Методологічні засади застосування методу Пампуро для забезпечення безпеки об’єктів критичної інфраструктури України

Methodological Foundations for Applying the Pampuro Method to Ensure the Security of Critical Infrastructure Facilities in Ukraine

Олена Азаренко [A]
доктор фізико-математичних наук, професор, заступник керівника Науково-дослідного лабораторно-експериментального центру, e-mail: azarenko_ev@ukr.net, ORCID ID: https://orcid.org/0000-0003-2927-5545

Олег Бляшенко [B]
доктор технічних наук, провідний науковий співробітник відділу науково-методичного забезпечення, e-mail: o.bliashenko@kai.edu.ua, ORCID ID: https://orcid.org/0000-0003-1500-0487

Михайло Дивизинюк [C]
доктор фізико-математичних наук, професор, головний науковий співробітник, e-mail: divizinyuk@ukr.net, ORCID ID: https://orcid.org/0000-0002-5657-2302

Олександр Фаррахов[D]
доктор технічних наук, старший дослідник, завідувач відділу проблем фізичного захисту об’єктів критичної інфраструктури, e-mail: center_zam@ukr.net, ORCID ID: https://orcid.org/0000-0003-4988-126X

Артем Гузь [F]
Corresponding author: ад’юнкт, e-mail: huz_artem@nuczu.edu.ua, ORCID ID: https://orcid.org/0009-0004-8869-2423

Olena Azarenko [A]
Doctor of Physical and Mathematical Sciences, Professor, Deputy Head of the Research Laboratory and Experimental Centre, e-mail: azarenko_ev@ukr.net, ORCID ID: https://orcid.org/0000-0003-2927-5545

Oleh Bliashenko [B]
Doctor of Technical Sciences, Leading Researcher of the Department of Scientific and Methodological Support of Activities, e-mail: o.bliashenko@kai.edu.ua, ORCID ID: https://orcid.org/0000-0003-1500-0487

Mykhailo Divizyniuk [C]
Doctor of Physical and Mathematical Sciences, Professor, Chief Researcher, e-mail: divizinyuk@ukr.net, ORCID ID: https://orcid.org/0000-0002-5657-2302

Oleksandr Farrakhov [D]
Doctor of Technical Sciences, Senior Researcher, Head of the Department of Physical Protection of Critical Infrastructure Facilities, e-mail: center_zam@ukr.net, ORCID ID: https://orcid.org/0000-0003-4988-126X

Artem Huz [F]
Corresponding author: Corresponding author: PhD Student, e-mail: huz_artem@nuczu.edu.ua, ORCID ID: https://orcid.org/0009-0004-8869-2423

[A] Науково-дослідний лабораторно-експериментальний центр “БРАНД ТРЕЙД”, м. Черкаси, Україна
[B] Державне некомерційне підприємство “Державний університет ‘Київський авіаційний інститут’”, м. Київ, Україна
[C] Інституту геохімії навколишнього середовища НАН України, м. Київ, Україна
[D] Центр інформаційно-аналітичного та технічного забезпечення моніторингу об’єктів атомної енергетики НАН України, м. Київ, Україна
[F] Національний університет цивільного захисту України, м. Черкаси, Україна

[A] Research Laboratory and Experimental Centre “BRAND TRADE”, Cherkasy, Ukraine
[B] State Non-Commercial Company “State University ‘Kyiv Aviation Institute’”, Kyiv, Ukraine
[C] Institute of Environmental Geochemistry of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
[D] Center for Information, Analytical and Technical Support for Monitoring of Nuclear Energy Facilities of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
[F] National University of Civil Protection of Ukraine, Cherkasy, Ukraine

Received: August 12, 2026 | Revised: September 26, 2026 | Accepted: October 31, 2026

УДК 351.86

DOI: https://doi.org/10.33445/sds.2026.16.5.47

Мета роботи. Обґрунтувати методологічні засади застосування концепції забезпечення максимального рівня безпеки за мінімальних сукупних витрат і структурно-інформаційного методу для побудови моделей та алгоритмів управління безпекою енергетичних об'єктів критичної інфраструктури.

Метод дослідження. Використано системний, структурний та інформаційний підходи, а також методи аналізу, узагальнення, порівняння й формалізації. Системний підхід застосовано для розгляду енергетичного об'єкта як сукупності взаємопов'язаних технічних, інформаційних, організаційних і керувальних елементів. Структурний та інформаційний підходи використано для представлення енергетично різнорідних елементів через їхні вхідні й вихідні інформаційні змінні та зв'язки між ними.

Результати. Розглянуто основні положення концепції забезпечення максимального рівня безпеки ядерного об'єкта за мінімальних сукупних витрат. Систематизовано вісім

Purpose. To substantiate the methodological foundations for applying the concept of achieving the maximum level of safety at minimum total cost and the structural-information method to the development of models and algorithms for managing the safety of critical energy infrastructure facilities.

Research Method. Systemic, structural, and information-based approaches were employed, along with methods of analysis, generalization, comparison, and formalization. The systemic approach was used to examine an energy facility as a set of interconnected technical, informational, organizational, and control elements. The structural and information-based approaches were applied to represent energetically heterogeneous elements through their input and output information variables and the relationships between them.

Results. The fundamental principles of the concept of ensuring the maximum level of safety of a nuclear facility at minimum total cost were examined. Eight postulates of the concept were

постулатів концепції, що охоплюють досягнення максимального ефекту за мінімальних витрат, урахування можливості настання катастрофічної події, використання доступних засобів її попередження, забезпечення резерву керованості, визначення верхньої межі розвитку небезпечного процесу, застосування екстремального управління, розрахунок сукупних витрат і дотримання системного підходу до управління безпекою. Обґрунтовано, що структурно-інформаційний метод дає змогу розглядати елементи з різними енергетичними та матеріальними потоками з єдиних інформаційних позицій. Показано, що зв'язки між елементами можуть бути представлені через вхідні та вихідні інформаційні змінні, які характеризують керований стан об'єкта.

Теоретична цінність дослідження. Уточнено методологічні засади поєднання концепції оптимального управління безпекою зі структурно-інформаційним методом стосовно енергетичних об'єктів критичної інфраструктури. Отримані результати становлять теоретичну основу для подальшого розроблення моделей і алгоритмів управління безпекою цих об'єктів.

Тип статті: теоретико-методична.

Ключові слова: критична інфраструктура, управління безпекою, максимальний рівень безпеки, мінімальні сукупні витрати, структурно-інформаційний метод, метод Пампуро.

systematized, covering the achievement of maximum effectiveness at minimum cost, consideration of potential catastrophic events, application of preventive measures, maintenance of a controllability reserve, identification of critical thresholds, implementation of control under extreme conditions, calculation of total costs, and adoption of a systemic approach to safety management. The structural-information method was shown to provide a unified framework for representing elements characterized by different energy and material flows through interconnected information variables.

Theoretical Implications. The methodological foundations for integrating the concept of optimal safety management with the structural-information method were clarified in the context of critical energy infrastructure. The findings provide a theoretical basis for the subsequent development of mathematical models and safety management algorithms.

Paper Type. Theoretical and methodological study.

Key words: critical infrastructure, safety management, maximum level of safety, minimum total cost, structural-information method, Pampuro method.

Вступ

Стабільне функціонування об'єктів критичної інфраструктури є необхідною умовою забезпечення державної безпеки [1]. Порушення функціонування енергетичних і ядерних об'єктів може спричинити значну шкоду населенню, майну, суспільству та довкіллю, що зумовлює необхідність забезпечення їх належного захисту [1–3].

Відповідно до Закону України “Про критичну інфраструктуру” державна політика у цій сфері передбачає реалізацію комплексу організаційних, нормативно-правових, інженерно-технічних, ресурсних, інформаційно-аналітичних і методологічних заходів [1]. Для ядерних установок та пов'язаних із ними об'єктів передбачено здійснення фізичного захисту, спрямованого на запобігання протиправним діям щодо ядерних матеріалів, радіоактивних відходів та інших джерел іонізуючого випромінювання [2, 3].

Захист стратегічних об'єктів та об'єктів критичної інфраструктури від терористичних, диверсійних та інших навмисних загроз є важливою складовою забезпечення державної безпеки [1, 2, 4]. Оцінювання рівня їх захищеності потребує врахування можливих сценаріїв впливу загроз, уразливості окремих елементів, наслідків порушення функціонування та ефективності заходів безпеки [4, 5].

Значна кількість і функціональна різноманітність об'єктів критичної інфраструктури зумовлюють необхідність розроблення та застосування загальних методологічних підходів до управління їх безпекою. Водночас конкретні технічні й організаційні рішення мають визначатися з урахуванням функціонального призначення об'єкта, характеру потенційних загроз, можливих наслідків їх реалізації та наявних ресурсів. Одним із таких підходів є концепція забезпечення максимального рівня безпеки за мінімальних сукупних витрат, викладена у працях В. І. Пампуро [6, 7].

Метою дослідження є обґрунтування методологічних засад застосування концепції забезпечення максимального рівня безпеки за мінімальних сукупних витрат і структурно-інформаційного методу для побудови моделей та алгоритмів управління безпекою енергетичних об'єктів критичної інфраструктури.

Для досягнення поставленої мети передбачено виконання таких завдань:

1. Розглянути основні положення концепції забезпечення максимального рівня безпеки ядерного об'єкта за мінімальних сукупних витрат.

