ідентифікації ризиків, удосконалення організаційно-правових рамок управління ризиками, інвестування в заходи зі зниження ризиків, підвищення ефективності оперативного реагування на загрози та відновлення після надзвичайних ситуацій. Доповнимо цей тезис стадіями розвитку надзвичайних ситуацій на об'єктах критичної інфраструктури, запропонованими колективом науковців на чолі з С. І. Азаровим [1]:

1) накопичення факторів ризику (відбувається у самому джерелі ризику);

2) ініціалізація надзвичайної ситуації на об'єктах критичної інфраструктури — представляє ~~собою~~ спусковий механізм на основі факторів ризику на стадії, коли уже неможливо стримати їхні вияви;

3) процес перебігу надзвичайної ситуації на об'єктах критичної інфраструктури — процес вивільнення факторів ризику, який здійснює прямий чи опосередкований вплив на людей, матеріальні об'єкти та природне середовище наслідки та є важко прогнозованим за складністю ситуації;

4) стадія затухання — період від перекриття (обмеження) джерела небезпеки, тобто локалізація факторів надзвичайної ситуації, які уражають, до повної ліквідації її прямих і непрямих наслідків [1].

Розкриємо змістовне наповнення поняття «ризик безпеки критичної інфраструктури» у державній політиці захисту. Це поняття можна охарактеризувати як атрибут полінаукового синтезу суспільних, технічних, економічних, природних та інших факторів. Відповідно під час визначення міри ризику для безпеки критичної інфраструктури варто виділяти соціальні, професійні, екологічні, техногенні, військові та інші небезпеки. Таким чином, ризик варто сприймати як мірило цілком реальних небезпек.

unz.univer.km.ua Університетські наукові записки, 2022, № 3 (87), С. 73-82

Під ризиком учені Д. Г. Бобро, С. П. Іванюта, С. І. Кондратов та О. М. Суходоля [2] розуміють очікувану частоту або ймовірність виникнення небезпек відповідного класу, або ж розмір нанесеного збитку (втрат, шкоди) від шкодочинної події, або ж певну комбінацію цих факторів. Звернемо також увагу на думку вчених В. В. Вітлінського та Г. І. Великоіваненка, які ризик трактують як «ситуацію, у якій домінує невизначеність, конфлікт, наявна багатоваріантність, і коли одночасно не всі альтернативні варіанти однаковою мірою сприятливі» [6]. Цю позицію підтримує і Л. І. Донець [7], пов'язуючи її з подоланням невизначеності в ситуації неминучого вибору, у процесі якого є можливість якісно і кількісно оцінити ймовірність досягнення передбаченого результату, невдачі, відхилення від мети. І. М. Посохов визначає ризик як «невід'ємну умову для здійснення дій з імовірнісними несприятливими наслідками, що виражається в можливості отримання негативного або небажаного результату [8]. Отже, проаналізувавши низку трактувань поняття ризику в управлінні безпекою критичної інфраструктури, можемо розтлумачити його як імовірність виникнення небезпеки, нещасного випадку, аварії або катастрофи під час виконання об'єктами критичної інфраструктури своїх функцій за певних обставин, управління якими здійснюється в умовах невизначеності та необхідності прогнозування множини альтернативних варіантів розвитку ситуації.

Різноманіття специфіки діяльності критичної інфраструктури та приналежності її об'єктів до різних галузей відображає багатоаспектність проблеми аналізу ризиків в управлінні безпекою (ризик-аналіз). Особливість критичного ризик-аналізу визначимо в тому, що аналізуються потенційно шкодочинні наслідки, які можуть виникнути в результаті відмови в роботі технічних систем, збоїв або помилок з боку персоналу об'єкта. Враховуючи це, варто приділити окрему увагу складника «управління критичними ризиками» як головного складника державної політики забезпечення безпеки критичної інфраструктури. Однак варто зауважити, що цю категорію варто розглянути під кутом зору «адміністрування» як сфери компетенції органів державної влади. У цьому випадку звернемось до дослідження О. Я. Лазор та О. Д. Лазор [9], які лобіюють позицію, що процес адміністрування передбачає організаційно-розпорядчу та консультативно-дорадчу діяльність органів державної влади. Тобто адміністрування з позиції державного управління вчені характеризують підпорядкованістю законам, узгодженістю інтересів учасників процесу та відповідальністю за стан керованої системи. Розширимо межі уявлення про цю категорію теорією В. В. Овчарука [10], який характеризує її як функцію менеджменту, управлінську діяльність, стиль управління або вид менеджменту.

