Інформаційно-технічний метод попередження надзвичайних ситуацій терористичного характеру шляхом оцінки можливості ступеневого росту деструктивних подій викликаних каскадними наслідками первинного терористичного впливу

The information and technical method of preventing emergency situations of a terrorist nature by assessing the possibility of gradual growth of destructive events caused by the cascading consequences of the primary terrorist impact

Рустам Мурасов [A]
Corresponding author: кан. техн. наук, професор кафедри, e-mail: rustamm@ukr.net, ORCID: 0000-0003-0800-2062
Іван Мещеряков [A]
доктор філософії, доцент кафедри, e-mail: shulyk3004@ukr.net, ORCID: 0000-0001-5797-0735

Rustam Murasov [A]
Corresponding author: candidate of technology Sciences, professor of the department, e-mail: rustamm@ukr.net, ORCID: 0000-0003-0800-206
Ivan Meshcheriakov [A]
Doctor of Philosophy, associate professor of the department, e-mail: shulyk3004@ukr.net, ORCID: 0000-0001-5797-0735

[A] Національний університет оборони України, м. Київ, Україна

[A]National Defense University of Ukraine, Kyiv, Ukraine

Received: October 1, 2023 | Revised: October 24, 2023 | Accepted: October 31, 2023

DOI: 10.33445/sds.2023.13.5.17

Мета роботи: розроблення методу попередження надзвичайних ситуацій терористичного характеру шляхом оцінки можливості ступеневого росту деструктивних подій.
Метод: метод теорії ймовірності, метод експертних оцінок.
Результати дослідження: розроблено інформаційно-технічний метод попередження надзвичайних ситуацій терористичного характеру шляхом оцінки можливості ступеневого росту деструктивних подій, викликаних каскадними наслідками первинного терористичного впливу який призначений для ідентифікації та прогнозування потенційних загроз і визначення деструктивного потенціалу таких подій.
Теоретична цінність дослідження: попередження надзвичайних ситуацій терористичного характеру шляхом оцінки деструктивних подій в умовах каскадних наслідків терористичного впливу.
Тип статті: описовий та дослідницький.

Purpose: development of a method of preventing emergency situations of a terrorist nature by assessing the possibility of gradual growth of destructive events.
Method: method of probability theory, method of expert evaluations.
Findings: developed information and technical method of preventing terrorist emergencies was developed by assessing the possibility of gradual growth of destructive events caused by the cascading consequences of the primary terrorist impact, which is designed to identify and forecast potential threats and determine the destructive potential of such events.
Theoretical implications: prevention of emergency situations of a terrorist nature by assessing destructive events in the conditions of cascading consequences of terrorist influence.
Papertype: descriptive and research.

Ключові слова: критична інфраструктура, надзвичайна ситуація, терористичний вплив, мінімізація наслідків, деструктивний потенціал.

Key words: critical infrastructure, emergency, terrorist impact, minimization of consequences, destructive potential.

1. Вступ

Актуальність проблеми оцінювання загроз обумовлена в першу чергу складною обстановкою в Україні, де значна кількість об'єктів критичної інфраструктури знаходиться в зоні впливу збройного конфлікту. Для складних технічних систем, до яких також відносяться об'єкти критичної інфраструктури (системи електроживлення та енергопостачання, водопостачання та водовідведення, об'єкти гірничо-добувної, хімічної та металургійної промисловості, система газо-, нафто- і продуктопроводів і т.ін.), актуальною проблемою є об'єктивне, достовірне та

своєчасне передбачення, прогнозування і попередження надзвичайних ситуацій і каскадних ефектів, що можуть призвести до техногенних аварій, катастроф або суттєво вплинути на їх функціональність, живучість, безпеку, ефективність та інші властивості. Ймовірність виникнення та наслідки таких ситуацій, умов і чинників визначаються як цілеспрямованими (диверсія, бойові дії, саботаж) так і стохастичними (хаотичними) процесами, що за своєю сутністю характеризуються як загрози та ризики.

Одним з перспективних напрямків дослідження щодо оцінки воєнно-техногенних загроз і ризиків для об'єктів критичної інфраструктури в зоні ведення бойових дій є аналіз кризових ситуацій, коли система захисту критичної інфраструктури не в змозі виконувати у повному обсязі покладені на неї завдання, що в подальшому внаслідок техногенної аварії чи катастрофи може призвести до значних людських жертв серед населення та небойових втрат серед військовослужбовців. При дії на систему критичної інфраструктури зовнішніх уражаючих чинників, які можуть бути раптовими та інтенсивними, система захисту критичної інфраструктури не в змозі протидіяти цим чинникам, що призведе до кризових ситуацій або значного погіршення їх функціональної стійкості.

2. Теоретичні основи дослідження

В ході аналізу останніх публікацій [1-4], що стосуються математичних підходів до оцінювання загроз і ризиків, було виявлено недостатній розвиток їх математичного і комп'ютерного моделювання для об'єктів критичної інфраструктури в умовах терористичного впливу. Головним чином автори використовують системний підхід з використанням експертних оцінок, що звужує можливості застосування даного підходу.

За думкою багатьох експертів [5-8], у наш час не існує загальноприйнятої методики оцінки ризиків та загроз для об'єктів критичної інфраструктури, є часткові рішення для конкретних об'єктів (випадків) [9-11].

