УДК: 351.861
DOI: **10.33099/2311-7249/2025-54-3-93-102**

ТЮТЮНИК Вадим Володимирович,
доктор технічних наук, професор,
Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна,
https://orcid.org/0000-0001-5394-6367

ТЮТЮНИК Ольга Олександрівна,
кандидат технічних наук, доцент,
Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна,
https://orcid.org/0000-0002-3330-8920

УСАЧОВ Дмитро Володимирович,
доктор філософії,
Національний університет цивільного захисту України, Черкаси, Україна,
https://orcid.org/0000-0002-1140-9798

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ НЕЧІТКИХ КОГНІТИВНИХ КАРТ ДЛЯ СЦЕНАРНОГО МОДЕЛЮВАННЯ ФУНКЦІОНУВАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ ВОЄННОГО ХАРАКТЕРУ

Мета статті. *Дослідження особливостей застосування нечітких когнітивних карт для сценарного моделювання функціонування об'єктів критичної інфраструктури в умовах надзвичайних ситуацій воєнного характеру.*

Методи дослідження. *Під час написання статті застосовано метод когнітивного (з використання нечітких когнітивних карт) моделювання, що дало змогу оцінити потенційну ефективність введення заходів для мінімізації ризиків та забезпечення стійкості об'єктів критичної інфраструктури особливо перед загрозами, які виникають в умовах уведення в державі правого режиму воєнного стану. Запропонований підхід дав змогу проведенню сценарного моделювання максимального негативного впливу найвагоміших концептів системи загроз на рівень безпеки функціонування критичної інфраструктури.*

Отримані результати дослідження. *Розроблено когнітивну модель функціонування об'єктів критичної інфраструктури в умовах впливу різного роду загроз, де ключові компоненти системи розбиті на три групи. Складові повсякденного функціонування враховують взаємозв'язки між показниками рівня фінансування, ресурсного забезпечення, станом технологічного обладнання, якістю продукції, а також чисельністю і кваліфікацією персоналу. Складові зовнішніх та внутрішніх загроз об'єднали різни види ризиків (фінансові, природні, техногенні, соціальні, застосування безпілотних літальних апаратів, застосування вогнепальної зброї, інформаційні, пожежні тощо) та враховують ступінь їх впливу на рівень нормального функціонування об'єкту. Наслідки від цих небезпек об'єднали соціальні, матеріальні та екологічні збитки.*

Елементи наукової новизни. *Запропонований підхід описує новий спосіб визначення негативного впливу найвагоміших загроз на рівень безпеки функціонування об'єктів критичної інфраструктури. Вперше застосовано використання нечітких когнітивних карт в частині оцінці наслідків від пожежних загроз, атак із застосуванням безпілотних літальних апаратів та терористичних дій із застосуванням вогнепальної зброї.*

Теоретична й практична значущість викладеного у статті. *Отримані результати мають прикладне значення для побудови адаптивних систем управління безпекою критичної інфраструктури на рівнях міст, регіонів та держави. Модель може бути інтегрована в існуючу єдину державну систему цивільного захисту, підвищуючи ефективність її функціональних та територіальних підсистем в режимах надзвичайного та воєнного станів.*

Ключові слова: *когнітивне моделювання, нечіткі когнітивні карти, об'єкти критичної інфраструктури, пожежні загрози, загрози застосування безпілотних літальних апаратів, загрози застосування вогнепальної зброї.*

Вступ

З початку повномасштабного вторгнення 24 лютого 2022 року російська федерація (далі – рф) проводить систематичну та цілеспрямовану кампанію з обстрілу об'єктів критичної інфраструктури (далі – ОКІ) України. Ці атаки, що є воєнним злочином, спрямовані на те, щоб підірвати українську економіку, позбавити цивільне населення базових послуг, таких як світло, тепло та вода [1]. Масовані та скоординовані удари по енергетичній інфраструктурі стали однією з основних тактик російських окупаційних військ. Так, у жовтні 2022 року рф розпочала першу масовану хвилю обстрілів енергетичних об'єктів. Протягом цього періоду було здійснено численні атаки із застосуванням крилатих та балістичних ракет, а також

© В. В. Тютюник, О. О. Тютюник, Д. В. Усачов
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

дронів-камікадзе. Одним із наймасштабніших став обстріл 15 листопада 2022 року, коли було випущено 96 ракет. Наслідком цих атак стали значні пошкодження електростанцій та високовольтних мереж, що призвело до тривалих відключень електроенергії по всій країні. Станом на квітень 2023 року енергосистема втратила майже половину своїх виробничих потужностей, а 42 з 95 високовольтних трансформаторів було пошкоджено [2].

З березня 2024 року рф відновила і посилила атаки на енергетику. Ця нова хвиля ударів характеризувалася ще більшою інтенсивністю та була спрямована не лише на об'єкти розподілу, а й безпосередньо на генеруючі потужності – теплові та гідроелектростанції. Внаслідок цих атак Україна втратила близько 9 гігават генеруючих потужностей, що становить половину обсягу, необхідного в зимовий період. Станом на червень 2024 року було виведено з ладу 73 % теплових електростанцій країни. Загалом, з жовтня 2022 року війська рф завдали понад тисячу ударів по об'єктах української енергетичної інфраструктури [3]. Наслідки цих атак є вкрай важкими. Окрім віялових відключень електроенергії, що стали звичним явищем для мільйонів українців, страждають й інші життєво важливі сфери: водопостачання, опалення, охорона здоров'я та освіта.

Окремим трагічним епізодом російської агресії стало руйнування греблі Каховської гідроелектростанції вночі 06 червня 2023 року. Цей акт, який кваліфікується як воєнний злочин та потенційний екоцид, призвів до масштабної техногенної та екологічної катастрофи [4]. Внаслідок руйнування було затоплено 620 км^2 території у Херсонській, Миколаївській, Дніпропетровській та Запорізькій областях, що безпосередньо торкнулося близько 100 тисяч мешканців. Загинули та зникли безвісти десятки людей. Загальні збитки, завдані Україні, оцінюються у 14 мільярдів доларів США. Катастрофа також створила ризики для безпеки Запорізької атомної електростанції, оскільки вода з Каховського водосховища була необхідна для її систем охолодження [5].

