Scientific and technical journal
«Technogenic and Ecological Safety»

RESEARCH ARTICLE
OPEN ACCESS

МЕТОДОЛОГІЧНИЙ ПІДХІД ДО ПІДВИЩЕННЯ БЕЗПЕКИ ТА СТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Н. М. Кічата[1], О. В. Третьяков[1], В. П. Федина[1], Є. В. Доронін[1]
[1]Національний авіаційний університет, Київ, Україна

УДК 351.863 + 338.246.87
DOI: 10.52363/2522-1892.2024.2.1
Отримано: 15 вересня 2024
Прийнято: 28 листопада 2024

Cite as: Kichata N., Tretyakov O., Fedyna V., Doronin E. (2024). Methodological approach to enhancing the security and resilience of critical infrastructure objects. Technogenic and ecological safety, 16(2/2024), 3–10. doi: 10.52363/2522-1892.2024.2.1

Анотація

У статті досліджується методологічний підхід до підвищення безпеки та стійкості об'єктів критичної інфраструктури, що є важливим елементом забезпечення національної безпеки України. В умовах сучасних терористичних загроз, воєнних дій, технічного прогресу необхідність розробки ефективних підходів до захисту таких об'єктів набуває особливої актуальності. Проаналізовано існуючі підходи з визначення певних рівнів гарантованої безпеки для об'єктів критичної інфраструктури (КІ). Надана їх оцінка та встановлені недоліки. Запропоновано використання кількісного методу для оцінки ймовірності та наслідків ризикованих подій на об'єктах КІ, що дозволяє підвищити точність оцінок і ефективність управління ризиками. Розроблено математичну модель каскадних ефектів різних типів при виникненні ризиків небезпеки для об'єктів критичної інфраструктури, яка дозволяє отримати ймовірнісні оцінки розвитку подій за визначеними сценаріями. Побудовано алгоритм протидій з появою відповідних загроз для типових об'єктів КІ. Розроблено пропозиції щодо заходів реагування на надзвичайні ситуації, які можуть бути успішно використані для прийняття обґрунтованих рішень щодо підвищення безпеки та стійкості об'єктів критичної інфраструктури, для розробки стратегічних планів та довгострокових політик стосовно управління критичною інфраструктурою. Запропонований підхід дозволяє оцінити усі загрози та проаналізувати можливі сценарії реалізації загроз, визначити пріоритети загроз за ступенем їх ймовірності, моделювати ймовірні наслідки реалізації загроз, враховуючи різні умови та чинники ризику, визначати вразливі місця у системах об'єктів КІ, створювати стратегії реагування на кризові ситуації.

Ключові слова: критична інфраструктура, об'єкти, загроза, небезпека, безпека, стійкість.

Постановка проблеми

Стійкість економічної системи є ключовим чинником для забезпечення зростання та нормального функціонування країни та її регіонів, для успішної діяльності економічних галузей на зовнішніх і внутрішніх ринках. У сучасних умовах війни в Україні, приймаючи до уваги особливості ситуації воєнного часу, коливання у світовій економіці та нестабільність зовнішнього середовища, критична інфраструктура (КІ) виявляє вразливість та обмежену здатність до адаптації на мікрорівні. Складові системи КІ не здатні ефективно протистояти та подолати існуючі труднощі без додаткових заходів безпеки.

Стійкість та підтримка розвитку КІ в умовах виникнення ризиків загроз є актуальним питанням витривалості економіки, захисту інфраструктури, як «критичної» структури для життєздатності суспільства, безпеки держави.

Підвищення безпеки та стійкості об'єктів критичної інфраструктури передбачає розробку та впровадження комплексних заходів, спрямованих на зниження вразливості та ризиків, пов'язаних із небезпечними подіями.

Реалізація загроз і небезпек на об'єктах КІ призводить до виникнення небезпечних подій або ситуацій, які здатні порушити їх функціонування або завдати значних збитків. До таких небезпечних подій належать різноманітні сценарії, включаючи терористичні атаки, природні катастрофи, технічні аварії, кібератаки, економічні труднощі та інші інциденти, що загрожують безпеці та нормальному функціонуванню критичних об'єктів інфраструктури [1].

Цей процес є постійним і динамічним, оскільки загрози змінюються з часом, і заходи захисту повинні адаптуватися до нових умов. Визначення загроз є важливою передумовою для розробки ефективної стратегії та планування заходів із захисту критичної інфраструктури.

У країнах, де національна безпека має високий пріоритет, термін «критична інфраструктура» стосується об'єктів і систем, які є надзвичайно важливими для життєдіяльності громадян і функціонування держави. До критичної інфраструктури належать особливо небезпечні промислові об'єкти, де незначні аварії спричиняють глобальні наслідки [2]. Будь-які перебої в їх роботі призводять до катастрофічних наслідків. Особливу загрозу становлять ситуації, коли вихід з ладу одного об'єкта критичної інфраструктури може спричинити збої в роботі інших об'єктів через їх взаємозалежність, створюючи «ефект доміно».

Безперебійна робота об'єктів критичної інфраструктури є основою стабільного функціонування держави, забезпечення життєдіяльності населення та підтримання економічної стабільності. Підвищення ефективності захисту КІ дозволить мінімізувати ризики зупинок і порушень у роботі соціально-економічної системи суспільства.

