Використання методів аналізу ризику стосовно терористичних загроз на об'єктах критичної інфраструктури, що охороняються

Use of risk analysis methods in relation to terrorist threats at protected critical infrastructure facilities

Михайло Дивізінюк * [1 A]

***Corresponding author**: доктор фізико-математичних наук, професор, e-mail: divizinyuk@ukr.net, ORCID: 0000-0002-5657-2302

Володимир Мірненко [2 B]

доктор технічних наук, професор, заслужений діяч освіти України, директор департаменту, e-mail: mirnenkovi@gmail.com, ORCID: 0000-0002-7484-1035

Василь Поліщук [3 C]

кандидат військових наук, старший викладач кафедри, e-mail: polva@ukr.net, ORCID: 0000-0001-8990-9648

[A] Інститу́т ге́охімії навко́лишнього середо́вища НАН України, м. Київ, Україна

[B] Департамент освіти та науки Міністерства оборони України, м. Київ, Україна

[C] Національний університет оборони України імені Івана Черняховського, м. Київ, Україна

Mykhailo Divizinyuk * [1 A]

***Corresponding author**: Doctor of Physico-Mathematical Sciences, professor, e-mail: divizinyuk@ukr.net, ORCID: 0000-0002-5657-2302

Volodymyr Mirnenko [2 B]

Doctor of Technical Sciences, Honored Worker of Education of Ukraine, Director of the Department, e-mail: mirnenkovi@gmail.com, ORCID: 0000-0002-7484-1035

Vasyl Polishchuk [3 C]

Candidate of military sciences, senior lecturer of the department, e-mail: polva@ukr.net, ORCID: 0000-0001-8990-9648

[A] Institute of Environmental Geochemistry of the National Academy of Sciences of Ukraine, Kyiv, Ukraine

[B] Department of Education and Science of the Ministry of Defense of Ukraine, Kyiv, Ukraine

[C] National Defense University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine

Received: July 15, 2022 | Revised: August 25, 2022 | Accepted: August 31, 2022

DOI: 10.33445/sds.2022.12.4.11

Мета роботи: на основі дослідження трансформації поняття ризику (стосовно об'єкту критичної інфраструктури, що охороняється), характеристик терористичного акту та терористичних загроз, розглянути методи аналізу ризику стосовно терористичних загроз на об'єктах критичної інфраструктури, що охороняються.

Дизайн/Метод/Підхід дослідження: методи теорії ймовірностей та математичної статистики, теорії нечітких множин та інтервальної математики, теорії ризиків та моделювання динамічних процесів.

Результати дослідження: показано, що стосовно охоронюваного об'єкта критичної інфраструктури ризик – це міра кількісного багатокомпонентного виміру небезпеки з включенням величини шкоди від впливу загроз, що виявляються у формі технічних та технологічних, природних та екологічних, економічних та психологічних, соціальних та інших інцидентів. Вони проявляються як збої та відмови, пригоди та аварії, вибухи та пожежі, призводять до зупинки або обмеження функціонування цих об'єктів. Показано, що типовий сценарій теракту складається з десяти етапів, а терористичні загрози на об'єктах критичної інфраструктури, що охороняються, це можливі суспільно небезпечні наслідки зловмисних дій, які призводять до зупинення або обмеження функціонування цих об'єктів. Зроблено висновок, що для аналізу ризику стосовно терористичних загроз на об'єктах критичної інфраструктури, дефіцит статистичних даних при оцінці різних загроз забезпечив домінування імовірнісно-евристичних методів, що ґрунтуються на використанні суб'єктивних ймовірностей, одержуваних за допомогою експертного оцінювання.

Теоретична цінність дослідження: полягає в тому, що дефіцит статистичних даних при оцінці різних загроз на об'єктах критичної інфраструктури, що охороняються, забезпечує домінування імовірнісно-евристичних методів, що ґрунтуються на використанні суб'єктивних ймовірностей, одержуваних за допомогою експертного оцінювання.

Тип статті: науково-практичний.

Purpose: on the basis of a study of the transformation of the concept of risk (relating to a protected critical infrastructure object), the characteristics of a terrorist act and terrorist threats, to consider methods of risk analysis in relation to terrorist threats on protected critical infrastructure objects.

Design/Method/Approach the methods of the theory of probabilities and mathematical statistics, the theory of fuzzy sets and interval mathematics, the theory of risks and the modeling of dynamic processes were used in the performance of this work.