Паралельно з ударами по енергетиці, рф цілеспрямовано атакує портову інфраструктуру та зерносховища України, особливо після виходу із «зернової угоди». Метою цих атак є зниження українського експортного потенціалу та провокування продовольчої кризи у світі [6; 7]. Протягом кількох місяців 2024 року було зафіксовано десятки атак на порти, цивільні судна та зерносховища. Цілями ставали порти Одеси, Рені та Ізмаїла. Внаслідок цих обстрілів було пошкоджено та знищено сотні об'єктів портової інфраструктури, транспортні засоби та цивільні судна. Зокрема, за три місяці 2024 року було зафіксовано майже 60 таких атак, які пошкодили близько 300 об'єктів. Це створює пряму загрозу для продовольчої безпеки країн, що залежать від постачання українського зерна [8; 9].

Атаки на критичну інфраструктуру (далі – КІ) України не припиняються. Навіть влітку 2025 року, як свідчить масована атака дронами в ніч на 16 липня, енергетична інфраструктура залишається однією з головних цілей ворога. Українська влада та енергетики докладають максимум зусиль для відновлення пошкоджених об'єктів, часто працюючи під загрозою нових ударів. Однак масштаби руйнувань є колосальними, і на повне відновлення знадобляться роки та мільярди доларів. Міжнародні партнери надають допомогу, проте Україна наголошує на нагальній потребі у посиленні протиповітряної оборони для захисту своєї критичної інфраструктури та цивільного населення [10; 11].

Виходячи з цих позицій, підвищення ефективності запобігання та ліквідації різного роду загроз для функціонування КІ держави є актуальним науково-практичним завданням у сфері безпеки та оборони, у вирішенні якої зацікавлені місцеві органи влади та громадськість України.

Постановка проблеми. Захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз є важливим завданням в умовах нерівномірного розподілу по території держави КІ, з низкою життєвоважливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України, зокрема: урядування та надання найважливіших публічних (адміністративних) послуг; енергозабезпечення (у тому числі постачання теплової енергії); водопостачання та водовідведення; продовольче забезпечення; охорона здоров'я; фармацевтична промисловість; виготовлення вакцин, стале функціонування біолабораторій; інформаційні послуги; електронні комунікації; фінансові послуги; транспортне забезпечення; оборона, державна безпека; правопорядок, здійснення правосуддя, тримання під вартою; цивільний захист населення та територій, служби порятунку; космічна діяльність, космічні технології та послуги; хімічна промисловість; дослідницька діяльність [12; 13].

Захист КІ, як одна із складових національної безпеки України, містить види діяльності, що виконуються перед або під час створення, функціонування, відновлення і реорганізації ОКІ. Крім того, вони спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці цих об'єктів, а також мінімізацію та ліквідацію наслідків у разі їх реалізації [14].

Одним з актуальних напрямів підвищення ефективності забезпечення безпеки ОКІ є розроблення адекватних моделей, спрямованих на підвищення ефективності прийнятих антикризових рішень в умовах багатокритеріальності й невизначеності за управління процесами запобігання виникнення надзвичайних ситуацій (далі – НС) на різного роду ОКІ. Це і обумовило напрям наших досліджень.

Аналіз останніх досліджень і публікацій. За визначенням проаналізованих джерел необхідними умовами ефективності рішень є їх своєчасність, повнота і оптимальність. Перераховані вимоги суперечливі й їх забезпечення пов'язане з серйозними труднощами [15–17]. Забезпечення повноти (комплексності) рішень вимагає якомога повнішого врахування внутрішніх і зовнішніх факторів, що

впливають на прийняття рішення, глибокого аналізу їх взаємозв'язків, що веде до зростання розмірності задачі прийняття рішень, її багатокритеріальності. У свою чергу це призводить до зростання невизначеності вихідних даних, що обумовлено неповнотою знань про взаємозв'язок факторів і, як наслідок, неточного їх опису, неможливістю або неточністю вимірювання деяких факторів, випадкових зовнішніх і внутрішніх впливів тощо. Додатковою складністю є те, що невизначеності різнорідні і можуть мати вигляд випадкових чи інтервальних величин, або нечітких множин. Підвищення ефективності прийнятих рішень пов'язано з необхідністю вирішення задач багатокритеріальної оптимізації в умовах невизначеності.

У процесі обговорення суспільних відносин у сфері захисту ОКІ важливо зауважити, що на сьогодні існує значна кількість наукових досліджень, що розглядають різні аспекти їх функціонування. Так, у роботі [18] запропонований системний підхід до проблеми захисту ОКІ, огляд міжнародних практик, визначення пріоритетних секторів і загроз, а також формулювання конкретних рекомендацій щодо вдосконалення нормативно-правової бази та координації дій. Автори роботи [19] використали симпліціальний аналіз для когнітивних моделей, що дало змогу визначити управляючі та зв'язні концепти системи, що сприяло підвищенню рівня інформаційної захищеності. У роботі [20], шляхом використання методів системного аналізу, оптимізації та теорії ризиків, розроблена концепція та методологія оцінювання та забезпечення безпеки критичної інформаційної інфраструктури, включаючи інформаційні та телекомунікаційні систем.

