http://doi.org/10.35668/2520-6524-2025-1-07
УДК 351:001.8:519.2

М. М. ДІВІЗІНЮК, д-р фіз.-мат. наук, проф.
О. В. ФАРРАХОВ, канд. техн. наук
Б. О. АВРАМЧУК, канд. екон. наук
Є. В. КОЧЕЛАБ, канд. фіз.-мат. наук
Р. С. САВІЦЬКИЙ, ст. викладач

КРИТИЧНА ІНФРАСТРУКТУРА ДЕРЖАВИ ТА ОСНОВНІ МЕТОДИ ОЦІНКИ РИЗИКІВ

Резюме. *Наведено параметри різновидів критичної інфраструктури держави та показано, що до її складу входять атомні та гідроелектростанції, хімічні й нафтохімічні комбінати, металургійні заводи та безліч інших державних підприємств і приватних установ стратегічного призначення.*

Розглянуто критичну інфраструктуру як сукупність підприємств, мереж, систем, вихід з ладу або порушення функціонування яких може призвести до втрати управління або завдати істотних збитків на загальнодержавному, регіональному, місцевому чи об'єктовому рівнях. До всіх складних техногенних об'єктів застосовується системний підхід у забезпеченні їхньої безпеки.

Акцентовано на тому, що всі європейські держави виділяють поняття «критичні національні інфраструктури», яке розуміють як комплекс систем, порушення функціонування однієї з яких може завдати серйозної шкоди економіці держави чи призвести до негативних соціальних наслідків для суспільства.

Здійснено аналіз наявних методів та концепцій дослідження загроз і ризиків. Розглянуто головні методи аналізу загроз і ризиків із позицій технократичної концепції, окреслено їхні переваги та недоліки.

Зазначено, що до всіх складних техногенних об'єктів застосовується системний підхід у гарантуванні їхньої безпеки, що передбачає ідентифікацію об'єктивних небезпек, визначення та ранжування загроз, оцінку ризику їх прояву та складання прогнозу, що робиться на користь запобігання катастрофічним подіям, обумовленим об'єктивними небезпеками.

Найбільш ефективними методами оцінки загроз і ризиків є методи, що інтегровані до систем моніторингу, системи підтримки прийняття рішень та інших систем автоматизованого управління. Події останніх років в Україні вимагають визначення терористичної загрози як першочергової та найголовнішої.

Ключові слова: *критична інфраструктура, катастрофічна подія, надзвичайна ситуація, терористична загроза, системний підхід, ранжування загроз, оцінка ризиків.*

ВСТУП ПОСТАНОВКА ПРОБЛЕМИ

Гарантування безпеки, охорона та захист стратегічних об'єктів від різних видів надзвичайних ситуацій — один зі складників державної безпеки України. Кількість цих об'єктів досить значна [1–3].

Безпека об'єкта, що охороняється, оцінюється ризиком настання будь-якої (самої неймовірної, гіпотетичної, іноді, що межує з фантастикою) катастрофічної події. Загальні або сумарні витрати, які йдуть на гарантування безпеки об'єкта, що охороняється, охоплюють дві складові. Перша — це витрати на запобігання чи недопущення катастрофічної події. Друга — це витрати на ліквідацію наслідків у разі настання катастрофічної події [4; 5]. Це стосується і гарантування безпеки конгломерації об'єктів критичної інфраструктури, що охороняються, тобто сукупності взаємопов'язаних основних виробництв, допоміжних підприємств, структур, що забезпечують об'єкт, житлових масивів, розташованих разом на обмеженій території (наприклад, електростанція і місто-супутник, прибережна зона і місто-порт).

Метою статті, з огляду на вищевикладене, є опис типів об'єктів критичної інфраструктури та методи оцінки ризиків настання катастрофічної події.

ВИКЛАДЕННЯ ОСНОВНОГО МАТЕРІАЛУ ХАРАКТЕРИСТИКА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Термін "інфраструктура" утворюється від злиття двох латинських слів *infa* — "нижче, під", і *struktura* — "структура, розташування". Інфраструктура — це комплекс взаємопов'язаних обслуговуючих об'єктів або структур, що становлять і забезпечують основу функціонування системи.

До головних типів інфраструктур можна зарахувати:

- соціальну інфраструктуру як сукупність галузей і підприємств, які забезпечують нормальну життєдіяльність населення;
- транспортну інфраструктуру як сукупність галузей і підприємств транспорту;
- інженерну інфраструктуру як сукупність систем інженерно-технічного забезпечення будівель і споруд та багато інших [6].

Між наявними інфраструктурами існують складні зв'язки та взаємовідносини. Наприклад, інфраструктура економіки являє собою сукупність галузей і видів діяльності, що обслуговують виробництво і господарство загалом, і охоплює інфраструктури важкої та легкої промисловості, енергетики, транспорту тощо. Транспортна інфраструктура натомість складається з інфраструктур авіаційного та залізничного транспорту, морського та річкового флотів, регіональних і міських транспортних інфраструктур.

У державних інфраструктурах є низка специфічних інфраструктур, які повноцінно функціонують за наявності закордонних, зовнішніх зв'язків:

- інноваційна, яка обслуговує інноваційну діяльність;
- ринкова, що забезпечує вільний рух товарів і послуг;
- інформаційна тощо.

Є й інші спеціалізовані інфраструктури (наприклад, військова), діяльність яких має закритий характер.