На основі аналітичного огляду інформаційних ресурсів щодо стану КІ в Україні відзначено такі чинники необхідності розробки методологічних підходів для посилення захисту об'єктів КІ:

1. Наслідки ракетних ударів, аварій, катастроф та інших надзвичайних ситуацій стають дедалі масштабнішими, що створює загрозу для безпеки населення, стабільного функціонування економіки та забезпечення життєво важливих потреб громадян. Це вимагає вдосконалення методів підвищення безпеки та стійкості критичних об'єктів для забезпечення безпеки громадян та стабільної роботи економіки, що є основою безпеки держави, сталого розвитку та підвищення рівня життя населення.

2. Кризові ситуації, що виникли в українському суспільстві під час військової агресії, є безпрецедентними для сучасного світу. Ці події підкреслили важливість узгодженої державної політики у сфері захисту критичної інфраструктури та необхідність суттєвих змін у цій галузі. Відповідність міжнародним стандартам і вимогам Європейського Союзу є важливою для інтеграції України в європейську спільноту, що вимагає впровадження сучасних методологій для підвищення безпеки і стійкості критичної інфраструктури.

3. Швидкий розвиток технологій, зокрема інформаційних та комунікаційних, створює нові можливості, в той же час і нові ризики небезпек, що вимагає адаптації методів забезпечення уникнення ризиків загроз і стійкості КІ до сучасних умов.

4. Недостатнє фінансування та обмежені ресурси не дозволяють здійснити комплексні заходи захисту на належному рівні. Внаслідок цього багато об'єктів залишалися вразливими через брак необхідних інвестицій в безпековий менеджмент.

5. Значна частина існуючих методологічних підходів уникнення ризик небезпеки не враховує взаємозалежності між різними об'єктами критичної інфраструктури та не передбачає регулярного моніторингу стану об'єктів та оцінки ризиків, що унеможливлює своєчасне виявлення та адекватне реагування на потенційні загрози.

Таким чином, розробка методологічних підходів для підвищення ефективності безпеки та стійкості об'єктів КІ в Україні є важливим і актуальним завданням забезпечення низького рівня ймовірності загроз у суспільстві та його потребам, що підкреслює значущість проведених досліджень.

Об'єктом дослідження є процес управління ризиками небезпечних подій для об'єктів критичної інфраструктури.

Предметом дослідження є розробка та впровадження методологічного підходу з оцінки ризиків для об'єктів критичної інфраструктури.

Аналіз останніх досліджень і публікацій

Питання формування критичної інфраструктури, обґрунтування концептуальних засад її розвитку та теоретико-методологічних підходів для підвищення ефективності функціонування в різних секторах економіки та суспільного життя є предметом наукових досліджень багатьох провідних зарубіжних та вітчизняних вчених: Л. Чернюк [3], В.Франчук [4], О. Лук'янчук [5], О. Яременко [6], С. Теленик [7], М. Домарацький [8], О. Єрменчук [9], Argyroudis et al. [10]; L. Galbusera et al. [11].

Вітчизняні вчені визначають захист критичної інфраструктури як «комплекс заходів, реалізованих через нормативно-правові, організаційні та технологічні інструменти, спрямовані на забезпечення безпеки та стійкості критичної інфраструктури» [12].

Водночас, деякі аспекти цієї важливої проблематики, зокрема питання розробки ефективних стратегій підвищення безпеки та стійкості об'єктів інфраструктури, залишаються недостатньо вивченими як з практичної, так і з теоретичної точки зору. Через неточність і неповноту інформації, необхідної для оцінки загроз і ризиків для критичної інфраструктури, врахування численних взаємозв'язків між об'єктами, досягнення універсальності доцільно звернутися до методів статистики та кількісних оцінок.

У ході проведення досліджень звернено увагу на певні недоліки сучасних методів і засобів підтримки безпеки об'єктів критичної інфраструктури, які необхідно усунути:

1. Багато підходів з підтримки безпеки об'єктів базуються на реакції на вже виявлені загрози та інциденти, тобто впровадження заходів безпеки передбачається після виникнення проблем. Це призводить у більшості випадків до затримок у реагуванні та реалізації серйозних наслідків.

2. Управління безпекою об'єктів критичної інфраструктури часто здійснюється окремими організаціями або секторами, що призводить до фрагментації заходів і відсутності єдиних стандартів. Це ускладнює співпрацю та обмін інформацією і створює неузгодженість у роботі між різними секторами підтримки безпеки на об'єктах.

3. Захист об'єктів критичної інфраструктури часто регулюється різними зацікавленими сторонами, такими як урядові органи та приватні компанії. Відсутність узгодженої стратегії та спільного плану дій призводить до розбіжностей і недосягнення загальних безпекових цілей.

4. Зростання кіберзагроз і атак ставить ризик небезпеки для об'єктів критичної інфраструктури. Постійне вдосконалення методів і технологій кіберзлочинців ускладнює завдання захисту, а недостатньо ефективні заходи та низька кібербезпекова свідомість персоналу створюють вразливі місця на об'єктах.

5. Забезпечення підтримки безпеки об'єктів критичної інфраструктури часто вимагає значних інвестицій, які є обмеженими. Недостатність фінансових ресурсів ускладнює оновлення систем безпеки, підготовку персоналу та впровадження сучасних технологій.

Вчасна ефективна оцінка безпеки та стійкості об'єктів критичної інфраструктури дозволяє забезпечити безперервність їх функціонування під час і після виникнення надзвичайних ситуацій.

Постановка завдання та його вирішення

Метою роботи є розробка методологічного підходу, який спрямований на уникнення ризик-загроз і підвищення безпеки та стійкості об'єктів КІ.

Оцінка потенційного впливу загроз і небезпек є важливим етапом у створенні стратегій та планів захисту критичної інфраструктури. Вона дозволяє визначити пріоритети та необхідні заходи для запобігання, реагування і мінімізації наслідків загроз і небезпек.