2. Охарактеризувати методологічні підходи до застосування структурно-інформаційного методу Пампуро для побудови моделей та алгоритмів управління безпекою енергетичних об'єктів критичної інфраструктури.

Огляд літератури

Дослідження критичної інфраструктури охоплюють виявлення міжсистемних залежностей, моделювання каскадних відмов, оцінювання вразливості та стійкості об'єктів. Один із підходів передбачає попередній аналіз небезпечних подій із подальшим детальним розглядом найбільш значущих сценаріїв поширення порушень [8]. При цьому критична інфраструктура розглядається як сукупність взаємопов'язаних систем, у якій відмова одного сектору може спричинити порушення функціонування інших. Зокрема, припинення електропостачання впливає на функціонування систем зв'язку, водопостачання та транспорту. Тому під час оцінювання ризиків необхідно враховувати міжсистемні залежності, спільні причини відмов і можливість каскадного розвитку аварій [9].

До основних методів моделювання взаємозалежної критичної інфраструктури належать емпіричні, агентні, системно-динамічні, економічні та мережеві підходи [10]. Емпіричні моделі залежать від повноти даних про реальні аварії; агентні потребують значної кількості початкових параметрів; системно-динамічні описують часові зміни та зворотні зв'язки; економічні дають змогу оцінювати міжгалузеві втрати; мережеві — визначати критичні вузли та шляхи поширення відмов. Водночас жоден із зазначених підходів окремо не забезпечує повного врахування фізичних, просторових, інформаційних та організаційних залежностей.

Під час визначення критичних елементів необхідно розрізняти їхнє структурне положення та функціональний вплив, оскільки центральний вузол мережі не завжди спричиняє найбільші наслідки в разі відмови. Тому топологічний аналіз доцільно доповнювати функціональними, динамічними та ймовірнісними моделями [11]. На початковому етапі, коли детальну кількісну модель ще не сформовано, застосовують попередній аналіз взаємозалежностей. Спочатку визначають об'єкти, послуги та зв'язки між ними, після чого для відібраних залежностей розраховують показники ризику, критичності або стійкості [12].

Сучасні обчислювальні підходи охоплюють мережево-топологічні, імітаційні, оптимізаційні методи, методи, засновані на даних, а також фізично обґрунтоване машинне навчання [13]. Їх застосовують для визначення критичних вузлів, моделювання сценаріїв порушення функціонування, розподілу ресурсів і встановлення черговості відновлення. Основними проблемами залишаються недостатня пояснюваність моделей, складність їх перенесення на інші об'єкти, забезпечення робастності та врахування участі людини в процесі прийняття рішень.

Для відображення міжсекторальних залежностей застосовують мультиплексні мережі, у яких окремі види інфраструктури утворюють відповідні шари, а міжшарові зв'язки характеризують їхню функціональну взаємодію [14]. Основні труднощі застосування таких моделей пов'язані з формуванням вихідних даних, вибором структури мережі та визначенням показників її стійкості.

Перехід від оцінювання вразливості до управління безпекою передбачає вибір захисних і відновлювальних заходів. Трирівнева модель, представлена в роботі [15], охоплює попередній захист, визначення найбільш несприятливого сценарію нападу та встановлення черговості ремонту пошкоджених компонентів. Розрахунки для дев’ятивузлової системи показали, що за обмеженого бюджету додаткові витрати на попередній захист забезпечують найбільше зменшення втрати стійкості. Водночас оптимальна стратегія залежить від масштабу нападу та наявних ресурсів відновлення.

У моделях захисту від цілеспрямованих дій враховують взаємозалежність рішень оператора та порушника. Ресурси захисту розподіляють між вузлами, зв’язками та критичними

ділянками з урахуванням можливих цілей і поведінки противника [16]. Теоретико-ігровий підхід, застосований до п'яти міських водоочисних споруд, передбачає врахування економічних і системних втрат, а також можливої шкоди людям [17]. Стратегія, визначена на основі рівноваги Неша, може відрізнятися від простого посилення захисту найбільш уразливого об'єкта. Проте отриманий результат залежить від заданих сценаріїв, структури втрат і ресурсних обмежень.

Системну теорію оптимального управління безпекою застосовано до геологічного сховища радіоактивних відходів. У роботі [18] розглянуто експлуатаційну безпеку під час функціонування сховища та довготривалу безпеку після його закриття. З огляду на специфіку геологічного захоронення ці положення потребують уточнення для застосування до енергетичних об'єктів з іншою структурою та режимами функціонування.

Окремим напрямом досліджень є кількісне оцінювання фізичного захисту. Для врахування результатів перевірок і нових експлуатаційних даних запропоновано байєсівське оновлення параметрів моделі [19]. Перераховані показники порівнюють з установленими граничними значеннями, що створює підстави для коригування структури системи захисту.

Для ядерної установки фізичний захист розглядають як поєднання засобів виявлення, затримання, передавання сигналу та реагування. Маршрути проникнення відображають за допомогою діаграми послідовності дій порушника, а модель EASI використовують для визначення ймовірності припинення його дій до досягнення цілі [20]. Це дає змогу встановити вразливі маршрути та ділянки, на яких необхідно підвищити ймовірність виявлення порушника або збільшити час його затримання.

Під час оцінювання внутрішніх загроз враховують права доступу, обізнаність щодо структури об'єкта та можливість обходу окремих засобів захисту. Мінімальні перерізи використовують для визначення комбінацій відмов, після чого стратегії захисту порівнюють за показниками ризику [21].

Водночас фізичний захист не охоплює всіх складових безпеки ядерного об'єкта, оскільки розвиток аварії залежить від стану технологічних систем, точності керування та можливостей її попередження. За відсутності даних про аварії їхній ризик пропонується оцінювати з урахуванням теоретичної можливості настання відповідної події та верхньої межі її наслідків [6].

У концепції забезпечення максимального рівня безпеки за мінімальних сукупних витрат таку подію розглядають як віртуальну аварію, закономірність і повторюваність якої неможливо достовірно встановити. Для запобігання переходу об'єкта до аварійного стану використовують запас керованості — інтервал між поточним або допустимим значенням контрольованого параметра та його граничним рівнем [7]. Контрольованими параметрами можуть бути температура, тиск, витрата, активність і нейтронний потік. Запас за показником ризику залежить від похибки технології попередження аварії та надійності систем керування [6, 7]. Управління безпекою передбачає розподіл ресурсів між попередженням аварії, послабленням її розвитку та усуненням наслідків із метою зниження ризику [7].

Для кількісного оцінювання фізичного захисту ядерних установок використовують показники ймовірності переривання та нейтралізації дій порушника, характеристики ядерного матеріалу, можливі наслідки та ефективність використання ресурсів захисту [23]. У подальшій методиці перелік показників розширено шляхом урахування законодавчого й інституційного забезпечення, обліку ядерних матеріалів і людських ресурсів [22]. Результати такого оцінювання залежать від прийнятих шкал, сценаріїв та експертних оцінок.

Для сховища відпрацьованого ядерного палива оцінювання безпеки доповнено моделюванням поширення радіонуклідів і визначенням радіаційного ризику [24]. Технологія управління екологічною безпекою поєднує моніторинг, оброблення даних, моделювання просторового поширення забруднення та підтримку прийняття управлінських рішень [25].

Водночас її практичне застосування потребує апробації на основі сценарних розрахунків і фактичних даних моніторингу.

Для електроенергетичної інфраструктури топологічний аналіз поєднують із положеннями теорії ігор. На прикладі електричної підстанції визначено компоненти, пошкодження яких найбільше впливає на функціонування об'єкта, та порівняно варіанти розподілу ресурсів захисту [5]. За розглянутих сценаріїв терористичного впливу підвищення робастності критичних компонентів виявилося ефективнішим, ніж створення додаткових резервних зв'язків. Водночас запропонована модель не враховує змін технічного стану обладнання під час експлуатації та динаміки його відновлення.

Для оцінювання стійкості електроенергетичної інфраструктури запропоновано п'ятиетапну схему [26]. Вона дає змогу визначити рівень стійкості об'єктів та обґрунтувати заходи щодо його підвищення. Практичне застосування цієї схеми розглянуто переважно стосовно природних загроз, зокрема повеней. Її використання для конкретного об'єкта потребує уточнення складу показників і способів їх оцінювання.

Практичне управління безпекою передбачає перетворення даних моніторингу на керувальні дії. Алгоритм інформаційно-технічного методу охоплює збирання та аналіз даних, визначення пріоритетних ділянок, вибір схеми моніторингу, проведення контролю та прийняття рішень щодо обмеження небезпечних наслідків [27]. Оскільки зазначений метод розроблено для територій, які зазнали ракетно-артилерійських уражень, його застосування до енергетичних об'єктів потребує уточнення контрольованих параметрів, їхніх граничних значень і змісту відповідних керувальних дій.

Захист критичної інфраструктури від терористичного впливу передбачає поєднання організаційних, режимних та інформаційно-технічних заходів [28]. У межах цивільного захисту управління надзвичайними ситуаціями охоплює запобігання їх виникненню, попередження про загрози, локалізацію та ліквідацію наслідків. Водночас прогнозування, моніторинг і моделювання формують інформаційну основу для прийняття відповідних управлінських рішень [29]. Кібернетичний підхід доповнює зазначені положення дослідженням інформаційних, організаційних, функціональних і керувальних зв'язків між елементами системи, а також механізмів її адаптації до змін внутрішніх і зовнішніх умов [30].