Однією із форм забезпечення необхідного рівня безпеки та функціонування критичної інфраструктури і суспільства є мінімізація наслідків надзвичайних ситуацій викликаних ураженням терористами об'єктів критичної інфраструктури.

Світовий досвід досліджень даної проблематики зводиться до аналізу і пошуку прийнятних рішень в обмеженому просторі для ліквідації або мінімізації наслідків надзвичайних ситуацій. При чому обмеження сил і засобів для ліквідації або мінімізації наслідків там не розглядається.

В ході аналізу встановлено, що чинники воєнно-техногенної безпеки залежать від ефективного розподілу сил і засобів охорони і оборони об'єктів критичної інфраструктури з метою недопущення або мінімізації наслідків надзвичайних ситуацій природного, техногенного і воєнного характеру. Тому виникає необхідність, щодо розробки підходів до створення математичної моделі оцінювання загроз для об'єктів критичної інфраструктури з використанням структурно-логічної моделі каскадних ефектів первинного терористичного впливу [12].

3. Постановка проблеми

Важливим етапом в розробці математичної моделі оцінки імовірності ураження одиночного об'єкта критичної інфраструктури є аналіз різних видів можливих уражень. Це передбачає детальне вивчення різноманітних сценаріїв, в яких об'єкти критичної інфраструктури можуть бути піддані впливу, таких як терористичні атаки, кібератаки, диверсії тощо. Враховуючи ці сценарії, слід розглянути ймовірність їх реалізації і вплив на об'єкт.

Таким чином, розробка математичної моделі оцінки імовірності ураження та розрахунку деструктивного потенціалу наслідків вимагає детального дослідження можливих

сценаріїв уражень, аналізу їхнього впливу та об'єднання отриманих даних в одну комплексну модель.

4. Результати

Необхідність формалізованої математичної моделі оцінки можливості ступеневого росту деструктивних подій в умовах каскадних наслідків первинного терористичного впливу опирається на критичну важливість такої інфраструктури для функціювання суспільства. Ці об'єкти, такі як електростанції, об'єкти очищення води і транспортні мережі, є необхідними для щоденного життя осіб і функціювання економіки. Можлива аварія або навантаження цих об'єктів через загрози і ризики, такі як природні катастрофи, кібератаки або терористичні акти, може мати серйозні наслідки для безпеки населення і стійкості життєво-важливих послуг.

Оскільки об'єкти критичної інфраструктури (ОКІ) мають різне призначення, природу, рівень захищеності, можливість відновлення, рівень небезпеки для людства та інших ОКІ, виникає необхідність математичної формалізації для синтезу математичної моделі загроз і ризиків для ОКІ. Це дозволить оперувати математичними методами та складати чітку ієрархію загроз. Кожен ОКІ є потенційним джерелом небезпеки, оскільки їх функціювання представляє собою постійну небезпеку життю і здоров'ю людей, котра може бути визначена як постійна техногенна загроза. Джерела природних і техногенних небезпек, як правило, відомі і для нейтралізації пов'язаних з ними постійних загроз своєчасно вживаються відповідні міри безпеки.

Головним і майже непередбачуваним джерелом небезпеки є протиправна діяльність терористичних угрупувань та ураження (руйнування) ОКІ.

Всі ці загрози не є сталими і можуть варіюватись в залежності від ситуації. Ця обставина ускладнює задачу формалізації, оскільки люба система безпеки може бути ефективна проти конкретних загроз і конкретних форм їх реалізації. Тому, для підтримання необхідного рівня безпеки об'єктів необхідно здійснювати постійний моніторинг змін можливостей і способів дій джерел небезпеки та своєчасне коректування списку загроз у відповідності до виявлених змін. Сукупність всіх відомих і можливих, на даний момент часу загроз і способів їх реалізації критичним об'єктам інфраструктури складає модель загроз. Модель загроз є вихідним моментом побудови системи забезпечення безпеки, де кожному можливому способу реалізації загрози визначаються заходи щодо його нейтралізації.

Схема оцінювання загроз і ризиків для ОКІ наведена на рис. 1 [13, 14].

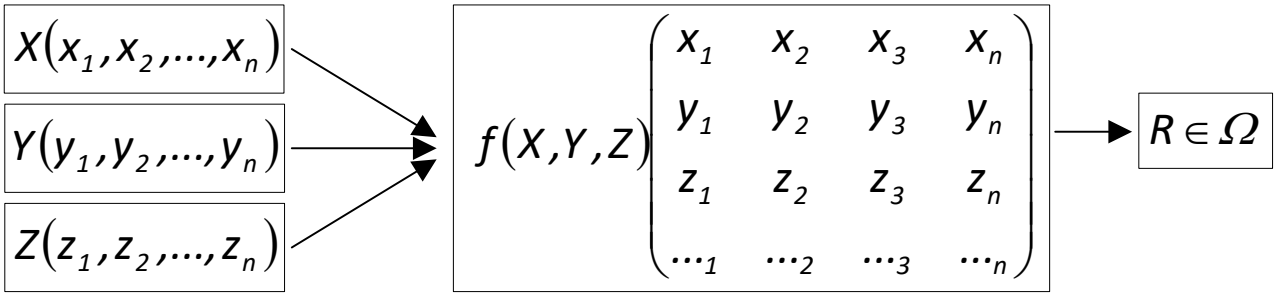

Рисунок 1. Схема оцінки можливості ступеневого росту деструктивних подій одиночного об'єкту критичної інфраструктури

Де – X, Y, Z вектори станів ОКІ (кількість векторів необмежена і залежить від факторів які впливають), а функція f (методичний апарат) дозволяє отримати оцінку прогнозу загроз і ризиків для ОКІ R (яка входить до множини станів ОКІ).