Під національною чи державною інфраструктурою прийнято розуміти комплекс усіх галузей промисловості та сільського господарства, споруд, установ, транспорту та комунікаційних мереж, що дають змогу забезпечити життєдіяльність організацій і виробництв цієї країни, наприклад, залізниці та автомобільні дороги, трубопроводи та лінії електропередач, стаціонарні та розвідні мости, аеродроми та порти, житлові будинки та виробничі споруди, електростанції та сховища різного призначення, телефон та телеграф, радіо та телебачення, інтернет та інші засоби масової інформації [7].

В інфраструктурі суверенної держави особливо виділяють мережі, системи та сектори (сукупність елементів різних інфраструктур), від безпечної діяльності яких залежить стан навколишнього природного середовища, здоров'я і життя громадян та існування суспільства загалом. Комплекс таких секторів, систем або мереж, вихід з ладу чи порушення функціонування яких здатне призвести до кризи на загальнодержавному, регіональному або місцевому рівнях, почали називати критичною інфраструктурою [8].

Наприкінці XX ст. у зв'язку зі зростанням терористичної загрози в розвинених країнах розпочалися дискусії щодо вразливості національних інфраструктур. Увага експертів була спрямована не лише на інформаційні (кібернетичні) інфраструктури, а й на всі інші сфери забезпечення життєдіяльності суспільства.

Серед країн Європи проблематикою забезпечення безпеки об'єктів критичної інфраструктури першими почали займатися у Великій Британії, де було дано визначення критичної національної інфраструктури як сукупності систем, які насамперед важливі для функціонування держави. До них були зараховані об'єкти, ліквідація або порушення роботи яких могла б наразити на загрозу життя громадян, завдати серйозних негативних економічних або соціальних збитків для суспільства загалом або значної його частини. Це органи державного управління та рятувальні служби, джерела теплової та електричної енергії. Це сховища палива, водопровід, каналізація та телекомунікації. Це продовольство та санітарія (утилізація сміття), фінанси та економіка, комунікаційні мережі та служби, юстиція та захист громадського порядку. Це соціальне обслуговування, освіта та наука, прогноз та інформування про екстремальні гідрометеорологічні явища.

У 1998 р. доктриною 63-го президента США критичну інфраструктуру було визначено як сукупність основних систем, які мають матеріальну або віртуальну платформу та впливають на фундаментальність економіки держави — це телекомунікації, енергосистеми, банківський та фінансовий сектори, транспортна система, система водопостачання та рятувальні служби.

Усі європейські держави згодом також стали виділяти критичні національні інфраструктури, які визначали як комплекс систем, порушення функціонування однієї з яких може завдати серйозної шкоди економіці держави або призвести до негативних соціальних наслідків для суспільства.

Після подій 11 вересня 2001 р. в лютому 2003 р. в США було прийнято Національну стратегію фізичної охорони критичної інфраструктури. У порівнянні з доктриною 1998 р. до її складу були включені ядерні електростанції, греблі, хімічна промисловість, сховища небезпечних речовин, бази оборонної промисловості.

Наразі в країнах ЄС визначено, що критична інфраструктура охоплює фізичні об'єкти, ресурси, послуги та інформаційно-технічні засоби, мережі та інші інфраструктурні активи, порушення чи знищення яких призводить до серйозних наслідків для здоров'я, безпеки чи економічного

добробуту громадян або ефективного функціонування уряду.

В Україні на законодавчому рівні критична інфраструктура з'явилася у 2017 р. та остаточно оформилася у 2022 році. Відповідний Закон України містить основні визначення, що відповідають європейським стандартам.

Таким чином, критичну інфраструктуру варто розуміти як сукупність підприємств, мереж, систем, вихід із ладу або порушення функціонування яких може спричинити втрату управління чи завдати істотних збитків на загальнодержавному, регіональному, місцевому чи об'єктовому рівнях. До критичної інфраструктури належать атомні та гідроелектростанції, хімічні та нафтохімічні комбінати, металургійні заводи та безліч інших державних підприємств і приватних установ стратегічного призначення.

Головні методи оцінки ризиків: переваги та недоліки

Завдання аналізу загроз полягають у виявленні причиново-наслідкових зв'язків дії певних факторів, що визначають загрози на конкретних об'єктах, та настання катастрофічних подій, викликаних цими загрозами.

Завдання оцінки ризиків — це якісне визначення чи кількісний розрахунок можливості наступу катастрофічних подій на конкретних об'єктах, викликаних погрозами, що розглядаються.

Визначають вісім основних груп методів оцінки загроз і ризиків: детерміновані, імовірнісні (теоретико-імовірнісні), статистичні, експертні, евристичні, комбіновані, нечіткі, нейромережеві.

Детерміновані методи передбачають аналіз етапів розвитку катастрофічної події, починаючи від обраного початкового стану об'єкта, що розглядається, через послідовність передбачуваних відмов, негативних (помилкових) дій та інших факторів, що впливають, до певного (вибраного, встановленого, проміжного) кінцевого стану. Розвиток катастрофічної події (виникнення аварійної ситуації, розвиток небезпечного явища як пожежі, затоплення, антропогенного забруднення тощо) вивчається та передбачається за допомогою моделей. Модель – це штучно створений новий об'єкт, який відображає суттєві особливості прототипу, що вивчається: об'єкта, явища або процесу. Так, під час дослідження загроз і ризиків стосовно небезпечного об'єкта можуть використовуватися детерміновані, стохастичні, лінгвістичні, математичні, ігрові, евристичні та інші моделі. Головна особливість детермінованих моделей полягає в тому, що даючи аналітичне уявлення закономірності як сукупності вхідних значень на виході системи можна отримати єдиний результат.

