

# Удосконалення науково-методичного апарату обчислення ризиків виникнення та аналізу сценаріїв надзвичайних ситуацій на об'єктах критичної інфраструктури

## Improvement of the scientific and methodological apparatus for calculating the risks of occurrence and analyzing scenarios of emergency situations at critical infrastructure facilities

**Рустам Мурасов<sup>A</sup>**

Corresponding author: к. техн. наук, професор кафедри, e-mail: [rustamm@ukr.net](mailto:rustamm@ukr.net), ORCID: 0000-0003-0800-2062

**Анатолій Нікітін<sup>A</sup>**

Доктор філософії, професор кафедри, e-mail: [tolik-nikitin@ukr.net](mailto:tolik-nikitin@ukr.net), ORCID: 0000-0003-1487-0616

**Іван Мещеряков<sup>A</sup>**

Доктор філософії, доцент кафедри, e-mail: [shulyk3004@ukr.net](mailto:shulyk3004@ukr.net), ORCID: 0000-0001-5797-0735

**Микола Підгородецький<sup>A</sup>**

к. техн. наук, начальник кафедри, e-mail: [nickpidhorodetskyi@gmail.com](mailto:nickpidhorodetskyi@gmail.com), ORCID: 0000-0003-4807-8635

**Сергій Поплавець<sup>B</sup>**

Доктор філософії, професор кафедри, e-mail: [serg751505@gmail.com](mailto:serg751505@gmail.com), ORCID: 0009-0003-7538-0941

**Rustam Murasov<sup>A</sup>**

Corresponding author: Candidate of Technology Sciences, Professor of the Department, e-mail: [rustamm@ukr.net](mailto:rustamm@ukr.net), ORCID: 0000-0003-0800-2062

**Anatolii Nikitin<sup>A</sup>**

Doctor of Philosophy, professor of the department, e-mail: [tolik-nikitin@ukr.net](mailto:tolik-nikitin@ukr.net), ORCID: 0000-0003-1487-0616

**Ivan Meshcheriakov<sup>A</sup>**

Doctor of Philosophy, associate professor of the department, e-mail: [shulyk3004@ukr.net](mailto:shulyk3004@ukr.net), ORCID: 0000-0001-5797-0735

**Mykola Pidhorodetskyi<sup>A</sup>**

Candidate of Technology Sciences, Head of the Department, e-mail: [nickpidhorodetskyi@gmail.com](mailto:nickpidhorodetskyi@gmail.com), ORCID: 0000-0003-4807-8635

**Serhii Poplavets<sup>B</sup>**

Doctor of Philosophy, Professor of the Department, e-mail: [serg751505@gmail.com](mailto:serg751505@gmail.com), ORCID: 0009-0003-7538-0941

<sup>A</sup> Національний університет оборони України, м. Київ, Україна

<sup>B</sup> Харківський національний університет Повітряних Сил імені Івана Кожедуба, м. Харків, Україна

<sup>A</sup> National Defense University of Ukraine, Kyiv, Ukraine

<sup>B</sup> Kharkiv National University of the Air Force named after Ivan Kozhedub, Kharkiv, Ukraine

Received: February 1, 2024 | Revised: February 20, 2024 | Accepted: February 29, 2024

DOI: 10.33445/sds.2024.14.1.17

**Мета роботи:** мінімізація наслідків надзвичайних ситуацій шляхом застосування удосконаленого науково-методичного апарату.

**Метод:** теорія ймовірності, теорія графів, алгебра логіки, імітаційне моделювання.

**Результати дослідження:** удосконалено науково-методичний апарат обчислення ризиків виникнення та аналізу сценаріїв надзвичайних ситуацій на об'єктах критичної інфраструктури з метою запобігання виникнення та мінімізації впливу наслідків надзвичайних ситуацій.

**Теоретична цінність дослідження:** попередження надзвичайних ситуацій терористичного характеру шляхом оцінки деструктивних подій в умовах каскадних наслідків терористичного впливу.

**Тип статті:** описовий та дослідницький.

**Ключові слова:** критична інфраструктура, надзвичайна ситуація, мінімізація наслідків надзвичайних ситуацій, розробка моделей надзвичайних ситуацій.

**Purpose:** minimization of the consequences of emergency situations through the use of advanced scientific and methodological apparatus.

**Method:** probability theory, graph theory, logic algebra, simulation modeling.

**Findings:** the scientific and methodical apparatus for calculating the risks of occurrence and analyzing scenarios of emergency situations at critical infrastructure objects has been improved in order to prevent the occurrence and minimize the impact of the consequences of emergency situations.

**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.

**Key words:** critical infrastructure, emergency situation, minimization of consequences, development of emergency models.

## Вступ

Повномасштабна агресія росії проти України свідчить про те, що класичні методи та апарати оцінювання ризиків виникнення надзвичайних ситуацій та їх наслідків потребує суттєвого доопрацювання та удосконалення. Особливо актуально це є в умовах цілеспрямованого нанесення ракетно-дронових ударів росією по об'єктах критичної інфраструктури на всю глибину території України з метою виклику масштабних екологічних, техногенних то соціо-гуманітарних катастроф (рис. 1). Головною метою вчинення таких нелюдських дій є масштабні вторинні деструктивні наслідки знищення населення та екології на території України. В умовах обмеження сил і засобів оборони держави з метою своєчасного і ефективного прикриття визначених об'єктів критичної інфраструктури та мінімізації наслідків надзвичайних ситуацій Силам оборони України вкрай необхідно розробити моделі процесів виникнення, розвитку, локалізації та ліквідації надзвичайних ситуацій.