Моделювання комбінацій загроз і ризиків, складання загальної оцінки наслідків збитків та втрат дозволить визначити та скласти чітку ієрархію загроз. Виробити своєчасні рішення по протидії (запобігання) та нейтралізації загроз ОКІ.

Символами X,Y,Z представлено вектори станів ОКІ (кількість векторів необмежена і залежить від чинників що впливають на критичну інфраструктуру).

Функція f представляє собою науково-методичний апарат, який дозволяє отримати прогнозну оцінку загроз і ризиків для ОКІ R, що поєднує множинні стани ОКІ. Вона дозволяє перетворити інформацію про стани ОКІ в прогнозні оцінки можливих наслідків при різних умовах. Це дозволяє враховувати різноманітність факторів і створювати більш реалістичні сценарії.

Моделювання комбінацій загроз і ризиків з метою складання загальної оцінки можливих негативних наслідків і соціо-еколого-економічних збитків і втрат дозволить чітко визначити та упорядкувати чітку ієрархію можливих загроз та розробити своєчасне управлінське рішення що попередження та нейтралізації загроз ОКІ.

Для визначення імовірності ураження ОКІ російською федерацією використовується набір можливих типів уражень, включаючи авіаційні, ракетні, артилерійські удари та кібератаки. Ці удари можуть застосовуватись як окремо, так і комбіновано з іншими типами уражень.

Імовірність ураження ОКІ визначається шляхом врахування імовірностей кожного типу ураження ($P_1,P_2,...,P_n$), де n - кількість типів уражень, що використовує противник проти ОКІ. Імовірність ураження ОКІ буде визначатись так:

$$P_{ураж} = \{P_1,P_2,...,P_n\}, \quad (1)$$

де $n=\overline{1,I}$, а I – кількість типів ураження, що застосовує противник по ОКІ в даному випадку.

Ця формула враховує незалежність імовірностей і обчислює загальну імовірність ураження ОКІ шляхом віднімання від одиниці добутку виразів $(1-P_1),(1-P_2),...,(1-P_n)$.

Загальна формула розрахунку імовірності ураження одиночного ОКІ буде мати наступний вигляд:

$$P_{ураж} = 1 - \prod_{n=1}^{I}(1 - P_n), \quad (2)$$

Імовірності уражень кожного окремого типу ($P_1,P_2,...,P_n$) можуть бути розраховані на основі аналізу історичних даних, експертної оцінки або інформації, отриманої від розвідувальних джерел. Формули для розрахунку імовірностей уражень залежать від конкретного контексту, характеристик об'єктів критичної інфраструктури і ситуації загрози.

Введемо поняття Деструктивного потенціалу (ДП) D під яким будемо розуміти інтегральну характеристику кореляційних процесів спрямованих на розвиток катастрофічних процесів системи критичної інфраструктури, в глобальних масштабах з великими (понад 1000 чол.) людськими втратами та подальшою ланцюговою реакцією поширення військово-техногенних катастроф, які також мають прямий вплив на соціальні та економічні сфери.

Деструктивний потенціал об'єкту критичної інфраструктури реалізується через утворення площ вторинного ураження техногенними аномаліями і розвиток локальних небезпечних екзогенних геологічних процесів.

Деструктивний потенціал визначається як інтегральна характеристика, що враховує сумування величин потенційних збитків, що можуть виникнути в результаті каскадних деструктивних процесів в системі критичної інфраструктури.

Для визначення ДП необхідно провести оцінку різних факторів, які можуть призвести до пошкодження або знищення об'єкту. Ці фактори можуть бути різних типів, наприклад.

Природні фактори: землетруси, повені, урагани, торнадо, пожежі тощо; техногенні фактори: аварії на транспорті, вибухи, пожежі, техногенні катастрофи, війна, терористичні акти тощо; Соціальні фактори: війна, терористичні акти, соціальні заворушення, масові вбивства тощо.

Для оцінки деструктивного потенціалу D можна використати таку формулу:

$$D = \sum_{i=1}^{I} D_i, \tag{3}$$

де D_i – потенційні збитки, що можуть виникнути в результаті деструктивних процесів в критичної інфраструктури;

I – кількість ОКІ які утворюють . збитки у даному сценарії.

Інтегральна характеристика ДП може бути визначена на основі декількох факторів, які впливають на імовірність виникнення катастрофічних подій, а також на масштаб і ступінь їх наслідків.

Для вимірювання ДП доцільно застосувати грошовий еквівалент.

Грошовий еквівалент дозволяє оцінити потенційні збитки в економічному виразі і зрозуміти їх вплив на фінансову стійкість та ефективність системи критичної інфраструктури.

Вимірювання ДП в гривнях дозволяє зробити порівняння між різними об'єктами критичної інфраструктури та оцінити їх уразливість до потенційних деструктивних процесів. Крім того, вимірювання в грошовому еквіваленті сприяє зручній комунікації результатів аналізу та прийняттю рішень, оскільки вартість збитків в гривнях більш зрозуміла для зацікавлених сторін.