Отже, дійдемо висновку, що «управління критичними ризиками» варто здійснювати як з позиції публічного адміністрування (стосується органів публічної влади), так і з позиції менеджменту, що є ширшим поняттям (стосується як органів публічної влади, так і приватних суб'єктів господарювання). Слушним у цьому випадку вважаємо доповнення структури державної політики у сфері захисту критичної інфраструктури «критичним ризик-менеджментом». Це дозволить посилити складник захисту як державних критичних об'єктів, так і приватних. Слушним у цьому розумінні

Університетські наукові записки, 2022, № 3 (87), С. 73-82. unz.univer.km.ua

вважаємо позицію вчених В. О. Мусієнка та М. Е. Зінченка [11], які ризик-менеджмент визначають як «процес прийняття та виконання управлінських рішень, спрямованих на зменшення ступеня ймовірності виникнення результату несприятливого характеру та мінімізацію можливих втрат, які викликані його реалізацією». Варто розглядати систему критичного ризик-менеджменту як частину системного підходу до прийняття управлінських рішень [12]. Отже, вважаємо доцільним сприймати критичний ризик-менеджмент як спектр процедур і практичних заходів, спрямованих на вирішення завдань з попередження та мінімізації рівня потенційних загроз та ризиків виникнення небезпек, що загрожують стабільності роботи об'єктів критичної інфраструктури, зменшення потенційних втрат та інших негативних наслідків. По суті, мова йде про попередження виникнення надзвичайних ситуацій на критично-важливих об'єктах та заплановані заходи щодо локалізації та мінімізації негативних наслідків за умов їх виникнення. Оскільки, як зазначалося вище, управління ризиками в захисті критичної інфраструктури реалізується в умовах невизначеності, в основу варто покласти технічний та соціальний аналіз і методи прогнозування під час оцінки ризику (рис. 1).

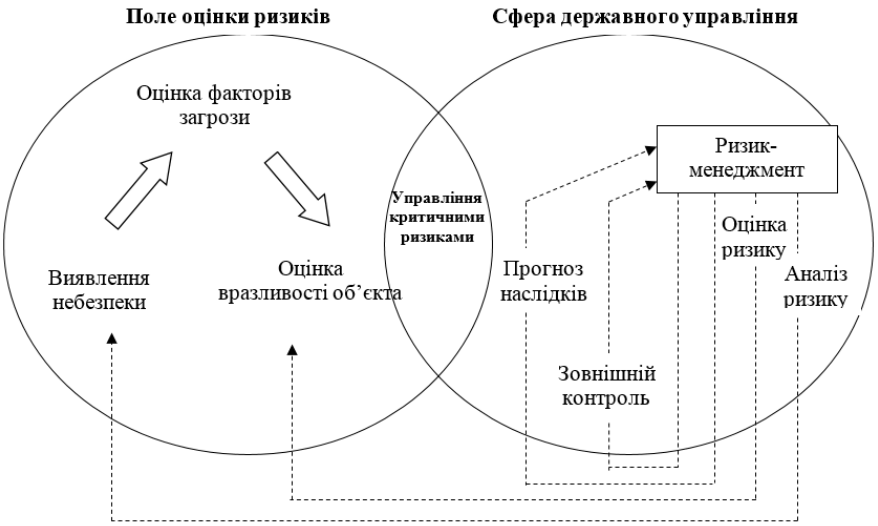

Рис. 1. Алгоритм забезпечення критичного ризик-менеджменту як складника державної політики захисту критичної інфраструктури

Примітка: розроблено авторами.