Одним з перспективних напрямків дослідження ризику виникнення, оцінки наслідків та аналізу протікання надзвичайних ситуацій у разі зруйнування об'єктів критичної інфраструктури є розробка сценаріїв самих надзвичайних ситуацій. Даний підхід дозволяє генерувати множину варіантів надзвичайних ситуацій, здійснювати пошук за визначеними параметрами, ключовими об'єктами та обирати максимально небезпечні варіанти дій з метою запобігання та мінімізації руйнівних наслідків.

## Теоретичні основи дослідження

Аналіз останніх публікацій [1-4], що стосується підходів до оцінювання загроз і ризиків, показав що було виявлено недостатній розвиток їх математичного і комп'ютерного моделювання для об'єктів критичної інфраструктури (ОКІ) в умовах війни (рис. 2). Головним чином автори використовують оціночний підхід з використанням експертних оцінок, що звужує можливості вірного та послідовного оцінювання ситуації.

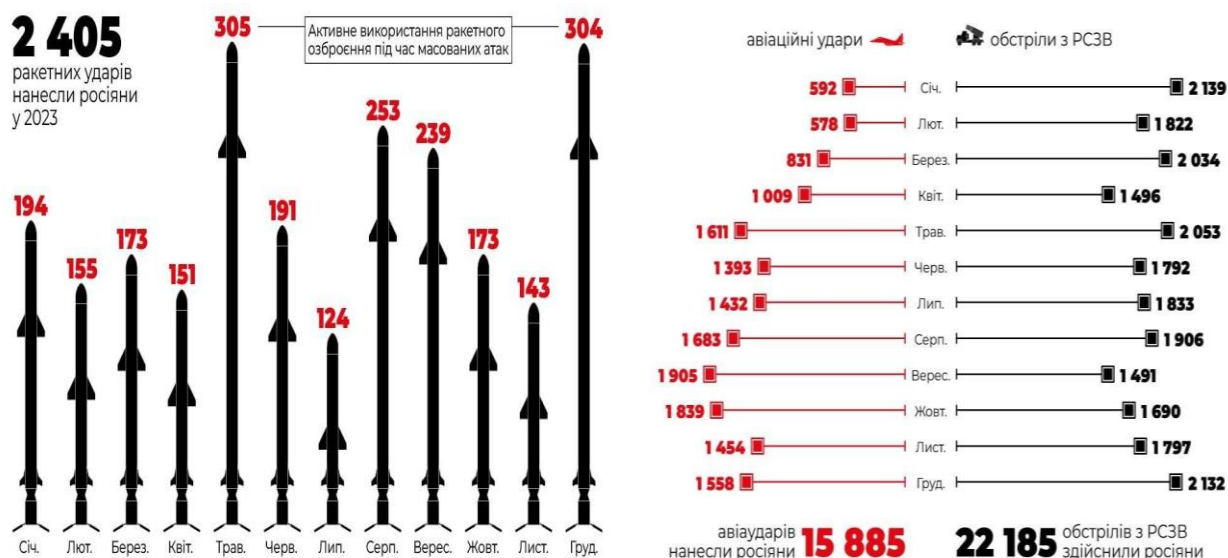


Рисунок 1 – Кількість ракетних ударів, авіа-ударів та артобстрілів нанесених рф по Силах оборони України та населених пунктах у 2023 році [15]

За думкою багатьох провідних фахівців [5-10], у наш час не існує загальноприйнятої методики оцінки ризиків та загроз для ОКІ, особливо в умовах ракетно-дронових ударів, є часткові рішення для конкретних об'єктів (випадків) [11-13]. Основною вимогою було забезпечення мінімізації наслідків надзвичайної ситуації (НС) на ОКІ, розвиток сценаріїв як

правило не розглядався. Світовий досвід також обмежувався ліквідацією наслідків техногенної або природної катастрофи для певного ОКІ. При чому обмеження сил і засобів для ліквідації або мінімізації наслідків там не розглядається.