Проте більшість досліджень лише частково зачіпають аспекти захисту зазначених об'єктів, оскільки їхня увага в основному зосереджується або на правовому статусі суб'єктів суспільних відносин, або на окремих напрямках та умовах їхнього функціонування. З цього постає питання про те, що існуючі дослідження, переважно, мають тенденцію обмежувати свою сферу інтересів, не охоплюючи в повному обсязі аспекти безпеки на ОКІ. Базуючись на цих аспектах, виникає необхідність у моделюванні процесів антикризового управління безпекою ОКІ з погляду аналізу динамічних процесів, пов'язаних з аналізом ОКІ, визначенням основних загроз, прогнозуванням можливої аварійної ситуації, прийняттям антикризового рішення, його впливом на елементи системи та аналізом нової ситуації. Так, в умовах невизначеності та недостовірності інформації про параметри можливої НС, одним з перспективних методів підтримки прийняття антикризових управлінських рішень на ОКІ є метод моделювання процесів управління та оцінки впливу на систему об'єкта внутрішніх та зовнішніх факторів, що впливають на виникнення аварійної ситуації, шляхом використання нечітких когнітивних карт (далі – НКК). Це зумовило необхідність формулювання мети та завдань дослідження.

Метою статті є дослідження особливостей застосування нечітких когнітивних карт для сценарного моделювання функціонування об'єктів критичної інфраструктури в умовах надзвичайного стану НС воєнного характеру. Для досягнення мети поставлені для розв'язання такі завдання: провести аналіз причинно-наслідкових зв'язків між елементами функціональної системи гіпотетичного ОКІ; шляхом застосування методу НКК провести моделювання ефективності прийняття рішень із запобігання виникнення НС на ОКІ; провести дослідження сценаріїв впливу загроз на рівень безпеки ОКІ.

Виклад основного матеріалу дослідження

Аналіз причинно-наслідкових зв'язків між елементами функціональної системи гіпотетичного ОКІ. Для забезпечення ефективного функціонування ОКІ, безперебійної роботи кожного елемента технологічного процесу та успішного виконання всіх завдань необхідно надати особливу увагу організації загальної безпеки об'єкта. КІ та її ресурси постійно перебувають під загрозою атак різного характеру: соціальних, техногенних, природних і військових. Такі атаки можуть спричинити серйозні наслідки, зокрема, порушення роботи життєвоважливих компонентів об'єкта, загрозу життю та здоров'ю персоналу, несанкціонований доступ до інформаційних ресурсів, збоїв у технологічних процесах або навіть повне порушення роботи системи. Для запобігання подібним ризикам необхідно ретельно аналізувати вплив потенційних загроз, оцінювати міцність взаємозв'язків між компонентами системи та виділяти найбільш критичні з них.

Розв'язання цього завдання можливе завдяки методам статистичного аналізу, таким як дисперсійний і кореляційно-регресійний аналіз. Однак їх застосування потребує значних обчислювальних ресурсів, наявності повної статистичної інформації та тривалого часу для обробки даних. У зв'язку з цим доцільно використовувати когнітивний підхід, який допомагає вирішувати задачі зі складною або неповною формалізацією. Цей підхід сприяє візуалізації досліджуваної системи чи проблеми, роботі з нечіткою, неповною інформацією, а також врахуванню суб'єктивних експертних оцінок. Він дає змогу створювати гнучкі моделі, здатні адекватно реагувати на зміни та ефективно відображати реальну ситуацію.

Враховуючи вищезазначені переваги когнітивного моделювання, проведемо на його основі дослідження функціонування гіпотетичного ОКІ та впливу загроз на рівень захищеності об'єкту. Схема взаємозв'язків між складовими функціонування ОКІ наведена на рис. 1.

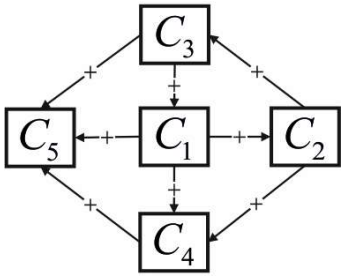

Рисунок – 1. Схема взаємозв'язків між складовими повсякденного функціонування ОКІ

На основі проведеного авторами опитування експертів було визначено пріоритетні концепти системи та ступінь впливу взаємозв'язків між ними в технологічному процесі. Цей процес ОКІ складається з таких елементів:

1. Концепт C_1 – обладнання. Обладнання забезпечує завантаження виробничої потужності відносно максимального рівня. Це основа системи КІ, яка підтримує виконання головних технологічних і виробничих процесів. Відсутність належного обладнання робить функціонування системи неможливим.

2. Концепт C_2 – фінансування. Фінансування забезпечує можливість придбання ресурсів, підтримку обладнання та наймання персоналу. Це критичний елемент стабільного функціонування, що безпосередньо впливає на матеріальну базу об'єкта.

3. Концепт C_3 – ресурси. До ресурсів належать паливо-мастильні матеріали, сировина, енергія та технології. Вони потрібні для обслуговування та безперервної роботи обладнання. Ефективність виробництва значною мірою залежить від наявності цих ресурсів.

4. Концепт C_4 – персонал. Персонал є важливим елементом для виконання завдань об'єкта. Його чисельність і кваліфікація безпосередньо впливають на підтримку працездатності обладнання та процесів. Помилки персоналу можуть вплинути на продуктивність та безпеку.

5. Концепт C_5 – продукція. Продукція характеризується обсягом виробництва та випуском кінцевого продукту, наприклад, енергетичних ресурсів у випадку енергетичних об'єктів. Це кінцевий результат діяльності об'єкта, що має вирішальне значення для забезпечення потреб споживачів і стабільності системи.

ОКІ функціонує як збалансована система, де кожен компонент тісно пов'язаний з іншими. Для забезпечення стійкості функціонування ОКІ важливо підтримувати достатній рівень фінансування, якість ресурсів і кваліфікацію персоналу. Зміни або збої в одному з елементів можуть вплинути на всю систему, зокрема, на можливість виробництва продукції. Такий підхід до опису системи дає змогу виявляти критичні точки, які потребують уваги для забезпечення безперебійного функціонування об'єкта. У дослідженні метод експертних оцінок був інтегрований із використанням НКК. Це дало змогу врахувати не лише кількісні, але й якісні аспекти взаємозв'язків, які важко формалізувати традиційними математичними методами. Експертні дані було використано для побудови графічної моделі технологічного процесу, де вузли відображають концепти, а зв'язки між ними показують характер і силу взаємного впливу.