Таким чином, наявні дослідження охоплюють моделювання взаємозалежностей і каскадних відмов, оцінювання стійкості та фізичного захисту, розподіл ресурсів, прогнозування радіаційних наслідків та інформаційне забезпечення прийняття управлінських рішень. Проте розглянуті підходи переважно спрямовані на розв'язання окремих завдань і не формують єдиної процедури, яка забезпечувала б взаємозв'язок між структурою енергетичного об'єкта, поточними значеннями контрольованих параметрів, межами безпечного стану, резервом керованості, можливими наслідками небезпечних подій і витратами на реалізацію захисних заходів. Це обґрунтовує доцільність застосування структурно-інформаційного методу для подальшого розроблення моделей та алгоритмів управління безпекою енергетичних об'єктів критичної інфраструктури.

Методологія дослідження

Дослідження має теоретико-методологічний характер. Для досягнення поставленої мети застосовано системний, структурний та інформаційний підходи, а також методи аналізу, узагальнення, порівняння й формалізації.

Дослідження здійснено у два послідовні етапи. На першому етапі проаналізовано концепцію забезпечення максимального рівня безпеки ядерного об'єкта за мінімальних сукупних витрат, систематизовано її основні постулати, визначено порогові стани, резерв керованості та взаємозв'язок між рівнем ризику й витратами на забезпечення безпеки.

На другому етапі розглянуто основні положення структурно-інформаційного методу Пампуро та визначено можливості представлення енергетично різнорідних елементів через вхідні й вихідні інформаційні змінні та зв'язки між ними. На цій основі обґрунтовано методологічні засади застосування зазначеного методу для подальшого розроблення моделей і алгоритмів управління безпекою енергетичних об'єктів критичної інфраструктури.

Результати дослідження

Концепцію забезпечення максимального рівня безпеки ядерного об'єкта за оптимально мінімальних сукупних витрат доцільно розглядати не як окремий авторський винахід, а як систематизований виклад одного з фундаментальних принципів оптимального управління безпекою [6, 7]. Її сутність проілюстровано на рис. 1.

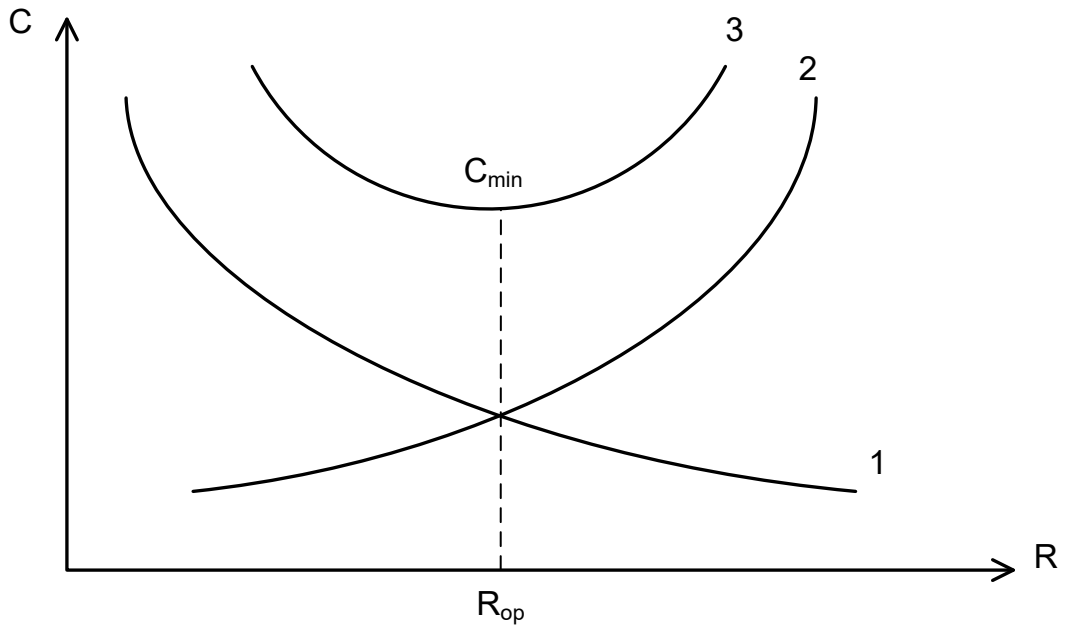


Рисунок 1: Залежність витрат на безпеку від ризику катастрофічної події [6, 7].

На осі абсцис відкладено нормований інтегральний показник ризику, значення якого змінюється в межах від 0 до 1. Цей показник формується на основі контрольованих параметрів, експертних оцінок і даних про поточний стан об'єкта. Отже, він характеризує рівень ризику, але не обов'язково є статистичною частотою або безпосередньою ймовірністю настання катастрофічної події.

На осі ординат відкладено сукупні витрати, пов'язані із забезпеченням безпеки об'єкта. Їх можна визначати у гривнях або умовних грошових одиницях. Вони охоплюють витрати на запобігання небезпечним подіям, підтримання працездатності систем захисту, реагування та ліквідацію можливих наслідків.

Концепція, викладена у працях В. І. Пампуро, ґрунтується на восьми постулатах:

1. Оптимальне управління безпекою об'єкта, що охороняється, тобто досягнення максимального ефекту за мінімальних витрат.
2. Можливість настання будь-якої гіпотетичної (віртуальної) катастрофічної події як на об'єкті, що охороняється, так і безпосередньо поблизу нього.
3. Необхідність використання всіх можливих технічних засобів, технологій, закономірностей і знань для запобігання гіпотетичним катастрофічним подіям на об'єкті, що охороняється, та безпосередньо поблизу нього.
4. Наявність резерву керованості безпекою об'єкта, що охороняється.

5. Визначення верхніх меж розвитку гіпотетичних катастрофічних подій, у разі досягнення яких можлива втрата керування як безпекою об'єкта, що охороняється, так і самим об'єктом, зокрема його основним технологічним циклом.

6. Передбачення варіантів екстремального управління об'єктом, що охороняється, у разі досягнення верхніх меж розвитку гіпотетичних катастрофічних подій.

7. Розрахунок сукупних витрат на забезпечення безпеки об'єкта, що охороняється.

8. Дотримання системного підходу до управління об'єктом, що охороняється, та забезпечення його безпеки.

Розглянемо зазначені постулати послідовно.

Перший постулат — оптимальне управління безпекою об'єкта, що охороняється, тобто досягнення максимального ефекту за мінімальних витрат.

Це положення можна розглядати не лише як постулат, а й як основний принцип оптимального управління безпекою. При цьому під безпекою стратегічного ядерного об'єкта, що охороняється, слід розуміти сукупність усіх видів безпеки та фізичного захисту об'єкта, які визначають ступінь його стійкості й здатність протистояти загрозам.

Загроза — це потенційно можлива подія, дія, процес або явище, що можуть спричинити шкоду. Для стратегічного ядерного об'єкта безпека означає здатність протистояти воєнним, терористичним, політичним, соціальним, правовим та організаційним загрозам. Вона також передбачає здатність протидіяти техногенним, інформаційним, екологічним і кримінальним загрозам, а також загрозам, зумовленим дією природних сил.

Забезпечення максимального рівня безпеки досягається шляхом практичної реалізації відповідних заходів. При цьому їх здійснення має характеризуватися максимально можливою економічною ефективністю, тобто мінімізацією сукупних витрат на безпеку та їх оптимальним розподілом.

На рис. 1 наведено криві витрат, що характеризують дві технології, які застосовують на ядерному об'єкті. Перша крива відображає витрати на запобігання гіпотетичній катастрофічній події. Чим більшими є ці витрати, тим меншим є ризик її виникнення, і навпаки.

Друга крива характеризує витрати на ліквідацію наслідків гіпотетичної катастрофічної події, що вже настала. У деяких випадках їх називають витратами на страхування. У цьому разі зі зростанням ризику збільшуються й відповідні витрати.

Третя крива відображає сукупні витрати на реалізацію обох технологій. Її мінімум відповідає оптимальному управлінню безпекою ядерного об'єкта, що охороняється. За таких умов забезпечується оптимальне, тобто прийнятне, значення ризику настання гіпотетичної катастрофічної події за мінімальних сукупних витрат.

Другий постулат — можливість настання будь-якої гіпотетичної (віртуальної) катастрофічної події як на об'єкті, що охороняється, так і безпосередньо поблизу нього.

Нині запобігання катастрофічним подіям, зокрема техногенним аваріям різного масштабу, ґрунтується на оцінюванні ймовірності їх настання. Це пояснюється тим, що такі події характеризуються певною повторюваністю. Результати відповідного аналізу становлять основу для запобігання аваріям та іншим надзвичайним ситуаціям.

За результатами таких досліджень формують дерева подій, що охоплюють сукупність можливих варіантів розвитку катастрофічних ситуацій. На їх основі розробляють симптомно-орієнтовані інструкції щодо запобігання надзвичайним ситуаціям.

Гіпотетична катастрофічна подія не характеризується статистичною стійкістю. За відсутності достатньої кількості даних імовірність її настання неможливо надійно визначити статистичними методами. Іншими словами, немає достатніх підстав стверджувати про наявність статистичної закономірності виникнення такої катастрофічної події. Водночас теоретично неможливо повністю виключити можливість її настання.