Детерміновані методи, що застосовуються до конкретних катастрофічних подій на ядерних об'єктах, можуть використовувати десятки моделей, кожна з яких застосовується для певного етапу технологічного циклу, конкретного технічного пристрою або організаційної структури. Ці методи передбачають наявність функціональних чи жорстко детермінованих зв'язків, коли кожному значенню факторної ознаки (складової частини загрози) відповідає цілком певне, а не випадкове значення результативної ознаки. Вони також передбачають порівняння будь-яких параметрів (наприклад параметрів безпеки) із заздалегідь заданими. Приймаючи в розрахунках найгірші варіанти подій, що призводять до катастрофічної ситуації, вказують конкретні умови розрахунків і можливі припущення, що виправдовує порівнянність результатів [9].

Переваги детермінованих методів: 1) достатній для різноманітних реальних ситуацій набір необхідних відомостей; 2) порівняна простота використання методів; 3) високий рівень завершеності елементів цих методів; 4) однозначність розв'язання задач; 5) детерміновані методи дають змогу зробити пріоритетний вибір із переліку заходів захисту від певного виду загроз, регламентованих нормами (керівними документами, такими як накази, інструкції, правила тощо) стосовно небезпечного об'єкта, що розглядається.

Недоліки детермінованих методів: 1) обмежена можливість варіювання, яка жорстко пов'язана з умовами створення детермінованої моделі; 2) складність побудови адекватних функціональних математичних моделей; 3) необхідність проведення складних і дорогих експериментальних досліджень; 4) наявність потенційної можливості упустити послідовності розвитку катастрофічних подій, що рідко реалізуються (аварій, природних катаклізмів тощо) [10].

Імовірнісний (у класичному розумінні цього терміна) метод — це неконструктивний метод доказу існування математичного об'єкта із заданими властивостями, що використовується переважно в комбінаториці та в теорії чисел, лінійній алгебрі та математичному аналізі, в інформатиці (наприклад, для ймовірнісного округлення) та теорії інформації. Метод полягає в оцінці ймовірності того, що випадковий об'єкт із заданого класу задовольняє потрібну умову. Якщо підтверджено, що ця можливість позитивна, то вважається, що об'єкт із необхідними якостями існує. Попри те, що при доказі

використовуються ймовірності, остаточний висновок робиться без будь-якої неоднозначності. Тим не менш, імовірнісний метод нині вважається одним із найбільш перспективних, що проявляється в одній із поширених його модифікацій, що отримала назву — теоретико-імовірнісний метод. Метод заснований на використанні ймовірнісних математичних моделей, в основу яких покладено закономірності переростання подій, що ініціюють у надзвичайні ситуації та настання катастрофічних подій. Це можуть бути декомпозиції завдань щодо оцінки спеціальних показників або визначення частоти (ймовірності) рідкісних негативних подій з урахуванням взаємозв'язку зі спеціальними показниками. Спеціальні показники визначають з аналізу джерел загроз і потенційних небезпек (наприклад, на території, що розглядається або ядерному об'єкті), статистик їх реалізації у формі ініціюючих подій, передбачуваних сценаріїв розвитку і наступних наслідків [11].

Імовірнісні (теоретико-імовірнісні) методи мають певні переваги. По-перше, вони можуть застосовуватися для оцінки частот або ймовірностей рідкісних катастрофічних подій із тяжкими наслідками, за якими статистика практично відсутня (наприклад, Трі-Майл-Айленд, Чорнобиль, Фукусіма). Ці події відбуваються в середньому один раз на декілька десятків років. Навіть відсутність цих катастроф упродовж досить тривалого часу не виключає їхньої появи в майбутньому. По-друге, подібна оцінка ризику цих катастроф протягом заданого проміжку часу є значним чинником, який необхідно враховувати під час планування соціально-економічного розвитку території, міста супутника ядерного об'єкта тощо. Вони дають змогу завчасно розробляти заходи, створені задля подолання соціально-політичних і психологічних наслідків цих катастроф. По-третє, розрахункові математичні моделі, що використовуються, можна істотно спростити в порівнянні з детермінованими методами.

Імовірнісні (теоретико-імовірнісні) методи мають також певні недоліки. По-перше, вони досить трудомісткі. Ці методи вимагають великої кількості розрахунків відносних ймовірностей розгалужених ланцюжків подій і відмов різних шляхів розвитку процесів, що аналізуються, необхідні оцінки повної ймовірності настання катастрофічного події. По-друге, застосування спрощених розрахункових схем знижує достовірність одержуваних оцінок ризику катастрофічних подій [12].

Статистичні методи оцінки ризику полягають у визначенні ймовірності виникнення негативних подій на основі статистичних даних попереднього періоду та встановленні областей (просторово-часових масштабів) ризику та інших характеристик ризику. Розмір чи ступінь, ризику вимірюється з допомогою двох головних показників. Це середнє очікуване значення та коливання можливого результату. Середня величина є узагальненою кількісною характеристикою. За її значенням досить важко ухвалити рішення на користь будь-якого варіанта. З цією метою вимірюється коливання, розмах отриманого результату. Коливання — це ступінь відхилення очікуваного значення результату від його середньої величини. Для визначення обчислюють дві статистичні величини: дисперсія і середнє квадратичне відхилення. Дисперсія і середнє відхилення є заходами абсолютного коливання. Вони вимірюються в тих же одиницях, що і ознака, яка варіює. Для аналізу ступеня відхилення часто використовується коефіцієнт варіації як відношення середнього квадратичного відхилення до середнього очікуваного значення, що дає змогу порівнювати коливання ознак, які мають різні одиниці виміру.