З метою виявлення загальних взаємозв'язків блоків технологічного процесу дослідимо умови функціонування ОКІ за допомогою методу НКК. Метод використання НКК будується на основі математичного апарату знакових та зважених графів, які дають змогу формалізувати взаємодію основних позитивних та негативних зворотних впливів, що існують між підсистемами. У процесі побудови таких моделей можна використовувати неповну, нечітку і навіть суперечливу інформацію. Когнітивні карти допомагають отримати попередню якісну оцінку наслідків прийнятих рішень. За допомогою когнітивних карт можна вибрати таку множину рішень, яка переведе систему у сприятливу ситуацію. У цьому під ситуацією розуміється безліч чинників зі змінними, які описують ступінь впливу чинників один на одного. Когнітивні карти дають загальну якісну картину розвитку НС як результат спільної взаємодії різних факторів (як внутрішніх, так і зовнішніх) на певному відрізку часу. Водночас, самі фактори можуть змінюватись у часі. На основі когнітивних карток можна аналізувати та прогнозувати стратегію розвитку складних систем, виникнення кризових ситуацій.

Когнітивне моделювання ефективності прийняття рішень із запобігання виникнення надзвичайної ситуації на ОКІ. У роботі моделювання виконано з використанням програмного забезпечення Mental Modeler, яке реалізує методи когнітивного моделювання, базуючись на принципах когнітивних карт причинно-наслідкових взаємозв'язків. Основна ідея полягає у представленні системи як мережі концептів (елементів) і взаємозв'язків між ними, які можуть бути кількісно оцінені. Кожен концепт C_i має числове значення $A_i(t)$, що визначає його стан у момент часу *t*. Значення A_i в момент часу $t+1$ змінюється відповідно до функції активації *f* (обмежує значення концепту в межах від -1 до 1) з урахуванням впливу інших концептів:

$$A_i(t+1) = f\left(A_i(t) + \sum_{j=1}^{n} w_{ji} A_j(t)\right), \qquad (1)$$

де $A_i(t)$ – значення i концепту у момент часу t;

$A_j(t)$ – значення j концепту у момент часу t;

w_{ji} – вага взаємозв'язку між j та i концептами (показує силу впливу від -1 до 1).

У цій статті застосовано причинно-наслідкову мережу ОКІ з відповідними значеннями ваги зв'язків. Вага зв'язків визначає тип і силу впливу одного концепту на інший: $w_{ji} > 0$ – позитивний вплив (зростання одного концепту призводить до збільшення іншого); $w_{ji} < 0$ – негативний вплив (зростання одного концепту зменшує значення іншого); $w_{ji} = 0$ – відсутність впливу.

Сформований перелік концептів $C_1 - C_5$ допомагає оцінити силу взаємного впливу між кожною парою концептів шляхом аналізу даних, отриманих у результаті експертного опитування. Для цього використовується нечітка лінгвістична шкала, яка являє собою впорядковану множину лінгвістичних

термінів, що відображають оцінки ймовірних наслідків впливу одного концепту на інший, а саме:

$$W_{ij} = \{\text{не впливає, слабка, середня, сильна}\}, \quad (2)$$

де W_{ij} – інтенсивність взаємодії.

Кожному з цих термінів відповідає певний числовий діапазон: значення з інтервалу $[0;\ 1]$ застосовуються для додатних взаємозв'язків, а значення з інтервалу $[-1;\ 0]$ – для від'ємних. Для інтенсивності взаємодії пропонується така градація:

$W_{ij} = [0,7;\ 1,0]$ – позитивна сильна;

$W_{ij} = [0,3;\ 0,7]$ – позитивна середня;

$W_{ij} = [0;\ 0,3]$ – позитивна слабка;

$W_{ij} = 0$ – не впливає;

$W_{ij} = [0;\ -0,3]$ – негативна слабка;

$W_{ij} = [-0,3;\ -0,7]$ – негативна середня;

$W_{ij} = [-0,7;\ -1,0]$ – негативна сильна.

Загрози, що впливають на ОКІ, мають комплексний характер і охоплюють широкий спектр потенційних впливів. За одержання інформації про можливе виникнення НС, управління об'єктом переводять ОКІ у режим аварійного стану, коли стан об'єкту вимагає вживання негайних заходів щодо недопущення виникнення аварійної чи надзвичайної ситуації. В умовах аварійного режиму роботи ОКІ враховуються зовнішні та внутрішні фактори, що позначені зовнішніми стрілками на концептуальній моделі рис. 2.

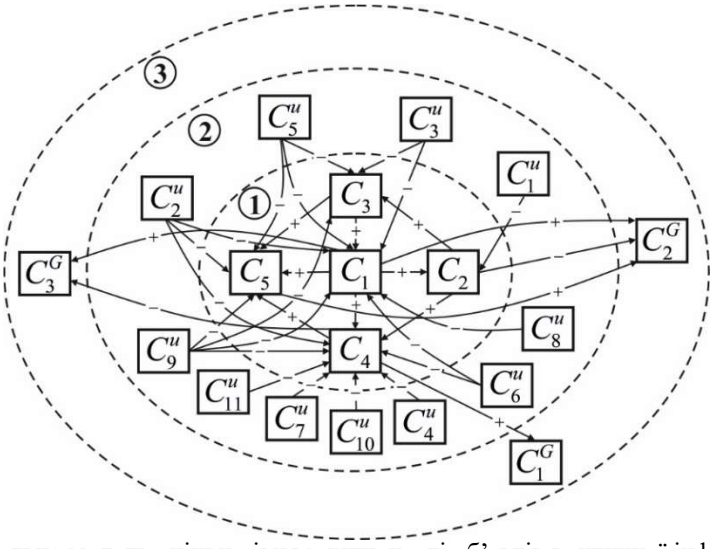

Рисунок 2 – Концептуальна модель оцінки рівня захищеності об'єктів критичної інфраструктури на основі методу нечітких когнітивних карт

Концепти об'єднані у три групи:

1 – складові повсякденного функціонування;

