

# Системні передумови оцінювання загроз для об'єктів критичної енергетичної інфраструктури в умовах збройного протистояння в Україні

## Systemic prerequisites for assessing threats to critical energy infrastructure facilities in the context of armed conflict in Ukraine

Микола Хомік <sup>A</sup>

**Corresponding author:** д.т.н., професор, головний науковий співробітник науково-дослідного управління, e-mail: [nkhomik@ukr.net](mailto:nkhomik@ukr.net), ORCID: 0000-0002-1201-7702

Петро Мацько <sup>B</sup>

начальник управління підготовки, e-mail: [petiamm79@gmail.com](mailto:petiamm79@gmail.com)

Mykola Khomik <sup>A</sup>

**Corresponding author:** Dr of Sciences, Professor,, Chief Researcher of the Scientific Research Department, e-mail: [nkhomik@ukr.net](mailto:nkhomik@ukr.net), ORCID: 0000-0002-1201-7702

Petro Matsko <sup>B</sup>

Chief of Training Directorate, e-mail: [petiamm79@gmail.com](mailto:petiamm79@gmail.com)

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

<sup>B</sup> Командування Сил підтримки Збройних Сил України, м. Київ, Україна

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

<sup>B</sup> Command of the Support Forces of the Armed Forces of Ukraine, Kyiv, Ukraine

Received: October 14, 2024 | Revised: October 27, 2024 | Accepted: October 31, 2024

DOI: 10.33445/sds.2024.14.5.19

**Мета роботи:** полягає у розробці підходів до системного оцінювання загроз і ризиків для об'єктів критичної енергетичної інфраструктури в умовах збройного конфлікту в Україні.

**Метод дослідження:** використовується теорія стохастичних процесів і системний аналіз.

**Практична цінність дослідження:** Запропонований підхід щодо системного оцінювання загроз і ризиків для об'єктів критичної енергетичної інфраструктури в умовах збройного конфлікту. Зазначений підхід передбачає розглядати воєнно-техногенну безпеку системи критичної енергетичної інфраструктури як стохастичну систему, яка може перебувати в трьох станах. Користуючись графом "станів і переходів" було складено систему диференціальних рівнянь (Колмогорова) для темпів («швидкості у часі») зміни імовірностей станів при зміні станів з відомими темпами переходів. Вирішення цієї системи рівнянь з врахуванням умов «стаціонарності» процесу переходів та «повноти» даної множини станів для їх імовірності, дозволило отримати імовірності перебування системи в кожному зі станів, математичне сподівання відвернених системою воєнно-техногенної безпеки збитків і нанесених системі збитків, тобто – потенціальний та реальний «ризик».

**Майбутні дослідження:** подальші дослідження слід спрямувати на системні дослідження оцінювання загроз і ризиків системі критичної енергетичної інфраструктури в аспекті воєнно-техногенної безпеки сил оборони України.

**Тип статті:** теоретичний.

**Ключові слова:** воєнна безпека держави, воєнно-техногенна безпека, система критичної енергетичної інфраструктури, об'єкти критичної енергетичної інфраструктури, структурно-функціональна модель, оцінювання, загроза, ризик.

**Purpose:** is to develop approaches to the systematic assessment of threats and risks for objects of critical energy infrastructure in the conditions of the armed conflict in Ukraine.

**Method:** the theory of stochastic processes and system analysis is used.

**Practical value of the research:** The proposed approach to the systematic assessment of threats and risks for critical energy infrastructure facilities in conditions of armed conflict. This approach involves considering the military-technological security of the critical energy infrastructure system as a stochastic system that can be in three states. Using the "states and transitions" graph, a system of differential equations (Kolmogorov) was compiled for the rates ("speed in time") of changing state probabilities when changing states with known rates of transitions. Solving this system of equations, taking into account the conditions of "stationarity" of the process of transitions and the "completeness" of a given set of states for their probability, made it possible to obtain the probabilities of the system being in each of the states, the mathematical expectation of the losses averted by the military-technological security system and the losses caused to the system, that is, the potential and real "risk".

**Future Research:** further research should be directed to systematic studies of the assessment of threats and risks to the system of critical energy infrastructure in the aspect of military-technological security of the defense forces of Ukraine.

**Paper type:** theoretical.

**Key words:** military security of the state, military-technological security, critical energy infrastructure system, critical energy infrastructure objects, structural-functional model, assessment, threat, risk.

## **Вступ**

Потужна і надійна енергетика країни є головною умовою функціонування усіх її сфер діяльності, а тому, в умовах збройної агресії російської федерації проти України, стає найважливішою системою стратегічних об'єктів "відповідальності" для сфери воєнної безпеки держави і її складової – воєнно-техногенної безпеки.

З початком бойових дій на Сході України, а особливо під час широкомасштабної збройної агресії російської федерації проти України утворилося нове явище – техногенна безпека суспільства в ході війни.

І зрозуміло, виникла нова парадигма, яка полягає в необхідності захисту не тільки населення, території, об'єктів від наслідків надзвичайних ситуацій, а сил оборони України. Причому, на перше місце виходить захист від надзвичайних ситуацій воєнного характеру.

В зв'язку з зазначеним, автори роблять спробу ввести нову дефініцію – воєнно-техногенна безпека сил оборони України.