Окреслимо переваги статистичних методів: по-перше, можливість аналізу статистичних даних щодо несприятливих подій, що мали місце в минулому; по-друге, реалізованість теоретичного аналізу структури причиново-наслідкових зв'язків процесів, що генеруються розглянутими загрозами та небезпеками.

Недоліки статистичних методів: по-перше, необхідність використання в них імовірнісних характеристик; по-друге, можливість аналізу та оцінки різних варіантів розвитку подій і врахування різних факторів ризиків виключно в рамках одного підходу.

Експертні методи — це розв'язання завдань на основі судження (думки) висококваліфікованих фахівців у відповідній галузі знань. Вони використовуються в умовах повної невизначеності. Під час експертної оцінки подій (явищ) необхідно: чітко сформулювати мету дослідження; правильно визначити час здійснення подій; розробити організацію опитування (інтерв'ю) та анкетування; сформувати групу експертів; забезпечити взаємну незалежність їх суджень, відсутність авторитету посади чи особи, які впливають на вибір альтернатив, узагальнити отримані результати.

Відбір експертів для реалізації експертного аналізу відбувається на основі низки вимог. Зазвичай це компетентність у сфері прийняття рішень у предметній галузі та креативність (здатність до творчості). Відсутність особистої зацікавленості та нонконформізм (нездатність піддаватися впливу інших людей), здатність працювати в команді однодумців тощо. Кіль-

кість експертів залежить від багатьох факторів, але переважно воно визначається як мінімально необхідне. Методи експертного аналізу прийнято розділяти на індивідуальні та колективні. До індивідуальних належать анкетування, інтерв'ювання, аналітична експертна оцінка тощо, а до колективних — метод круглого столу та інверсії, коли експерти формулюють нові рішення у протилежному напрямку від заданого пошуком. Це метод емпатії (особистої аналогії — між логікою та інтуїцією) та синектики (коли експерти різних спеціальностей і кваліфікації, навчаються один у одного в процесі розв'язання проблеми). Метод критичних питань та мозкового штурму. Метод Дельфі — спосіб організації колективного інтелекту, розроблений у США в 1960-ті рр. для прогнозування впливу майбутніх наукових розробок. Метод сценаріїв передбачає створення технологій розробки сценаріїв, які забезпечують більш високу ймовірність вироблення ефективного рішення в тих ситуаціях, коли це можливо, і більш високу ймовірність зведення очікуваних втрат до мінімуму у тих ситуаціях, коли втрати неминучі. Це один із методів, що застосовуються в дослідженнях майбутнього. Сценарії є набір однаково переконливих історій, кожна з яких описує одне з потенційно можливих варіантів майбутнього.

Експертні методи мають певні переваги. По-перше, відносна простота застосування за умов повної невизначеності. По-друге, використання для дослідження процесів і проблем, що не піддаються математичній формалізації. По-третє, можливість отримання якісної та кількісної (рейтингової, бальної) оцінки.

Окреслимо також недоліки експертних методів. По-перше, трудомісткість та відносно велика тривалість експертиз. По-друге, необхідність повної поінформованості експертів про властивості, що досліджуються.

Евристичні методи оцінки ризику. Евристика – це наукова галузь, що вивчає специфіку творчої діяльності. У когнітивістиці (міждисциплінарному науковому напрямі, що об'єднує теорію пізнання, когнітивну психологію, нейрофізіологію, когнітивну лінгвістику, невербальну комунікацію і теорію штучного інтелекту) і поведінковій економіці (напрям економічних досліджень, який вивчає ухвалення економічних рішень окремими особами і установами) евристикою часто називають окремий розумовий прийом, який може призводити до помилок. Евристику також розуміють як мистецтво винаходу. Це керівництво про те, як методичним шляхом знаходити нове, причому індивід, який виконує пошук, робить помилки, навчається і знаходить нове правильне рішення. Тому евристичними методами вважають логічні прийоми та методичні правила наукового дослідження, які здатні забезпечити досягнення мети в критичних умовах. Ці умови характеризуються неповною початковою інформацією, а головне — відсутністю чіткої програми управління процесом розв'язання задачі. Нині розроблено та ефективно використовується декілька десятків евристичних методів, зокрема і для оцінки ризиків.

Багато хто з них повторює експертні методи, оскільки забезпечує оцінку в умовах невизначеності. Універсальних серед них немає, і в кожній конкретній ситуації рекомендовано застосовувати низку методів, оскільки головне їхнє призначення полягає в отриманні точної оцінки під час активізації творчої діяльності.

Переваги евристичних методів такі: по-перше, вони забезпечують вирішення завдання оцінки загроз і ризиків у критичних умовах, які характеризуються неповною початковою інформацією та відсутністю чіткої програми управління процесом розв'язання задачі; по-друге, сприяють навчанню та творчому розвитку експертів та залученого персоналу; по-третє, сприйнятливі (терпимі) до будь-якого новаторства.