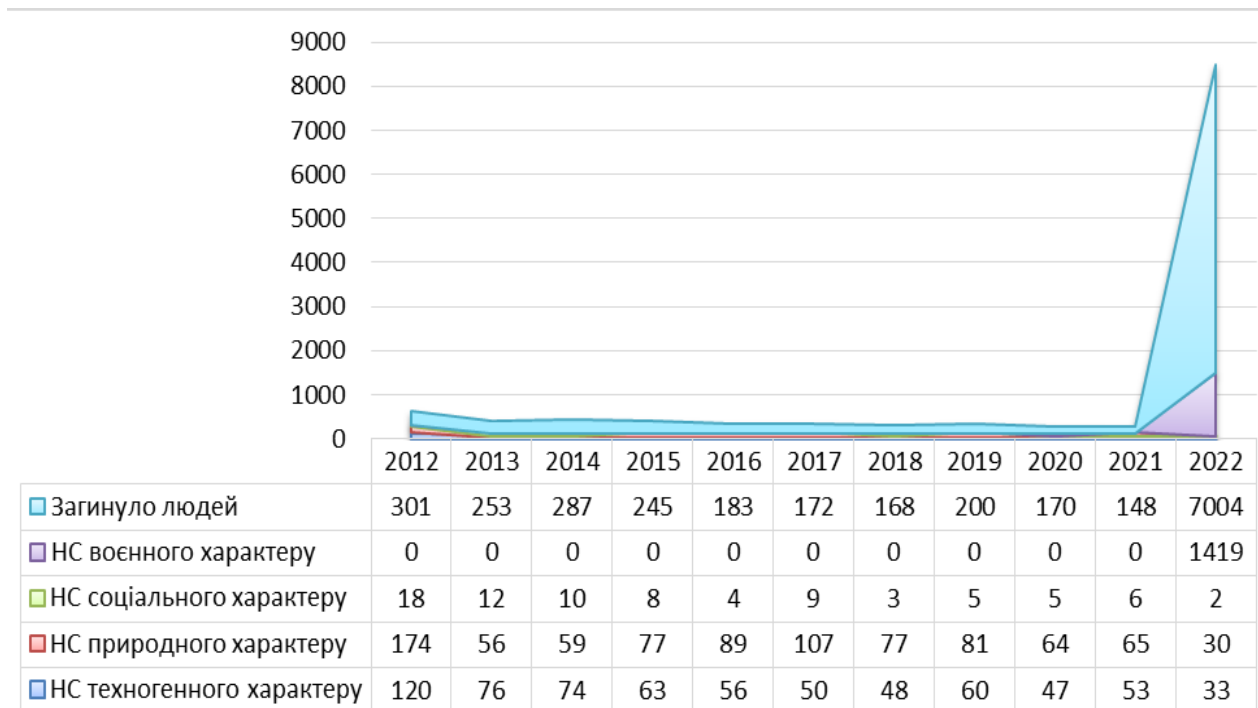


Рисунок 2 – Статистика надзвичайних ситуацій воєнного, соціального, природного, техногенного характеру та кількість жертв 2012 – 2022 р.р. [16]

Тому виникає необхідність, щодо удосконалення науково-методичного апарату обчислення ризиків виникнення та аналізу сценаріїв НС на ОКІ [14].

### **Постановка проблеми**

Важливим кроком подальших досліджень є саме перехід від концепції захисту одного ОКІ та ліквідації наслідків НС в наслідок його руйнування до формування сценаріїв НС з визначенням ключових ОКІ. Це передбачає детальне вивчення різноманітних сценаріїв, в яких ОКІ можуть бути зруйновані, та можливі наслідки цих дій. Враховуючи наведене доцільно визначити ризики виникнення НС на ОКІ.

Таким чином, удосконалення науково-методичного апарату обчислення ризиків виникнення та аналізу сценаріїв НС на ОКІ вимагає детального дослідження можливих варіантів зруйнувань ОКІ, аналізу їхнього впливу та формування найбільш деструктивних сценаріїв НС з метою запобігання виникнення та мінімізації впливу наслідків НС.

### **Результати**

Об'єкти критичної інфраструктури, складаються з множини технологічних елементів, розподілених в просторі. В результаті аналізу небезпеки і функціонування ОКІ виділяється множина їх дискретних джерел небезпеки ( $i = 1..J$ ), з'ясовується їх розташування і властивості, які необхідні для моделювання. Досліджувана система розбивається на підсистеми (блоки), до складу яких входять елементи моделі небезпечних сценаріїв, стан яких (відмова, спрацьовування) однозначно визначає небезпеку, що проявляється та її масштаб (потужність

прояви). Крім того, виділяється множина об'єктів (будівлі, конструкції, обладнання, об'єкти життєдіяльності, екологічні об'єкти т.і.), що мають цінність і потрапляють під вплив негативних факторів аварій. Ці об'єкти називаються "ключові об'єкти" які, розподілені в просторі та мають властивості і показники, які необхідні для моделювання технологічної системи об'єктів критичної інфраструктури (ТСОКІ).

Елементи ТСОКІ, що входять до складу блоків, переходять в різні стани в залежності від дискретних подій (відмова, спрацьовування, вплив) і процесів (поток, зміна температури, тиску і т. д.), що відбуваються в реальному часі і просторі. Аналіз причинно-наслідкових зв'язків таких переходів формалізується методами логічного моделювання. Для кожного  $i$ -го джерела небезпеки виділяється множина  $j$ -х станів, обумовлених сполученнями комбінацій відмов, відхилень, режимів роботи, що призводять до аварій, аварійних процесів зі значними негативними наслідками.

Розробка моделі небезпечних сценаріїв (МНС) досліджуваного ОКІ, на відміну від відомих методів дискретно-подієвого моделювання, здійснюється за рахунок формалізованого опису причинно-наслідкових зв'язків між стохастичними подіями і детермінованими процесами, які можуть відбуватися в ТСОКІ. Модель небезпечних сценаріїв, що розробляється в цьому дослідженні, дозволяє аналізувати сукупності сполучень подій і процесів, які відповідають цим сполученням по ланцюгам причинно-наслідкових зв'язків. При цьому обчислюються ймовірності переходу системи в різні стани і показники фізичних процесів, а також наслідків, до яких ці процеси призводять.

Моделювання з використанням операцій логіки проводиться по відношенню до стохастичних подій і процесів в ТСОКІ суміщеними методами побудови "графів відмов" (FTA – fault tree analysis) і "графів подій" (ETA – event tree analysis) [17].

Спочатку на основі визначення небезпеки і працездатності формалізуються та описуються причинно-наслідкові ланцюги подій в ТСОКІ у формі "графів відмов". Кількість "графів відмов" відповідає всім розглянутим в схемі формування моделі небезпечних сценаріїв, ініційованим аварійними подіями.

При створенні "графа відмов" застосовується низхідний метод аналізу. У цьому методі "верхня подія" є основним результатом аварійних поєднань (причин), об'єднаних логічними операціями кон'юнкції для спільних подій і диз'юнкції для несумісних подій у гілках графів відмов. Кожне ініціювання аварійної події може взаємодіяти з іншими, створюючи ланцюг подій.