На думку авторів, воєнно-техногенна безпека сил оборони України (складова воєнної безпеки держави) – стан захищеності сил оборони України від надзвичайних ситуацій воєнного характеру.

Враховуючи той факт, що на сьогоднішній день забезпечення безпеки критичної енергетичної інфраструктури є одним із ключових елементів забезпечення національної безпеки і обороноздатності виникає необхідність визначення комплексу заходів і раціонального розподілу сил для забезпечення захисту критичної енергетичної інфраструктури.

Це породжує завдання системного оцінювання загроз і ризиків в умовах швидкої зміни оперативної та воєнно-політичної обстановки при відбитті збройної агресії РФ.

## **Теоретичні основи дослідження**

Аналіз публікацій щодо рішень РНБО України [1, 2] показав, що на сьогоднішній день питання захисту критичної енергетичної інфраструктури є надзвичайно важливими для забезпечення функціонування єдиного комплексу заходів з виживання українського суспільства під час війни. Публікації Червоного Хреста підкреслюють важливість цих питань з точки зору гуманітарного вирішення захисту цивільного населення під час ударів по об'єктах енергетики, в тому числі й атомної [3, 4].

В наукових публікаціях Національного інституту стратегічних досліджень розглядаються як фундаментальні питання захисту критичної інфраструктури [5, 6] так і обґрунтування наукових підходів до оцінювання загроз і ризиків для об'єктів енергетичної інфраструктури [7].

Крім того, проблемі захисту об'єктів критичної інфраструктури, у тому числі, в аспекті накладання її на воєнно-техногенну безпеку сил оборони України присвячено низьку робіт таких вчених: М. Дівізінюк, І. Романенко, С. Чумаченко, М. Хомік, В. Коцюруба, Р. Мурасов.

Однак по сьогоднішній день немає єдиного підходу щодо вирішення завдання обґрунтування наукових підходів до оцінювання загроз і ризиків для об'єктів енергетичної інфраструктури, особливо в умовах воєнного стану.

Наведене підтверджує актуальність та перспективність обраного дослідження.

## **Постановка проблеми**

Мета статті полягає у розробці підходів до системного оцінювання загроз і ризиків для об'єктів критичної енергетичної інфраструктури в умовах збройного конфлікту в Україні.

## Результати

1. Загальний аналіз воєнно-техногенної безпеки системи критичної енергетичної інфраструктури.

З точки зору системного підходу до системи критичної енергетичної інфраструктури (СКЕІ), як сукупності взаємопов'язаних об'єктів, які забезпечують стан захищеності національних інтересів у енергетичній сфері, належать (рис. 1):

- система забезпечення енергоносіями (СЗЕН);
- система забезпечення електроенергією (СЗЕЕ);
- система теплоенергетики (СТЕ).

Система забезпечення енергоносіями включає:

- критичну інфраструктуру об'єктів добичі енергоносіїв природного походження чи інших об'єктів – джерел енергетичної сировини (вугілля, нафта, газ, уранові руди, хімічна сировина для неорганічних енергоносіїв, тощо);
- критичну інфраструктуру об'єктів їх переробки на гірничо-збагачувальних та гірничо-переробних підприємствах (у нафтопродукти, ракетне паливо, рідкий газ, активні елементи для ядерних реакторів);
- критичну інфраструктуру об'єктів постачання перероблених енергоносіїв (транспортування, накопичення, зберігання та розподіл).

Систему забезпечення електроенергією утворює інфраструктура об'єктів запасів (сховищ) енергоносіїв, об'єктів "генерування" електроенергії (теплові, атомні та гідроелектростанції) та об'єктів її постачання (лінії електропередач ЛЕП, трансформаторні підстанції (ТП) розподілу електроенергії).