Складність розробки підходу для ідентифікації загроз на об'єктах критичної інфраструктури полягає у великій різноманітності об'єктів і систем, що належать до різних секторів, їх численності, необхідності врахування різних характеристик самих об'єктів, їх вразливості та наслідків усіх імовірних загроз.

Використання сучасних методів і передових технологій для оцінки ризиків і загроз, моделювання кризових ситуацій та розробки прогнозів на основі сценаріїв дозволяє підвищити надійність отриманих результатів і створити широку науково обґрунтовану базу даних для подальшого аналізу.

Для визначення рівня ризику необхідно здійснювати його розрахунок на основі об'єктивних даних. Кількісний метод оцінки ризиків загроз використовує числові показники та моделі для оцінки ймовірності та наслідків небезпечних подій. Цей підхід заснований на математичних розрахунках і включає такі елементи, як статистичний аналіз, моделювання подій, використання ймовірнісних розподілів та інші методи кількісного оцінювання. Він дозволяє отримати конкретні числові значення ризику, які дозволяють порівнювати між собою різні чинник-причини і чинник-наслідки для прийняття рішень щодо управління ризиками [7].

Кількісна оцінка ризику передбачає необхідність визначення усіх можливих наслідків від певних дій і надання результату у кількісному або порівняльному вигляді. При кількісній оцінці рівня ризику використовують такі показники, як потенційний результат, очікуване значення рівня ризику та відхилення від цього значення. Кількісна оцінка ризику ускладнюється визначенням ймовірності ризику. Об'єктивний метод визначення ймовірності ризику базується на розрахунку частоти настання небезпечної події за визначений період.

Розробка імітаційної моделі для каскадних ефектів від ризик-небезпеки на об'єктах КІ на основі кількісного методу дозволяє отримати ймовірнісні оцінки розвитку подій за визначеними сценаріями та оцінити загрози для об'єкта критичної інфраструктури за величиною ймовірності настання подій і переходів між ними.

Цей підхід включає створення математичної моделі за послідовністю таких етапів:

– визначення подій у сценарії розвитку ситуації (компоненти сценарію, які ймовірно впливають на реалізацію загрози);

– встановлення множини можливих станів подій, що впливають на рівень загрози;

– формування сценаріїв розвитку загрози (визначення послідовних кроків, які ведуть до виникнення загрози) через індивідуальні елементи, що створюють ланцюжки подій та їх переходи до заданих станів; це відображається в структурно-логічній моделі розвитку кризової ситуації з різними варіантами сценаріїв на прикладі об'єктів критичної інфраструктури;

– формування оргграфу сценаріїв загроз (структурно-логічна модель, що охоплює всі можливі сценарії реалізації загрози);

– оцінка ймовірностей різних подій і переходів між ними;

– оцінка ймовірності реалізації сценаріїв загроз.

Алгоритм реалізації цього підходу складається з таких функціональних подій.

1. Ідентифікація небезпечних подій у сценарії розвитку ситуації: аспекти сценарію, які можуть вплинути на здійснення загрози.

2. Визначення різних імовірних станів подій, що вірогідно впливатимуть на рівень загрози. Множини можливих станів подій визначаються шляхом аналізу різних чинників та врахування ймовірних сценаріїв.

3. Створення сценаріїв виникнення та розвитку загрози. Формуються сценарії розвитку загрози, у яких визначаються ланки, що складаються з пар «подія – перехід у заданий стан». Це досягається шляхом створення структурно-логічної моделі розвитку кризової ситуації. На цьому етапі розробляються сценарії розвитку загрози, де визначаються послідовність подій і переходи між ними. Структурно-логічна модель формулюється шляхом організації переходів відповідно до послідовності та взаємозв'язків подій. Модель надається у вигляді графа, де вузли відповідають різним станам системи, а ребра – переходам між ними. Така модель допомагає виявити потенційні загрози і встановити ефективні заходи для їх запобігання та управління.

4. Створення графічного подання різних варіантів розвитку загрози. На основі визначених подій та їх зв'язків створюється структурно-логічна модель, що включає всі вірогідні сценарії реалізації загрози. У цій моделі кожна подія надається як вузол, а зв'язки між подіями – як ребра. Наявність певних ребер дозволяє визначити послідовність імовірних переходів між станами для кожного сценарію, відображаючи розвиток небезпечної ситуації.

5. Аналіз ймовірності різних сценаріїв та їх переходів. Оцінка ймовірностей станів подій і їх переходів у орієнтованому графі сценаріїв загроз є ключовим етапом для розуміння потенційних ризиків і розробки ефективних стратегій управління ними.

Ймовірності подій надаються у відсотках, частках або інших формах, залежно від специфіки моделювання. Аналіз даних проводиться на основі статистичних відомостей, які дозволяють отримати об'єктивне уявлення про розподіл, зв'язки та взаємозв'язки між різними явищами. Для цього

використовуються такі джерела статистичних даних, як Державна служба статистики України, Державна служба України з надзвичайних ситуацій, Всесвітня організація охорони здоров'я, МАГАТЕ, науково-дослідні установи, університети та засоби масової інформації.

6. Оцінка ймовірності реалізації сценаріїв загроз є базовим етапом в управлінні ризиками та забезпеченні стійкості критичної інфраструктури. Цей процес вимагає врахування багатьох чинників і детального обстеження об'єкта.