Такий підхід визначає розуміння природи виникнення гіпотетичної катастрофічної події, а також методів її запобігання. За відсутності даних про статистичні закономірності очікуваної катастрофічної події інформацію, необхідну для управління безпекою ядерного об'єкта, що охороняється, слід отримувати з фактичної обстановки всередині об'єкта та навколо нього з урахуванням тенденцій її розвитку.

Третій постулат — необхідність використання всіх можливих технічних засобів, технологій, закономірностей і знань для запобігання гіпотетичним катастрофічним подіям на об'єкті, що охороняється, та безпосередньо поблизу нього.

Узагальнюючи комплекс організаційних, інженерних, інформаційних та інших заходів із забезпечення безпеки ядерного об'єкта, що охороняється, їх можна розглядати як складові двох технологій.

Перша технологія полягає в запобіганні гіпотетичній катастрофічній події. Друга — у мінімізації та ліквідації її наслідків у разі настання.

Обидві технології можуть постійно вдосконалюватися завдяки розробленню нових наукоємних технічних засобів, способів і методів їх застосування, використанню нових матеріалів та врахуванню нововиявлених властивостей навколишнього світу. Тому третій постулат оптимального управління безпекою визначає пріоритетність першої технології, а саме запобігання гіпотетичній катастрофічній події.

Четвертий постулат — наявність резерву керованості безпекою об’єкта, що охороняється.

Це одне з ключових понять оптимального управління безпекою такого об’єкта. Воно безпосередньо пов’язане з можливістю виникнення гіпотетичної катастрофічної події, а точніше – із сукупністю таких подій.

До них можуть належати техногенні надзвичайні ситуації на об’єкті, що охороняється, які порушують його основний виробничий цикл. Наприклад, знеструмлення частини приміщень унаслідок вогневого ураження електричної підстанції, пожежа, спричинена вибухом безпілотного літального апарата, пошкодження однієї з магістральних комунікацій унаслідок дистанційного підриву заздалегідь закладеного вибухового пристрою тощо.

Резерв керованості безпекою об’єкта визначає зону потенційної небезпеки його переходу з працездатного стану до надзвичайного аварійного стану. Для пояснення цього положення розглянемо схему, наведену на рис. 2.

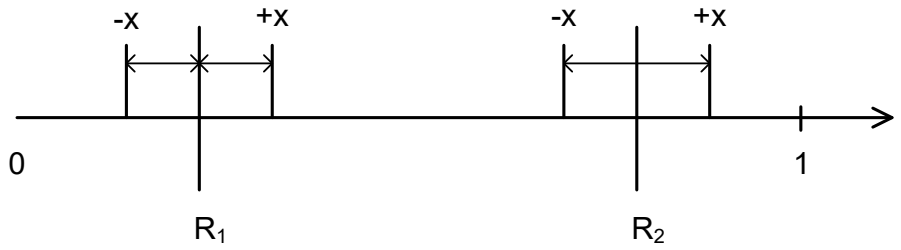


Рисунок 2. Схема резерву керованості безпекою.
Джерело: адаптовано авторами за [6, 7].

На рисунку зображено числову вісь від нуля до одиниці, що відображає зміну нормованого інтегрального показника ризику. У точці 0 ризик гіпотетичної катастрофічної події є мінімальним, а в точці 1 досягає граничного значення. Останнє відповідає стану, за якого катастрофічна подія вже настала або її подальший розвиток стає неминучим. Така подія може мати миттєвий характер або розвиватися протягом певного проміжку часу, наприклад у разі пожежі чи викиду радіоактивних речовин.

Порогове значення ризику настання гіпотетичної катастрофічної події є першою ключовою точкою у процесі управління безпекою об’єкта, що охороняється. На відрізку від нуля до цього порогового значення об'єкт перебуває в нормальному стані та експлуатується за призначенням. Після перевищення порогового значення ризику він переходить із безпечного стану до стану потенційної небезпеки.

Слід зазначити, що множина порогових значень визначається кількістю гіпотетичних катастрофічних подій. Кожна така подія характеризується сукупністю параметрів об’єктивного приладового контролю, зміна яких свідчить про перехід об'єкта з безпечного стану до стану потенційної небезпеки.

Наприклад, катастрофічна подія, пов’язана зі знеструмленням частини приміщень об'єкта, може характеризуватися одним параметром об'єктивного контролю – напругою в електричній мережі. Її зниження нижче допустимого рівня або повна відсутність можуть свідчити про перехід об’єкта до потенційно небезпечного стану.

Інша катастрофічна подія – виникнення пожежі внаслідок спрацювання дистанційно керованого вибухового пристрою – може характеризуватися двома параметрами об'єктивного контролю: підвищенням температури та збільшенням задимленості приміщень. Ці зміни фіксують відповідно датчики температури та засоби контролю задимленості.

Порушення герметичності першого контуру реакторної установки внаслідок спрацювання дистанційно керованого вибухового пристрою може характеризуватися підвищенням контрольованих рівнів іонізуючого випромінювання, зокрема гамма-, бета- та альфа-випромінювання.

Виявлення атакувального безпілотного літального апарата типу “Shahed” може здійснюватися за чотирма параметрами об’єктивного контролю: реєстрацією відбитих радіолокаційних сигналів, а також результатами оптичного, акустичного та інфрачервоного спостереження.

Отже, перехід об’єкта, що охороняється, із безпечного стану до стану підвищеної небезпеки характеризується сукупністю порогових значень нормованого показника ризику, установлених для відповідних гіпотетичних катастрофічних подій (1):

$$R_1 = \sum_{j=1}^{n} R_{1j} \tag{1}$$

Загальну кількість різних технічних параметрів об'єктивного контролю, які використовують для виявлення переходу об'єкта до стану підвищеної небезпеки, визначають за виразом (2):

$$z = \sum_{i,j=1}^{m,n} z_{ij} \tag{2}$$

де j – номер гіпотетичної катастрофічної події;

i – номер технічного параметра, який характеризує відповідну подію;

z_{ij} окремий контрольований параметр;

z – загальна кількість параметрів об’єктивного контролю для всієї сукупності подій.

Наступне порогове значення ризику R_1, або ймовірності настання гіпотетичної катастрофічної події R_2, свідчить про перехід об’єкта, що охороняється, зі стану підвищеної небезпеки до критичного стану, за якого відбувається втрата керованості безпекою об’єкта. Раніше цей стан визначали як балансування на межі, що може завершитися як настанням катастрофічної події, так і її відтермінуванням.

Різницю між пороговими значеннями нормованого інтегрального показника ризику R_2 та R_1, які характеризують відповідно перехід об'єкта до критичного стану та стану підвищеної небезпеки, прийнято називати резервом керованості безпекою об’єкта (3):

$$U = R_2 - R_1 \quad (3)$$

При цьому $0 \le R_1 < R_2 \le 1$обидва порогові показники R_1 і R_2 мають бути визначені в однаковій нормованій шкалі. Величина U резерву характеризує інтервал між пороговими станами, проте безпосередньо не визначає запасу часу та можливості здійснення керувальних дій. Останні залежать від швидкості розвитку небезпечного процесу й характеристик системи управління.

П’ятий постулат – визначення верхньої межі розвитку гіпотетичних катастрофічних подій, у разі досягнення якої можлива втрата керування як безпекою об’єкта, що охороняється, так і самим об’єктом, зокрема його основним технологічним циклом.

Цю межу визначають пороговим значенням нормованого інтегрального показника ризику R_2. Перевищення зазначеного значення свідчить про перехід об’єкта до критичного стану, за якого можлива втрата керованості та розвиток катастрофічної події.

Однак у цьому разі виникають питання, пов’язані з похибками реєстрації технічних параметрів об'єктивного контролю. З урахуванням виразу (2) найбільша сумарна похибка реєстрації сукупності технічних параметрів об'єктивного контролю катастрофічної події, що розвивається, визначається відповідними похибками вимірювання цих параметрів. Тоді межу переходу об’єкта, що охороняється, з безпечного стану до стану підвищеної небезпеки визначають за виразом (4):

$$R_1 = R_{1,j} \pm \chi \quad (4)$$

де χ – агрегована невизначеність оцінювання порогового показника ризику, приведена до нормованої шкали R на основі похибок технічних засобів контролю.

Аналогічно визначають межу переходу об'єкта, що охороняється, зі стану підвищеної небезпеки до критичного стану, тобто верхню межу розвитку гіпотетичних катастрофічних подій (5):

$$R_2 = R_{2,j} \pm \chi \quad (5)$$

Порогові значення ризику встановлюють з урахуванням допустимих і критичних значень контрольованих параметрів конкретного об'єкта. Агреговану невизначеність визначають на основі похибок вимірювання цих параметрів та способу їх перетворення на нормований інтегральний показник ризику, який не ототожнюють з імовірністю катастрофічної події без відповідного обґрунтування.

Шостий постулат — передбачення варіантів екстремального управління об’єктом, що охороняється, у разі досягнення верхньої межі розвитку гіпотетичної катастрофічної події.

Оскільки можливість виникнення такої події принципово не можна повністю виключити, необхідно заздалегідь передбачати варіанти екстремального управління об'єктом або його безпекою залежно від поточного стану.

Прикладом відпрацювання дій з екстремального управління є тренування оперативного персоналу ядерних установок, а також командного складу екіпажів морських і повітряних суден.

Оперативний персонал, який здійснює управління ядерною енергетичною установкою, у навчально-тренувальних центрах при атомних електростанціях відпрацьовує злагодженість дій у разі виникнення аварійних ситуацій, передбачених затвердженим переліком.