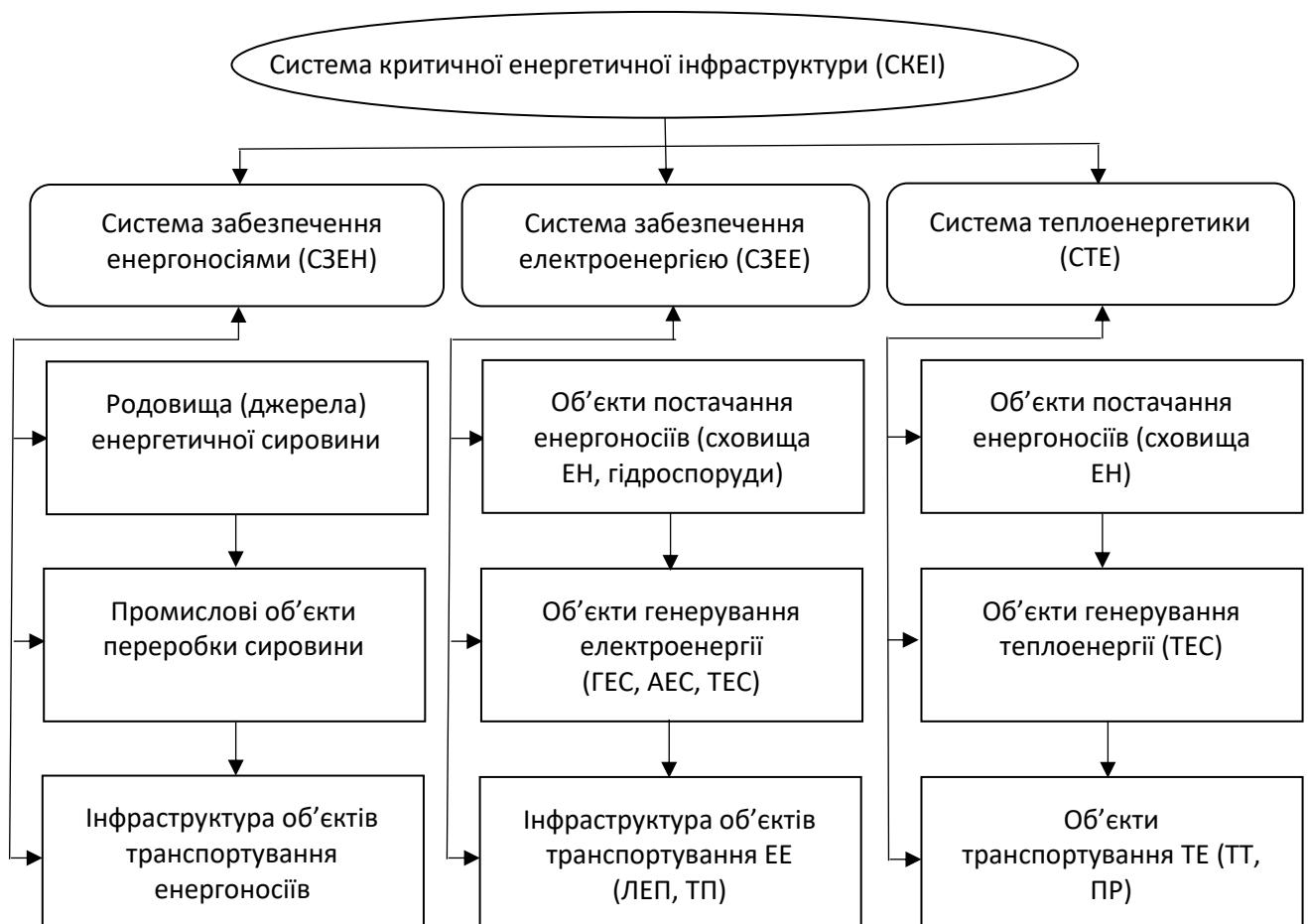


Рисунок 1 – Структурно-функціональна модель системи критичної енергетичної інфраструктури

Систему теплоенергетики утворює інфраструктура об'єктів накопичення (постачання) енергоносіїв (ЕН), об'єктів вироблення ("генерування") теплової енергії (теплоцентралі) та об'єктів її постачання (теплотраси ТТ та пункти розподілу – ПР теплоносіїв).

СКЕІ є однією із основних складових забезпечення необхідного рівня воєнно-економічного потенціалу країни, що визначає її обороноздатність. З іншого боку, сили оборони України для СКЕІ України є також одним з основних споживачів, оскільки енергоносії, електроенергія та тепла енергія в цілому є головним джерелом боєздатності ЗС.

В Сухопутних Військах споживачами великих об'ємів пального, електро- та теплової енергії є механізовані, аеромобільні й танкові частини, армійська авіація, ракетні війська і артилерія, армійська ППО, війська (сили) бойового та матеріально-технічного забезпечення.

В Повітряних Силах споживачами різноманітного пального, електро- та теплової енергії є тактична та транспортна авіація, зенітно-ракетні і радіотехнічні війська та авіація протиповітряної оборони (ППО), сили бойового та матеріально-технічного забезпечення.

У Військово-Морських Силах споживачами різноманітного пального, електро- та теплової енергії є кораблі бойового складу та складу сил забезпечення, військово-морські бази, війська (сили) берегової оборони.

Крім Збройних Сил України, споживачами значного обсягу зазначених ресурсів є Державна служба спеціального зв'язку та захисту інформації України, Державна спеціальна служба транспорту, інші військові формування, правоохоронні та розвідувальні органи.

Пальне для військ (сил) у мирний час накопичується у сховищах пально-мастильних матеріалів (ПММ) на об'єктах споживання. Під час бойових дій постачання пального військам (силам) здійснюється як "танкерними" системами (залізничний, водний та автомобільний транспорт), так і "трубопровідними" системами (стаціонарними і тимчасовими, які розгортаються на території країни у воєнний час).

Окремими об'єктами системи енергоносіїв є сховища компонентів ракетного палива. Дані компоненти (гептил й меланж) будуть знову потрібні у випадку створення балістичних ракет й авіаційно-космічних комплексів з повітряним стартом важких ракет-носіїв орбітальних об'єктів воєнного призначення (розвідки, попередження, навігації, зв'язку, управління, ударних) в інтересах оборони країни.

У мирний час Збройні Сили використовують державні системи енергетики, під час бойових дій для систем зброї і військової техніки застосовуються накопичені запаси ЕН, штатні автономні системи електро- та теплоенергетики.

Об'єкти СКЕІ завжди відносять до об'єктів захисту ("відповідальності") найбільшої оперативно-стратегічної важливості, які є для противника одними з "першочергових" об'єктів знищення або захоплення і, на жаль, мають високий ступень уразливості. Фахівцями США досліджено, що диверсійна група з 7 осіб може паралізувати мільйонне місто своїми діями саме по об'єктах СКЕІ, звичайно результати такої диверсії можуть впливати і на рівень енергетичної забезпеченості Сил оборони України.