Побудова моделі визначення ризику розпочинається зі збору достовірних статистичних даних, що відображають історичні випадки загроз і їх наслідки: природні катастрофи, техногенні аварії або кібератаки, інформація про відмови та несправності технічного обладнання. На основі вхідних даних проводиться статистичний аналіз для виявлення причин та частоти відмов систем на об'єкті КІ. Джерела даних включають інформаційно-аналітичні довідки про надзвичайні ситуації, аналітичні звіти підприємств, офіційні державні органи (статистична служба), метеорологічну службу та медіа. Використовувані дані ідентифікуються, аналізуються та верифікуються на точність і надаються для оцінки ймовірності виникнення подій, їх тривалості, вірогідних збитків і впливу на функціонування об'єктів (табл. 1).

Таблиця 1 – Характеристики небезпечних подій

№ подій	Опис відповідної події	№ подій	Опис відповідної події
1	**Природні чинники (природні катаклізми)**	**4**	**Терористичні акти**
1.1	**Зсув**	**4.1**	**Теракт**
1.1.1	Небажана подія на 1-му елементі ОКІ	4.1.1	Небажана подія на 1-му елементі ОКІ
1.1.2	Небажана подія на 2-му елементі ОКІ	4.1.2	Небажана подія на 2-му елементі ОКІ
…	…	…	…
1.2	**Повінь**	**4.2**	**Замах**
1.2.1	Небажана подія на 1-му елементі ОКІ	4.2.1	Небажана подія на 1-му елементі ОКІ
1.2.2	Небажана подія на 2-му елементі ОКІ	4.2.2	Небажана подія на 2-му елементі ОКІ
…	…	…	…
1.3	**Землетрус**	**4.3**	**Вибух**
1.3.1	Небажана подія на 1-му елементі ОКІ	4.3.1	Небажана подія на 1-му елементі ОКІ
1.3.2	Небажана подія на 2-му елементі ОКІ	4.3.2	Небажана подія на 2му елементі ОКІ
…	…	…	…
1.4	**Ураган**	**4.4**	**Напад**
1.4.1	Небажана подія на 1-му елементі ОКІ	4.4.1	Небажана подія на 1-му елементі ОКІ
1.4.2	Небажана подія на 2-му елементі ОКІ	4.4.2	Небажана подія на 2-му елементі ОКІ
…	…	…	…
2	**Техногенні чинники**	**5**	**Соціально-політичні чинники**
2.1	**Аварія**	**5.1**	**Політична криза**
2.1.1	Небажана подія на 1-му елементі ОКІ	5.1.1	Небажана подія на 1-му елементі ОКІ
2.1.2	Небажана подія на 2-му елементі ОКІ	5.1.2	Небажана подія на 2-му елементі ОКІ
…	…	…	…
2.2	**Вибух**	**5.2**	**Масовий протест**
2.3	Небажана подія на 1-му елементі ОКІ	5.2.1	Небажана подія на 1-му елементі ОКІ
2.3.1	Небажана подія на 2-му елементі ОКІ	5.2.2	Небажана подія на 2-му елементі ОКІ
…	…	…	…
2.3	**Технічна помилка**	**5.3**	**Збройна сутичка**
2.3.1	Небажана подія на 1-му елементі ОКІ	5.3.1	Небажана подія на 1-му елементі ОКІ
2.3.2	Небажана подія на 2-му елементі ОКІ	5.3.2	Небажана подія на 2-му елементі ОКІ
…	…	…	…
2.4	**Збій апаратного забезпечення**	**6**	**Економічні чинники**
2.4.1	Небажана подія на 1-му елементі ОКІ	**6.1**	**Економічна криза**
2.4.2	Небажана подія на 2-му елементі ОКІ	6.1.1	Небажана подія на 1-му елементі ОКІ
…	…	6.1.2	Небажана подія на 2-му елементі ОКІ
3	**Кібератаки**	…	…
3.1	Хакерська атака	**6.2**	**Банкрутство**
3.1.1	Небажана подія на 1-му елементі ОКІ	6.2.1	Небажана подія на 1-му елементі ОКІ
3.1.2	Небажана подія на 2-му елементі ОКІ	6.2.2	Небажана подія на 2-му елементі ОКІ
…	…	…	…
3.2	**Вірус**	**6.3**	**Безробіття**
3.2.1	Небажана подія на 1-му елементі ОКІ	6.3.1	Небажана подія на 1-му елементі ОКІ
3.2.2	Небажана подія на 2-му елементі ОКІ	6.3.2	Небажана подія на 2-му елементі ОКІ
…	…	…	…
3.3	**Шкідлива програма**	**6.4**	**Зростання цін**
3.3.1	Небажана подія на 1-му елементі ОКІ	6.4.1	Небажана подія на 1-му елементі ОКІ
3.3.2	Небажана подія на 2-му елементі ОКІ	6.4.2	Небажана подія на 2-му елементі ОКІ
…	…	…	…

Складові елементи з таблиці 1 допомагають створити різноманітні сценарії розвитку ситуації на об'єкті КІ.

Кожен сценарій детально моделюється з використанням статистичних методів, що дозволяє аналізувати ризики різних видів загроз для кожного конкретного об'єкта і встановлювати зв'язки між чинниками для прогнозування ймовірності та наслідків ризиків.

На основі ідентифікованих подій і їх класифікації формується множина можливих станів, що враховують різні комбінації та ймовірності виникнення цих подій. Це допомагає оцінити рівень загрози та розробити відповідні стратегії управління ризиками в подальшому.