Крім того, персонал навчається діяти в разі появи різноманітних симптомів, зокрема незрозумілих або нетипових показань приладів, які фіксують технічні параметри об'єктивного контролю. Такі показання, своєю чергою, можуть свідчити про розвиток гіпотетичної катастрофічної події.

Командний склад екіпажів морських суден на навігаційних тренажерах відпрацьовує дії під час проходження проток і вузьких ділянок водного шляху, розходження з іншими суднами, обходу навігаційних небезпек тощо.

Екіпажі повітряних суден на авіаційних тренажерах навчаються виконувати зліт і захід на посадку, а також діяти в аварійних ситуаціях, зокрема в разі пожежі на борту, розгерметизації повітряного судна, відмови одного з двигунів тощо.

Відповідно до цього постулату необхідно заздалегідь сформувати сценарії екстремальних станів об'єкта, що охороняється, щоб залежно від його поточного стану можна було вибрати варіант дій, який найбільше відповідає конкретній ситуації.

Сьомий постулат — розрахунок сукупних витрат на забезпечення безпеки об’єкта, що охороняється.

Для практичної реалізації оптимального управління безпекою такого об'єкта необхідно враховувати сукупні витрати на безпеку, які охоплюють два види витрат.

Перший вид — витрати на реалізацію технології запобігання гіпотетичній катастрофічній події та послаблення її розвитку. Ці витрати загалом ураховуються концепцією глибокоешелонованого захисту.

Другий вид — витрати на ліквідацію наслідків гіпотетичної катастрофічної події, що настала, або на страхування від таких наслідків. Ці витрати, як правило, не враховуються концепцією глибокоешелонованого захисту.

Отже, у теорії оптимального управління безпекою об’єкта, що охороняється, показник ризику настання гіпотетичної катастрофічної події розглядають у взаємозв’язку з економічними показниками. Натомість у концепції глибокоешелонованого захисту оцінювання ризику катастрофічної події розглядають як окреме завдання, без безпосереднього зв’язку із сукупними економічними витратами.

Сукупні витрати на забезпечення безпеки об’єкта, що охороняється, визначають за виразом (6):

$$C = C_1 + C_2 \tag{6}$$

де $C_1 = \varphi_1(R)$ – функція витрат на попередження та послаблення гіпотетичної катастрофічної події залежно від показника ризику;

$C_2 = \varphi_2(R)$ – функція ймовірних витрат на страхування наслідків настання гіпотетичної катастрофічної події залежно від показника ризику.

Своєю чергою, це дає змогу розглядати показник ризику настання гіпотетичної катастрофічної події як функцію відповідних вартісних показників (7):

$$R = f(C_1, C_2) \tag{7}$$

Практичне застосування критерію мінімізації сукупних витрат потребує встановлення кількісних залежностей між витратами та ризиком з урахуванням допустимого рівня ризику, технічних і ресурсних обмежень конкретного об’єкта.

Восьмий постулат — дотримання системності під час управління об'єктом, що охороняється, та забезпечення його безпеки.

Системність ґрунтується на аксіоматичному положенні про неможливість розв'язання комплексної проблеми на основі лише однієї теорії. Кожна теорія дає змогу розв'язувати певне коло завдань і тому має принципові методологічні обмеження.

Системність охоплює методологію управління, яка забезпечує структурний синтез локальних теорій, а також математичний апарат, що дає змогу розробляти алгоритми оптимального управління об'єктами, що охороняються, та реалізовувати управління у вигляді наукоємної технології.

Водночас системність, як і будь-яка теорія, що ґрунтується на аксіоматиці, має формальні обмеження. Вони визначаються інтуїцією, філософськими та методологічними засадами, математичним апаратом і сферою застосування.

Слід зазначити, що теорію оптимального управління стосовно об'єкта, що охороняється, застосовують для розв'язання проблеми безпеки у взаємодії з локальними теоріями на кількісній оптимізаційній основі. Вона забезпечує оптимальне поєднання цих теорій у загальний алгоритм управління безпекою об'єкта, що охороняється, за критерієм ефективності.

Таким чином, концепція забезпечення максимальної безпеки ядерного об'єкта за мінімальних витрат ґрунтується на восьми постулатах: досягненні максимального ефекту за мінімальних витрат; урахуванні можливості настання будь-якої гіпотетичної (віртуальної) катастрофічної події; використанні всіх доступних технічних засобів, технологій і знань для запобігання такій події; наявності резерву керованості; визначенні верхньої межі розвитку катастрофічної події; передбаченні варіантів екстремального управління; розрахунку сукупних витрат на безпеку; дотриманні системного підходу до управління об'єктом.

Концепція оптимального управління безпекою визначає мету управління, порогові стани об'єкта, резерв керованості та економічний критерій прийняття рішень. Для практичної реалізації цих положень необхідна модель, здатна відображати взаємодію різнорідних технічних, інформаційних, організаційних і керувальних елементів. Таким апаратом у межах цього дослідження є структурно-інформаційний метод.

Застосування теорії оптимального управління дає змогу розглядати проблему безпеки у взаємозв'язку з локальними теоріями на кількісній оптимізаційній основі. Її функція полягає в об'єднанні цих теорій у загальний алгоритм управління безпекою за критерієм ефективності.

Структура інформаційно-технічного методу охоплює три взаємопов'язані елементи.

Першим елементом є модель, що описує досліджуваний процес, у цьому випадку – процес управління безпекою. Залежно від характеру поставленого завдання вона може бути когнітивною, математичною, імітаційною або комбінованою.

Другим елементом є керувальний алгоритм, який реалізує модель, відображає взаємозв'язки між складовими процесу та може бути покладений в основу відповідного програмного забезпечення.

Третім елементом є процедури, що визначають порядок практичного застосування методу. Вони становлять сукупність протоколів і встановлену послідовність їх виконання для досягнення визначеного результату.

Основним видом моделі в межах дослідження є математична модель. Принципи її побудови для керованої лінійної структури залежать від характеру елементів системи та способів їх з'єднання. Відповідні підходи розглядаються в теорії автоматичного управління, теорії інформаційно-вимірювальних систем, теорії механізмів і машин, теорії оптоелектронних і радіотехнічних систем, теорії транспортних задач, теорії електричних кіл та інших структурних детерміністичних теоріях.

З методологічного погляду детерміністичні методи побудови математичних моделей аналогових систем можна поділити на два типи. До першого належать методи, у яких енергетичні або речовинні потоки між структурними елементами є однорідними. До другого – методи, у яких взаємодіють неоднорідні потоки.

У системах першого типу через елементи та їхні з'єднання проходять однорідні матеріальні або енергетичні потоки. Закони відповідної предметної теорії встановлюють зв'язок між потоками в окремих елементах і потоками в системі загалом. Прикладами є закони Кірхгофа в електричних колах і закони розподілу потоків у транспортних задачах.

До основних способів з'єднання елементів належать послідовне, паралельне, змішане з'єднання та з'єднання за схемою зворотного зв'язку. Найповніше ці види з'єднань

представлені в теорії електричних кіл. Тому її положення можна використовувати як методологічну основу для побудови математичних моделей аналогових систем.

Елементи електричної схеми, зокрема чотириполюсники, можна розглядати як двонапрямлені з урахуванням внутрішнього зворотного зв'язку, за якого вихідні сигнали впливають на вхідні. Спільною основою їхньої взаємодії є потік електричної енергії, що проходить через усі елементи кола та пов'язується відповідними законами з потоком енергії системи загалом.

У системах другого типу взаємодіють різні за природою матеріальні, енергетичні або інформаційні потоки. Прикладом є система автоматичного управління, що складається з об'єкта управління та керувальної підсистеми. Вони можуть мати різну фізичну природу. Наприклад, механічним об'єктом може керувати електронна система.

У теорії автоматичного управління об'єкт розглядають як систему з одним або кількома контурами зворотного зв'язку. Її елементи – об'єкт і керувальна підсистема – характеризуються неоднорідними потоками. Унаслідок цього зв'язки між ними не завжди можна безпосередньо описати через послідовне, паралельне або змішане з'єднання в тому розумінні, у якому ці поняття застосовують у теорії електричних кіл.

У прикладному аналізі складних аналогових об'єктів використовують положення як теорії електричних кіл, так і теорії автоматичного управління. Остання стала складовою кібернетики, у межах якої її застосовують для дослідження систем живої та неживої природи.

Узагальненням зазначених підходів є метод детерміністичного інформаційного аналізу аналогових лінійних систем з однонапрямленими та двонапрямленими елементами. Його основою є врахування інформаційних потоків, що проходять між елементами системи.

Структурно-інформаційний метод дає змогу з єдиних позицій аналізувати широкий спектр аналогових систем різної природи, зокрема електричні, електронні, механічні та автоматичні системи. Це забезпечує можливість поєднання методологічних положень теорії електричних кіл і теорії автоматичного управління в межах єдиного підходу.

Відповідно до структурно-інформаційного аналізу аналогову систему представляють у вигляді структурної схеми. Під елементом розуміють найменшу неподільну частину системи, а під структурою – сукупність елементів, з’єднаних відповідно до визначених закономірностей інформаційної взаємодії. Зв'язки між елементами та підсистемами відображають з урахуванням напрямів передавання інформації, характеру взаємного впливу та наявності зворотних зв’язків.

Зображення двополюсного елемента наведено на рис. 3, а. Йому відповідає еквівалентне координатне ребро, зображене на рис. 3, б.