Варто відзначити, що при обранні грошового еквіваленту для виміру ДП важливо мати точні дані про вартість ремонту, відновлення або заміни пошкоджених об'єктів критичної інфраструктури. Додатково, необхідно враховувати інфляційні та економічні фактори, щоб забезпечити точність оцінки.

Для виконання зазначеної задачі необхідно поєднати воєдино два попередніх фактори.

Це означає, що необхідно застосовуючи імовірності ураження ОКІ різними типами ураження та визначення деструктивного потенціалу здійснити обчислення ризику R втрат та збитків при настанні даних подій, яка визначається (3.3)

$$R_n = \sum_{i=1}^{I} (P_i D_{i+1}). \tag{4}$$

Об'єднуючи систему з (2) і (3) та вираз (4) в одну систему отримаємо потрібну математичну модель оцінки імовірності ураження одиночного об'єкту критичної інфраструктури і розрахунку деструктивного потенціалу наслідків:

$$\begin{cases} P_{ураж} = 1 - \prod_{n=1}^{I} (1 - P_n) \\ D = \sum_{i=1}^{I} D_i \\ R_n = \sum_{i=1}^{I} (P_i D_{i+1}) \end{cases}, \tag{5}$$

де, $P_{ураж}$ – імовірності ураження одиночного ОКІ;

P_n – імовірність кожного типу ураження ($P_1, P_2, \ldots, P_n$), де n – кількість типів уражень, що використовує противник проти ОКІ;

D – деструктивний потенціал;

D_i – потенційні збитки, що можуть виникнути в результаті деструктивних процесів в критичної інфраструктури, I – кількість ОКІ які утворюють . збитки у даному сценарії;

R_n – ризик, який вираховується для критичної інфраструктури.

У цьому рівнянні R_n означає ризик, який вираховується для системи критичної інфраструктури. Цей ризик є сумою добутків ймовірностей виникнення (P_i) та потенційних збитків ($D(i+1)$) для кожного типу ураження або фактору, який був врахований.

Коефіцієнт і в рівнянні представляє загальну кількість типів уражень, які були враховані в аналізі. Це можуть бути, наприклад, авіаційні удари, ракетні удари, артилерійські удари, кібератаки тощо.

Таким чином, математична модель оцінки імовірності ураження одиночного об'єкту критичної інфраструктури і розрахунку деструктивного потенціалу наслідків представляє собою систему з двох структур. Перша система дозволяє розраховувати імовірність сумарного ураження об'єкту критичної інфраструктури різними видами ураження. Друга залежність дозволяє оцінити деструктивний потенціал ураження об'єкту критичної інфраструктури, який вимірюється у грошовому еквіваленті (гривнях).

Математична модель оцінки імовірності ураження одиночного об'єкту дає нам змогу практично реалізувати у вигляді алгоритму. В результаті алгоритмічної реалізації математичної моделі оцінки імовірності ураження одиночного об'єкту критичної інфраструктури і розрахунку деструктивного потенціалу наслідків був розроблений управляючий алгоритм. Він складається з сьомі модулей, розташованих на п'яти рівнях, як показано на рис. 2.

На першому ієрархічному рівні розташований один блок. Це перший модуль – блок збору даних по ОКІ.

На другому рівні розташований блок введення даних. В залежності від вибору режиму здійснюється формування бази даних або уточнення даних. В залежності від задачі що вирішується дані можуть зберігатись в різних форматах або декілька об'єктів по сукупним властивостям та взаємозв'язкам об'єднуватись в один.

На третьому рівні в модулі визначення імовірності ураження одиночного ОКІ різними видами ураження розраховується імовірність ураження. В залежності від обстановки та при отриманні нових даних здійснюється перерахунок імовірності для визначених ОКІ.

На четвертому рівні розташований блок розрахунку деструктивного потенціалу ОКІ. Застосовуючи дані попередніх блоків здійснюється оцінка деструктивного потенціалу ОКІ, який вимірюється у грошовому еквіваленті (гривнях).

На останньому п'ятому рівні розташований модуль розрахунку ризиків критичної інфраструктури та визначення збитків. У даному модулі застосовуються усі отримані та оброблені дані з першого по четвертий блоки.

Також, з першого по п'ятий рівні усі модулі зв'язані послідовним наданням інформації та з четвертого та п'ятого рівня мають зворотній зв'язок.

Таким чином, управляючий алгоритм інформаційно-технічного методу попередження надзвичайних ситуацій терористичного характеру шляхом оцінки можливості ступеневого росту деструктивних подій викликаних каскадними наслідками первинного терористичного впливу складається з семи блоків розташованих на п'яти ієрархічних рівнях, з'єднаних послідовними і зворотними зв'язками.

Метод призначений для ідентифікації та прогнозування потенційних загроз і визначення деструктивного потенціалу таких подій. Враховуючи деструктивний потенціал, цей метод допомагає розрахувати можливі наслідки терористичних актів та встановити необхідні заходи безпеки та захисту для зменшення ризиків та мінімізації збитків. Його використання спрямоване на забезпечення безпеки об'єктів та ефективного реагування на потенційні катастрофічні події.