Окреслимо недоліки евристичних методів. По-перше, припускають появу помилкових рішень. По-друге, висувають досить жорсткі вимоги до внутрішніх (особистих) якостей експертів. По-третє, у низці випадків необхідні відносно великі часові витрати.

Комбіновані методи оцінки ризиків є об'єднання окремих методів або його елементів. Оскільки ризик є імовірнісною оцінкою, його кількісний вимір не може бути однозначним і передбаченим. Їх застосовують в оцінці комплексних ризиків від сукупності небезпек. Наприклад, імовірнісно-евристичні методи засновані на використанні суб'єктивних ймовірностей, одержуваних за допомогою експертного оцінювання, а також на математичних моделях, точність яких не є високою.

Комбіновані методи мають певні переваги. По-перше, вони ліквідують недоліки, притаманні певним методам, від яких експерти змушені відмовитися. По-друге, вони надають можливість отримати (принаймні двохсторонню) оцінку ризику. По-третє, вони можуть застосовуватися як інтегральна оцінка багатофакторних ризиків.

Недоліки комбінованих методів полягають в тому, що зазвичай вони є результатом вибору об'єднаних методів оцінки.

Нечіткі методи оцінки загроз і ризиків ґрунтуються на використанні нечіткої логіки. Нечітку логіку запропонував професор та завідувач

кафедри електротехніки Каліфорнійського університету Лотфі Заде у праці "Нечіткі множини" (1965). На відміну від двозначної класичної логіки, нечітка логіка є багатозначною. Вона має справу зі ступенями відповідності та ступенями правди. Нечітка логіка використовує континуум логічних значень між нулем (повністю хибним) та одиницею (повністю вірно). Замість просто чорного та білого, використовує спектр кольорів, приймаючи те, що поняття можуть бути частково вірними та частково хибними одночасно. Оцінка ризиків, побудована на основі застосування нечіткої логіки, може характеризуватися логічністю та високою стійкістю особливо в тих випадках, коли аналіз ризиків проводиться в умовах нестачі даних і знань. Вона дає змогу експертам сфокусуватися на самій суті оцінки ризиків, що передбачає аналіз не лише причиново-наслідкових зв'язків між ключовими факторами ризиків, а й аналіз впливу кожного окремо взятого ризику. Строго кажучи, це система управління, у якій оцінка ризиків є складовою. Значення початкових змінних, що виникають під час виникнення екстремальної (катастрофічної) події, надходять до системи з метою отримання оцінної величини втрат для кожного певного ризику. Їх також можуть коригувати залучені експерти, проте необхідно враховувати те, що експерти можуть мати різні рівні розуміння ситуації та різний практичний досвід.

Окреслимо переваги нечітких методів. По-перше, вони зазвичай інтегруються в системи управління, де здійснюється комплексне завдання аналізу загроз, оцінки ризиків та управління надзвичайною ситуацією, що розвивається навколо конкретної катастрофічної події на певному об'єкті чи території. По-друге, реалізація цих методів в автоматизованих системах управління (АСУ) дозволяє використовувати електронні бази даних та знань та штучний інтелект як незалежний (резюмуючий) експерт.

Недоліки нечітких методів такі: по-перше, практично відсутні в широкому доступі методики застосування цих методів унаслідок того, що вони є корпоративною інтелектуальною власністю; по-друге, реалізація цих методів в АСУ ускладнює їх використання експертами (наприклад, у разі віддаленого доступу).

Нейронні методи оцінки загроз і ризиків ґрунтуються на використанні штучних нейронних мереж. Нейронна мережа – це нерозривна тріада, сукупність математичної моделі, її програмної реалізації та апаратного втілення (виготовлення, створення, вбудовування). Вона будується за принципом організації та функціонування біологічних нейронних мереж із нервових клітин живого організму. Штучна нейронна мережа (ШНМ) є системою з'єднаних і взаємодіючих між собою простих процесорів – штучних нейронів. Ці процесори значно простіше в порівнянні з процесорами, які використовуються в персональних комп'ютерах. Кожен процесор в ШНМ працює лише з сигналами, які він періодично отримує, та сигналами, які він періодично передає іншим процесорам. Штучні нейрони, з'єднані у велику ШНМ із керованою взаємодією, здатні виконувати досить складні завдання. Можливість навчання — одна з головних переваг нейронних мереж перед традиційними алгоритмами. Технічно навчання полягає в знаходженні коефіцієнтів зв'язків між нейронами. У процесі навчання нейронна мережа здатна виявляти складні залежності між вхідними даними та вихідними, а також виконувати узагальнення. Це означає, що в разі успішного навчання мережа зможе повернути правильний результат на підставі даних, які були відсутні в навчальній вибірці, а також неповних або частково спотворених даних.

Нейронні методи мають певні переваги. По-перше, вони є невіддільною частиною штучного інтелекту системи управління, де здійснюється комплексне завдання аналізу загроз, оцінки ризиків та управління надзвичайною ситуацією, що розвивається навколо конкретної катастрофічної події на певному об'єкті чи території. По-друге, ШНМ, що реалізує ці методи, здатний вдосконалюватися (навчатися). По-третє, використання цих методів в АСУ надає можливість у найкоротші терміни оцінювати загрози та ризики, прогнозувати розвиток надзвичайної ситуації та пропонувати варіанти управлінських рішень.