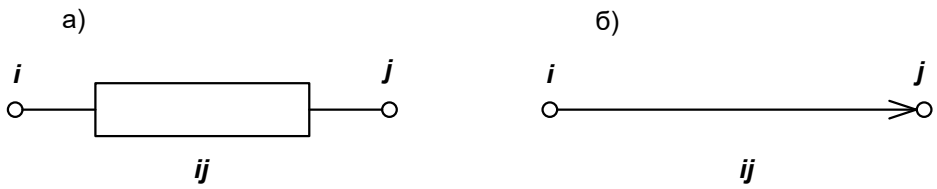


Рисунок 3. Двополюсний елемент (а) та відповідне йому координатне ребро (б) [31].

Позначення вершин координатного ребра, а також вхідного й вихідного полюсів двополюсного елемента збігаються. Це забезпечує узгодженість позначень із математичною моделлю інформаційного графа та відповідає індексам коефіцієнтів лінійного рівняння або передавальної функції.

Слід ураховувати, що позначення координатного ребра відрізняється від загальноприйнятого позначення орієнтованого ребра (дуги) у теорії графів.

Складніші елементи, або підсхеми, можуть мати кілька вхідних і вихідних полюсів, як показано на рис. 4.

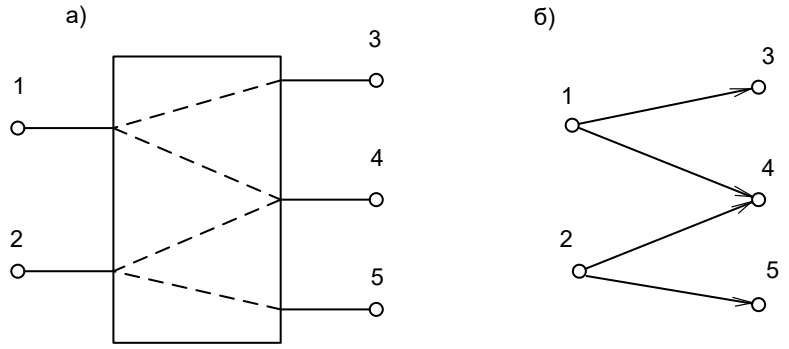


Рисунок 4. Підсхема (а) та відповідний їй граф (б) [31].

Граф (б) із вхідними вершинами 1 і 2 та вихідними вершинами 3, 4 і 5 є еквівалентним підсхемі (а).

Для опису структури графа як сукупності його координатних ребер доцільно послідовно перелічити всі вершини графа, а також координатні ребра, орієнтовані до кожної з них.

На рис. 5 наведено підграф зі спільною вершиною та структурними ребрами, орієнтованими до неї, а також еквівалентну йому частину структурної схеми з двополюсними елементами.

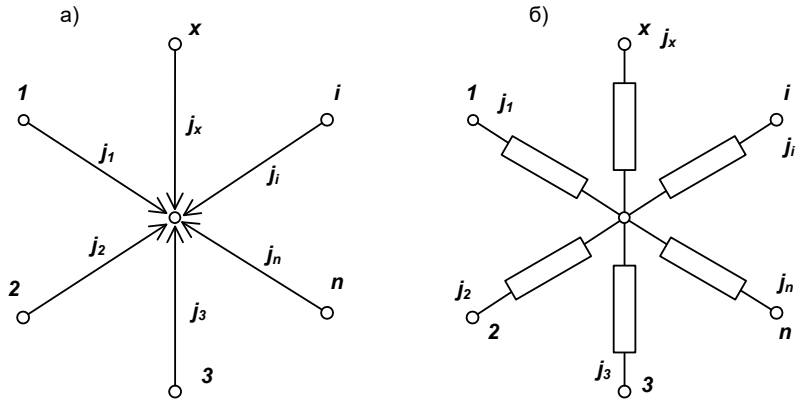


Рисунок 5. Підграф (а) та еквівалентна йому схема з’єднання елементів (б) [31].

Використовуючи прийняті позначення елементів і встановлені закономірності їх взаємозв’язку у структурі об'єкта як керованої системи, можна побудувати структурну схему об'єкта, що складається з енергетично різнорідних елементів.

Таким чином, застосування методу Пампуро під час розроблення інформаційно-технічних методів забезпечення державної безпеки України становить методологічну основу побудови систем управління аналоговими об'єктами, що складаються з енергетично різнорідних елементів. Основою цієї методології є інформаційний підхід.

Елементи з різними енергетичними або матеріальними потоками розглядають із єдиних інформаційних позицій – через взаємозв'язок інформаційних потоків. Для цього у структурі об'єкта враховують зв’язки між вхідними та вихідними інформаційними змінними елементів, еквівалентними відповідним інформаційним потокам.

Інформаційна змінна — це контрольована, вимірювана, діагностована, обчислювана, передавана, перетворювана за заданим законом або регульована величина, яка прямо чи опосередковано характеризує керований стан об’єкта.

Таким чином, у дослідженні систематизовано положення концепції оптимального управління безпекою та структурно-інформаційного методу В. І. Пампуро.

У дослідженні систематизовано положення концепції оптимального управління безпекою та структурно-інформаційного методу В. І. Пампуро. На основі їх узагальнення обґрунтовано методологічний підхід до спільного застосування зазначених положень у процесі управління безпекою енергетичних об'єктів критичної інфраструктури.

Авторський внесок полягає в обґрунтуванні методологічного зв’язку між структурним представленням енергетично різнорідних елементів об’єкта, їхніми вхідними та вихідними інформаційними змінними, контрольованими параметрами, пороговими станами й резервом керованості безпекою. Запропоноване поєднання цих складових формує концептуальну основу для подальшого розроблення математичних моделей та алгоритмів підтримки управлінських рішень щодо забезпечення безпеки енергетичних об'єктів критичної інфраструктури.

Отримані результати мають теоретико-методологічний характер. Перевірка працездатності та ефективності запропонованого підходу потребує подальшої формалізації математичних залежностей, розроблення відповідних алгоритмів і проведення сценарних розрахунків з урахуванням характеристик конкретних об'єктів.

Обговорення

Результати дослідження свідчать про методологічну можливість поєднання концепції оптимального управління безпекою та структурно-інформаційного методу В. І. Пампуро для аналізу енергетичних об’єктів критичної інфраструктури.

На відміну від підходів, орієнтованих переважно на окремі аспекти оцінювання ризиків, моделювання відмов або визначення стійкості інфраструктурних систем, розглянуте поєднання методологічних положень передбачає взаємопов’язаний аналіз структури об'єкта, його інформаційних змінних, контрольованих параметрів і порогових станів.

Водночас структурно-інформаційний метод не слід розглядати як альтернативу мережевому, імітаційному або ймовірнісному моделюванню. Зазначені підходи можуть застосовуватися взаємодоповнювально залежно від характеру досліджуваного об'єкта, наявності вихідних даних і поставлених завдань.

Методологічне значення отриманих результатів полягає в обґрунтуванні можливості формування спільної структурної основи для опису енергетично різнорідних елементів об'єкта та пов'язування їхнього стану з контрольованими параметрами й резервом керованості безпекою.

Основними обмеженнями дослідження є його теоретико-методологічний характер, відсутність практичної апробації на конкретному енергетичному об'єкті та необхідність подальшого визначення кількісних залежностей між інформаційними змінними, пороговими станами й показниками ризику.

Подальші дослідження доцільно спрямувати на розроблення математичної моделі управління безпекою конкретного енергетичного об'єкта, формування алгоритму оброблення контрольованих параметрів, визначення порогових значень та оцінювання резерву керованості з використанням сценарних розрахунків і даних моніторингу.

Висновки

1. Розглянуто основні положення концепції забезпечення максимального рівня безпеки ядерного об'єкта за мінімальних сукупних витрат. Установлено, що її основу становлять вісім постулатів, які передбачають урахування можливості виникнення гіпотетичних катастрофічних подій, визначення порогових станів об'єкта та резерву керованості його безпекою, застосування заходів запобігання катастрофічним подіям і екстремального управління, а також оптимізацію сукупних витрат на забезпечення безпеки.

2. Охарактеризовано методологічні підходи до застосування структурно-інформаційного методу Пампуро для побудови моделей та алгоритмів управління безпекою енергетичних об'єктів критичної інфраструктури. Установлено, що метод ґрунтується на представленні енергетично різнорідних елементів системи через вхідні та вихідні інформаційні змінні й взаємозв'язки між ними. Такий підхід створює методологічну основу для побудови структурних схем, математичних моделей та алгоритмів управління безпекою з урахуванням контрольованих параметрів, порогових станів об'єкта та резерву керованості його безпекою.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конфлікту інтересів.

Використання штучного інтелекту

Автори заявляють, що використовували ШІ для перевірки правопису та пошуку ресурсів.