СЗЕН мають у складі в основному стаціонарні об'єкти здобичі сировини (чи термінали зовнішніх джерел), об'єкти переробки сировини (нафтоперегінні і нафтогазові підприємства) та об'єкти транспортування ЕН (інфраструктура об'єктів "танкерного" водного, залізничного, авіаційного і автомобільного транспорту та стаціонарних об'єктів трубопровідних магістралей). Комплекси об'єктів ЕН мають масштабне у просторі розташування та значну уразливість щодо деструктивного впливу. У випадку ураження даних об'єктів можливі масштабні руйнівні та шкідливі екологічні наслідки, які пов'язані зі значними витратами сил, засобів і часу на їх ліквідацію.

СЗЕЕ мають у складі стаціонарні об'єкти накопичення ЕН (сховища пального, гідротехнічні споруди ГЕС), об'єкти генерування ЕЕ (ТЕС, ГЕС, АЕС) та об'єкти транспортування й розподілу ЕЕ. Об'єкти накопичення ЕН мають значну уразливість щодо деструктивного

впливу. Найбільш небезпечними щодо ураження об'єктами генерування ЕЕ є енергоблоки з ядерними реакторами АЕС. Наземні лінії електропередач, як об'єкти транспортування ЕЕ, найбільш уразливі щодо виведення їх з ладу та небезпечні для військ і населення при їх руйнуванні через виникнення масштабних пожеж при "короткому" замиканні в електромережах та ураження високою напругою. Кабельні лінії електропередач менш уразливі щодо руйнування, але застосовуються лише на невеликих відстанях передачі ЕЕ.

СТЕ мають у складі стаціонарні об'єкти ЕН (сховища пального), об'єкти генерування ТЕ (ТЕЦ) та об'єкти транспортування й розподілу ТЕ. Об'єкти накопичення ЕН мають значну уразливість щодо деструктивного впливу, у випадку ураження цих об'єктів можливі масштабні руйнівні та шкідливі екологічні наслідки, які пов'язані зі значними трудовитратами сил і нарядами засобів на їх ліквідацію. Об'єкти генерування та транспортування ТЕ також мають уразливість щодо деструктивного впливу, але наслідки їх руйнування менш небезпечні.

Трубопровідні магістралі (ТМ) військового призначення в останній час набули поширення у збройних силах розвинутих країн. Вони розгортаються під час воєнного стану для постачання військам (силам) основних енергоносіїв (пального) для військової техніки та інших оперативно-стратегічних об'єктів.

Станції (пункти) забору (завантаження) енергоносіїв ТМ розгортаються на нафтопереробних підприємствах країни та сховищах ЕН.

Станції розподілу енергоносіїв розгортаються на об'єктах :

- аеродроми тактичної та транспортної авіації ПС;
- пункти заправки рухомої військової техніки;
- військово-морські бази ВМС;
- об'єкти військово-промислового (оборонного) комплексу;
- об'єкти критичної інфраструктури оперативно-стратегічного значення.

Кожна "нитка" ТМ від станції забору до стацій розподілу представляє собою збірний трубопровід, секція якого має діаметр навколо 12,5 см і довжину до декількох десятків метрів. Секції з'єднуються гнучким герметичним манжетом та укладаються спеціальною технікою на глибину до 0,5 м в ґрунт (до 0,5 км за годину) чи на поверхню ґрунту (до 5 км за годину). Для підтримання потрібної продуктивності транспортування енергоносіїв вздовж "нитки" ТМ через кожні приблизно 50 км розташовуються компресорні станції, пункти управління та забезпечення відповідними ресурсами. Під час транспортування трубопровід завантажується енергоносієм об'ємом приблизно 10 м<sup>3</sup> продукту на 1 погонний км, швидкість транспортування – до 25 км/год. ТМ визнана значно більш ефективним засобом постачання енергоносіїв в порівнянні з "танкерним" транспортуванням, тому буде й в майбутньому головним засобом постачання енергоносіїв військам (силам) під час проведення операцій. Але ТМ, через стаціонарне розташування своїх елементів системи на значній площі, на жаль, має підвищену уразливість як саме "ниток" трубопроводів, так і станцій забору, компресорних станцій, станцій розподілу та пунктів управління їх забезпеченням.

Таким чином, усі об'єкти СКЕІ у воєнний час безумовно можуть бути об'єктами вогневого ураження для ударної авіації і ракетних комплексів, а також об'єктами диверсійних дій з боку противника. Виведення з ладу СКЕІ противником пов'язане, по-перше, зі зривом забезпечення енергією об'єктів воєнно-економічного (оборонного) потенціалу, об'єктів усіх інших сфер діяльності країни та бойових дій угруповань військ (сил) в операціях, і, по-друге, з нанесенням величезних економічних втрат, виникненням небезпечних екологічних наслідків для об'єктів критичної інфраструктури (ОКІ), населення, навколишнього природного середовища (НПС) і безумовно, Сил оборони України. Небезпека для об'єктів енергетики стає надзвичайно великою саме через максимально високу концентрацію джерел хімічної енергії безпосередньо у енергоносіїв, так і механічної, електричної та теплової енергії на об'єктах її генерування, яка вивільняється при техногенних аваріях і катастрофах. Тому вже є багато

прикладів НС із загибеллю людей та багатомільярдними збитками через знищення ОКІ і витратами на ліквідацію наслідків катастроф – пожежі та вибухи через аварії на вугільних шахтах, нафтопереробних підприємствах і сховищах пально-мастильних матеріалів, трубопровідних магістралях, техногенні катастрофи через руйнування АЕС із радіоактивним забрудненням НПС (Чорнобиль, Фукусіма).