Верхня подія кожного "графа відмов" може бути початковою подією "графа подій" або ініціювати аварійний фізичний процес, що призводить до втрат. У першому випадку будується бінарний "граф подій", відображаючи логіку та ймовірність надійності і ефективності засобів захисту. Гілки цього графа відображають виникнення різних аварійних фізичних процесів.

Моделювання ланцюгів подій для графа станів системи, яке отримується за допомогою низхідного та висхідного аналізу, дозволяє отримати логічну структуру подій, що призводять до різних сценаріїв аварій. Цей підхід вирізняється тим, що поєднує методи функціонального та елементарного аналізу, встановлюючи відповідність між гілками елементарного аналізу та математичними моделями детермінованих фізичних процесів.

Отримані ланцюги об'єднуються в граф станів, що дозволяє провести аналіз за алгоритмом. Розрахунки можливих станів системи за допомогою такого графа, на відміну від інших методів, дозволяють врахувати просторово-часові особливості виникнення і розвитку аварій з урахуванням стохастичних показників, що відображають рівень непевності та ймовірності в системі.

На рис. 3 представлена структурно-логічна схема формування моделі сценаріїв НС.

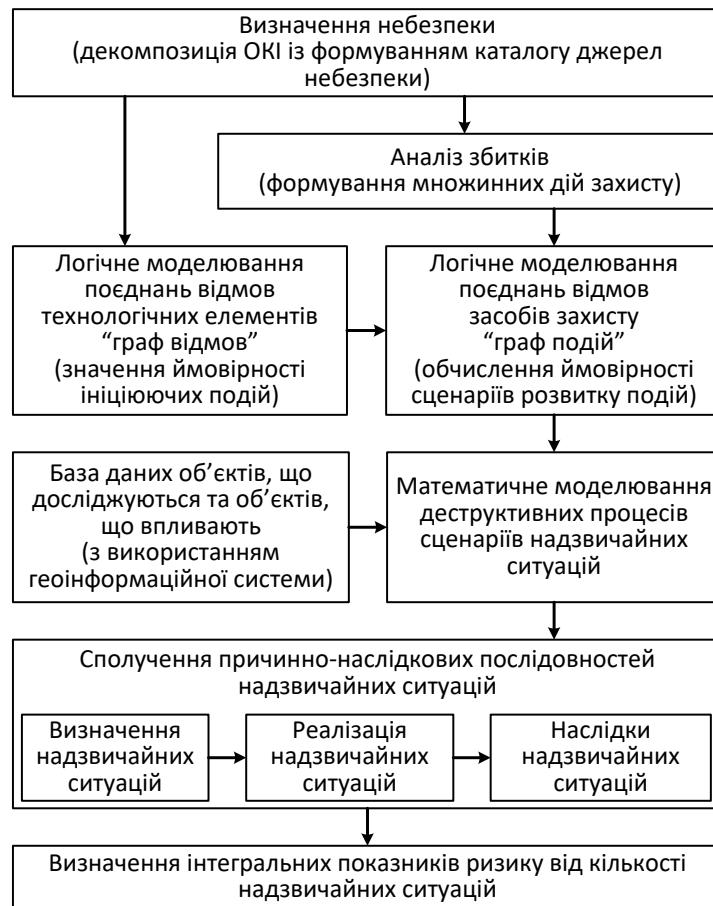


Рисунок 3 – Структурно-логічна схема формування моделі сценаріїв НС

Пропонується використовувати методи, моделі та інформаційні технології для оцінки техногенного ризику, що відрізняються від існуючих комбінованим підходом до моделювання станів ТСОКІ, що враховує просторове взаємне розташування джерел небезпеки, причинно-наслідкові зв'язки між спільними і несумісними подіями і процесами в ТСОКІ, сполучення між різними моделями. Застосування таких зв'язкових методів моделювання дозволяє автоматично отримувати інтегральні показники ризику.

Інтегральні показники ризику нормовані і представлені в різних джерелах [4, 18].

До інтегральних показників ризику, обумовленого множинними незалежними джерелами небезпеки, в основному відносяться:

1. Імовірність ураження ( $k=\{\text{смертельного, тяжкого, легкого}\}$ ) людини в результаті негативного впливу, що обумовлений  $j$ -ми аварійними процесами  $i$ -х джерел небезпеки:

$$P_t^k(x, y) = \sum_i \sum_j P_{ij}^k(x, y), \quad (1)$$

територіальний ризик є просторовою характеристикою небезпеки.

2. Імовірність ураження індивідуума з урахуванням його знаходження в просторі впливу уражаючих факторів протягом часу перебування:

$$P_t^k = \sum_s T_s(x, y) \cdot P_t^k(x, y), \quad (2)$$

де,  $T_s(x, y)$  – функція ймовірності знаходження індивідуума в  $s$  – зоні ураження в період часу, що відповідає імовірності ураження  $P_t^k$ .

3. Очікуване число уражених:

$$Nm = \int \int_{x y} P_I^k(x, y) \cdot n(x, y) dy dx, \quad (3)$$

де,  $n(x, y)$  – математичне очікування розподілу щільності людей, що попадають до уражаючого впливу джерел небезпеки ОКІ.

4. Очікувані матеріальні збитки:

$$Um = \sum_i \sum_j P_{f_{ij}} \cdot Ud_{ij}, \quad (4)$$

де,  $P_{f_{ij}}$  – ймовірність  $j$ -ї аварії  $i$ -го джерела небезпеки з заданими параметрами для ОКІ;

$Ud_{ij}$  – значення можливого збитку, що настає при реалізації  $j$ -ї аварії.