Недоліки нейронних методів такі: по-перше, необхідність постійної розробки та вдосконалення спеціальних навчальних алгоритмів; по-друге, у ряді випадків великі тимчасові витрати на навчання ШНМ; по-третє, досить висока вартість систем, які реалізують ці методи [13–14].

Таким чином, до всіх складних техногенних об'єктів застосовується системний підхід у забезпеченні їхньої безпеки, який передбачає ідентифікацію об'єктивних небезпек, визначення та ранжування загроз, оцінку ризику їх прояву і складання прогнозу, що робиться на користь запобігання катастрофічним подіям, обумовленим об'єктивними небезпеками. Найбільш ефективними методами оцінки загроз і ризиків є методи, що інтегровані до систем моніторингу, системи підтримки прийняття рішень та інші системи автоматизованого управління.

ВИСНОВКИ

1. Критичну інфраструктуру варто розуміти як сукупність підприємств, мереж, систем, вихід

з ладу або порушення функціонування яких може призвести до втрати управління або завдати істотних збитків на загальнодержавному, регіональному, місцевому чи об'єктовому рівнях. До її складу входять атомні та гідроелектростанції, хімічні та нафтохімічні комбінати, металургійні заводи та безліч інших державних підприємств і приватних установ стратегічного призначення.

2. До всіх складних техногенних об'єктів застосовується системний підхід у гарантуванні їхньої безпеки, який передбачає ідентифікацію об'єктивних небезпек, визначення та ранжування загроз, оцінку ризику їх прояву та складання прогнозу, що робиться на користь запобігання катастрофічним подіям, обумовленим об'єктивними небезпеками. Найбільш ефективними методами оцінки загроз і ризиків є методи, інтегровані до систем моніторингу, системи підтримки прийняття рішень та інших систем автоматизованого управління. Події останніх років в Україні вимагають визначення терористичної загрози як першочергової та найголовнішої.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Гора І. В.* Окремі питання захисту об'єктів критичної інфраструктури: зарубіжний досвід / І. В. Гора, О. В. Батюк // Соціально-правові студії. — 2021. – Вип. 1 (11). — С. 132–139. DOI: https://doi.org/10.32518/2617-4162-2021-1-132-139.
2. *Єрменчук О. П.* Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монографія / О. П. Єрменчук. — Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. – 180 с.
3. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. Міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов; за заг. ред. О. М. Суходолі. — Київ : НІСД, 2016. — 176 с.
4. *Бірюков Д. С*. Стратегія захисту критичної інфраструктури в системі національної безпеки держави / Д. С. Бірюков, С. І. Кондратов // Стратегічні пріоритети. — 2012. — Вип. 3. — С. 107–113.
5. *Каніщев Г.* Критична інфраструктура тимчасово окупованих територій України в українському законодавстві / Г. Каніщев, І. Тур // Соціально-правові студії. — 2024. — С. 18–25.
6. *Уряднікова І. В.* Наукові підходи до визначення терміну "критична інфраструктура" / І. В. Уряднікова, В. М. Заплатинський // Вісті Донецького гірничого інституту. — 2020. — № 2 (47). — С. 184–193. DOI: https://doi.org/10.31474/1999-981X-2020-2-184-193.
7. *Франчук В. І.* Безпека об'єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи [Електронний ресурс] / В. І. Франчук, П. Я. Пригунов, С. І. Мельник // Соціально-правові студії. — 2021. — Вип. 3 (13). — С. 142–148. — Режим доступу: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3984/1/19.pdf.
8. *Сметана М.* Захист критичної інфраструктури. Підходи держав Європейського Союзу до визначення елементів критичної інфраструктури / М. Сметана. — Острава : ВШБ — Технічний університет Острава, 2014/2015. — 60 с. (текст для курсів, що готуються в рамках співпраці Чеська Республіка - Молдова).
9. *Іванюта С. П.* Загрози критичній інфраструктурі та їх вплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки) : Аналітична записка / С. П. Іванюта. — Київ : НІСД, 2017. — 10 с.
10. Моделювання та оцінка сценаріїв загроз для об'єктів критичної інфраструктури / Д. С. Бірюков, В. А. Заславський, В. В. Євгієнко, О. В. Франчук // Наукові записки НаУКМА. — 2009. — Т. 99. Комп'ютерні науки. — С. 97–101.
11. *Лисиченко Г. В.* Природний, техногенний та екологічний ризики: аналіз, оцінка, управління : монографія / Г. В. Лисиченко, Ю. Л. Забулонов, Г. А. Хміль. — Київ : Наукова думка, 2008. — 542 с.
12. Застосування експертно-аналітичних методів для оцінювання ризиків надзвичайних ситуацій на об'єктах критичної інфраструктури / І. В. Уряднікова, С. М. Чумаченко, С. В. Кармазін, О. М. Тесленко // Науковий вісник Академії муніципального управління. Серія: Техніка. — 2015. — Вип. 1. – С. 206–218.
13. *Магомедов А. О.* Ризики та загрози для об'єктів критичної інфраструктури та шляхи їх подолання / А. О. Магомедов // Інвестиції: практика та досвід. — 2024. — № 15. — С. 216–221. DOI: https://doi.org/10.32702/2306-6814.2024.15.216.
14. *Березуцький В.* Ризики критичної інфраструктури під час війни / В. Березуцький, Т. Тохтамиш // Право та інноваційне суспільство. — 2024. — №2 (23). — С. 55–70. DOI: https://doi.org/10.37772/2309-9275-2024-2(23)-5.