Findings: it is shown that in relation to a protected object of critical infrastructure, risk is a measure of a quantitative, multi-component measure of danger, including the amount of damage from the impact of threats that appear in the form of technical and technological, natural and ecological, economic and psychological, social and other incidents. They manifest themselves as failures and failures, accidents and accidents, explosions and fires, collapses and disasters and lead to stopping or limiting the functioning of these objects. Then it is shown that a typical scenario of a terrorist attack consists of ten stages, and terrorist threats on protected critical infrastructure facilities are possible socially dangerous consequences of malicious actions that lead to stopping or limiting the functioning of these facilities. It was concluded that for the risk analysis of terrorist threats on protected critical infrastructure facilities, the lack of statistical data in the assessment of various threats ensured the dominance of probabilistic heuristic methods based on the use of subjective probabilities obtained through expert assessment.

Theoretical implications: lies in the fact that the lack of statistical data in the assessment of various threats to protected critical infrastructure facilities ensures the dominance of probabilistic heuristic methods based on the use of subjective probabilities obtained through expert assessment.

Papertype: scientific and practical.

Ключові слова: ризик, надзвичайна ситуація, критична інфраструктура, аналіз ризику, об'єкт.

Key words: risk, emergency, critical infrastructure, risk analysis, protected object.

1. Вступ

У наше повсякденне життя та професійну діяльність все більше і густо входить поняття ризику [1-3]. Це облік, планування та управління ризиками. Ці терміни дедалі частіше вживаються менеджерами різного рівня [3, 5 ,6], та постійно озвучуються дикторами і блогерами у засобах масової інформації, використовуються політиками і військовими, і величезною кількістю простих громадян.

На перший погляд, ці терміни вже давно застосовуються у сфері забезпечення державної безпеки та захисту його критичної інфраструктури [7-12]. Вітчизняні [7-9] та зарубіжні [10-12] фахівці у цій галузі вважають, що набагато ефективнішими будуть точкові диверсії або, говорячи сучасною мовою, терористичні акти на ключових об'єктах критичної інфраструктури, як показав досвід російсько-української війни, а саме захоплення окупантами атомних електростанцій, шантажування, погрози та знищення критичної інфраструктури України. Виведення подібних об'єктів з ладу істотно послаблюють економіку держави [25, 26], а запозичення коштів та ресурсів у сусідів на їх відновлення чи будівництво нових об'єктів призводить до добросусідського підпорядкування державам – позичальникам. З цих причин розгляд ризику терористичних загроз на об'єктах критичної інфраструктури є актуальною науково-практичною проблемою, що постійно перебуває у полі зору структур, які забезпечують національну безпеку держави.

2. Теоретичні основи дослідження

Теоретична цінність дослідження: полягає в тому, що дефіцит статистичних даних при оцінці різних загроз на об'єктах критичної інфраструктури, що охороняються, забезпечує домінування імовірнісно-евристичних методів, що ґрунтуються на використанні суб'єктивних ймовірностей, одержуваних за допомогою експертного оцінювання.

3. Постановка проблеми

Мета даної роботи – систематизувати існуючі визначення ризику, поняття аналізу та оцінки ризику в різних галузях діяльності та застосувати їх до терористичних загроз на об'єктах критичної інфраструктури, що охороняються.

Досягнення поставленої мети необхідно послідовно вирішити такі наукові завдання. По-перше, проаналізувати появу і трансформації поняття ризику (стосовно об'єкта критичної інфраструктури, що охороняється). По-друге, дати характеристику терористичного акту та терористичних загроз. По-третє, розглянути методи аналізу ризику стосовно терористичних загроз на об'єктах критичної інфраструктури, що охороняються.

4. Методологія дослідження

Для реалізації мети дослідження проведемо її декомпозицію та застосовано такі методи наукового пізнання: методи теорії ймовірностей та математичної статистики, теорії нечітких множин та інтервальної математики, теорії ризиків та моделювання динамічних процесів.

5. Результати

5.1. Поява і трансформація поняття ризику (стосовно об'єкта критичної інфраструктури, що охороняється)

У суцільних природних середовищах, до яких відноситься і водне середовище, і атмосфера, пружні і інерційні сили обумовлені, відповідно, пружною взаємодією часток

середовища і інерцією їх маси. В таких середовищах з розподіленими параметрами можна порушити коливання стиснення і розрідження, що поширюються з певною швидкістю. У рідинах і газах, що характеризуються лише об'ємної пружністю, можуть виникати поздовжні акустичні хвилі, в яких напрямок коливань частинок середовища збігається з напрямком поширення хвилі [4].