Відповідно до зображеної схеми, відзначимо, що захист критичної інфраструктури повинен базуватися на механізмах державного управління та оцінці критичних ризиків. Сфера державного управління для побудови дієвого захисту критичної інфраструктури має включати складник ризик-менеджменту, який базується на відпрацюванні альтернатив з викорис-

unz.univer.km.ua Університетські наукові записки, 2022, № 3 (87), С. 73-82

танням результатів оцінки ризиків, аналізу ризиків та прогнозування наслідків для їх мінімізації. Тобто цей процес передбачає реалізацію багатокритеріальних завдань, які передують прийняттю рішення в умовах невизначеності. Оцінка ризику є основою для дослідження і вироблення заходів ризик-менеджменту відповідно до алгоритму дій із виявлення небезпек, оцінки факторів загроз та оцінки вразливості критичного об'єкта . У свою чергу, це потребує створення додаткового алгоритму, який дозволить змоделювати обставини надзвичайної ситуації і в подальшому допоможе керівництву та персоналу критичних об'єктів адаптуватись до них у реальному житті. Таким чином, інтеграція ризик-менеджменту в структуру державної політики забезпечить механізм ідентифікації та управління загрозами критичним об'єктам.

Для просторово-часового опису зазначеного алгоритму ризикової ситуації критично важливого об'єкта можна застосувати напрацювання В. В. Вітлінського та Г. І. Великоіваненко [6], де вчені пропонують використовувати три критерії:

— чітке визначення загрози, з якої може сформуватися ризикова ситуація;

— імовірність настання цієї ситуації;

— ступінь зниження негативних наслідків після її виникнення.

Подібна схема задовольняє логіку наукового дослідження забезпечення захисту критичної інфраструктури через механізми адміністративно-правового регулювання в умовах невизначеності. Доречною у цьому випадку також вважаємо теорію учених О. Є. Кузьміна, О. Г. Мельника та М. Є. Адамів [13], які наголошують, що за інтенсивного зростання дефіциту інформаційно-часових ресурсів при обґрунтуванні управлінських рішень інтенсифікується загроза неадекватного сприйняття поточних умов діяльності критичних об'єктів, що відбивається на дієвості такого рішення. Виходом із цієї ситуації вчені вбачають інтеграцію антисипативного управління, спрямованого на прогнозування можливих ризиків внутрішнього та зовнішнього середовища. Зауважимо, що наявність розпливчатості результатів у процесі прийняття рішення детермінує необхідність прогнозування його наслідків, що можна забезпечити вірогідністною моделлю, на основі застосування методів розпливчастих множин, які не піддаються строгій формалізації і мають логіко-аналітичний характер (у нашому випадку — критичний ризик-менеджмент). Опираючись на дослідження учених С. В. Козловського [14], С. А. Олизаренка, А. В. Перепелиці та В. А. Капранов [15], можна стверджувати, що саме для таких завдань доцільно використовувати теорію нечіткої логіки як засіб моделювання для структурування управлінських моделей і когнітивних методів з використанням штучного інтелекту та інженерії наукових знань.

Загальна методика моделювання на основі теорії нечіткої логіки, адаптована під вимоги забезпечення безпеки критичної інфраструктури, повинна передбачати поетапне розв'язання таких завдань: виокремлення основних факторів впливу на критичну інфраструктуру та взаємозв'язків між ними; визначення і формалізацію лінгвістичних оцінок факторів; побудову нечіткої бази знань про взаємозв'язки між факторами; виведення

Університетські наукові записки, 2022, № 3 (87), С. 73-82. unz.univer.km.ua

нечітких логічних рівнянь на основі лінгвістичних оцінок і нечіткої бази знань; оптимізацію параметрів нечіткої моделі [16]. І. Г. Фадєєва [17] пропонує кілька алгоритмів у системах нечіткого умовиводу, опис яких заснований на поділі вихідного процесу на низку послідовних етапів:

1. Формування бази даних правил нечіткого висновку системи.
2. Фазифікація вхідних змінних.
3. Агрегація підумов у нечітких умовах правила дії.
4. Активізація або композиція підвисновків у правила нечіткої умови-дії.
5. Накопичення висновків нечіткої умови правила дії.
6. Дефазифікація вихідних змінних.