REFERENCES

1. Hora, I. V., & Batiuk, O. V. (2021). Okremi pytannia zakhystu obiektiv krytychnoi infrastruktury: zarubizhnyi dosvid [Certain issues of protecting critical infrastructure facilities: foreign experience]. *Sotsialno-pravovi studii* [Social & Legal Studios]. *1* (11), 132–139. [in Ukr.].
2. Yermenchuk, O. P. (2018). Osnovni pidkhody do orhanizatsii zakhystu krytychnoi infrastruktury v krainakh Yevropy: dosvid dlia Ukrainy [Basic approaches to organizing critical infrastructure protection in European countries: experience for Ukraine]. Dnipro, 180 p. [in Ukr.].
3. Biriukov, D. S., Kondratov, S. I. (Compilers), & Sukhodoli, O. M. (Ed.). (2016). *Zelena knyha z pytan zakhystu krytychnoi infrastruktury v Ukraini*: zb. mizhnar. ekspert. narad [*Green Paper on Critical Infrastructure Protection in Ukraine*]. Proceedings of an International Expert Meeting. Kyiv, 176 p. [in Ukr.].
4. Biriukov, D. S., & Kondratov, S. I. (2012). Stratehiia zakhystu krytychnoi infrastruktury v systemi natsionalnoi bezpeky derzhavy [Critical Infrastructure Protection Strategy in the National Security System of the State]. *Stratehichni priorytety* [Strategic priorities]. *3*, 107–113. [in Ukr.].
5. Kanishchev, H., & Tur, I. 2024.Krytychna infrastruktura tymchasovo okupovanykh terytorii Ukrainy v ukrainskomu zakonodavstvi. Sotsialno-pravovi studii — Social & Legal Studios, P. 18–25. [in Ukr.].
6. Uriadnikova I. V., & Zaplatynskyi, V. M. (2020). Naukovi pidkhody do vyznachennia terminu "krytychna infrastruktura" [Scientific approaches to defining the term "critical infrastructure"]. *Visti Donetskoho hirnychoho instytutu [News of the Donetsk*

Mining Institute]. 2 (47), 184–193. DOI: https://doi.org/10.31474/1999-981X-2020-2-184-193 [in Ukr.].
7. Franchuk, V.I., Pryhunov, P. Ya., & Melnyk, S.I. (2021). Bezpeka obiektiv krytychnoi infrastruktury v Ukraini: orhanizatsiino-normatyvni problemy ta pidkhody [Security of critical infrastructure facilities in Ukraine: organizational and regulatory issues and approaches]. *Sotsialno-pravovi studii* [Social & Legal Studios]. *3* (13), 142–148. Retrieved from: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3984/1/19.pdf. [in Ukr.].
8. Smetana, M. (2014/2015). Zakhyst krytychnoi infrastruktury. Pidkhody derzhav Yevropeiskoho Soiuzu do vyznachennia elementiv krytychnoi infrastruktury [Critical Infrastructure Protection. Approaches of European Union States to the Definition of Critical Infrastructure Elements]. Ostrava, 60 p. [in Ukr.].
9. Ivaniuta, S. P. (2017). Zahrozy krytychnii infrastrukturi ta yikh vplyv na stan natsionalnoi bezpeky (monitorynh realizatsii Stratehii natsionalnoi bezpeky) [Threats to critical infrastructure and their impact on the state of national security (monitoring the implementation of the National Security Strategy]. Kyiv, 10 p. [in Ukr.].
10. Biriukov, D. S., Zaslavskyi, V. A., Yevhiienko, V. V., & Franchuk, O. V. (2009). Modeliuvannia ta otsinka stsenariiv zahroz dlia obiektiv krytychnoi infrastruktury [Modeling and assessing threat scenarios for critical infrastructure facilities]. *Naukovi zapysky NaUKMA [Scientific notes of NaUKMA]. 99,* 97–101.
11. Lysychenko, H. V., Zabulonov, Yu. L., & Khmil, H. A. (2008). Pryrodnyi, tekhnohennyi ta ekolohichnyi ryzyky: analiz, otsinka,upravlinnia [Natural, man-made and ecological risks: analysis, assessment, management]. Kyiv, 542 p. [in Ukr.].
12. Uriadnikova, I. V., Chumachenko, S. M., Karmazin, S. V., & Teslenko, O. M. (2015). Zastosuvannia ekspertno-analitychnykh metodiv dlia otsiniuvannia ryzykiv nadzvychainykh sytuatsii na obiektakh krytychnoi infrastruktury [Application of expert and analytical methods for assessing the risks of emergency situations at critical infrastructure facilities]. *Naukovyi visnyk Akademii munitsypalnoho upravlinnia. Seriia: Tekhnika* [Scientific Bulletin of the Academy of Municipal Administration. Series: Technology]. *1*, 206–218. [in Ukr.].
13. Mahomedov, A. O. (2024). Ryzyky ta zahrozy dlia obiektiv krytychnoi infrastruktury ta shliakhy yikh podolannia [Risks and threats to critical infrastructure facilities and ways to overcome them]. *Investytsii praktyka ta dosvid [Investments: practice and experience]. 15,* 216–221. DOI: https://doi.org/10.32702/2306-6814.2024.15.216. [in Ukr.].
14. Berezutskyi, V., & Tokhtamysh, T. (2024). Ryzyky krytychnoi infrastruktury pid chas viiny [Critical Infrastructure Risks During War]. *Pravo ta innovatsiine suspilstvo* [Law and innovative society]. *2* (23), 55–70. DOI: https://doi.org/10.37772/2309-9275-2024-2(23)-5. [in Ukr.].