Пропонується визначати рівень прийняттого ризику як доповнення до характерного побутового ризику всіх його носіїв на підставі довірчого інтервалу для ймовірності, характерної для побутового ризику.

В кожному окремому випадку прийнятний рівень ризику може бути переглянутий, за винятком встановленого в законодавчому порядку.

Прийнятність ризику економічних втрат визначається на основі аналізу наслідків і їх ймовірності, а також можливостей підприємства по ліквідації наслідків і відновлення. У разі очевидної неможливості вкладення коштів на ліквідацію наслідків і відновлення при можливих максимальних наслідках, ризик неприйнятний. У великій мірі це визначається страхуванням і можливістю акумуляції фінансових коштів. У будь-якому випадку, очікувані витрати на запобігання аварій не повинні перевищувати очікуваний збиток, інакше попереджувальні заходи є надмірними.

Показниками прийняттого ризику можуть вважатися критеріальні значення, що визначають:

– граничне значення припустимого територіального ризику  $Pt_L$ , визначається як вірогідність смертельного ураження людини на даній території протягом року;

– граничне значення припустимого індивідуального ризику  $Pl_L$ , визначається як вірогідність смертельного ураження індивідуума в результаті можливого прояву небезпек від ОКІ протягом року;

– граничне значення очікуваного числа уражених  $Nm_L$  протягом року в результаті можливого прояву небезпек від ОКІ;

– значення граничного соціального (колективного) ризику  $Ps_L$ , що визначається зазвичай як ймовірність загибелі 10 і більше осіб;

– граничний очікуваний матеріальний збиток  $Um_L$ , значення якого визначається на підставі фінансових можливостей підприємства і страхових компаній.

Описані показники є вхідними обмежувачами простору допустимого ризику.

Для визначення основних показників ризику (ймовірностей подій і кількісних показників їх наслідків) необхідно моделювання техногенних процесів і обробка інформаційних потоків методами, що дозволяють виділити сценарії виникнення і розвитку надзвичайних ситуацій, в яких перевищені допустимі показники. На рис. 4 наведена структурно-логічна схема процесу оцінювання ризиків виникнення НС на ОКІ.

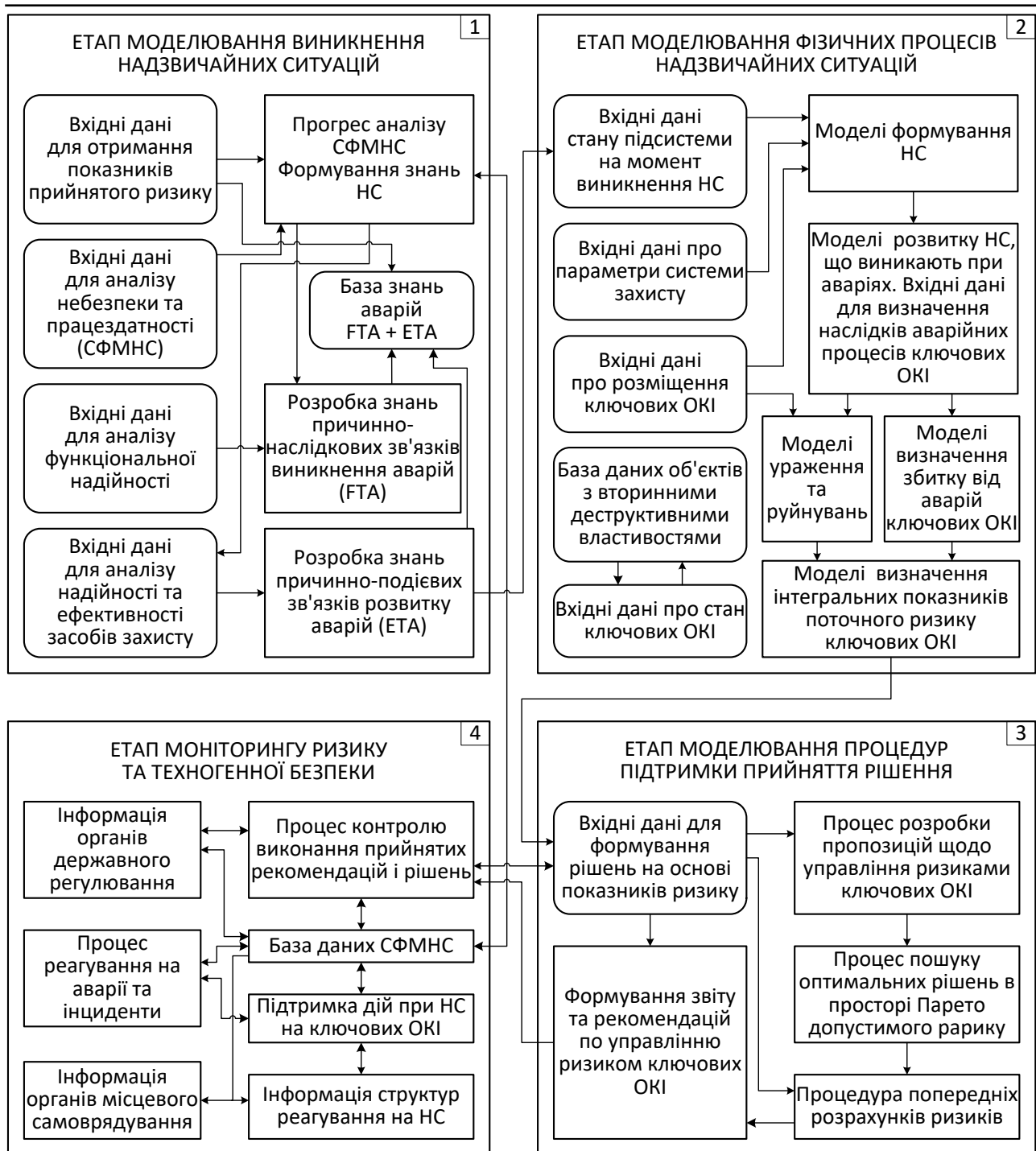


Рисунок 4 – Структурно-логічна схема процесу оцінювання ризиків виникнення надзвичайних ситуацій на об'єктах критичної інфраструктури