Тобто при створенні алгоритму керівник критичного об'єкта буде аналізувати поточну ситуацію, порівнюючи її з раніше розробленими шаблонами критеріальних факторів, які є ознаками надзвичайної ситуації. Відповідно описану алгоритмізацію нечітких умовиводів у межах критичного ризик-менеджменту можна застосовувати у ситуаціях, відносно незмінних у короткий проміжок часу і з невеликим обсягом ситуаційної інформації, а формалізовані алгоритмічні висновки відповідають умовам для прийняття екстрених управлінських рішень на критичних об'єктах.

Аналіз наукових підходів до обґрунтування заходів державного управління у сфері безпеки критичної інфраструктури дає підстави зробити висновки про необхідність ідентифікації загроз і ризиків як фундаменту наукового обґрунтування політики захисту. Складність та невизначеність у зовнішньому та внутрішньому середовищі сприяють розширенню спектру критичних загроз та ризиків. Їх динамічний та важкопрогнозований характер детермінує необхідність інтеграції сучасних управлінських моделей у сферу державного управління. Саме тому сфера державного управління для побудови дієвого захисту критичної інфраструктури має включати складник ризик-менеджменту, який базується на відпрацюванні альтернатив з використанням результатів оцінки ризиків, аналізу ризиків та прогнозування наслідків для їх мінімізації. Він дозволить забезпечити на основі глибокого та диференційованого аналізу зовнішнього і внутрішнього середовища комплексний дієвий захист об'єктів критичної інфраструктури, як державної, так і приватної власності. Цей процес також забезпечить врахування багатокритеріальності загроз та ризиків у прийнятті управлінського рішення в умовах невизначеності. Така процедура є досить складною, неструктурованою та трудомісткою, що визначає потребу у ґрунтовності фахових знань, експертних міркуваннях та оцінках, які характеризуються нечіткістю їхнього характеру.

Гостро також постає проблема збору та обробки інформації, оскільки критична інфраструктура нашої держави характеризується просторовою розпорошеністю об'єктів. Неповнота або відсутність статистичної інформації про стан ризиків та загроз для об'єктів критичної інфраструктури обмежує використання формалізованих моделей. Зважаючи на це, ефективним способом оптимізації політики безпеки об'єктів критичної інфраструктури розглядаємо використання в межах критичного ризик-менеджменту теорії

unz.univer.km.ua Університетські наукові записки, 2022, № 3 (87), С. 73-82

нечіткої логіки, яка створює підстави для розширення методів моделювання складних соціально-економічних систем, формалізуючи невизначені (нечіткі) процеси й описуючи алгоритм діагностики стану об'єктів критичної інфраструктури за допомогою моделювання вихідних (факторних) даних.