Поняття ризику, на думку Макса Фасмера (відомого лінгвіста), є терміном, взятим із французької та італійської мов, які, у свою чергу, запозичили його з давньогрецької від слова, що означає скеля або підніжжя гори. Звідси термін "ризикувати" перекладається з французької та італійської як "лавірувати між скель" [1,2].

Деякі автори поняття ризику застосовують до реального явища (ризик пожежі або загоряння, ризик аварійної події), інші – до моделі реального явища, побудованої за допомогою тих чи інших математичних засобів, наприклад, апарату теорії ймовірностей та математичної статистики, теорії нечітких множин, інтервальної математики. Тоді ризик – це характеристика ситуації, має невизначеність результату за обов'язкового наявності несприятливих наслідків [5]. Він може застосовується для опису реальної події, а під ризиком розуміється ймовірність виникнення збитків чи отримання менших доходів проти прогнозованим варіантом [6]. Йти на ризик, тобто чекати на можливу небезпеку або діяти, сподіваючись на щасливий результат. І тут ризик – це небажана можливість.

У той самий час розробки автоматизованих систем прогнозування і запобігання подій на транспорті і небезпечних виробництвах ризик – це міра кількісного багатокомпонентного виміру небезпеки. Вона, з одного боку, включає величини очікуваного збитку від впливу загроз для безпеки, з іншого визначає ймовірності виникнення цих загроз.

Наявність загальних підходів, понять та термінів у єдиній теорії ризику дозволяє одноманітно розвивати його приватні теорії [7-9]. Ця теорія пропонує класифікацію ризиків, умовно поділених на шість груп.

У першу групу входять планетарні ризики, що відбуваються лише на рівні планети Земля загалом. Це стихійні лиха такі як землетруси та виверження вулканів, цунамі та повені, смерчі чи урагани. Це – ризики, пов'язані з космічним простором, наприклад, зіткнення Землі з астероїдом або зміна магнітних полюсів планети Земля, ризики світових епідемій насамперед небезпечних для життя. Це ризик настання світової фінансової кризи чи світової економічної кризи; ризики, пов'язані зі зміною клімату, як глобальне потепління чи похолодання та інше.

Друга група – глобальні ризики, що виникають лише на рівні однієї чи кількох держав. Це ризики виникнення революцій, переворотів, змов; ризики, пов'язані із зміною політичного чи економічного курсу держави. Це ризик озброєної агресії чи терористичних актів; ризики міжнародних санкцій чи дефолту. Це демографічні та міграційні ризики; ризик, пов'язаний із голодом. Сюди також належать ризики виникнення глобальних техногенних катастроф, наприклад, на атомних електростанціях чи хімічному підприємстві; екологічні ризики та ризики виснаження природних ресурсів.

Третя група визначається як фінансові ризики. Це інфляційний ризик (ризик того, що при зростанні цін одержувані грошові доходи з погляду реальної купівельної спроможності знецінюються швидше, ніж зростають); ризики зміни ставок за відсотками та зміни курсів валют. До цієї групи входять ризики, пов'язані з нестабільністю законодавства та інші.

До четвертої групи входять комерційні ризики. Це ризики лише на рівні безпосереднього оточення компанії.

П'ята група – це виробничі (внутрішні) ризики. Це ризики помилок при проектуванні продукції та технології виробництва; ризик виробництва дефектної продукції. Це ризики, пов'язані з промисловою безпекою, та екологічні ризики у процесі виробництва; соціальні

ризики на виробництві та ризики персоналу. Це також ризики втрат, не пов'язаних зі свідомою діяльністю людей, та інше.

Шоста група – особисті ризики. Це ризик захворювання чи раптової смерті; ризик нестачі засобів існування та ризик нещасного випадку, що не призводить до смерті; ризик зазнати впливу кримінальних елементів та інше.

Нині за критичною інфраструктурою в Євросоюзі та в Україні розуміють сукупність підприємств, мереж, систем, вихід з ладу або порушення функціонування яких може спричинити втрату управління або завдати істотних збитків на загальнодержавному, регіональному, місцевому чи об'єктовому рівні. До її складу входять атомні та гідроелектростанції, хімічні та нафтохімічні комбінати, металургійні заводи та безліч інших державних підприємств та приватних установ стратегічного призначення, які так само прийнято називати об'єктами критичної інфраструктури, що охороняються. Висновок зі стоячи саме цих об'єктів завдає найбільш згубного впливу на економіку держави.