2 – складові зовнішніх і внутрішніх загроз;

3 – наслідки від небезпек

У результаті проведення аналізу можливих загроз безпеки ОКІ було сформовано перелік зовнішніх та внутрішніх загроз C_1^u – C_{11}^u, а саме:

C_1^u – фінансові загрози (макроекономічні чинники, такі як рівень інфляції в державі та співвідношення заробітної плати до прожиткового мінімуму тощо);

C_2^u – природні загрози (геофізичні, геологічні, метеорологічні та гідрологічні НС, а також ситуації, пов'язані з пожежами у природних екологічних системах та медико-біологічними факторами тощо);

C_3^u – техногенні загрози (аварії та катастрофи на транспорті, витоки небезпечних хімічних або радіоактивних речовин, руйнування будівель і споруд, збій в електроенергетичних системах, аварії на очисних спорудах та в нафтогазовій промисловості тощо);

C_4^u – соціальні загрози (акти насилля, захоплення ОКІ, терористичні акти, викрадення людей, а також захоплення заручників тощо);

C_5^u – загрози застосування безпілотних літальних апаратів (далі – БпЛА) (загрози, пов'язані з використанням БпЛА для розвідувальних цілей або проведення атак на ОКІ тощо);

C_6^u – інформаційні загрози (витоки інформації, кібератаки та інші дії, пов'язані з порушенням інформаційної безпеки);

C_7^u – неякісне виконання службових обов'язків (неефективне використання методів стимулювання праці персоналу, недбале виконання обов'язків тощо);

C_8^u – порушення режимів технологічного процесу (зношеність або несправність обладнання, порушення режимів технологічного процесу та неефективне управління персоналом тощо);

C_9^u – пожежні загрози (недотримання вимог пожежної безпеки, необережне поводження з вогнем, порушення правил монтажу та експлуатації

обладнання, а також недосконалість систем пожежної сигналізації та пожежогасіння);

C_{10}^{u} – загрози виробничого травматизму (неправильно організована праця, відсутність засобів захисту чи спеціального одягу, а також порушення трудової дисципліни тощо);

C_{11}^{u} – загрози застосування вогнепальної зброї (бойові дії та терористичні акти із використанням зброї).

У наведеній на рис. 2 концептуальній схемі крім концептів C_i^u також зазначені концепти C_i^G, що характеризують наслідки (збитки) різного характеру, а саме:

C_1^G – соціальні збитки;

C_2^G – матеріальні збитки;

C_3^G – екологічні збитки.

Для проведення аналізу НКК слід врахувати всі опосередковані взаємовпливи між концептами. З цією метою, на основі створеної когнітивної карти, у роботі проведено аналіз основних системних показників на основі матриці суміжності:

$$W = \left[C_i / C_j \right]_{n \times n} \quad (3)$$

Так, за наближення значень змінних до відповідного інтервалу $\left[-0,7;\ -1,0\right]$ – стан ОКІ суттєво змінюється, змінюються зв'язки між концептами, а деякі концепти втрачають свою значущість. Для визначення таких змін параметрів проаналізована модель причинно-наслідкових взаємозв'язків стану ОКІ за умови загрози виникнення аварійної ситуації та виявленні найвагоміші загрози з відповідними значеннями змінних в умовах уведення в державі правового режиму воєнного стану. Результати наведено у табл. 1.

Таблиця 1

Значущість впливу концептів зовнішніх і внутрішніх загроз на функціонування об'єктів критичної інфраструктури в умовах надзвичайних ситуацій воєнного стану

Загрози	Вхідний ступінь	Вихідний ступінь	Центральність
C_1^u – фінансові загрози	0,00	0,30	0,30
C_2^u – природні загрози	0,00	1,10	1,10
C_3^u – техногенні загрози	0,00	0,80	0,80
C_4^u – соціальні загрози	0,00	0,45	0,45
C_5^u – загрози застосування БпЛА	0,60	1,65	2,25
C_6^u – інформаційні загрози	0,00	0,80	0,80
C_7^u – неякісне виконання службових обов'язків	0,00	0,30	0,30
C_8^u – порушення режимів технологічного процесу	0,00	0,60	0,60
C_9^u – пожежні загрози	0,70	2,45	3,15
C_{10}^u – загрози виробничого травматизму	0,00	0,60	0,60
C_{11}^u – загрози застосування вогнепальної зброї	0,50	0,67	1,17

Проаналізувавши значення наведених у табл. 1 показників можна зробити висновок, що в умовах уведення в державі правого режиму воєнного стану найвагомішими концептами досліджуваної системи загроз є:

C_5^u – загрози застосування БпЛА;

C_9^u – пожежні загрози;

C_{11}^u – загрози застосування вогнепальної зброї. Також доцільно зазначити, що найменший вплив на умови функціонування ОКІ мають такі концепти як C_1^u та C_7^u. Заразом, значення, які наведені авторами в табл. 1, не мають одиниць виміру, оскільки вони є безрозмірними величинами і є відносними показниками. Вони характеризують модель функціонування (у режимах повсякденного та аварійного функціонування) ОКІ, побудованої з використанням програмного забезпечення Mental Modeler, і стосуються взаємозв'язків між компонентами цієї моделі:

Вхідний ступінь – кількість взаємозв'язків, що спрямовані до певного компонента;

Вихідний ступінь – кількість взаємозв'язків, що виходять від певного компонента;

Центральність – значимість компонента у моделі на основі його взаємозв'язків.

Дослідження сценаріїв впливу загроз на рівень безпеки ОКІ. Для прогнозування розвитку НС визначимо відносну зміну концептів системи методом сценарного аналізу під впливом найвагоміших факторів за їх максимального значення. Сценарний аналіз дає змогу спрогнозувати розвиток досліджуваної ситуації, визначити, оцінити та зменшити невизначеність, пов'язану з впливом ключових концептів, що впливають на захищеність ОКІ. Це, у свою чергу, допомагає формувати ефективні рішення із запобігання НС на ОКІ. Разом із тим, побудова сценаріїв дала змогу авторам найбільш детально дослідити вплив основних загроз, які характерні для уведеного в державі правого режиму воєнного стану, на рівень безпеки ОКІ в умовах невизначеності та динамічних змін вхідних даних.