Існує також величезний ризик техногенних катастроф на об'єктах зберігання великих об'ємів агресивних компонент ракетного палива (гептил та меланж). Все це є наслідками низького рівня «живучості» об'єктів СКЕІ через неефективність заходів попередження і запобігання НС на них.

2. Підхід щодо системного оцінювання загроз і ризиків для об'єктів критичної енергетичної інфраструктури в умовах збройного конфлікту.

Практика експлуатації СКЕІ показує, що функції всебічної воєнно-техногенної безпеки ОКІ не можуть покладатися на персонал, який має основну функцію експлуатації СКЕІ за призначенням, і потребують створення “системи (служби) воєнно-техногенної безпеки”, як підсистеми “забезпечення”, з відповідними специфічними функціями.

“Живучість” об'єкта СКЕІ є здатність збереження саме його “системної функції” при “деструктивному” на нього впливі. Проблема “живучості” систем підвищеного ризику щодо виникнення воєнно-техногенної небезпеки в умовах “загроз” вимагає докладного розгляду окремих положень теорії воєнно-техногенної безпеки на ґрунті “системного підходу”.

Вже існують нібито науково “канонізовані” погляди [8, 9] на визначення понять в галузі безпеки, але вони, на жаль, є евристичними і не мають підґрунтя саме системного підходу щодо аналізу безпеки “складних” систем.

“Загроза” є джерелом “небезпеки”, але не її синонімом. Функціональною “загрозою” для складної системи даного призначення є виникнення умови переходу системи в стан “небезпеки”, коли вона не спроможна відвернути власними силами неприйнятні (для її “існування”) збитки через дію деструктивних факторів. Якщо на поточний момент часу не існує реальна можливість виникнення неприйнятних збитків, то загроза є потенціальною, якщо існує – то реальною. Це надає додаткову ознаку стану “небезпеки” системи – “потенційна небезпека” чи “реальна небезпека”. Потенційна загроза пов'язана з “відкладеним” у часі ризиком, реальна – з наявним.

Так, виведення з ладу ОКІ можливим деструктивним впливом при відсутності підсистеми “попередження, запобігання й захисту” є реальною загрозою, яка усувається створенням даної підсистеми [10]. Недосконалість підсистеми “запобігання й захисту” СКЕІ (можлива її “відмова”) при реальному деструктивному впливі є потенційною загрозою, яка усувається її вдосконаленням (максимізацією ефективності підсистеми).

Досягнення системою у стані небезпеки спроможності відвернути неприйнятні збитки є усуненням загрози, коли виникає умова переходу системи у стан “безпеки”

Таким чином, якщо система воєнно-техногенної безпеки СКЕІ спроможна відвернути неприйнятні збитки, то над-система “СКЕІ” знаходиться у стані “безпеки”, тобто “відсутності загрози». Очевидно, стани “безпеки” та “небезпеки” складають “повну групу” станів системи СКЕІ щодо подій “наявності” чи “відсутності” загроз.

Розглянемо воєнно-техногенну безпеку СКЕІ як стохастичну систему.

Очікувані збитки при “небезпеці” (виникненні загроз) для СКЕІ поділяються на “воєнні”, “матеріальні” та “екологічні”. “Воєнні” збитки вимірюються зниженням “о.-с. важливості” (об'єму продукції) СКЕІ при вогневому ураженні або захопленні ОКІ противником. “Матеріальні” збитки вимірюються втратами основного ресурсу технологічної системи (персоналу й обладнання) на об'єктах СКЕІ при аваріях (катастрофах) техногенного походження. “Екологічні” збитки СКЕІ вимірюються екологічними наслідками вогневого ураження чи надзвичайних ситуацій техногенного походження на об'єктах СКЕІ.

“О.-с. важливість” для СКЕІ багатьма розвиненими країнами розуміється як “вартість” об’єктів системи (при їх втраті) чи вартість їх відновлення (при руйнуванні). Военний аспект “О.-с. важливості” припускає її оцінку кількісною мірою “впливу” СКЕІ на утримання стану воєнної безпеки силами оборони України, тому “О.-с. важливість” доцільно вимірювати безрозмірним показником ( $0 \leq C \leq 100$ ), значення якого є, як правило, експертною оцінкою.