Суспільно небезпечні наслідки залежно від конкретної шкоди поділяються на матеріальні (фізичні (збитки життю або здоров'ю людини) та майнову шкоду) та нематеріальні (політичні, правові, інформаційні шкоди). Матеріальні збитки в залежності від розмірів можуть бути значними, великими і особливо великими.

Суспільно небезпечні наслідки на об'єктах критичної інфраструктури, що охороняються (ОКІО), наступають в результаті певного впливу, що викликає порушення нормальних умов існування і функціонування цих об'єктів і навколишніх територій і акваторій. Цей вплив, як правило, може бути у формі різних інцидентів (неприємних подій, випадковостей, зіткнень) технічних та технологічних, природних та екологічних, економічних та психологічних, соціальних та інших. Вони виявляються на ОКІО як збої та відмови, пригоди та аварії, вибухи та пожежі, обвалення та катастрофи та призводять до зупинки або обмеження функціонування цих об'єктів.

Таким чином, стосовно об'єкту критичної інфраструктури що охороняється, ризик – це міра кількісного багатокомпонентного виміру небезпеки з включенням величини шкоди від впливу загроз, що виявляються у формі технічних та технологічних, природних та екологічних, економічних та психологічних, соціальних та інших інцидентів.

5.2. Характеристика терористичного акту та терористичних загроз

У загальному випадку під терористичною загрозою розуміють сукупність умов і факторів, що створюють небезпеку навмисного протиправного знищення або заподіяння шкоди об'єкту, загибелі людей, заподіяння їм значної майнової шкоди із застосуванням холодної, вогнепальної зброї, вибухових речовин або наслідків інших суспільно небезпечних. На ОКІО суспільно небезпечні наслідки виявляються як збої та відмови, пригоди та аварії, вибухи та пожежі, обвалення та катастрофи та призводять до зупинки або обмеження функціонування цих об'єктів. Безумовно, ці події можуть статися з різних причин, але наявність у діях суб'єктів прямого наміру вчинити злодіяння (злого наміру) є ознакою терористичної загрози.

Підготовка терористичного акту є досить тривалим та потайливим процесом і, як правило, описуватиметься сценарієм у вигляді певної послідовністю подій чи дій. Для конкретизації галузі опису підготовки терористичних актів вважатимемо, що метою теракту є ОКІО, такий як АЕС, підприємства ядерно-паливного циклу (ЯПЦ), підприємства з зберігання та переробки радіоактивних відходів, хімічні та нафтопереробні виробництва та інші державні та недержавні установи, що мають систему фізичного захисту.

Підготовка будь-якого теракту починається з формування його мети, тобто, яку країну, політичну партію, організацію або її лідера зазнати терористичного впливу. Про кінцеву мету теракту, як правило, може знати дуже обмежене коло людей. Це перший етап.

Коли мету визначено, починається другий етап – детальне вивчення об'єкта майбутнього теракту, людей, які працюють на ньому та обслуговують його, систем його управління, обслуговування та комунікацій. Збір інформації може здійснюватися як спеціально підготовленими та навченими терористами, так і людьми, які не мають жодного уявлення про те, що вони беруть участь у цьому процесі. Це може відбуватися в період відвідування об'єкта різними представництвами та делегаціями, природоохоронними структурами та організаціями щодо дотримання правил техніки безпеки. А також у період зустрічей ветеранів та пусків нових черг об'єкта, внаслідок обміну думками на відомчих та міжнародних конференціях та інше. Збір інформації про об'єкт, розпочавшись один раз, вже більше не припиняється і продовжується на всіх подальших етапах теракту та після його закінчення.

Завдання третього етапу – це виявлення вразливих місць об'єкта спеціалістами у різних сферах його діяльності, як правило, які не підозрюють про існування один одного. Одні визначають стійкість пожежних та рятувальних систем, інші оцінюють живучість та захищеність засобів зв'язку та управління персоналом, треті виконують експертизу місцевих погодних, геологічних та інших природних умов, що впливають на функціонування об'єкта. Отримані оцінки стану вразливих місць об'єкта планованого терористичного акту концентруються лише в руках. Починається четвертий етап – вироблення задуму терористичного акту, який може формуватися як майбутніми виконавцями, і їх ідейними натхненниками. Це можуть бути спеціально найняті експерти в галузі кризових ситуацій, які роблять науково обґрунтовані висновки про те, за яких умов уразливі місця об'єкта провокують надзвичайні ситуації та якого масштабу.