Сценарій 1. Аналіз зміни стану функціонування ОКІ за умови максимального збільшення значення

концепту C_5^u – загрози застосування БпЛА, до яких належать дії, пов'язані з використанням БпЛА. БпЛА здатні нести засоби ураження та вибухові пристрої, засоби радіоелектронної боротьби, а також використовуватися для несанкціонованого моніторингу або збору даних. Загроза полягає у тому, що завдяки високій маневреності, непомітності та можливості подолати традиційні системи захисту БпЛА можуть завдати шкоди ОКІ та обслуговуючому персоналу.

Згідно з даними, наведених на рис. 3, у досліджуваній системі концепт C_5^u безпосередньо впливає на такі головні показники: C_5 – продукція, з максимальним значенням у системі ($-0,78$); C_4 – персонал ($-0,54$); C_1 – обладнання ($-0,46$), C_3 – ресурси ($-0,41$); C_2 – фінансування ($-0,39$).

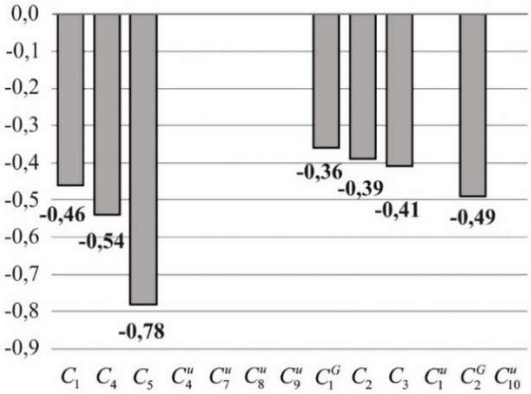

Рисунок – 3 Гістограма реакції стану функціонування об'єктів критичної інфраструктури на максимально негативні зміни концепту C_5^u – загрози застосування безпілотних літальних апаратів

Отримана за допомогою програмного забезпечення Mental Modeler гістограма демонструє, що ураження об'єкта за допомогою БПЛА призводить до таких наслідків як: C_1^G – соціальні збитки ($-0,36$); C_2^G – матеріальні збитки ($-0,49$). Тому загроза БпЛА призводить до значного погіршення функціонування ОКІ, зокрема, у виробничій, фінансовій та безпековій сферах, що потребує впровадження додаткових заходів для посилення захисту та зменшення рівня негативних наслідків.

Сценарій 2. Дослідження ступеню зміни концептів функціонування ОКІ за максимального збільшення негативного впливу на них концепту C_{11}^u – загрози застосування вогнепальної зброї.

Згідно з даними, наведеними на рис. 4, застосування вогнепальної зброї під час терористичних актів на ОКІ становить значну загрозу як для фізичної безпеки об'єкта, так і для його функціонування. Напади терористів із застосуванням вогнепальної зброї можуть бути спрямовані на знищення головних елементів інфраструктури, завдання шкоди персоналу та створення хаосу, що призводить до зупинки критично важливих процесів.

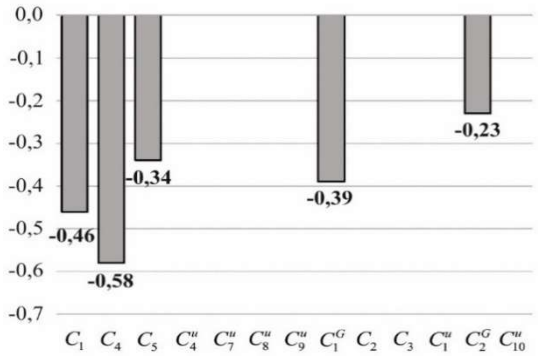

Рисунок – 4 Гістограма реакції стану функціонування об'єктів критичної інфраструктури на максимально негативні зміни концепту C_{11}^u – загрози застосування вогнепальної зброї

За умов максимального збільшення значення концепту C_{11}^u – загрози застосування вогнепальної зброї, система функціонування ОКІ зазнає суттєвих негативних змін. Так, за результатами проведеного когнітивного моделювання найбільше зниження спостерігається у концептах C_4 – персонал ($-0,58$) та C_5 – продукція ($-0,34$). Також спостерігається зниження концептів C_1^G – соціальні збитки на $0,39$ та C_2^G – матеріальні збитки на $0,23$. Загалом, зазначені зміни вказують на необхідність термінового посилення заходів захисту для мінімізації ризиків та забезпечення стійкості ОКІ перед загрозами терористичних актів. Першочергову увагу слід надати захисту персоналу, оскільки людський ресурс є основним елементом, від якого залежить ефективність функціонування ОКІ та можливість швидкого відновлення після інциденту.

Сценарій 3. Аналіз зміни концептів функціонування ОКІ за умови максимального збільшення значення концепту C_9^u – пожежні загрози.

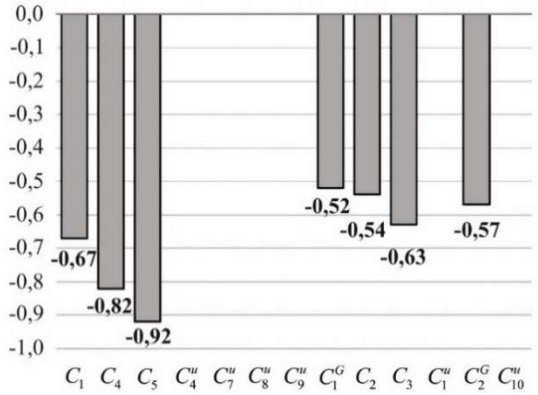

Рисунок – 5 Гістограма реакції стану функціонування об'єктів критичної інфраструктури на максимально негативні зміни концепту C_9^u – пожежні загрози