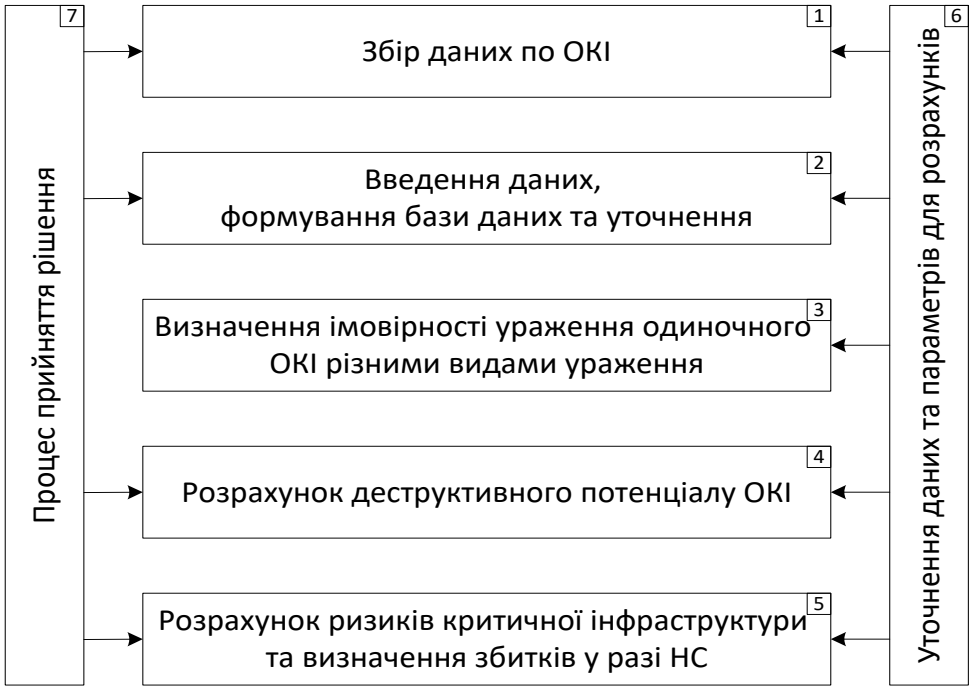

Рисунок 2 – Схема управляючого алгоритму інформаційно-технічного методу попередження надзвичайних ситуацій терористичного характеру шляхом оцінки можливості ступеневого росту деструктивних подій викликаних каскадними наслідками первинного терористичного впливу

Застосування інформаційно-технічного методу попередження надзвичайних ситуацій терористичного характеру шляхом оцінки можливості ступеневого росту деструктивних подій викликаних каскадними наслідками первинного терористичного впливу, забезпечується виконанням п'яти процедур:

1. Збір даних по ОКІ.
2. Введення даних, формування бази даних та уточнення.
3. Визначення імовірності ураження одиночного ОКІ різними видами ураження.
4. Розрахунок деструктивного потенціалу ОКІ.
5. Розрахунок ризиків КІ та визначення збитків у разі НС.

Послідовно розглянемо їх.

Перша процедура – збір даних по ОКІ – має наступні кроки. Визначення необхідних параметрів та характеристик ОКІ, які потрібно зібрати для оцінки його безпеки та уразливості. Це можуть бути такі дані, як фізична структура об'єкту, розміри, розташування, типи систем, функціональні можливості тощо. Встановлення процедури збору даних, які можуть включати документальний аналіз, інтерв'ю з фахівцями, огляд території та будівель, використання сучасних технологій моніторингу, сенсорів та інших засобів. Збір даних про можливі загрози терористичного характеру, які можуть вплинути на ОКІ. Це включає оцінку потенційних терористичних сценаріїв, ідентифікацію ризикованих зон та часових рамок, оцінку доступності об'єкту для терористичних атак. Збір даних про системи захисту та безпеки, які вже застосовуються для захисту ОКІ. Це можуть бути системи виявлення та реагування на загрози, системи контролю доступу, системи відеоспостереження тощо.

Ця процедура дозволяє зібрати всю необхідну інформацію про ОКІ, його характеристики, потенційні загрози та застосовані системи захисту. Отримані дані будуть використовуватись в подальших кроках для оцінки ризику та розрахунку деструктивного потенціалу.

Друга процедура – введення даних, формування бази даних та уточнення – має наступні кроки. Вибір режиму роботи системи залежно від потреб оцінки ризику та розрахунку деструктивного потенціалу. Режими можуть включати створення нової бази даних або уточнення існуючої бази даних з додатковою інформацією.

Введення отриманих даних з першої процедури в базу даних. Це може включати структурування та організацію даних відповідно до вимог моделі оцінки ризику і розрахунку деструктивного потенціалу.

Уточнення даних за допомогою додаткових джерел інформації або детальніших досліджень. Це може включати виправлення помилок, оновлення даних згідно зі змінами в об'єкті або внесення нової інформації.

Валідація та перевірка достовірності даних в базі даних. Це включає перевірку правильності введення даних, виявлення можливих протирічь чи неповних даних та їх виправлення.

Забезпечення доступу та конфіденційності до бази даних, забезпечення резервного копіювання та захисту даних від несанкціонованого доступу або втрати.

Ця процедура дозволяє створити або оновити базу даних із зібраними та уточненими даними про ОКІ. Вона забезпечує належну організацію даних та їх достовірність для подальшого використання в розрахунках і оцінках ризику та деструктивного потенціалу.