П'ятий етап – етап планування теракту, який також виконують спеціалісти у відповідній галузі.

Шостий етап – використання об'єкта майбутніх виконавців чи співвиконавців і доопрацювання плану. Працевлаштування відбувається спочатку легально і на перший погляд не викликає жодних побоювань навіть у кадрових органів підприємства. Можливий і інший варіант – підкуп чи шантаж посадових осіб підприємства для вирішення цілком конкретних завдань, а саме: уточнення специфічних виробничих питань, визначення прихованих схильностей працівників та особливостей їхнього характеру. Наприклад, хто зі співробітників і як сумлінно ставиться до радіаційного контролю в спецзоні АЕС (пунктуально виконує всі заходи або схильний до прояву недбалості, має фінансові проблеми в сім'ї, цікавиться виключно можливістю швидкого збагачення тощо, тощо). Знаючи ці та безліч інших особливостей людського фактора можна впливати на технологічний процес об'єкта, що вивчається, загострюючи ситуацію в його вразливих місцях. З урахуванням усіх виявлених специфічних особливостей об'єкта остаточно коригується сценарій запланованого теракту.

Сьомий етап – формування стійкої ударної сили, як правило, з людей, які пройшли спеціальну підготовку, які побували в гарячих точках або раніше брали участь в інших силових акціях. Ударна сила завчасно вивчає об'єкт, формує основу підготовки подалі від об'єкта, ніж привертати увагу, потай приїжджає місце і знайомиться з нею у безпосередній близькості.

Восьмий етап – зосередження ударних сил – безпосередніх виконавців та необхідних засобів – зброї, боєприпасів, засобів зв'язку, за допомогою яких можливе проникнення на об'єкт та реалізація задуманого плану теракту. Люди та зброя різними шляхами прибувають у райони, що знаходяться у безпосередній близькості до об'єкту теракту.

Дев'ятий етап – безпосередня підготовка до теракту, коли виконавці займають вихідні позиції.

Десятий етап – виконання теракту.

На думку окремих вітчизняних і зарубіжних фахівців, перші п'ять етапів підготовки терактів мають дуже високу скритність. У формуванні мети теракту, розробці його задуму може брати участь необмежену кількість зацікавлених осіб. Дослідження об'єктів критичної інфраструктури може бути побудовано за системним принципом у вигляді соцопитувань, маркетингових досліджень та інше, при цьому можуть залучатись офіційні державні установи та громадські організації, що з погляду міжнародного права не є протизаконним. Далі відбувається використання агентів на об'єкт шляхом влаштування працювати чи вербуванням морально нестійких співробітників, з допомогою яких виконується дослідження безпосередньо технологічних і виробничих особливостей у сфері коригування сценарію теракту. Ці дії вже підлягають кримінальної відповідальності, і тому мають своєчасно виявлятися і припинятися добре поставленої оперативно-розшукової діяльністю.

Шостий – десятий етапи розвитку теракту на критично важливому об'єкті носять явно ворожий характер: проникнення на об'єкт у вигляді порушення роботи його пропускної системи, відкритий напад – прорив периметра, що охороняється, захоплення посадових осіб або членів їх сімей. Подібні дії повинні рішуче припинятися системою фізичного захисту об'єкта, що охороняється.

Таким чином, типовий сценарій теракту складається з десяти етапів, а саме: формування мети теракту, вивчення об'єкта теракту, виявлення його вразливих місць, формування задуму, планування теракту, впровадження на об'єкт та доопрацювання плану, формування стійкої ударної сили, зосередження ударних сил та засобів, безпосередня підготовка до теракту та його виконання.

Терористичні загрози на об'єктах критичної інфраструктури, що охороняються, це можливі суспільно небезпечні наслідки зловмисних дій, які призводять до зупинення або обмеження функціонування цих об'єктів.

5.3. Методи аналізу ризику стосовно терористичних загроз на об'єктах критичної інфраструктури, що охороняються

При вирішенні різних прикладних завдань, у числі аналізу терористичних загроз, можуть застосовуватися такі методи. Це детерміновані; імовірнісно-статистичні (статистичні, теоретико-ймовірнісні та ймовірнісно-евристичні); методи, що застосовуються в умовах невизначеності нестатистичної природи (нечіткі та нейромережні) та комбіновані, що включають різні комбінації перерахованих вище методів. Послідовно розглянемо їх.