Список використаних джерел

1. Про критичну інфраструктуру : Закон України від 16 листопада 2021 р. № 1882-IX. Відомості Верховної Ради України. 2023. № 5. Ст. 13. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 02.08.2026).
2. Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання : Закон України від 19 жовтня 2000 р. № 2064-III. Відомості Верховної Ради України. 2001. № 1. Ст. 1. URL: https://zakon.rada.gov.ua/laws/show/2064-14 (дата звернення: 02.08.2026).
3. International Atomic Energy Agency. Objective and Essential Elements of a State's Nuclear Security Regime. IAEA Nuclear Security Series No. 20. Vienna : IAEA, 2013. 15 p. DOI: https://doi.org/10.61092/iaea.ajrj-ymul.
4. United Nations Office of Counter-Terrorism. The Protection of Critical Infrastructures against Terrorist Attacks: Compendium of Good Practices. 2022 Update. URL: https://www.un.org/counterterrorism/en/compendium-good-practices-2022-update-protection-critical-infrastructure-against-terrorist-attacks (accessed 02 August 2026).
5. Yao X., Wei H.-H., Shohet I. M., Skibniewski M. J. Assessment of Terrorism Risk to Critical Infrastructures: The Case of a Power-Supply Substation. Applied Sciences. 2020. Vol. 10, No. 20. Art. 7162. DOI: https://doi.org/10.3390/app10207162.
6. Пампуро В. И. Концепция тяжелой аварии и верхняя оценка ее риска. Доповіді Національної академії наук України. 2001. № 7. С. 185–190.
7. Пампуро В. И. Концепция максимальной безопасности АЭС при минимальных затратах. Двадцать лет Чернобыльской катастрофы. Взгляд в будущее : сб. докл. Междунар. конф., Киев, 24–26 апреля 2006 г. Киев, 2006. Т. 3. Доклад Т3-22.
8. Utne I. B., Hokstad P., Vatn J. A Method for Risk Modeling of Interdependencies in Critical Infrastructures. Reliability Engineering & System Safety. 2011. Vol. 96, No. 6. P. 671–678. DOI: https://doi.org/10.1016/j.ress.2010.12.006.
9. Kröger W. Critical Infrastructures at Risk: A Need for a New Conceptual Approach and Extended Analytical Tools. Reliability Engineering & System Safety. 2008. Vol. 93, No. 12. P. 1781–1787. DOI: https://doi.org/10.1016/j.ress.2008.03.005.

10. Ouyang M. Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems. Reliability Engineering & System Safety. 2014. Vol. 121. P. 43–60. DOI: https://doi.org/10.1016/j.ress.2013.06.040.
11. Zio E. Challenges in the Vulnerability and Risk Analysis of Critical Infrastructures. Reliability Engineering & System Safety. 2016. Vol. 152. P. 137–150. DOI: https://doi.org/10.1016/j.ress.2016.02.009.
12. Bloomfield R. E., Popov P., Salako K., Stankovic V., Wright D. Preliminary Interdependency Analysis: An Approach to Support Critical-Infrastructure Risk-Assessment. Reliability Engineering & System Safety. 2017. Vol. 167. P. 198–217. DOI: https://doi.org/10.1016/j.ress.2017.05.030.
13. Ji A., He R., Chen W., Zhang L. Computational Methodologies for Critical Infrastructure Resilience Modeling: A Review. Advanced Engineering Informatics. 2024. Vol. 62. Art. 102663. DOI: https://doi.org/10.1016/j.aei.2024.102663.
14. Wang Y., Zhao O., Zhang L. Multiplex Networks in Resilience Modeling of Critical Infrastructure Systems: A Systematic Review. Reliability Engineering & System Safety. 2024. Vol. 250. Art. 110300. DOI: https://doi.org/10.1016/j.ress.2024.110300.
15. Ouyang M., Fang Y. A Mathematical Framework to Optimize Critical Infrastructure Resilience against Intentional Attacks. Computer-Aided Civil and Infrastructure Engineering. 2017. Vol. 32, No. 11. P. 909–929. DOI: https://doi.org/10.1111/mice.12252.
16. Quijano E. G., Ríos Insua D., Cano J. Critical Networked Infrastructure Protection from Adversaries. Reliability Engineering & System Safety. 2018. Vol. 179. P. 27–36. DOI: https://doi.org/10.1016/j.ress.2016.10.015.
17. Chen S., Zhao X., Chen Z., Hou B., Wu Y. A Game-Theoretic Method to Optimize Allocation of Defensive Resource to Protect Urban Water Treatment Plants against Physical Attacks. International Journal of Critical Infrastructure Protection. 2022. Vol. 36. Art. 100494. DOI: https://doi.org/10.1016/j.ijcip.2021.100494.
18. Шестопалов В. М., Пампуро В. И., Шибецкий Ю. А. Проблемы оптимального управления безопасностью геологического захоронения радиоактивных отходов. Киев : Альт-Арт, 2008. 172 с. ISBN 978-966-413-067-4.
19. Kampova K., Lovecek T., Rehak D. Quantitative Approach to Physical Protection Systems Assessment of Critical Infrastructure Elements: Use Case in the Slovak Republic. International Journal of Critical Infrastructure Protection. 2020. Vol. 30. Art. 100376. DOI: https://doi.org/10.1016/j.ijcip.2020.100376.
20. El Wely I. C., Chetaine A. Analysis of Physical Protection System Effectiveness of Nuclear Power Plants Based on Performance Approach. Annals of Nuclear Energy. 2021. Vol. 152. Art. 107980. DOI: https://doi.org/10.1016/j.anucene.2020.107980.
21. Björkman K., Holmberg J.-E., Mätäsniemi T. Comparing Physical Protection Strategies against Insider Threats Using Probabilistic Risk Assessment. Nuclear Engineering and Design. 2022. Vol. 391. Art. 111738. DOI: https://doi.org/10.1016/j.nucengdes.2022.111738.
22. Yoo H., Lee N., Ham T., Seo J. Methodology for Analyzing Risk at Nuclear Facilities. Annals of Nuclear Energy. 2015. Vol. 81. P. 213–218. DOI: https://doi.org/10.1016/j.anucene.2015.02.041.
23. Yoo H. A New Physical Protection Measure for Evaluating Risks at Nuclear Facilities. Annals of Nuclear Energy. 2009. Vol. 36, No. 9. P. 1463–1468. DOI: https://doi.org/10.1016/j.anucene.2009.06.014.
24. Краснов В. А., Рашкевич Н. В. Оцінка радіаційного впливу під час аварії на сховищі відпрацьованого ядерного палива. Комунальне господарство міст. 2025. Т. 6, вип. 194. С. 74–81. DOI: https://doi.org/10.33042/3083-6727-2025-6-194-74-81.

25. Краснов В., Рашкевич Н., Шевченко О., Погрібна Ю., Тригуб В. Розробка технології управління екологічною безпекою у разі аварії на сховищі відпрацьованого ядерного палива. Social Development and Security. 2026. Vol. 16, No. 2. P. 173–185. DOI: https://doi.org/10.33445/sds.2026.16.2.15.
26. Dvorak Z., Chovancikova N., Bruk J., Hromada M. Methodological Framework for Resilience Assessment of Electricity Infrastructure in Conditions of Slovak Republic. International Journal of Environmental Research and Public Health. 2021. Vol. 18, No. 16. Art. 8286. DOI: https://doi.org/10.3390/ijerph18168286.
27. Рашкевич Н. В., Шевченко Р. І., Нешпор О. В. Формування алгоритму інформаційно-технічного методу попередження надзвичайної ситуації на територіях, що зазнали ракетно-артилерійських уражень. Комунальне господарство міст. 2024. Т. 3, вип. 184. С. 223–228. DOI: https://doi.org/10.33042/2522-1809-2024-3-184-223-228.
28. Азаренко Е. В., Гончаренко Ю. Ю., Дивизинюк М. М., Ожиганова М. И. Защита критической инфраструктуры государства от террористического воздействия. Киев : ИГНС НАН Украины, 2018. 84 с. ISBN 978-617-7187-25-6.
29. Дівізінюк М. М., Єременко С. А., Лєвтеров О. А., Пруський А. В., Стрілець В. М., Стрілець В. В., Шевченко Р. І. Теоретичні засади парадигми «Цивільний захист» : монографія. Київ : ТОВ «Азимут-Принт», 2022. 335 с. ISBN 978-617-8015-20-6.
30. Теслер Г. С. Новая кибернетика как фундаментальная наука. Математичні машини і системи. 2005. № 4. С. 3–14.
31. Азаренко О. В., Гвоздь В. М., Гончаренко Ю. Ю., Дівізінюк М. М., Фаррахов О. В., Сівоха І. М. Метод побудови систем управління аналоговими об’єктами (метод Пампуро). Collection of Scientific Papers «ΛΌГОΣ»: матеріали IV Міжнародної науково-практичної конференції, Болонья, 29 вересня 2023 р. С. 95–98. DOI: https://doi.org/10.36074/logos-29.09.2023.25.