СКЕІ щодо її воєнно-техногенної безпеки розглядається як “стохастична система”, яка може перебувати в наступних станах (рис. 2):

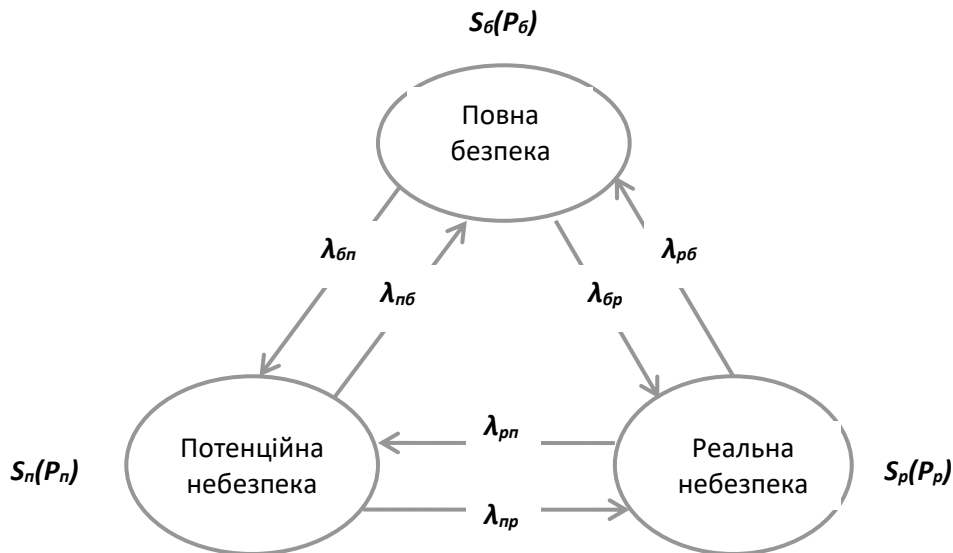


Рисунок 2 – Граф станів й переходів стохастичної системи СКЕІ

- де  $S_b$  – стан, коли СКЕІ здатна відвернути неприпустимі для її існування збитки власним ресурсом (ознака стану – “повна безпека”);
- $S_n$  – стан, коли СКЕІ не здатна відвернути неприпустимі для її існування потенційні збитки власним ресурсом (ознака стану – “потенційна небезпека”);
- $S_p$  – стан, коли СКЕІ не здатна відвернути неприпустимі для її існування реальні збитки власним ресурсом (ознака стану – “реальна небезпека”).

Множина даних станів складає так звану “повну групу”, для якої сума ймовірностей перебування СКЕІ в кожному відповідному стані ( $P_b, P_n, P_p$ ) дорівнює одиниці.

У поточному часі СКЕІ знаходиться в одному з перелічених станів, змінюючи їх випадковим чином як по “напрямку”, так і по “моменту часу”, за дією впливів випадкових подій:

“виникнення реальної загрози” з темпом у часі  $\lambda_{bп}$ ;

“усунення реальної загрози” з темпом у часі  $\lambda_{pb}$ ;

“виникнення потенційної загрози” з темпом у часі  $\lambda_{bn}$ ;

“усунення потенційної загрози” з темпом у часі  $\lambda_{nb}$ ;

“перетворення потенційної загрози в реальну” з темпом у часі  $\lambda_{np}$ ;

“перетворення реальної загрози в потенційну” з темпом у часі  $\lambda_{pn}$ .

Впливи подій із “загрозами” вважаються “пуассонівськими”, причому інтенсивності подій “виникнення (чи збільшення) загрози” визначаються зовнішніми факторами, а подій “усунення (чи зменшення) загрози” – внутрішніми факторами, пов’язаними з “можливостями” системи щодо “середніх” витрат часу  $\tau$  на усунення реальної (чи потенційної) загрози –

$$\lambda_{pb} = (1 / \tau_{pb}); \quad \lambda_{nb} = (1 / \tau_{nb}); \quad \lambda_{pn} = (1 / \tau_{pn}). \quad (1)$$

Тому СКЕІ з розглянутим внутрішнім процесом зміни “станів” типу “неперервний ланцюг Маркова” слід вважати “стохастичною системою” щодо її функціональної сталості. Проаналізуємо дану стохастичну систему .

Користуючись графом “станів і переходів” (рис. 2), складемо систему диференціальних рівнянь (Колмогорова) для темпів (“швидкості у часі”) зміни імовірностей станів ( $S_{\bar{o}}, S_n, S_p$ ) при зміні станів з відомими темпами переходів ( $\lambda$ ) для системи –

$$\begin{aligned}\frac{dp_{\bar{o}}}{dt} &= -(\lambda_{\bar{o}n} + \lambda_{\bar{o}p}) \cdot p_{\bar{o}}(t) + \lambda_{n\bar{o}} \cdot p_n(t) + \lambda_{p\bar{o}} \cdot p_p(t) \\ \frac{dp_n}{dt} &= \lambda_{\bar{o}n} \cdot p_{\bar{o}}(t) - (\lambda_{n\bar{o}} + \lambda_{np}) \cdot p_n(t) + \lambda_{pn} \cdot p_p(t) \\ \frac{dp_p}{dt} &= \lambda_{\bar{o}p} \cdot p_{\bar{o}}(t) + \lambda_{np} \cdot p_n(t) - (\lambda_{p\bar{o}} + \lambda_{pn}) \cdot p_p(t).\end{aligned}\quad (2)$$

Запишемо умову “стаціонарності” процесу переходів (для  $t \rightarrow \infty$ ), коли похідні за часом обертаються в нуль і поточні ймовірності станів досягають відповідних асимптотичних значень ( $P_{\bar{o}}, P_n, P_p$ ); тобто –

$$\begin{aligned}-(\lambda_{\bar{o}n} + \lambda_{\bar{o}p})P_{\bar{o}} + \lambda_{n\bar{o}}P_n + \lambda_{p\bar{o}}P_p &= 0 \\ \lambda_{\bar{o}n}P_{\bar{o}} - (\lambda_{n\bar{o}} + \lambda_{np})P_n + \lambda_{pn}P_p &= 0 \\ \lambda_{\bar{o}p}P_{\bar{o}} + \lambda_{np}P_n - (\lambda_{p\bar{o}} + \lambda_{pn})P_p &= 0.\end{aligned}\quad (3)$$