Детерміновані методи передбачають аналіз етапів розвитку аварій, починаючи від вихідної події через послідовність передбачуваних відмов до кінцевого стану, що встановився. Хід аварійного процесу вивчається та передбачається за допомогою математичних імітаційних моделей. Недоліками методу є: потенційна можливість прогаяти рідко реалізовані, але важливі ланцюжки розвитку аварій; складність побудови досить адекватних математичних моделей; необхідність проведення складних та дорогих експериментальних досліджень.

Імовірнісно-статистичні методи аналізу ризику передбачають як оцінку ймовірності виникнення аварії, і розрахунок відносних ймовірностей тієї чи іншої шляху розвитку процесів. При цьому аналізуються розгалужені ланцюжки подій та відмов, вибирається відповідний математичний апарат та оцінюється повна ймовірність аварії. Розрахункові математичні моделі у своїй можна значно спростити проти детермінованими методами. Основні обмеження методу пов'язані з недостатньою статистикою щодо відмов обладнання. Крім того, застосування спрощених розрахункових схем знижує достовірність оцінок ризику для важких аварій. Проте, імовірнісний метод нині вважається одним із найперспективніших. На його основі побудовано різні методики оцінки ризиків. Залежно від наявної вихідної інформації вони поділяються на три групи. Перша – статистичні, коли ймовірності

визначаються за наявними статистичними даними (за наявності). Друга – це теоретико-імовірнісні методики. Їх використовують з оцінки ризиків від рідкісних подій, коли статистика практично відсутня. Третя група – імовірнісно-евристичні методики, що ґрунтуються на використанні суб'єктивних ймовірностей, одержуваних за допомогою експертного оцінювання. Вони використовуються в оцінці комплексних ризиків від сукупності небезпек, коли відсутні як статистичні дані, а й математичні моделі (чи їх точність занадто низька).

Методи аналізу ризику в умовах невизначеностей нестатистичної природи призначені для опису невизначеностей джерела ризику, пов'язаних з відсутністю або неповнотою інформації про процеси виникнення та розвитку аварії; людськими помилками; припущення застосовуваних моделей для опису розвитку аварійного процесу.

Усі перелічені вище методи аналізу ризику поділяють за характером вихідної та результуючої інформації на якісні та кількісні.

Методи кількісного аналізу ризику характеризуються розрахунком показників ризику. Проведення кількісного аналізу потребує високої кваліфікації виконавців, великого обсягу інформації щодо аварійності, надійності обладнання, обліку особливостей навколишньої місцевості, метео умов, часу перебування людей на території та поблизу об'єкта, щільності населення та інших факторів.

Складні та дорогі розрахунки найчастіше дають значення ризику, точність якого невелика. Для небезпечних виробничих об'єктів точність розрахунків індивідуального ризику, навіть у разі наявності всієї необхідної інформації, не вище за один порядок. При цьому проведення кількісної оцінки ризику корисніше для порівняння різних варіантів (наприклад, розміщення обладнання), ніж для висновку про рівень безпеки об'єкта. Досвід показує [25-28], що найбільший обсяг рекомендацій щодо забезпечення безпеки виробляється із застосуванням якісних методів аналізу ризику, які використовують менший обсяг інформації та витрат праці. Проте кількісні методи оцінки ризику завжди дуже корисні, а деяких ситуаціях – єдино допустимі порівняння небезпек різної природи і за експертизі небезпечних виробничих об'єктів.

Необхідно зазначити, що при оцінці різних загроз на об'єктах критичної інфраструктури, що охороняються, дефіцит статистичних даних. Тому можливості застосування точних математичних методів обмежені відсутністю достатньої статистичної інформації, а також відсутністю надійних математичних моделей, що описують реальний стан системи фізичного захисту об'єкта, що охороняється. Внаслідок цього використовуються імовірнісно-евристичні методи, що ґрунтуються на використанні суб'єктивних ймовірностей, що отримуються за допомогою експертного оцінювання.