Третя процедура – визначення імовірності ураження одиночного об'єкту критичної інфраструктури різними видами ураження – включає наступні кроки. Вибір типів уражень, які планується враховувати в оцінці.

Визначення параметрів та характеристик кожного типу ураження. Це включає ймовірність виникнення ураження, ймовірність його поширення, інтенсивність впливу, можливі наслідки та інші важливі параметри.

Оцінка ймовірності ураження для кожного типу відповідно до наявних даних та аналізу обстановки. Це може включати використання статистичних даних, експертних оцінок, моделювання або інших методів для визначення ймовірності ураження.

Врахування можливих взаємодій між різними типами уражень. Деякі типи уражень можуть спричиняти інші види уражень або змінювати їх імовірності. Цей крок полягає в аналізі можливих сценаріїв та оцінці впливу взаємодій на імовірність ураження.

Розрахунок сумарної імовірності ураження об'єкту критичної інфраструктури. Це включає сумування імовірностей уражень кожного типу з урахуванням їх взаємодій та інших факторів. Результатом є оцінка загальної імовірності ураження об'єкту.

Періодичний перерахунок імовірності ураження залежно від зміни обстановки, отримання нових даних або оновлення параметрів. Це забезпечує актуальність оцінки імовірності ураження відповідно до умов що змінюються.

Ця процедура дозволяє визначити імовірність ураження ОКІ різними видами уражень. Вона базується на зборі та аналізі даних, оцінці параметрів та врахуванні можливих взаємодій між ураженнями. Результатом є кількісна оцінка імовірності ураження, яка використовується для подальшої оцінки ризику та розрахунку деструктивного потенціалу.

Четверта процедура – розрахунок деструктивного потенціалу об'єкта критичної інфраструктури – має наступні кроки.

Використання даних з попередніх блоків. Для розрахунку деструктивного потенціалу ОКІ використовуються дані, отримані з попередніх модулів, зокрема імовірності ураження різними видами ураження та інші характеристики об'єктів.

Вибір методу розрахунку. Залежно від характеру об'єкта, видів ураження та доступних даних, обирається метод розрахунку деструктивного потенціалу. Це може бути аналітичний метод, статистичний аналіз, моделювання катастрофічних процесів тощо.

Розрахунок деструктивного потенціалу для кожного виду ураження. Застосовуючи обраний метод, проводиться розрахунок деструктивного потенціалу для кожного виду ураження. Це включає оцінку величин потенційних збитків, що можуть виникнути внаслідок деструктивних процесів, і їх сумування.

Визначення деструктивного потенціалу ОКІ. Шляхом агрегації результатів розрахунків для різних видів ураження, визначається деструктивний потенціал об'єкта критичної інфраструктури. Це може бути виміряно у грошовому еквіваленті, що відображає сумарні втрати.

Документування результатів розрахунків. Результати розрахунків деструктивного потенціалу фіксуються та документуються для подальшого аналізу та використання в оцінці ризику та прийнятті рішень.

Ця процедура дозволяє оцінити деструктивний потенціал об'єкта критичної інфраструктури на основі розрахунку втрат і збитків, що можуть виникнути внаслідок деструктивних процесів. Результати розрахунків надають уявлення про масштаб можливих наслідків та їх вплив на систему критичної інфраструктури.

П'ята процедура – розрахунок ризиків критичної інфраструктури та визначення збитків у разі НС – включає такі кроки. Використання результатів попередніх блоків. Для розрахунку ризиків критичної інфраструктури та визначення збитків використовуються дані, отримані з попередніх модулів, зокрема імовірності ураження, деструктивний потенціал та інші характеристики об'єктів.

Оцінка ризиків. Застосовуючи імовірності ураження та деструктивний потенціал, проводиться оцінка ризиків, пов'язаних з можливими надзвичайними ситуаціями в критичній інфраструктурі. Це включає врахування імовірності виникнення подій та їх наслідків.

Визначення збитків. На основі розрахунку ризиків та характеристик об'єктів, визначаються збитки, які можуть виникнути у разі надзвичайних ситуацій. Це може бути виміряно у грошовому еквіваленті або інших фізичних одиницях, що відображають втрати.

Аналіз ризиків та збитків. Отримані результати розрахунків підлягають аналізу з метою оцінки рівня ризиків та виявлення критичних зон, де можливі значні збитки. Це допомагає зорієнтуватися на найбільш вразливі об'єкти та виробити стратегії зменшення ризиків.

Документування результатів. Результати розрахунків ризиків та збитків фіксуються та документуються для подальшого використання в прийнятті рішень та розробці заходів з попередження надзвичайних ситуацій.

Ця процедура дозволяє оцінити ризики та збитки, пов'язані з можливими надзвичайними ситуаціями в критичній інфраструктурі. Результати розрахунків надають інформацію про потенційні наслідки та допомагають ухвалити обґрунтовані рішення з метою запобігання та зменшення негативних наслідків таких ситуацій.

Таким чином, інформаційно-технічний метод попередження надзвичайних ситуацій терористичного характеру шляхом оцінки можливості ступеневого росту деструктивних подій, викликаних каскадними наслідками первинного терористичного впливу, призначений для ідентифікації та прогнозування потенційних загроз і визначення деструктивного потенціалу таких подій.