References

1. Verkhovna Rada Ukrainy (2021) Pro krytychnu infrastrukturu: Zakon Ukrainy vid 16 lystopada 2021 r. № 1882-IX [On Critical Infrastructure: Law of Ukraine of November 16, 2021 No. 1882-IX]. *Vidomosti Verkhovnoi Rady Ukrainy*, 2023, no. 5, art. 13. https://zakon.rada.gov.ua/laws/show/1882-20 (accessed 02 August 2026).
2. Verkhovna Rada Ukrainy (2000) Pro fizychnyi zakhyst yadernykh ustanovok, yadernykh materialiv, radioaktyvnykh vidkhodiv, inshykh dzherel ionizuiuchoho vyprominiuvannia: Zakon Ukrainy vid 19 zhovtnia 2000 r. № 2064-III [On Physical Protection of Nuclear Installations, Nuclear Materials, Radioactive Waste and Other Sources of Ionizing Radiation: Law of Ukraine of October 19, 2000 No. 2064-III]. *Vidomosti Verkhovnoi Rady Ukrainy*, 2001, no. 1, art. 1. https://zakon.rada.gov.ua/laws/show/2064-14 (accessed 02 August 2026).
3. International Atomic Energy Agency (2013) *Objective and Essential Elements of a State’s Nuclear Security Regime*. IAEA Nuclear Security Series No. 20. Vienna: IAEA, 15 p. https://doi.org/10.61092/iaea.ajrj-ymul
4. United Nations Office of Counter-Terrorism (2022) *The Protection of Critical Infrastructures against Terrorist Attacks: Compendium of Good Practices. 2022 Update*. https://www.un.org/counterterrorism/en/compendium-good-practices-2022-update-protection-critical-infrastructure-against-terrorist-attacks (accessed 02 August 2026).
5. Yao X., Wei H.-H., Shohet I. M., Skibniewski M. J. (2020) Assessment of terrorism risk to critical infrastructures: The case of a power-supply substation. *Applied Sciences*, vol. 10, no. 20, art. 7162. https://doi.org/10.3390/app10207162

6. Pampuro V. I. (2001) Kontseptsiia tiazheloi avarii i verkhniaia otsenka ee riska [Concept of a severe accident and an upper estimate of its risk]. *Dopovidi Natsionalnoi akademii nauk Ukrainy* [Reports of the National Academy of Sciences of Ukraine], no. 7, pp. 185–190.
7. Pampuro V. I. (2006) Kontseptsiia maksimalnoi bezopasnosti AES pri minimalnykh zatratakh [Concept of maximum nuclear power plant safety at minimum cost]. *Dvadtsat let Chernobylskoi katastrofy. Vzgliad v budushchee: sbornik dokladov Mezhdunarodnoi konferentsii, Kyiv, 24–26 aprelia 2006 g.* [Twenty Years after the Chernobyl Disaster. Looking to the Future: Proceedings of the International Conference, Kyiv, April 24–26, 2006]. Kyiv, vol. 3, report T3-22.
8. Utne I. B., Hokstad P., Vatn J. (2011) A method for risk modeling of interdependencies in critical infrastructures. *Reliability Engineering & System Safety*, vol. 96, no. 6, pp. 671–678. https://doi.org/10.1016/j.ress.2010.12.006
9. Kröger W. (2008) Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering & System Safety*, vol. 93, no. 12, pp. 1781–1787. https://doi.org/10.1016/j.ress.2008.03.005
10. Ouyang M. (2014) Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, vol. 121, pp. 43–60. https://doi.org/10.1016/j.ress.2013.06.040
11. Zio E. (2016) Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety*, vol. 152, pp. 137–150. https://doi.org/10.1016/j.ress.2016.02.009
12. Bloomfield R. E., Popov P., Salako K., Stankovic V., Wright D. (2017) Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment. *Reliability Engineering & System Safety*, vol. 167, pp. 198–217. https://doi.org/10.1016/j.ress.2017.05.030
13. Ji A., He R., Chen W., Zhang L. (2024) Computational methodologies for critical infrastructure resilience modeling: A review. *Advanced Engineering Informatics*, vol. 62, art. 102663. https://doi.org/10.1016/j.aei.2024.102663
14. Wang Y., Zhao O., Zhang L. (2024) Multiplex networks in resilience modeling of critical infrastructure systems: A systematic review. *Reliability Engineering & System Safety*, vol. 250, art. 110300. https://doi.org/10.1016/j.ress.2024.110300
15. Ouyang M., Fang Y. (2017) A mathematical framework to optimize critical infrastructure resilience against intentional attacks. *Computer-Aided Civil and Infrastructure Engineering*, vol. 32, no. 11, pp. 909–929. https://doi.org/10.1111/mice.12252
16. Quijano E. G., Ríos Insua D., Cano J. (2018) Critical networked infrastructure protection from adversaries. *Reliability Engineering & System Safety*, vol. 179, pp. 27–36. https://doi.org/10.1016/j.ress.2016.10.015
17. Chen S., Zhao X., Chen Z., Hou B., Wu Y. (2022) A game-theoretic method to optimize allocation of defensive resource to protect urban water treatment plants against physical attacks. *International Journal of Critical Infrastructure Protection*, vol. 36, art. 100494. https://doi.org/10.1016/j.ijcip.2021.100494
18. Shestopalov V. M., Pampuro V. I., Shibetskii Yu. A. (2008) *Problemy optimalnogo upravleniia bezopasnostiu geologicheskogo zakhoroneniia radioaktivnykh otkhodov* [Problems of optimal safety management of geological disposal of radioactive waste]. Kyiv: Alt-Art, 172 p. ISBN 978-966-413-067-4.
19. Kampova K., Lovecek T., Rehak D. (2020) Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic. *International Journal of Critical Infrastructure Protection*, vol. 30, art. 100376. https://doi.org/10.1016/j.ijcip.2020.100376

20. El Wely I. C., Chetaine A. (2021) Analysis of physical protection system effectiveness of nuclear power plants based on performance approach. *Annals of Nuclear Energy*, vol. 152, art. 107980. https://doi.org/10.1016/j.anucene.2020.107980
21. Björkman K., Holmberg J.-E., Mätäsniemi T. (2022) Comparing physical protection strategies against insider threats using probabilistic risk assessment. *Nuclear Engineering and Design*, vol. 391, art. 111738. https://doi.org/10.1016/j.nucengdes.2022.111738
22. Yoo H., Lee N., Ham T., Seo J. (2015) Methodology for analyzing risk at nuclear facilities. *Annals of Nuclear Energy*, vol. 81, pp. 213–218. https://doi.org/10.1016/j.anucene.2015.02.041
23. Yoo H. (2009) A new physical protection measure for evaluating risks at nuclear facilities. *Annals of Nuclear Energy*, vol. 36, no. 9, pp. 1463–1468. https://doi.org/10.1016/j.anucene.2009.06.014
24. Krasnov V. A., Rashkevich N. V. (2025) Otsinka radiatsiinoho vplyvu pid chas avarii na skhovyshchi vidpratsovanoho yadernoho palyva [Assessment of radiation impact during an accident at a spent nuclear fuel storage facility]. *Komunalne hospodarstvo mist* [Municipal Economy of Cities], vol. 6, no. 194, pp. 74–81. https://doi.org/10.33042/3083-6727-2025-6-194-74-81
25. Krasnov V., Rashkevich N., Shevchenko O., Pohribna Yu., Tryhub V. (2026) Rozrobka tekhnolohii upravlinnia ekolohichnoiu bezpekoiu u razi avarii na skhovyshchi vidpratsovanoho yadernoho palyva [Development of an environmental safety management technology in the event of an accident at a spent nuclear fuel storage facility]. *Social Development and Security*, vol. 16, no. 2, pp. 173–185. https://doi.org/10.33445/sds.2026.16.2.15
26. Dvorak Z., Chovancikova N., Bruk J., Hromada M. (2021) Methodological framework for resilience assessment of electricity infrastructure in conditions of Slovak Republic. *International Journal of Environmental Research and Public Health*, vol. 18, no. 16, art. 8286. https://doi.org/10.3390/ijerph18168286
27. Rashkevich N. V., Shevchenko R. I., Neshpor O. V. (2024) Formuvannia alhorytmu informatsiino-tekhnichnoho metodu poperedzhennia nadzvychainoi sytuatsii na terytoriiakh, shcho zaznaly raketno-artyleriiskykh urazhen [Formation of an algorithm of an information and technical method for preventing an emergency in territories affected by missile and artillery strikes]. *Komunalne hospodarstvo mist* [Municipal Economy of Cities], vol. 3, no. 184, pp. 223–228. DOI: https://doi.org/10.33042/2522-1809-2024-3-184-223-228
28. Azarenko E. V., Goncharenko Yu. Yu., Diviziniuk M. M., Ozhiganova M. I. (2018) *Zashchita kriticheskoi infrastruktury gosudarstva ot terroristicheskogo vozdeistviia* [Protection of the state's critical infrastructure against terrorist impacts]. Kyiv: IGNS NAN Ukrainy, 84 p. ISBN 978-617-7187-25-6.
29. Diviziniuk M. M., Yeremenko S. A., Lievtierov O. A., Pruskyi A. V., Strilets V. M., Strilets V. V., Shevchenko R. I. (2022) *Teoretychni zasady paradyhmy "Tsyvilnyi zakhyst": monohrafiia* [Theoretical foundations of the "Civil Protection" paradigm: monograph]. Kyiv: TOV "Azymut-Prynt", 335 p. ISBN 978-617-8015-20-6.
30. Tesler G. S. (2005) Novaia kibernetika kak fundamentalnaia nauka [New cybernetics as a fundamental science]. *Matematychni mashyny i systemy* [Mathematical Machines and Systems], no. 4, pp. 3–14.
31. Azarenko O. V., Hvozd V. M., Honcharenko Yu. Yu., Diviziniuk M. M., Farrakhov O. V., Sivokha I. M. (2023) Metod pobudovy system upravlinnia analohovymy obiektamy (metod Pampuro) [Method for constructing control systems for analog objects (Pampuro method)]. *Collection of Scientific Papers "ΛΌГОΣ": Proceedings of the IV International Scientific and Practical Conference, Bologna, 29 September 2023*, pp. 95–98. https://doi.org/10.36074/logos-29.09.2023.25

This is an open access journal and all published articles are licensed under a Creative Commons «Attribution» 4.0.