Представлена на рис. 4 структура, що складається з 4-х послідовних етапів, а саме:

1. Етап моделювання виникнення НС;
2. Етап моделювання фізичних процесів НС;
3. Етап моделювання процедур підтримки прийняття рішень;
4. Етап моніторингу ризику та техногенної безпеки до етапів моніторингу ризику.

Розглянемо зміст етапів більш детально:

**Перший етап моделювання виникнення надзвичайних ситуацій** призначений для локалізації завдання дослідження, збору та обробки вхідних даних і процесу формування знань про ОКІ, території та об'єктах відповідальності, що дозволяють провести моделювання

можливих негативних наслідків, що лежать в основі ризику. На цьому етапі реалізуються методи аналізу небезпеки і виробляються критеріальні значення прийнятного ризику для досліджуваних ОКІ. В результаті створюється база знань небезпечних процесів на ОКІ і визначаються кількісні показники надійності і ефективності засобів захисту і засобів подвійного призначення, формується основа для моделювання оцінки ризику;

**Другий етап моделювання фізичних процесів надзвичайних ситуацій** дозволяє застосувати вхідні дані, моделі виникнення і розвитку НС для визначення можливих і очікуваних наслідків аварійних процесів на ОКІ;

**Третій етап моделювання процедур підтримки прийняття рішень** забезпечує процеси розробки звіту і вироблення рекомендацій та вимог до корегування ризику виникнення НС на ОКІ. На цьому етапі вибираються рішення, оптимальні в сенсі Парето та формування рекомендацій по управлінню ризиком ключових ОКІ;

**Четвертий етап моніторингу ризику та техногенної безпеки** призначений для контролю і організації виконання прийнятих рішень і підтримки та здійснення інформування відповідних органів та структур.

На відміну від існуючих інформаційних технологій, моделей і методів оцінки ризику, пропонується авторами статті інформаційна технологія передбачає комплексне моделювання процесів оцінки ризику виникнення НС на ОКІ шляхом ситуаційно-орієнтованої спрямованої формалізації сценаріїв виникнення, розвитку та впливів процесів ТСОКІ. При цьому синтез моделей здійснюється шляхом поєднання формальних методів математичної логіки і математичних моделей деструктивних процесів ОКІ, що відбуваються в часі і просторі в послідовності, яка задається.

При цьому повний набір об'єднаних синтезованих моделей представляється як орієнтовний граф.

На відміну від відомих методів дискретно-подієвого моделювання (DES - Discrete Event Simulation) [19] пропонується врахувати як стохастичні параметри, що виникають в графі подій, так і послідовність (хронологію) і динамічні характеристики сполучень взаємовпливаючих і взаємозалежних подій. Для такої формалізації пропонується нижченаведений математичний апарат.

Орієнтовний граф визначається як

$$Ge = (E \rightarrow U), \quad (5)$$

- де,  $E$  – множина подій (станів, відмов, спрацьовувань і т. д. елементів ТСОКІ);  
 $\rightarrow$  – відношення, що визначає причинно-наслідковий зв'язок подій, що формують ребра графа станів;  
 $U$  – сигнатура графа, яка містить множину логічних операцій. Крім цього вводиться відношення слідування, в якому враховується часовий наслідок подій  $\rightarrow^{dt}$ , яке встановлює бінарне відношення логічної ситуації виду:

$$f(a) \rightarrow^{dt} event. \quad (6)$$

Таке відношення встановлює зв'язок між логічною функцією висловлювань “причини” (що ініціюють події або впливи в системі)  $f(a)$  і зв'язковою з ними наступним протягом проміжку часу  $dt$  подією  $event$ . Логічна функція приймає значення “істина” відповідно до логічної формули висловлювання, записаної в галузі “графа подій” і крім цього містить обчислену вагу ймовірності настання події. Логічні висловлювання між подіями-попередниками і подіями-наслідками формально описують незалежні і спільні події, що визначаються логікою, виявленої при аналізі небезпеки.

Наприклад: запис виду  $(e_2 \vee e_3)e_1 \wedge c \rightarrow^{dt_1} e_4$  означає, що за умови виникнення істинного поєднання подій  $e_1$  і  $e_2$  або  $e_1$  і  $e_3$  через час  $dt_1$  настає подія  $e_4$ .

Послідовність орграфу станів можуть характеризуватися потоками подій (аварійними поєднаннями), які можуть містити змішані стохастичні і детерміновані події. Для аналізованих формальних описів ТСОКІ характерні неоднорідні потоки подій  $Te = (e_i | i = \overline{1, n})$ , де події характеризуються якимись параметрами події  $p_{1_i}, \dots, p_{k_i}$  (ознаками його настання)  $e_i = \langle t_i, p_{1_i}, \dots, p_{k_i} \rangle$ ,  $t_i$  – час настання події. Якщо час настання події не впливає на наслідки їх реалізації, то воно обнуляється. При цьому потоком залежних подій називається впорядкована множина  $Te = (e_i | i = \overline{1, n})$ , така що:

$$\forall e_i \in Te / \{e_1\} \exists! e_j \in Te \left( (e_j \wedge c_j \rightarrow^{dt_j} e_i) \oplus (e_j \wedge c_j \rightarrow_{\text{can}}^{dt} e_i) \right), \quad (7)$$

де,  $c_j$  і  $dt_j$  – відповідно умова і час виконання або відмови події  $e_i$ , що є наслідком події  $e_j$ .