Нехай для події $i \in I$ визначено m_{ijk} (задане скінчене число) різних станів, що впливають на реалізацію сценарію загрози. Кожній події присвоєно свій індекс. Позначається множина станів подій : $i \in I$:

$$S_i = \left\{ s_{1jk}, s_{2jk}, \ldots, s_{ijk}\left(m_{ijk}\right) \right\} \subset N . \qquad (1)$$

Для кожної події $i \in I$ множина S_i містить індекси, що відповідають властивим для даної події станам безпеки або небезпеки.

Всю сукупність подій відображається у вигляді графа, де вузли визначають різні стани системи, а ребра – переходи між ними (рис. 1).

Модель охоплює всі можливі сценарії реалізації загрози, оцінюючи ймовірності станів подій та їх переходів. Аналіз розпочинається з початкових елементів (вершин, що мають лише вихідні ребра) і просувається вздовж направлених ребер від одного логічного елемента до іншого, розкриваючи структуру логічної схеми. Це допомагає виявити найбільш критичні ситуації та визначити ключові події, які можуть призвести до інших можливих каскадних ефектів, виявляючи логічні залежності між компонентами, де одна подія є передумовою для іншої.

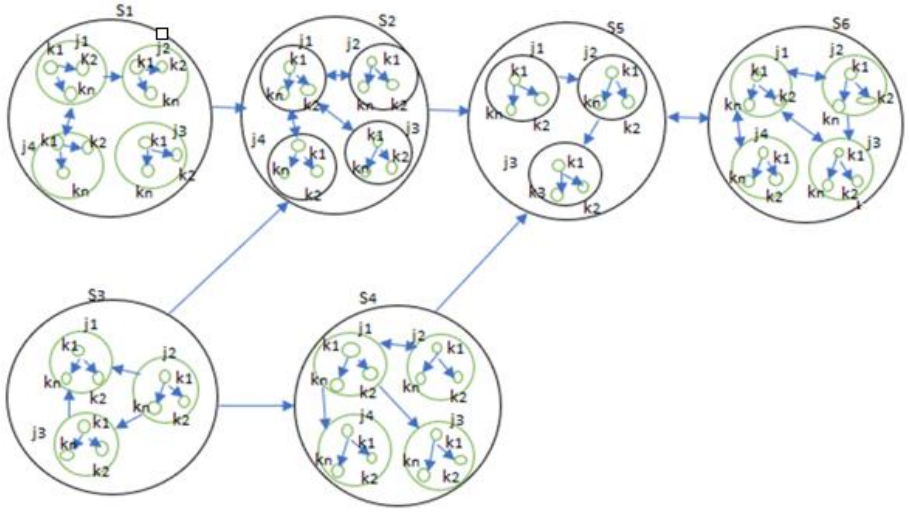

Рисунок 1 – Структурно-логічна модель розвитку кризової ситуації в результаті ураження об'єкту критичної інфраструктури

На рисунку 1 всі події структуровані у вигляді орграфу, враховуючи його вершини. У цій моделі виділяють три основні множини:

$S = \{S_i\}$ – множина загальних небезпек різних чинників, де i – кількість елементів чинників; $J = \{j_n\}$ – множина небезпек одного чинника, де n – кількість елементів чинника; $K = \{K_n\}$ – множина небажаних подій на елементах об'єкту КІ, де n – кількість небажаних подій на різних елементах об'єкту КІ.

У результаті формується структурно-логічна модель розвитку кризової ситуації, що виникає через різні види загроз для об'єкта КІ.

Наступний етап полягає в оцінці ймовірностей станів подій у сценаріях загроз для об'єкта. Для розрахунку ймовірностей використовуються статистичні дані про об'єкт за певний період. На основі цього аналізу визначаються числові значення ймовірностей для кожного стану події та можливих переходів між станами.

Стан події $i \in I$ описується дискретною випадковою величиною x_i. Позначається $p_i(s)$ – ймовірність перебування події $i \in I$ в стані $s \in S_i$, тобто, $p_i(s) = P\{x_{ijk} = s\}$, $s \in S_i$.

Кожне ребро орієнтовного графа буде мати відповідне значення P_{jk} де $0 \le P \le 1$. Припускається, що величини x_i, $i \in I$ стохастично незалежні, а ймовірності $p_i(s) = P\{x_{ijk} = s\}$, $s \in S_i$ задані на основі статистичних даних. Кожна ймовірність переходів від однієї потенційної події до іншої оцінюється кількісним методом. На основі аналізу даних визначаються числові значення ймовірностей для кожного стану події та можливих переходів між станами.

Оцінювання ймовірності реалізації сценаріїв загроз проводиться відповідно до теореми повної ймовірності [13]:

$$P_{сценарію} = 1 - \prod \left(1 - P_{ijk}\right),\ i \in A_k , \qquad (2)$$

де P_i ($i = \overline{1,n}$) – ймовірність виникнення критичної ситуації, A_k – це k-й сценарій розвитку ситуації, що містить визначені події.

За допомогою проведених розрахунків оцінюється значущість ризиків реалізації загроз на об'єктах інфраструктури та виявляються потенційні загрози каскадних ефектів у різних сценаріях подій на об'єктах критичної інфраструктури, що дозволяє прийняти управлінські заходи для попередження та усунення цих ризиків.

Оцінка загроз і ризиків проводиться з урахуванням їх потенційного впливу та ймовірності виникнення. Кожному ризику на об'єкті критичної інфраструктури присвоюється пріоритет на основі ймовірності його реалізації. Усі ризики загроз мають різний ступінь небезпеки, ризики ранжуються за важливістю та потенційним впливом, що дозволяє зосередити зусилля на більш критичних загрозах. Ранжування допомагає виокремити більш критичні загрози, на які слід звернути увагу в першу чергу, і розробити відповідні заходи захисту та реагування.