Згідно з даними, наведеними на рис. 5, пожежні загрози на ОКІ становлять серйозну небезпеку для функціональної стійкості об'єктів та безпеки персоналу як у повсякденному режимі роботи, так і в режимі НС. Пожежі можуть виникати через технічні несправності, людський фактор або зовнішні впливи, такі як

терористичні атаки чи природні катастрофи. Наслідками пожеж може бути фізичне пошкодження обладнання, зупинка робочих процесів, перебої в електропостачанні та передачі даних, що може спричинити масштабний збій в роботі цілих міст, регіонів чи галузей. У результаті пожежної загрози спостерігається значне погіршення показників функціонування ОКІ. За результатами проведеного когнітивного моделювання найбільше зниження фіксується для концептів: C_5 – продукція ($-0,92$), що вказує на критичний вплив пожеж на виробничі процеси та загальну продуктивність системи; C_4 – персонал ($-0,82$), що свідчить про значну загрозу для життя та здоров'я персоналу, а також потенційні втрати серед робочої сили; C_1 – обладнання ($-0,67$), що відображає руйнування та пошкодження важливих технічних ресурсів і обладнання; C_2 – фінансування ($-0,54$); C_3 – ресурси ($-0,63$), що вказує на дефіцит ресурсів, необхідних для відновлення після пожежі. Спостерігається зниження концептів C_1^G – соціальні збитки на $0,52$ та C_2^G – матеріальні збитки на $0,57$.

Отже, рис. 2 відображає концептуальну модель для оцінювання негативного впливу найбільш значущих загроз на рівень безпеки функціонування ОКІ. Отримані результати мають явне прикладне значення для формування та впровадження адаптивних систем управління безпекою КІ на рівнях міста, регіону та держави. Запропонована модель може бути інтегрована до існуючої єдиної державної системи цивільного захисту, що дозволить підвищити ефективність функціональних підсистем (моніторинг, оповіщення, реагування) та територіальної організації заходів у режимах надзвичайного та воєнного станів. Інтеграція моделі сприятиме оперативнішому прийняттю рішень, кращій координації між суб'єктами реагування і зниженню ризиків для населення й критичної інфраструктури.

Висновки й перспективи подальших досліджень

Викладені результати дослідження особливостей застосування нечітких когнітивних карт для сценарного моделювання функціонування об'єктів критичної інфраструктури в умовах надзвичайних ситуацій воєнного характеру та визначення пріоритетів щодо запобігання, локалізації або мінімізації потенційних загроз – розроблено когнітивну модель функціонування об'єктів критичної інфраструктури в умовах впливу різного роду загроз, де головні компоненти системи функціонування об'єкту захисту розділені на три групи. Перша група – складові повсякденного функціонування враховують взаємозв'язки між показниками рівня фінансування, ресурсного забезпечення, станом технологічного обладнання, якістю продукції, а також чисельністю і кваліфікацією персоналу. Друга група – складові зовнішніх і внутрішніх загроз об'єднали різни види ризиків (фінансові, природні, техногенні, соціальні, застосування безпілотних літальних апаратів, застосування вогнепальної зброї, інформаційні, пожежні тощо) та враховують ступінь їх впливу на рівень нормального функціонування об'єкту. Третя група – наслідки від цих небезпек об'єднали соціальні, матеріальні та екологічні збитки. Проведено структурно-топологічний аналіз побудованої нечітких когнітивних карт та встановлено, що ця карта є адекватною для оцінювання впливу зовнішніх і внутрішніх загроз. Для запропонованої на рис. 2 когнітивної моделі визначено концепти, які мають найвищу структурну значимість. Зокрема, проаналізувавши значення складових побудованої нечітких когнітивних карт визначено, що в умовах уведення в державі правого режиму воєнного стану найвагомішими концептами досліджуваної системи загроз є загрози застосування безпілотних літальних апаратів, пожежні загрози та загрози застосування вогнепальної зброї.

Перспективами подальших досліджень є сценарне моделювання впливу результатів впровадження на об'єктів критичної інфраструктури системи акустичного моніторингу для виявленню та ідентифікації пожежних загроз, атак із застосуванням безпілотних літальних апаратів та терористичних дій із застосуванням вогнепальної зброї. Попередні результати проведених авторами експериментальних досліджень можливостей акустичного методу щодо ідентифікації джерел надзвичайних ситуацій воєнного характеру узагальнені у роботі [21].

Список бібліографічних посилань

1. Дослідження. Як на міграцію населення України вплинули російські обстріли в жовтні 2022–січні 2023 року. URL: https://www.oporaua.org/viyna/doslidzhennya-yak-na-migraciyu-naselennya-ukrayini-vplinuli-rosiys-ki-obstrili-v-zhovtni-2022-sichni-2023-roku-25359 (дата звернення: 05.09.2025). **2. Російські удари руйнують українську енергетику. Який масштаб втрат і що робити?** URL: https://www.radiosvoboda.org/a/ruynuvannya-ukrayinskoyi-enerhetyky-pid-chas-viyny/33237255.html (дата звернення: 05.09.2025). **3. Росія відновила удари по енергооб'єктах України.** URL: https://suspilne.media/1047395-rosia-vidnovila-udari-po-energoobektah-ukraini-galusenko/ (дата звернення: 05.09.2025). **4. Руйнування Каховської ГЕС – це не лише злочин проти енергетичної інфраструктури, а й масштабний екоцид.** URL: https://uhe.gov.ua/media_tsentr/novyny/ruynuvannya-kakhovskoyi-hes-tse-ne-lyshe-zlochyn-proty-enerhetychnoyi (дата звернення: 05.09.2025). **5. Річниця катастрофи на Каховській ГЕС: хронологія великої біди і що тепер із територією.** URL: https://glavcom.ua/country/society/richnitsja-katastrofi-na-kakhovskij-hes-jak-vidreahuvav-svit-jaki-naslidki-ta-shcho-zaraz-iz-teritorijeju-vodoskhovishcha-1003838.html (дата звернення: 05.09.2025). **6. Кулеба розповів про наслідки атак рф на порти, судна та зерносховища за останні три місяці.** URL: https://epravda.com.ua/news/2024/10/10/720438/ (дата звернення: 05.09.2025). **7. Атаки рф на українські порти: пошкоджено 300 об'єктів, постраждало 79 цивільних – Кулеба.** URL: https://latifundist.com/novosti/65760-ataki-rf-na-ukrayinski-porti-poshkodzheno-300-obyektiv-postrazhdalo-79-tsivilnih--kuleba (дата звернення: 05.09.2025). **8. Серпень 2023: Нічні атаки на порти та будівництво нових елеваторів.** URL: https://elevatorist.com/blog/read/865-pidsumki-serpnya-2023-ataki-na-porti-ta-budivnitstvo-novih-elevatoriv (дата звернення: 05.09.2025). **9. Кулеба: за останні три місяці сили рф здійснили майже 60 атак на порти, цивільні судна та зерносховища.** URL: https://www.radiosvoboda.org/a/news-ataky-rf-portova-infrastruktura-viyna/33154225.html (дата звернення: 05.09.2025). **10. Поранені 15 людей, є влучання по**