Потоки подій можуть мати властивості таких, що перетинаються, таких, що не перетинаються, паралельних, послідовних, а події в різних потоках можуть бути спільними, несумісними і незалежними.

Потоки, в яких підсумкові події сценаріїв збігаються, є такими, що сходяться, в разі збігу вхідних подій – розбіжними. Таким чином, правильно побудовані “графи відмов” характеризуються потоками, що сходяться, а “графи подій” – розходяться. Так як в різних графах присутні елементи ТСОКІ, що мають багатофункціональне призначення або які є засобами подвійного призначення (технологічного та протиаварійного), потоки різних графів можуть перетинатися.

Наведені вище формальні символічні представлення, що описують причинно-наслідкові зв'язки подій, потоків подій і операцій над потоками і виразами, а також можливість формально включати в потоки подій математичні моделі фізичних процесів з урахуванням їх динаміки в сукупності представляють собою алгебру подій і їх відповідностей. Така алгебра дозволяє в формальному вигляді імітувати поведінку складної дискретної системи як на рівні елементарних подій і впливів, що збурюють, так і на рівні процесів і явищ, що проявляються при виникненні і розвитку аварій. Запропонований формальний механізм дозволяє синтезувати, перетворювати і аналізувати подієві моделі в різних напрямках і розробити алгоритми автоматичних обчислень параметра графа станів, який є моделлю, що описує поведінку ТСОКІ.

## Висновки

У статті удосконалено науково-методичний апарат обчислення ризиків виникнення та аналізу сценаріїв НС на ОКІ за рахунок детального дослідження можливих варіантів зруйнувань ОКІ, аналізу їхнього впливу та формування найбільш деструктивних сценаріїв НС з метою запобігання виникнення та мінімізації впливу наслідків НС. Розроблена структурно-логічна схема формування моделі сценаріїв НС, у якій на відміну від відомих методів дискретно-подієвого моделювання застосовується формалізований опис причинно-наслідкових зв'язків між стохастичними подіями і детермінованими процесами, які можуть відбуватися в ТСОКІ. Застосування таких зв'язкових методів моделювання дозволяє автоматично отримувати інтегральні показники ризику. В статті наведена структурно-логічна схема процесу оцінювання ризиків виникнення НС на ОКІ, завдяки якій можливо виділити сценарії виникнення і розвитку надзвичайних ситуацій, в яких перевищені допустимі показники. Запропонований в статті

математичний апарат дозволяє провести формалізацію як стохастичних параметрів, що виникають в графі подій, так і послідовності (хронології) і динамічні характеристики сполучень взаємовпливаючих і взаємозалежних подій.

### **Фінансування**

Це дослідження не отримало конкретної фінансової підтримки.

### **Конкуруючі інтереси**

Автори заявляють, що у них немає конкуруючих інтересів.

### **Список використаних джерел**

1. Лисенко О., Чеканов І., Кутувий 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](http://nbuv.gov.ua/UJRN/Nvundipb_2015_1_18) [Дата звернення 1 лютого 2024].
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](http://nbuv.gov.ua/UJRN/spe_2015_4_12) [Дата звернення 1 лютого 2024].
4. Лисиченко Г., Забулонов Ю. та Хміль Г. (2008). Природний, техногенний та екологічний ризики: аналіз, оцінка, управління. Монографія, НАН України, Ін-т геохімії навколиш. середовища, 542 с.
5. Pederson P., Dudenhofer D., Hartley S. & Permann M. (2006). Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research. Idaho National Laboratory, 126 p. URL: <http://cip.management.dal.ca/publications/Critical%20Infrastructure%20Interdependency%20Modeling.pdf> [Дата звернення 1 лютого 2024].
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](https://www.osce.org/files/f/documents/4/3/362566_0.pdf) [Дата звернення 1 лютого 2024].
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 1 лютого 2024].
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](http://nbuv.gov.ua/UJRN/Nvamu_teh_2015_1_24) [Дата звернення 1 лютого 2024].
9. Мурасов Р., Нікітін А., Мещеряков І., Підгородецький М. та Поплавець С. (2023). Методика оцінювання загроз і ризиків для об'єктів критичної інфраструктури за сценаріями розвитку надзвичайних ситуацій. Сучасні інформаційні технології у сфері безпеки та оборони, 3(48)/2023, 35-43. <https://doi.org/10.33099/2311-7249/2023-48-3-35-43> [Дата звернення 1 лютого 2024].
10. Мурасов Р., Мещеряков І. (2023). Інформаційно-технічний метод попередження надзвичайних ситуацій терористичного характеру шляхом оцінки можливості ступеневого росту

деструктивних подій викликаних каскадними наслідками первинного терористичного впливу. *Social Development & Security*, 13(5), 180-191. <https://doi.org/10.33445/sds.2023.13.5.17> [Дата звернення 1 лютого 2024].