Кожен показник ймовірності загрози оцінюється статистичним методом від 0 до 1, де 0 відповідає мінімальній мірі впливу показника небезпеки для об'єкту, а 1 – максимальній. Упорядкування небезпек починається з більшого показника ймовірності загрози.

Після завершення ранжування загроз ухвалюється рішення про те, які з них слід вважати пріоритетними, визначаються об'єкти критичної інфраструктури, які потребують термінової уваги та фінансування.

Далі розпочинається етап зниження ризиків, на якому ключовим є визначення пріоритетів і ефективний розподіл наявних ресурсів. Мета цієї фази – планування та реалізація заходів, спрямованих на зменшення виявлених ризиків. Після впровадження запланованих заходів переходять до оцінки ризиків, що включає постійний моніторинг визначених ризиків та аналіз ефективності вжитих заходів. Якщо ризик знижується до прийнятного рівня, захід вважається успішним. В іншому випадку, або при появі нових ризиків, ініціюється новий цикл управління, починаючи з фази визначення ризиків.

З метою підвищення загальної безпеки та надійності держави у сфері захисту об'єктів КІ необхідно розробляти конкретні заходи захисту для кожного об'єкта. Це включає заходи з кіберзахисту, фізичного забезпечення, резервування та відновлення, плани екстреного реагування. Оскільки багато об'єктів КІ перебувають у приватній власності, ефективна політика захисту вимагає партнерства і співпраці між державними органами та приватним сектором для спільного забезпечення захисту.

Для оцінки ефективності політики захисту критичної інфраструктури необхідно мати систему моніторингу та аналітики для постійного відстеження потенційних загроз та реагування на них. Така інформаційна система включає використання систем спостереження для виявлення змін у рівні безпеки кожного об'єкта, що свідчить про ймовірні загрози, прогностичні моделі для передбачення вірогідних загроз у геополітичному, екологічному або соціальному контексті. Аналіз вразливості КІ дозволяє ідентифікувати початок загроз і вчасно реагувати на них.

Обов'язковою складовою ефективної політики захисту КІ є розроблення алгоритму дій при появі відповідних загроз для типових об'єктів КІ. (рис. 2).

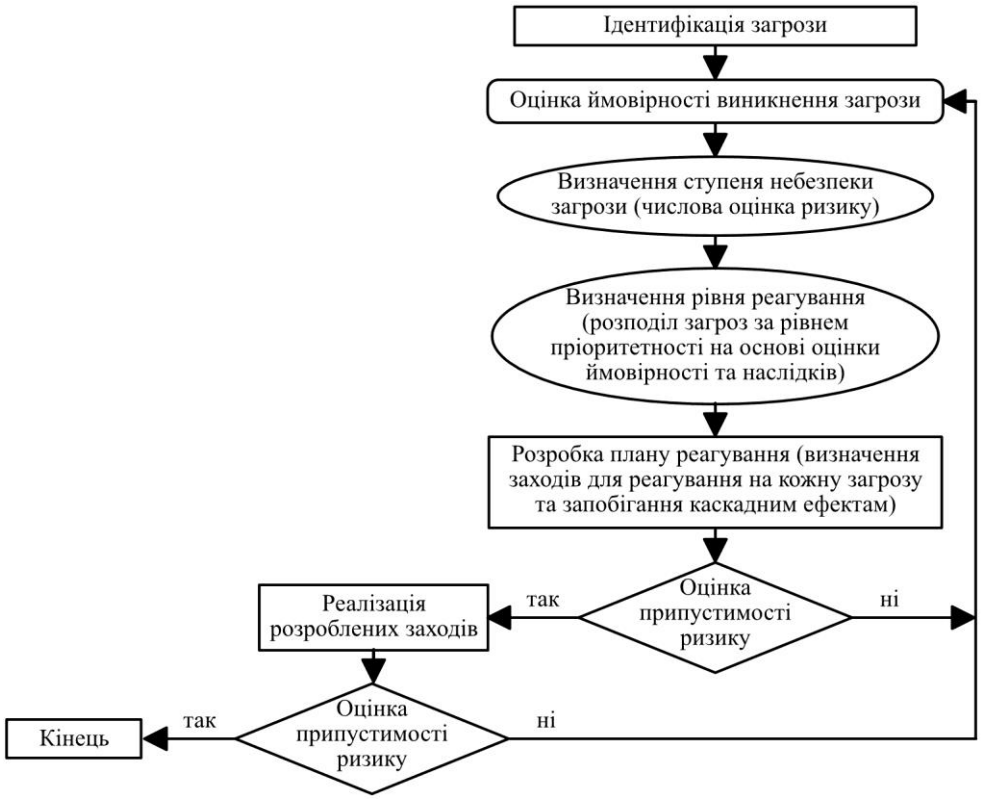

Рисунок 2 – Схема алгоритму визначення реагування у разі реалізації загрози

До заходів реагування відносяться створення детальних планів для різних видів надзвичайних ситуацій, проведення регулярних навчань для персоналу, організація резервів матеріальних ресурсів і технічних засобів, впровадження системи швидкої комунікації між різними службами та відомствами. Означений підхід реалізовано для Долинського газопереробного заводу, комплексу водопідготовки «Донець» та АЗС «Укрнафта».

Висновки

Основною перевагою розробленого методологічного підходу оцінки ризик-небезпеки для КІ є можливість систематичного врахування різних ризикових чинників та прийняття обґрунтованих рішень для підвищення безпеки та стійкості об'єктів критичної інфраструктури, забезпечувати її надійне функціонування в умовах зовнішніх і внутрішніх загроз.