Виділяють два рівні використання експертних оцінок: якісний та кількісний. На якісному рівні визначаються можливі сценарії розвитку небезпечної ситуації через відмову системи, вибір остаточного варіанта вирішення та інше. Точність кількісних (бальних) оцінок залежить від наукової кваліфікації експертів, їх здібностей оцінювати ті чи інші стани, явища, шляхи розвитку ситуації. Тому для аналізу різних джерел небезпеки на ООКИ методи на основі експертних оцінок можуть використовуватися для побудови сценаріїв розвитку аварій, пов'язаних із відмовами технічних засобів, обладнання та установок; для ранжування джерел небезпеки.

Таким чином, для аналізу ризику стосовно терористичних загроз на об'єктах критичної інфраструктури, що охороняються, можуть використовуватися детерміновані; імовірнісно-статистичні (статистичні, теоретико-імовірнісні та імовірнісно-евристичні); методи, що застосовуються в умовах невизначеності нестатистичної природи (нечіткі та нейромережеві) та комбіновані, що включають різні комбінації перерахованих вище методів. Всі ці методи так само поділяються за характером вихідної та результуючої інформації на якісні та кількісні.

Дефіцит статистичних даних при оцінці різних загроз на об'єктах критичної інфраструктури, що охороняються, забезпечив домінування імовірнісно-евристичних методів, що ґрунтуються на використанні суб'єктивних ймовірностей, одержуваних за допомогою експертного оцінювання.

6. Обговорення

Наукова новизна результатів дослідження та їх практичне значення підтримані у ході дискусії між науково-педагогічним складом кафедри логістики Повітряних Сил інституту авіації та протиповітряної оборони Національного університету оборони України імені Івана Черняховського.

7. Висновки

Щодо охоронюваного об'єкта критичної інфраструктури ризик – це міра кількісного багатокомпонентного виміру небезпеки з включенням величини шкоди від впливу загроз, що виявляються у формі технічних та технологічних, природних та екологічних, економічних та психологічних, соціальних та інших інцидентів. Вони проявляються як збої та відмови, пригоди та аварії, вибухи та пожежі, обвалення та катастрофи та призводять до зупинки або обмеження функціонування цих об'єктів.

Типовий сценарій теракту складається з десяти етапів, а саме: формування мети теракту, вивчення об'єкта теракту, виявлення його вразливих місць, формування задуму, планування теракту, впровадження на об'єкт та доопрацювання плану, формування стійкої ударної сили, зосередження ударних сил та засобів, безпосередня підготовка до теракту та його виконання.

Терористичні загрози на об'єктах критичної інфраструктури, що охороняються, це можливі суспільно небезпечні наслідки зловмисних дій, які призводять до зупинення або обмеження функціонування цих об'єктів.

Для аналізу ризику стосовно терористичних загроз на об'єктах критичної інфраструктури, що охороняються, можуть використовуватися детерміновані; імовірнісно-статистичні (статистичні, теоретико-ймовірнісні та імовірнісно-евристичні); методи, що застосовуються в умовах невизначеності нестатистичної природи (нечіткі та нейромережеві) та комбіновані, що включають різні комбінації перерахованих вище методів. Всі ці методи так само поділяються за характером вихідної та результуючої інформації на якісні та кількісні.

Дефіцит статистичних даних при оцінці різних загроз на об'єктах критичної інфраструктури, що охороняються, забезпечив домінування імовірнісно-евристичних методів, що ґрунтуються на використанні суб'єктивних ймовірностей, одержуваних за допомогою експертного оцінювання.

8. Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

9. Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Ризик – Вікіпедія. URL : https://ua.wikipedia.org/wiki/%D0%A0 % D0% B8% D1%81
2. Орлов А. И., Пугач О. В. Підходи до

References

1. Risk – Wikipedia. Available from : https://ua.wikipedia.org/wiki/%D0%A0 %D0% B8% D1%81
2. Orlov A.I., Pugach O.V. Approaches to the