Дана система лінійних рівнянь є “лінійно залежною”, бо сума будь-яких двох з них дорівнює третьому. Тому виключимо з даної системи, наприклад, останнє (третє), замість якого додамо рівняння умови “повноти” даної множини станів для їх імовірності; одержимо

$$\begin{aligned}-(\lambda_{\bar{o}n} + \lambda_{\bar{o}p})P_{\bar{o}} + \lambda_{n\bar{o}}P_n + \lambda_{p\bar{o}}P_p &= 0 \\ \lambda_{\bar{o}n}P_{\bar{o}} - (\lambda_{n\bar{o}} + \lambda_{np})P_n + \lambda_{pn}P_p &= 0 \\ P_{\bar{o}} + P_n + P_p &= 1.\end{aligned}\quad (4)$$

Вирішимо дану систему рівнянь (наприклад, методом Крамера).

Детермінант системи –

$$\Delta = \begin{vmatrix} -(\lambda_{\bar{o}n} + \lambda_{\bar{o}p}) & \lambda_{n\bar{o}} & \lambda_{p\bar{o}} \\ \lambda_{\bar{o}n} & -(\lambda_{n\bar{o}} + \lambda_{np}) & \lambda_{pn} \\ 1 & 1 & 1 \end{vmatrix}, \quad (5)$$

часткові детермінанти (для стовпчика “вільних” членів системи рівнянь) відповідно –

$$\Delta_{\bar{o}} = \begin{vmatrix} 0 & \lambda_{n\bar{o}} & \lambda_{p\bar{o}} \\ 0 & -(\lambda_{n\bar{o}} + \lambda_{np}) & \lambda_{pn} \\ 1 & 1 & 1 \end{vmatrix}, \quad (6)$$

$$A_n = \begin{vmatrix} -(\lambda_{on} + \lambda_{op}) & 0 & \lambda_{p\bar{o}} \\ \lambda_{on} & 0 & \lambda_{pn} \\ 1 & 1 & 1 \end{vmatrix}, \quad (7)$$

$$A_p = \begin{vmatrix} -(\lambda_{on} + \lambda_{op}) & \lambda_{n\bar{o}} & 0 \\ \lambda_{on} & -(\lambda_{n\bar{o}} + \lambda_{np}) & 0 \\ 1 & 1 & 1 \end{vmatrix}. \quad (8)$$

Остаточно рішенням даної системи рівнянь є “асимптотичні” значення імовірності перебування системи в кожному стані –

$$P_{\bar{o}} = (A_{\bar{o}} / \Delta), \quad P_n = (A_n / \Delta), \quad P_p = (A_p / \Delta). \quad (9)$$

Саме значення імовірності  $P_{\bar{o}}$  слід вважати оцінкою “живучості”, а значення  $P_p$  – оцінкою “вразливості” системи.

Якщо дана система енергетики має оперативно-стратегічну важливість  $AS$ , то завдяки “повноті групи подій” (станів “безпеки” та “небезпеки” СКЕІ) математичне сподівання відвернених системою воєнно-техногенної безпеки збитків –

$$VS = P_{\bar{o}} \times AS, \quad (10)$$

і математичне сподівання нанесених системі збитків (потенціальний та реальний “ризик”) –

$$WS_n = P_n \times AS; \quad WS_p = P_p \times AS. \quad (11)$$

## Висновки

В ході проведеного дослідження:

1. Проведений аналіз воєнно-техногенної безпеки системи критичної енергетичної інфраструктури. На основі цього аналізу була узагальнена структурно-функціональна модель системи критичної енергетичної інфраструктури з точки зору воєнно-техногенної безпеки сил оборони України.

2. Запропонований підхід щодо системного оцінювання загроз і ризиків для об’єктів критичної енергетичної інфраструктури в умовах збройного конфлікту. Зазначений підхід передбачає розглядати воєнно-техногенну безпеку системи критичної енергетичної інфраструктури як стохастичну систему, яка може перебувати в трьох станах: “повна безпека”; “потенційна небезпека”; “реальна небезпека”.

3. Користуючись графом “станів і переходів” було складено систему диференційних рівнянь (Колмогорова) для темпів (“швидкості у часі”) зміни імовірностей станів при зміні станів з відомими темпами переходів.

Вирішення цієї системи рівнянь з врахуванням умов “стаціонарності” процесу переходів та “повноти” даної множини станів для їх імовірності дозволило отримати імовірності перебування системи в кожному зі станів, математичне сподівання відвернених системою воєнно-техногенної безпеки збитків та математичне сподівання нанесених системі збитків, тобто – потенціальний та реальний “ризик”.

4. Запропоновано створення системи (служби) воєнно-техногенної безпеки, як підсистеми забезпечення захисту критичної енергетичної інфраструктури в умовах ведення бойових дій з відповідними специфічними функціями запобігання, попередження і ліквідації надзвичайних ситуацій воєнного характеру.

## Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

## Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

## Список використаних джерел

1. Олександр Литвиненко: Важливо максимально підсилити рівень організації інженерного захисту об'єктів критичної інфраструктури. URL: <https://www.ukrinform.ua/rubric-economy/3854309-zahist-kriticnoi-infrastrukturi-sekretar-rnbo-proviv-naradu.html>.
2. Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій: Рішення Ради Національної Безпеки і Оборони України від 17 жовтня 2023 року. Введено в дію Указом Президента України від 17 жовтня 2023 року № 695/2023. URL: <https://zakon.rada.gov.ua/laws/show/n0040525-23#Text>.
3. Коли гасне світло: Захист енергетичної інфраструктури в умовах збройного конфлікту. URL: <https://blogs.icrc.org/ua/2023/07/203/6217/>.
4. Еббі Зейт та Ейріні Гюргу, Небезпечні сили: захист атомних електростанцій в умовах збройного конфлікту, 18 жовтня 2022 року. URL: <https://blogs.icrc.org/law-and-policy/2022/10/18/protection-nuclear-power-plants-armed-conflict/>.
5. Суходоля О. М. Захист енергетичної інфраструктури: аналіз української законодавчої бази. Аналітична записка. URL: <http://www.niss.gov.ua/articles/1568/>.
6. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Аналітична доповідь. – К.: НІСД, 2012. – 57 с.
7. Оцінка загрози ядерного тероризму: проектна загроза: Науково-методологічний посібник / С. І. Кондратов, Ю. М. Скалецький, В. І. Кравцов та ін.; за заг. ред. В. П. Горбуліна. – К.: ДП «НВЦ «Євроатлантикінформ», 2006. – 76 с.
8. Качинський А. Безпека, загрози і ризик: наукові концепції та математичні методи. – К.: «Поліграфконсалтинг», 2004. – 472 с.
9. Машков О. А, Іващенко Т. Г., Мухін Є. А., Мухіна К. Є., Триснюк В. М., Чумаченко С. М. Системний підхід в екологічних науках: системний аналіз та синтез управлінських екологічних рішень. – Монографія. — Дніпро: Адверта, Середняк Т.К., 2023. – 674 с. – ISBN 978-617-8245-31-3.
10. Потій О. Україна починає будувати систему захисту критичної інфраструктури відповідно до найкращих світових практик та чинних вимог європейського законодавства. URL: <https://cip.gov.ua/ua/news/ukrayina-pochinaye-buduvati-sistemu-zakhistu-kritichnoyi-infrastrukturi-vidpovidno-do-naikrashikh-svitovikh-praktik-ta-chinnikh-vimog-yevropeiskogo-zakonodavstva>.

## References

- 1 Oleksandr Lytvynenko: It is important to maximize the level of organization of engineering protection of critical infrastructure facilities. Available from : <https://www.ukrinform.ua/rubric-economy/3854309-zahist-kriticnoi-infrastrukturi-sekretar-rnbo-proviv-naradu.html>.
2. On the organization of protection and ensuring the safety of the functioning of critical infrastructure and energy facilities of Ukraine in the conditions of hostilities: Decision of the National Security and Defense Council of Ukraine of October 17, 2023. Enacted by the Decree

- of the President of Ukraine of October 17, 2023 No. 695/2023. Available from : <https://zakon.rada.gov.ua/laws/show/n0040525-23#Text>.
3. When the lights go out: Protection of energy infrastructure in the context of armed conflict. Available from : <https://blogs.icrc.org/ua/2023/07/203/6217/>.
  4. Ebbe Zeit, Eirini Hiorhu, Dangerous Forces: Protecting Nuclear Power Plants in Armed Conflict, October 18, 2022. Available from : <https://blogs.icrc.org/law-and-policy/2022/10/18/protection-nuclear-power-plants-armed-conflict/>.
  5. Sukhodolia O. M. Protection of Energy Infrastructure: Analysis of the Ukrainian Legislative Framework. Analytical note. Available from : <http://www.niss.gov.ua/articles/1568/>.
  6. Biriukov D. S., Kondratov S. I. Critical Infrastructure Protection: Problems and Prospects for Implementation in Ukraine. Analytical report. – Kyiv: NISR, 2012. – 57 p.
  7. Nuclear Terrorism Threat Assessment: Projected Threat: A scientific and methodological guide / S. I. Kondratov, Yu. M. Skaletskyi, V. I. Kravtsov and others; under the general editorship V. P. Horbulina. – Kyiv: State-owned enterprise «Scientific and publishing center «Yevroatlantykinform», 2006. – 76 p.
  8. Kachynskiy A. Security, threats and risk: scientific concepts and mathematical methods. – K.: «Polihrafkonsaltnykh», 2004. – 472 p.
  9. Mashkov O. A, Ivashchenko T. H., Mukhin Ye. A., Mukhina K. Ie., Trysniuk V. M., Chumachenko S. M. Systems approach in environmental sciences: system analysis and synthesis of environmental management decisions. – Monograph. – Dnipro: Adverta, 2023. – 674 p. – ISBN 978-617-8245-31-3.
  10. Potii O. Ukraine begins to build a critical infrastructure protection system in accordance with the best international practices and current requirements of European legislation. Available from : <https://cip.gov.ua/ua/news/ukrayina-pochinaye-buduvati-sistemu-zakhistu-kritichnoyi-infrastrukturi-vidpovidno-do-naikrashikh-svitovikh-praktik-ta-chinnikh-vimog-yevropeiskogo-zakonodavstva>.