M. M. DIVIZINIUK, Dc. S. of Physics and Mathematics, Professor
O. V. FARRAKHOV, PhD in Engineering
B. O. AVRAMCHUK, PhD in Economics
Ye. V. KOCHELAB, PhD in Physics and Mathematics
R. S. SAVITSKYI, Senior Lecturer

CRITICAL INFRASTRUCTURE OF THE STATE AND THE MAIN METHODS OF RISK ASSESSMENT

Abstract. *The article describes the parameters of the types of critical infrastructure of the State and shows that it includes nuclear and hydroelectric power plants, chemical and petrochemical plants, metallurgical plants and many other State enterprises and private institutions of strategic importance.*

The author considers critical infrastructure as a set of enterprises, networks, and systems whose failure or malfunctioning may result in loss of control or cause significant damage at the national, regional, local, or facility level. A systematic approach to ensuring their safety is applied to all complex man-made facilities.

It is emphasized that all European countries distinguish the concept of critical national infrastructures, which is understood as a set of systems, the disruption of which can cause serious damage to the economy of the State or lead to negative social consequences for society.

An analysis of existing methods of studying terrorist threats and risks is carried out. The basic concepts of threat and risk research are analyzed. The main methods of analyzing threats and risks from the standpoint of the technocratic concept, their advantages and disadvantages are considered.

It is noted that a systematic approach to ensuring their safety is applied to all complex technogenic facilities, which includes identification of objective hazards, identification and ranking of threats, assessment of the risk of their occurrence and forecasting, which is done in favor of preventing catastrophic events caused by objective hazards.

The most effective methods for assessing threats and risks are those integrated into monitoring systems, decision support systems, and other automated management systems. The events of recent years in Ukraine require that the terrorist threat be identified as the first and most important.

Keywords: *critical infrastructure, terrorist threat, systematic approach, threat ranking, risk assessment.*

ІНФОРМАЦІЯ ПРО АВТОРІВ

Дівізінюк Михайло Михайлович — д-р фіз.-мат. наук, професор, голов. н. с., Центр інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики Національної академії наук України, просп. акад. Палладіна, 34А, м. Київ, Україна, 03142; divizinyuk@ukr.net; ORCID: 0000-0002-5657-2302

Фаррахов Олександр Володимирович — канд. тех. наук, пров. н. с., Центр інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики Національної академії наук України, просп. акад. Палладіна, 34А, м. Київ, Україна, 03142; farrakhov@ukr.net; ORCID: 0000-0003-4988-126X

Аврамчук Богдан Олегович — канд. екон. наук, ст. дослідник, ДНУ "Український інститут науково-технічної експертизи та інформації", Антоновича, 180, м. Київ, Україна, 03150; avramchuk.bogdan@gmail.com; ORCID: 0000-0001-8505-2157

Кочелаб Євгенія Володимирівна — канд. фіз.-мат. наук, вчений секретар, Центр інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики Національної академії наук України, просп. акад. Палладіна, 34А, м. Київ, Україна, 03142; evk28@outlook.com; ORCID: 0009-0009-8354-8795

Савіцький Роман Святославович — ст. викладач кафедри інженерії програмного забезпечення Державного університету «Житомирська політехніка», вул. Черняховського 103, м. Житомир, Україна, 10029; roman.savitskyi@gmail.com; ORCID: 0000-0001-9804-3604

INFORMATION ABOUT THE AUTHORS

Diviziniuk M. M. — Dc.S. of Physical and Mathematical Sciences, Professor, Chief Research Associate, Center for Information-analytical and Technical Support of Nuclear Power Facilities Monitoring of the National Academy of Sciences of Ukraine, 34A, Academician Palladin Avenue, Kyiv, Ukraine, 03142; divizinyuk@ukr.net; ORCID: 0000-0002-5657-2302

Farrakhov O. V. — PhD in Engineering, Leading Researcher, Center for Information-analytical and Technical Support of Nuclear Power Facilities Monitoring of the National Academy of Sciences of Ukraine, 34A, Academician Palladin Avenue, Kyiv, Ukraine, 03142; farrakhov@ukr.net; ORCID: 0000-0003-4988-126X

Avramchuk B. O. — PhD in Economics, Senior Researcher, State Scientific Institution "Ukrainian Institute of Scientific Technical and Expertise and Information", 180, Antonovycha Str., Kyiv, Ukraine, 03150; avramchuk.bogdan@gmail.com; ORCID: 0000-0001-8505-2157

Kochelab Ye. V. — PhD in Physics and Mathematics, Scientific Secretary, Center for Information-analytical and Technical Support of Nuclear Power Facilities Monitoring of the National Academy of Sciences of Ukraine, 34 A, Academician Palladin Ave., Kyiv, Ukraine, 03142; evk28@outlook.com; ORCID: 0009-0009-8354-8795

Savitskyi R. S. — Senior Teacher of the Department of Software Engineering Zhytomyr Polytechnic State University, 103, Chudnivska Str., Zhytomyr, Ukraine, 10029; roman.savitskyi@gmail.com; ORCID: 0000-0001-9804-3604