загальної теорії ризику.
3. Бланк И. А. Управління фінансовими ризиками. – К.: Ніка-Центр, 2005. – 600 с.
4. Гончаренко Ю. Ю., Дивізінюк, М. М. Рижкін А. С. Особливості надзвичайних ситуацій, що призводять до забруднення атмосфери радіоактивними і отруйними речовинами. Вимірювальна та обчислювальна техніка в технологічних процесах. – Хмельницький: Хмельницький національний університет, 2016. – № 56. –С. 132 – 135.
5. Презентація на тему: Управління ризиками. URL : http://www.myshared.ua/slide/634569/
6. Азаренко, О., Гончаренко, Ю., Дівізінюк, М., Мірненко, В., & Сириця, Ю. (2020). Структурно-логічна модель управління надзвичайно ситуацією терористичного характеру та її особливостей, вбудованих скритим електромагнітним впливом на оперативний состав охороняемого об'єкта критичної інфраструктури. *Journal of Scientific Papers «Social Development and Security»*, *10*(1), 177-187. DOI : 10.33445/sds.2020.10.1.18
7. Азаренко О. В., Гончаренко Ю. Ю.,. Дивизинюк М. М, Коноваленко Н. В. Особливості радіолокаційної інформації як засоби запобігання надзвичайним ситуаціям терористичного характеру. Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – Київ: Державна служба спеціального зв'язку та захисту інформації в Україні НТУУ «КПІ», 2016. – Вип 2 (32). – С. 28 – 39.
8. Азаренко О. В. Захист критичної інфраструктури держави від терористичного впливу / О. В. Азаренко, Ю. Ю. Гончаренко, М. М. Дивізінюк, М. І. Ожиганова // К.: ІГНС НАНУ, 2018. 84 с. (ISBN 978-617-7187-25-6).
9. Ліпкан В.А. Інформаційна безпека України

general theory of risk.
3. Blank I.A. Upravlinnya finansovymy ryzykamy [Financial risk management]. Kyiv: Nika-Center, 2005. 600 p.
4. Honcharenko, Yu.Yu.,. Divizinyuk, M.M, Ryzhkin, A.S. (2016). Osoblyvosti nadzvychaynykh sytuatsiy, shcho pryzvodyat' do zabrudnennya atmosfery radioaktyvnymy i otruynymy rechovynamy [Peculiarities of emergency situations that lead to contamination of the atmosphere with radioactive and poisonous substances]. *Measuring and Computing Techniques in Technological Processes*. No. 56. P. 132-135.
5. Presentation on the topic: Risk management. Available from : http://www.myshared.ua/ slide/634569/
6. Azarenko, E., Honcharenko, Y., Divizinyuk, M, Mirnenko, V., & Syrytsia, I. (2020). Structural-logical model of emergency situation management of terrorist character and its features caused by latent electromagnetic influence on the operational staff of the guarded facility of critical infrastructure. *Journal of Scientific Papers «Social Development and Security»*, *10*(1), 177-187. DOI : 10.33445/sds.2020.10.1.18
7. Azarenko O.V., Honcharenko, Yu. Yu., Divyzynyuk, M. M., Konovalenko N. V. (2016). Osoblyvosti radiolokatsiynoyi informatsiyi yak zasoby zapobihannya nadzvychaynym sytuatsiyam terorystychnoho kharakteru [Peculiarities of radar information as a means of preventing emergency situations of a terrorist nature]. *Legal, regulatory and metrological support of information protection systems in Ukraine*., Issue 2 (32). P. 28-39.
8. Azarenko O.V., Honcharenko, Yu.Yu., Divizinyuk, M.M., Ozhiganova, M.I. (2018). Protection of the state's critical infrastructure from terrorist influence. Kyiv: IGNS of the National Academy of Sciences of the National Academy of Sciences, 2018. 84 p. (ISBN 978-617-

в умовах євроінтеграції: Серія «Національна і международная безпека». – К.: КНТ, 2006. –206 с.
10. Xovard B. Lazeracustic. Optronics. Sincepress. 1991. vol. 10. №10. p. 89-100.
11. Audio Inteligence Devices. Product Catalog, 2012. – 402 p.
12. Wenzel F. D6.1 – Decision-analytic frameworks for multi-hazard mitigation and adaptation, New methodologies for multi-hazard and multi-risk assessment meth-ods for Europe, Deliverable 6.1, 2012. 34 p. URL : http://matrix.gpi.kit.edu/ downloads/MA-TRIX-D6.1.pdf.

7187-25-6).
9. Lipkan V.A. Information security of Ukraine in the conditions of European integration: "National and international security" series. Kyiv: KNT, 2006. 206 p.
10. Xovard B. Lazeracoustic // Optronics. Sincepress. 1991. vol. 10. №10. p. 89-100.
11. Audio Intelligence Devices // Product Catalog, 2012. – 402 p.
12. Wenzel F. D6.1 – Decision-analytic frameworks for multi-hazard mitigation and adaptation, New methodologies for multi-hazard and multi-risk assessment methods for Europe, Deliverable 6.1, 2012. 34 p. Available from : http://matrix.gpi.kit.edu/ downloads/MA-TRIX-D6.1.pdf.