Новизною даного підходу є комплексне сполучення прогностичних і оцінювальних дій стосовно опису небезпеки для об'єктів КІ. Це дозволяє забезпечити уникнення реалізації загрози, критичних наслідків, завчасно мати інформацію про заходи зменшення рівня небезпеки для об'єктів критичної інфраструктури.

Алгоритм визначення реагування на потенційні загрози забезпечує систематизований підхід до реагування на різні типи загроз, передбачаючи ймовірність серйозних наслідків для об'єктів критичної інфраструктури. Це сприяє покращенню підготовки персоналу до надзвичайних ситуацій і дозволяє оперативно визначати необхідні дії для мінімізації впливу загроз.

Запропонований підхід дозволяє детально досліджувати структури об'єктів критичної інфраструктури, включаючи всі системи та компоненти, незалежно від секторальної приналежності; визначати критичні вузли та елементи, від яких залежить безперебійне функціонування об'єкта, і будувати моделі ймовірних сценаріїв розвитку кризових ситуацій унаслідок впливу небезпек на ці об'єкти.

Розроблений і апробований підхід дозволяє встановлювати пріоритетність заходів, які повинні бути першочергово впроваджені для запобігання та усунення потенційних небезпек, щоб уникнути каскадних ефектів на об'єктах критичної інфраструктури різних секторів.

ЛІТЕРАТУРА

1. Кічата Н. М., Третьяков О. В. Оцінка реалізації загроз на об'єктах критичної інфраструктури. *Old and new technologies of learning development in modern conditions*: proceedings of the VI International scientific and practical conference. (February 13-16, 2024). Berlin, Germany, 2024. С.319-321. DOI: 10.46299/ISG.2024.1.6.

2. Бірюков Д. С. Про доцільність та особливості визначення критичної інфраструктури в Україні: Аналітична записка. Київ: НІСД, 2013. URL: http://www.niss.gov.ua/articles/1026 (дата звернення: 02.08.2024).

3. Чернюк Л. Г., Ананьєва Л. С. Виробнича інфраструктура АПК України: стан та перспективи розвитку. Київ : РВПС НАН України, 2000. 102 с.

4. Франчук В. І., Пригунов П. Я., Мельник С. І. Безпека об'єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. *Соціально-правові студії*. 2021. Випуск 3 (13). С. 142-148. DOI: 10.32518/2617-4162-2021-3-142-148.

5. Лук'янчук О. М., Волкова Д. В. Інфраструктура: характеристика, види, функції та ефективність. *Бізнес Інформ*. 2018. № 4. С. 21-25. URL: https://www.business-inform.net/export_pdf/business-inform2018-4_0-pages-21_25.pdf (дата звернення: 05.08.2024).

6. Яременко О. І., Страхніцький Я. О. Теоретичні підходи до визначення дефініції критичної інфраструктури як об'єкту державного управління. *Публічне управління та митне адміністрування.* 2022. № 1. С. 76-82. DOI: 10.32836/2310-9653-2022-1.13.

7. Теленик С. С. Державна система захисту критичної інфраструктури України: концептуальні засади адміністративно-правового регулювання. Херсон : Видавничий дім «Гельветика», 2020. 602 с.

8. Домарацький М. Б. Особливості формування та функціонування державної системи моніторингу стану об'єктів критичної інфраструктури. *Публічне управління та митне адміністрування*. 2019. № 4. С. 170-174. DOI: 10.32840/pdu.2019.4.26.

9. Єрменчук О. Оцінка загроз критичній інфраструктурі як важлива складова частина діяльності із захисту державної безпеки. *Jurnalul juridic national: teorie si practica*. 2018. No. 6. P. 50-54. URL: http://jurnaluljuridic.md/index.php/main/article/view/541/491 (дата звернення: 05.08.2024).

10. Resilience assessment framework for critical infrastructure in a multi-hazard environment: case study on transport assets / S. A. Argyroudis et al. *Science of The Total Environment*. 2020. Vol. 714. Art. 136854. DOI: 10.1016/j.scitotenv.2020.136854.

11. Galbusera L., Trucco P., Giannopoulos G. Modeling interdependencies in multi-sectoral critical Infrastruture systems: evolving the DMCI approach. *Reliability Engineering and System Safety*. 2020. Vol. 203. Art. 107072. DOI: 10.1016/j.ress.2020.107072.

12. Економіко-правові засади забезпечення захисту критичної інфраструктури / В. В. Лойко, В. В. Храпкіна, С. А. Маляр, М. В. Руденко. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2020. № 4. С. 426-438.

13. Мурасов Р. К. Методика розрахунку імовірності успішної посадки літака. *Наука і техніка Повітряних Сил Збройних Сил України*. 2012. №3 (9). С. 53-57.

Kichata N., Tretyakov O., Fedyna V., Doronin E.