11. Чумаченко С., Кутувий 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 1 лютого 2024].
12. Фурсенко О.М., Чумаченко С.М. та Кармазин С.В. (2015) Експертна оцінка 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 1 лютого 2024].
13. Бірюков Д., Заславський В., Євгійко 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> [Дата звернення 1 лютого 2024].
14. 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> [Дата звернення 1 лютого 2024].
15. У 2023 році росіяни завдали по Україні десятки тисяч ударів: інфографіка. URL: <https://www.unian.ua/war/u-2023-roci-rosiyani-zavdali-po-ukrajini-desyatki-tisyach-udariv-infografika-12500187.html> [Дата звернення 1 лютого 2024].
16. Звіт про основні результати діяльності Державної служби України з надзвичайних ситуацій у 2022 році. URL: <https://dsns.gov.ua/upload/1/6/4/9/3/5/0/publicnii-zvit-2022-ostannia-versiia-1.pdf> [Дата звернення 1 лютого 2024].
17. Наказ Міністерства праці та соціальної політики від 04.12.2022 № 637 Про затвердження Методики визначення ризиків та їх прийнятих рівнів для декларування об'єктів підвищеної небезпеки. URL: [https://zakononline.com.ua/documents/show/34982\\_34982](https://zakononline.com.ua/documents/show/34982_34982) [Дата звернення 1 лютого 2024].
18. Хенли Э.Дж., Кумамото Х. (1984). Надежность технических систем и оценка риска. *Машиностроение*, 528 с. URL: [http://www.immsp.kiev.ua/postgraduate/Biblioteka\\_trudy/NadezhnostTekhnicheskikhSistemKumamoto1984.pdf](http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/NadezhnostTekhnicheskikhSistemKumamoto1984.pdf) [Дата звернення 1 лютого 2024].
19. Лоу А.М., Кельтон В.Д. (2004). Имитационное моделирование. *Классика CS*. 3-е изд. Издательская группа ВHV, 847 с. URL: [https://heterarchica.files.wordpress.com/2017/01/1kel\\_ton\\_v\\_lou\\_a\\_imitatsionnoe\\_modelirovanie.pdf](https://heterarchica.files.wordpress.com/2017/01/1kel_ton_v_lou_a_imitatsionnoe_modelirovanie.pdf) [Дата звернення 1 лютого 2024].

## 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](http://nbuv.gov.ua/UJRN/Nvundipb_2015_1_18) [View date February 1, 2024].
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](http://nbuv.gov.ua/UJRN/spe_2015_4_12)

[View date February 1, 2024].

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 from : <http://cip.management.dal.ca/publications/Critical%20Infrastructure%20Interdependency%20Modeling.pdf> [View date February 1, 2024].
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](https://www.osce.org/files/f/documents/4/3/362566_0.pdf) [View date February 1, 2024].
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](https://www.osce.org/files/f/documents/4/3/362566_0.pdf) [View date February 1, 2024].
8. Uryadnikova I., Chumachenko S., Karmazin S. & 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. Available from : [http://nbuv.gov.ua/UJRN/Nvamu\\_teh\\_2015\\_1\\_24](http://nbuv.gov.ua/UJRN/Nvamu_teh_2015_1_24) [View date February 1, 2024].
9. Murasov R., Nikitin A., Meshcheriakov I., Pidhorodetskyi M. & Poplavets S. (2023). Methodology for assessing threats and risks for critical infrastructure objects according to scenarios of the development of emergency situations. Modern information technologies in the field of security and defense, 3(48)/2023, 35-43. <https://doi.org/10.33099/2311-7249/2023-48-3-35-43> [View date February 1, 2024].
10. Murasov R., Meshcheriakov I. (2023). 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. *Social Development & Security*, 13(5), 180-191. <https://doi.org/10.33445/sds.2023.13.5.17> [View date February 1, 2024].
11. Chumachenko S., Kutovyi O. & 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 February 1, 2024].
12. Fursenko O.M., Chumachenko S.M. & 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 ecological safety and civil protection, 9, 68-77. Available from : <http://tes.igns.gov.ua/wp-content/uploads/2018/02/V9.pdf> [View date February 1, 2024].
13. 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 February 1, 2024].
14. 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 February 1, 2024].
15. In 2023, the Russians struck Ukraine with tens of thousands of strikes: infographic. Available from : <https://www.unian.ua/war/u-2023-roci-rosiyani-zavdali-po-ukrajini-desyatki-tisyach-udariv-infografika-12500187.html> [View date February 1, 2024].
16. Report on the main results of the State Emergency Service of Ukraine in 2022. Available from : <https://dsns.gov.ua/upload/1/6/4/9/3/5/0/publicnii-zvit-2022-ostannia-versiia-1.pdf> [View date February 1, 2024].
17. Order of the Ministry of Labor and Social Policy dated 04.12.2022 No. 637 On approval of the Methodology for determining risks and their accepted levels for declaring objects of increased danger. Available from : [https://zakononline.com.ua/documents/show/34982\\_34982](https://zakononline.com.ua/documents/show/34982_34982) [View date February 1, 2024].
18. Henley, E.J., Kumamoto, H. (1984). Reliability of technical systems and risk assessment. Mechanical engineering, 528 p. Available from : [http://www.immsp.kiev.ua/postgraduate/Biblioteka\\_trudy/NadezhnostTekhnicheskikhSistemKumamoto1984.pdf](http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/NadezhnostTekhnicheskikhSistemKumamoto1984.pdf) [View date February 1, 2024].
19. Law A.M., Kelton W.D. (2004). Simulation modeling. Classic CS. 3rd ed. BHV Publishing Group, 847 p. Available from : [https://heterarchica.files.wordpress.com/2017/01/1kel\\_ton\\_v\\_lou\\_a\\_imitatsionnoe\\_modelirovanie.pdf](https://heterarchica.files.wordpress.com/2017/01/1kel_ton_v_lou_a_imitatsionnoe_modelirovanie.pdf) [View date February 1, 2024].