Застосування методу забезпечується послідовним виконанням п'яти процедур: збір даних по об'єктах, формування бази даних, визначення імовірності ураження, розрахунок деструктивного потенціалу та оцінка ризиків та збитків.

5. Висновки

У статті розроблено математичну модель оцінки імовірності ураження одиночного об'єкта критичної інфраструктури і розрахунку деструктивного потенціалу наслідків, яка являє собою

систему з двох структур. Перша система дозволяє розраховувати імовірність сумарного ураження об'єкту критичної інфраструктури різними видами ураження. Друга залежність дозволяє оцінити деструктивний потенціал ураження об'єкту критичної інфраструктури, який вимірюється у грошовому еквіваленті (гривнях). Ця розроблена математична модель відрізняється від існуючих підходів завдяки своїй комплексності та здатності враховувати багатофакторну природу сучасних військових загроз критичній інфраструктурі такі як: імовірності ураженні одним типом боєприпасів, комбінованими типами боєприпасів, врахування деструктивного потенціалів об'єктів критичної інфраструктури. Вона створена для того, щоб надати більш точну та досконалу базу для прийняття управлінських рішень в умовах надзвичайних ситуацій та мінімізації можливих збитків та наслідків.

6. Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

7. Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Лисенко О., Чеканов І., Кутовий О. та Нікітін В. (2015) Стратегії управління ризиками на об'єктах критичної інфраструктури в умовах невизначеності. Науковий вісник УкрНДІПБ, 1, 134-139. URL: http://nbuv.gov.ua/UJRN/Nvundipb_2015_1_18 [Дата звернення 29 серпня 2023].
2. Чумаченко С., Троцький В. (2017). Оцінювання загроз об'єктам критичної інфраструктури. Науковий вісник: Цивільний захист та пожежна безпека, 1 (3), 41-47.
3. Бобро Д. (2015) Визначення критеріїв оцінки та загрози критичній інфраструктурі. Стратегічні пріоритети. Серія : Економіка, 4, 83-93. URL: http://nbuv.gov.ua/UJRN/spe_2015_4_12 [Дата звернення 29 серпня 2023].
4. Лисиченко Г., Забулонов Ю. та Хміль Г. (2008). Природний, техногенний та екологічний ризики: аналіз, оцінка, управління. Монографія, НАН України, Ін-т геохімії навколишнього середовища, 542 с.
5. Pederson P., Dudenhoeffer D., Hartley S. & Permann M. (2006). Critical Infrastructure Interdependency Modeling: A Survey of

References

1. Lysenko O., Chekanova I., Kutovyi O., Nikitin V. (2015) Risk management strategies on critical infrastructure objects under uncertainty. Scientific Bulletin of UkrNDIPB. 1, 134-139. Available from : http://nbuv.gov.ua/UJRN/Nvundipb_2015_1_18 [View date August 29, 2023].
2. Chumachenko S., Trotskyi V. (2017). Assessment of threats to critical infrastructure facilities. Scientific bulletin: *Civil defense and fire safety*, 1 (3), 41-47.
3. Bobro D. (2015). Determination of assessment criteria and threats to critical infrastructure. Strategic priorities. Series: Economy, 4, 83-93. Available from : http://nbuv.gov.ua/UJRN/spe_2015_4_12 [View date August 29, 2023].
4. Lysychenko G., Zabulonov Yu. & Khmil G. (2008) Natural, man-made and ecological risks: analysis, assessment, management. Monograph, National Academy of Sciences of Ukraine, Institute of geochemistry of the environment. environment, 542 p.
5. Pederson P., Dudenhoeffer D., Hartley S. & Permann M. (2006). Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research. Idaho National Laboratory, 126 p. Available

U.S. and International Research. Idaho National Laboratory, 126 p. URL: http://cip.management.dal.ca/publications/Critical%20Infrastructure%20Interdependency%20Modeling.pdf [Дата звернення 29 серпня 2023].

6. Environmental Assessment and Recovery Priorities for Eastern Ukraine / Denisov N., Averin D, Yushchuk A., Yermakov V., Ulytskyi O., Bystrov P., Zibtsev S., Chumachenko S, Nabyvanets Y. // Kyiv: VAITE, 2017. – 88 p. ISBN 978-966-2310-77-1. URL: https://www.osce.org/files/f/documents/4/3/362566_0.pdf [Дата звернення 29 серпня 2023].
7. Директива Ради 2008/114/ЄС від 8 грудня 2008 року Про ідентифікацію та позначення європейських критичних інфраструктур та оцінку потреби у покращенні їх захисту. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114 [Дата звернення 29 серпня 2023].
8. Уряднікова І., Чумаченко С., Кармазін С. та Тесленко О. (2015). Застосування експертно-аналітичних методів для оцінювання ризиків надзвичайних ситуацій на об'єктах критичної інфраструктури. Науковий вісник Академії муніципального управління. серія "Техніка", 1, 206-2018. URL: http://nbuv.gov.ua/UJRN/Nvamu_teh_2015_1_24 [Дата звернення 29 серпня 2023].
9. Чумаченко С., Кутовий О. та Михайлова А. (2020) Застосування експертно-аналітичних методів для оцінювання загроз об'єктам критичної інфраструктури оборонно-промислового комплексу на сході України. Інженерія природокористування, 4(18), 114-123. URL: https://repo.btu.kharkov.ua/bitstream/123456789/1580/1/17.pdf [Дата звернення 29 серпня 2023].
10. Фурсенко О.М., Чумаченко С.М. та Кармазин С.В. (2015) Експертна оцінка

from : http://cip.management.dal.ca/publications/Critical%20Infrastructure%20Interdependency%20Modeling.pdf [View date August 29, 2023].