METHODOLOGICAL APPROACH TO ENHANCING THE SECURITY AND RESILIENCE OF CRITICAL INFRASTRUCTURE OBJECTS

The article examines the methodological approach to increasing the safety and stability of critical infrastructure objects, which is an important element of ensuring Ukraine's national security. In the conditions of modern terrorist threats, military operations, and technological progress, the need to develop effective approaches to the protection of such objects becomes especially relevant. The existing approaches for determining certain levels of guaranteed security for critical infrastructure (CI) objects are analyzed. Their assessment is provided and the shortcomings are identified. The use of a quantitative method for assessing the probability and consequences of risky events at CI facilities is proposed, which allows to increase the accuracy of assessments and the effectiveness of risk management. A mathematical model of cascading effects of various types in the event of danger risks for critical infrastructure objects has been developed, which allows obtaining probabilistic estimates of the development of events under defined scenarios. An algorithm for countermeasures with the appearance of appropriate threats for typical CI objects has been built. Proposals for emergency response measures have been developed, which can be successfully used to make informed decisions about increasing the safety and stability of critical infrastructure objects, for the development of strategic plans and long-term policies regarding the management of critical infrastructure. The proposed approach allows you to assess all threats and analyze possible scenarios of threat implementation, prioritize threats according to their degree of probability, model the likely consequences of threat implementation, taking into account various conditions and risk factors, identify vulnerabilities in the systems of CI objects, create strategies for responding to crisis situations.

Key words: critical infrastructure, objects, threat, danger, security. resilience.

REFERENCES

1. Kichata, N. M., & Tretiakov, O. V. (2024). Otsinka realizatsii zahroz na obiektakh krytychnoi infrastruktury [Assessment of threat implementation at critical infrastructure facilities]. *Old and new technologies of learning development in modern conditions*: proceedings of the VI International scientific and practical conference. Berlin, Germany, 319-321. DOI: 10.46299/ISG.2024.1.6. [in Ukrainian]

2. Biriukov, D. S. (2013). *Pro dotsilnist ta osoblyvosti vyznachennia krytychnoi infrastruktury v Ukraini: Analitychna zapyska* [*On the expediency and peculiarities of defining critical infrastructure in Ukraine: Analytical note*]. Kyiv: NISD. URL: http://www.niss.gov.ua/articles/1026. [in Ukrainian]

3. Cherniuk, L. H., & Ananieva, L. S. (2000). *Vyrobnycha infrastruktura APK Ukrainy: stan ta perspektyvy rozvytku* [*Production infrastructure of the agricultural sector of Ukraine: state and prospects for development*]. Kyiv: RVPS NAN Ukrainy. [in Ukrainian]

4. 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 problems and approaches]. *Sotsialno-pravovi studii*, 3(13), 142-148. DOI: 10.32518/2617-4162-2021-3-142-148. [in Ukrainian]

5. Lukianchuk, O. M., & Volkova, D. V. (2018). Infrastruktura: kharakterystyka, vydy, funktsii ta efektyvnist [Infrastructure: characteristics, types, functions and efficiency]. *Business Inform*, 4, 21-25. URL: https://www.business-inform.net/export_pdf/business-inform2018-4_0-pages-21_25.pdf. [in Ukrainian]

6. Yaremenko, O. I., & Strakhnitskyi, Ya. O. (2022). Teoretychni pidkhody do vyznachennia definitsii krytychnoi infrastruktury yak obiektu derzhavnoho upravlinnia [Theoretical approaches to determining the definition of critical infrastructure as an object of public administration]. *Publichne upravlinnia ta mytne administruvannia*, 1, 76–82. DOI: 10.32836/2310-9653-2022-1.13. [in Ukrainian]

7. Telenyk, S. S. (2020). *Derzhavna systema zakhystu krytychnoi infrastruktury Ukrainy: kontseptualni zasady administratyvno-pravovoho rehuliuvannia* [*State system of protection of critical infrastructure of Ukraine: conceptual principles of administrative and legal regulation*]. Kherson: Vydavnychyi dim «Helvetyka». [in Ukrainian]

8. Domaratskyi, M. B. (2019). Osoblyvosti formuvannia ta funktsionuvannia derzhavnoi systemy monitorynhu stanu obiektiv krytychnoi infrastruktury [Peculiarities of the formation and functioning of the state system for monitoring the state of critical infrastructure objects]. *Publichne upravlinnia ta mytne administruvannia*, 4, 170-174. DOI: 10.32840/pdu.2019.4.26. [in Ukrainian]

9. Yermenchuk, O. (2018). Otsinka zahroz krytychnii infrastrukturi yak vazhlyva skladova chastyna diialnosti iz zakhystu derzhavnoi bezpeky [Assessment of threats to critical infrastructure as an important component of state security protection activities]. *Jurnalul juridic national: teorie si practica*, 6, 50-54. URL: http://jurnaluljuridic.md/index.php/main/article/view/541/491. [in Ukrainian]

10. Argyroudis, S. A., Mitoulis, S. A., Hofer, L., Zanini, M. A., Tubaldi, E., & Frangopol, D. M. (2020). Resilience assessment framework for critical infrastructure in a multi-hazard environment: case study on transport assets. *Science of The Total Environment*, 714, 136854. DOI: 10.1016/j.scitotenv.2020.136854.

11. Galbusera, L., Trucco, P., & Giannopoulos, G. (2020). Modeling interdependencies in multi-sectoral critical Infrastruture systems: evolving the DMCI approach. *Reliability Engineering and System Safety*, 203, 107072. DOI: https://doi.org/10.1016/j.ress.2020.107072.

12. Loiko, V. V., Khrapkina, V. V., Maliar, S. A., & Rudenko, M. V. (2020). Ekonomiko-pravovi zasady zabezpechennia zakhystu krytychnoi infrastruktury [Economic and legal principles of ensuring the protection of critical infrastructure]. *Finansovo-kredytna diialnist: problemy teorii ta praktyky*, 4, 426-438. [in Ukrainian]

13. Murasov, R. K. (2012). Metodyka rozrakhunku imovirnosti uspishnoi posadky litaka [Methodology for calculating the probability of a successful landing of an aircraft]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy*, 3(9), 53-57. [in Ukrainian]