Список використаних джерел

1. Захист критичної інфраструктури в умовах надзвичайних ситуацій / за заг. ред. П. Б. Волянського. Київ : НІСД, 2021. 375 с.
2. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналіт. доп. / Д. Г. Бобро, С. П. Іванюта, С. І. Кондратов, О. М. Суходоля. Київ : НІСД, 2019. 224 с.
3. Про критичну інфраструктуру. Закон України від 16.11.2021 р. № 1882–IX. *Верховна Рада України. Законодавство України.* URL: https://bit.ly/3FDavCV.
4. *Єрменчук О. П.* Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.
5. *Бірюков Д. С., Кондратов С. І.* Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Київ : НІСД, 2012. 96 с.
6. *Вітлінський В. В., Великоіваненко Г. І.* Ризикологія в економіці та підприємництві. Київ : КНЕУ, 2004. 480 с.
7. *Донець Л. І.* Економічні ризики та методи їх вимірювання. Київ : Центр навч. літ., 2006. 312 с.
8. *Посохов І. М.* Управління ризиками у підприємництві. Харків : НТУ «ХПІ», 2015. 220 с.
9. *Лазор О. Я., Лазор О. Д.* Публічне управління та адміністрування: ретроспектива деяких теоретичних аспектів. *Університетські наукові записки.* 2015. № 4. С. 111–121.
10. *Овчарук В. В.* Сутність адміністрування на підприємствах. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство.* 2018. Вип. 19 (2). С. 115–118.
11. *Мусієнко В. О., Зінченко М. Е.* Технологія ризик-менеджменту як елемент системи забезпечення економічної безпеки суб'єкта господарювання. *Економічний вісник Дніпровської політехніки.* 2020. № 3. С. 98–108.
12. Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT). Київ : Мінекономрозвитку України, 2015. 74 с.
13. *Кузмін О. Є., Мельник О. Г., Адамів М. Є.* Антисипативне управління підприємствами: процесно-структурований підхід. *Економіка: реалії часу.* 2012. № 2 (3). С. 71–77.
14. *Козловський С. В.* Управління сучасними економічними системами, їх розвитком та стійкістю. Вінниця : Меркьюрі-Поділля, 2010. 432 с.
15. *Олизаренко С. А., Перепелица А. В., Капранов В. А.* Интервальные нечеткие множества типа 2. Терминология, представление, операции. *Системи обробки інформації.* 2011. № 2 (92). С. 39–45.
16. *Матвійчук А. В.* Моделювання економічних процесів із застосуванням методів нечіткої логіки. Київ : КНЕУ, 2007. 264 с.
17. *Fadyeyeva I. G., Gryniuk O. I.* Fuzzy modelling in risk assessment of oil and gas production enterprises' activity. *Baltic Journal of Economic*

Studies. 2017. Vol. 3. No. 4. P. 256–264. https://doi.org/10.30525/2256-0742/2017-3-4-256-264.

Надійшла до редакції 03.05.2022
Рекомендовано до друку 20.06.2022

Oleksandr YAREMENKO,
Yaroslav STRAHNITSKYI
Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University

Detection and Management of Threats in the Structure of State Policy for Critical Infrastructure Protection

The article analyses the theoretical approaches to the content of the concept of «critical infrastructure protection». It is determined that the key emphasis in most approaches is on the problems of threats and risks of their occurrence for critical objects. It is noted that the foundation of the scientific substantiation of the state policy of critical infrastructure protection should be formed on the basis of theoretical and methodological approaches to the detection and management of these categories. The greatest danger to the functioning of critical infrastructure in Ukraine is recognized as military threats and risks of emergencies at critical facilities. The analysis of scientific developments on identification of the definition of «critical infrastructure security risk» in the state protection policy is carried out. It is disclosed as the probability of an accident, danger, accident or catastrophe in the operation of critical infrastructure. Management takes place in conditions of uncertainty and the need to predict many alternative situations. It is emphasized that the variety of problems of critical infrastructure protection determines the need for systematic risk analysis in security management (risk analysis). Features of critical risk analysis are the analysis of potentially negative consequences arising from the failure of technical systems, failures or errors by personnel of the facility. Emphasis is placed on the component of «critical risk management» as the main component of the state policy of critical infrastructure security. This category is analysed from the standpoint of administration and management. The conclusion is made that it is necessary to supplement the state policy of critical infrastructure protection with «critical risk management». The result will be a stronger component of the protection of public and private critical facilities. It is determined that making managerial decisions within the proposed critical risk management is carried out in conditions of uncertainty. To solve such problems, it is proposed to use the theory of fuzzy logic as a means of modelling.

***Keywords**: critical infrastructure, critical infrastructure protection, public policy, risks, threats, risk management, fuzzy logic theory.*