6. Environmental Assessment and Recovery Priorities for Eastern Ukraine / Denisov N., Averin D, Yushchuk A., Yermakov V., Ulytskyi O., Bystrov P., Zibtsev S., Chumachenko S, Nabyvanets Y. // Kyiv: VAITE, 2017. – 88 p. ISBN 978-966-2310-77-1. Available from : https://www.osce.org/files/f/documents/4/3/362566_0.pdf [View date August 29, 2023].
7. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Available from : https://www.osce.org/files/f/documents/4/3/362566_0.pdf [View date August 29, 2023].
8. Uryadnikova I., Chumachenko S., Karmazin S. and Teslenko O. (2015) Application of expert-analytical methods for assessing the risks of emergency situations at critical infrastructure facilities. Scientific Bulletin of the Academy of Municipal Management. series "Technology", 1, 206-2018. URL: http://nbuv.gov.ua/UJRN/Nvamu_teh_2015_1_24 [View date August 29, 2023].
9. Chumachenko S., Kutovyi O. and Mykhaylova A. (2020). Application of expert analytical methods to assess threats to critical infrastructure objects of the defense-industrial complex in eastern Ukraine. Environmental engineering, 4(18), 114-123. Available from : https://repo.btu.kharkov.ua/bitstream/123456789/1580/1/17.pdf [View date August 29, 2023].
10. Fursenko O. M., Chumachenko S. M. and Karmazyn S.V. (2015) Expert assessment of threats to objects of critical infrastructure of the gas transportation system of Ukraine using the method of analysis of hierarchies. Technogenic and

загроз для об'єктів критичної інфраструктури газотранспортної системи України з використанням методу аналізу ієрархій. Техногенно-екологічна безпека та цивільний захист, 9, 68-77. URL: http://tes.igns.gov.ua/wp-content/uploads/2018/02/V9.pdf [Дата звернення 29 серпня 2023].

11. Бірюков Д., Заславський В., Євгієнко В. та Франчук О. (2009) Моделювання та оцінка сценаріїв загроз для об'єктів критичної інфраструктури. Наукові записки, том 99, 97-101. URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/d255303b-5c2e-480d-9083-a7562058f849/content
12. Чумаченко С., Мурасов Р. та Мельник Я. (2021). Теоретико-методологічні основи інформаційного аналізу еколого-техногенних загроз для об'єктів критичної інфраструктури в умовах збройного конфлікту на сході України. Сучасні інформаційні технології у сфері безпеки та оборони, 1 (40)/2021, 117-122. https://doi.org/10.33099/2311-7249/2021-40-1-117-122
13. Мурасов Р, Чумаченко С., Пиріков О, Гуйда О. та Ківа І. (2021) Особливості побудови математичної моделі оцінювання загроз для об'єктів критичної інфраструктури з використанням теорії графів. Вчені записки ТНУ імені В.І. Вернадського серія "Технічні науки", 6, 110-116. https://doi.org/10.32838/2663-5941/2021.6/18
14. Мурасов Р., Куртсеїтов Т., Чумаченко С., Луньова О., Пиріков О., Луньов А. та Чумаченко С. (2022) Математична модель оцінки загроз для об'єктів критичної інфраструктури в зоні ведення бойових дій. Проблемне програмування, 3-4, 446-454. https://doi.org/10.15407/pp2022.03-04.446

ecological safety and civil protection, 9, 68-77. Available from : http://tes.igns.gov.ua/wp-content/uploads/2018/02/V9.pdf [View date August 29, 2023].

11. Biryukov D., Zaslavskii V., Evgienko V. & Franchuk O. (2009). Thread scenarios modeling and assessment for critical infrastructure. Scientific notes, volume 99, 97-101. Available from : https://ekmair.ukma.edu.ua/server/api/core/bitstreams/d255303b-5c2e-480d-9083-a7562058f849/content [View date August 29, 2023].
12. Chumachenko S., Murasov R. & Melnyk Y. (2021). Theoretical and methodological basis of information analysis of ecological and man-general threats for potentially hazardous facilities of critical infrastructure in the conditions of the armed conflict in the east of Ukraine. Modern information technologies in the field of security and defense, 1 (40)/2021, 117-122. https://doi.org/10.33099/2311-7249/2021-40-1-117-122 [View date August 29, 2023].
13. Murasov, R., Chumachenko, S., Pirikov, O., Huyda, O., and Kiva, I. (2021) Peculiarities of building a mathematical model of threat assessment for critical infrastructure objects using graph theory. Academic notes of TNU named after V.I. Vernadsky series "Technical Sciences", 6, 110-116. https://doi.org/10.32838/2663-5941/2021.6/18 [View date August 29, 2023].
14. Murasov R., Kurtseitov T., Chumachenko S., Lunyova O., Pirikov O., Lunyov A. and Chumachenko S. (2022). Mathematical model of threat assessment for critical infrastructure facilities in the war zone. Problem Programming, 3-4, 446-454. https://doi.org/10.15407/pp2022.03-04.446 [View date August 29, 2023].