енергетичній інфраструктурі: Зеленський показав наслідки атаки рф. URL: https://rubryka.com/2025/07/16/poraneni-15-lyudej-ye-vluchannya-po-energetychnij-infrastrukturi-zelenskyj-pokazav-naslidky-ataky-rf/ (дата звернення: 05.09.2025). **11. Україна відновлює об'єкти критичної інфраструктури, незважаючи на російські атаки.** URL: https://www.pap.pl/ua/ukrainian/news/ukraina-vidnovlyue-obekti-kritichnoi-infrastrukturi-nezvazhayuchi-na-rosiyski-ataki (дата звернення: 05.09.2025). **12. Про національну безпеку України** : Закон України від 21.06.2018 № 2469-VIII. URL: http://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 05.09.2025). **13. Про критичну інфраструктуру** : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/main/1882-20#Text (дата звернення: 05.09.2025). **14. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури** : Постанова кабінету Міністрів України від 22.07.2022 № 821. URL: https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#Text (дата звернення: 05.09.2025). **15. Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони** : Рішення Ради національної безпеки і оборони України від 04.06.2021. Введено в дію Указом Президента України від 18.06.2021 № 260/2021. URL: https://zakon.rada.gov.ua/laws/show/n0039525-21#Text (дата звернення: 05.09.2025). **16. Рубан І. В., Тютюник В. В., Тютюник О. О.** Особливості створення системи підтримки прийняття антикризових рішень в умовах невизначеності вхідної інформації при надзвичайних ситуаціях. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2021. Вип. 1(40). С. 75–84. DOI: https://doi.org/10.33099/2311-7249/2021-40-1-75-84. **17. Тютюник В. В., Ященко О. А., Рубан І. В., Тютюник О. О.** Особливості функціонування системи ситуаційних центрів на різних стадіях розвитку надзвичайних ситуацій. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2022. Вип. 1(43). С. 41–52. DOI: https://doi.org/10.33099/2311-7249/2022-43-1-41-52.
18. Салієва О. В., Яремчук Ю. Є. Симпліціальний аналіз структури когнітивної моделі для дослідження захищеності об'єкта критичної інфраструктури. *Реєстрація, зберігання і обробка даних*. 2020. Т. 22. № 3. С. 68–75. DOI: https://doi.org/10.35681/1560-9189.2020.22.3.218974.
19. Євсєєв В. О. Можливі шляхи удосконалення захисту критичної інфраструктури України з урахуванням світового досвіду. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2016. № 4. С. 168–172. URL: http://nbuv.gov.ua/UJRN/ZKhUPS_2016_4_35 (дата звернення: 05.09.2025). **20. Брежнєв Є. В., Фесенко Г. В., Харченко В. С.** Методологічні засади оцінювання та забезпечення безпеки критичних інформаційних інфраструктури. *Радіоелектронні і комп'ютерні системи*. 2018. №4. С. 78–85. DOI: https://doi.org/10.32620/reks.2018.4.08. **21. Тютюник В. В., Усачов Д. В.** Удосконалення методу запобігання виникненню надзвичайних ситуацій місцевого рівня за результатами моніторингу акустичного простору. *Social Development and Security*. 2025. № 15(2), С. 153–164. DOI: 10.33445/sds.2025.15.2.12.

FEATURES OF THE APPLICATION OF FUZZY COGNITIVE MAPS FOR SCENARIO MODELLING OF THE FUNCTIONING OF CRITICAL INFRASTRUCTURE IN CONDITIONS OF MILITARY EMERGENCIES

TIUTIUNYK Vadym, Doctor of Technical Sciences, Professor, Simon Kuznets Kharkiv National University of Economics, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine, https://orcid.org/0000-0001-5394-6367

TIUTIUNYK Olha, Candidate of Technical Sciences, Associate Professor, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine, https://orcid.org/0000-0002-3330-8920

USACHOV Dmytro, Doctor of Philosophy, National University of Civil Defence of Ukraine, Kharkiv, Ukraine, https://orcid.org/0000-0002-1140-9798

Formulation of the problem in general. *The purpose of this article is to examine the features of using fuzzy cognitive maps for scenario modelling of critical infrastructure facility operations in the context of a military emergency.*

Research methods. *When writing the article, the method of cognitive (using fuzzy cognitive maps) modelling was applied, which makes it possible to assess the potential effectiveness of introducing measures to minimise risks and ensure the stability of critical infrastructure facilities, especially against threats that arise in the conditions of the introduction of a legal regime of martial law in the state. The proposed approach enabled the conduct of scenario modelling to assess the maximum negative impact of the most significant concepts of the threat system on the security of critical infrastructure.*

Literature review. *The procedure for making management decisions to ensure the proper level of security of critical infrastructure facilities in conditions of military emergencies is complicated by the fact that most studies only partially affect the aspects of protecting these facilities, since their attention is mainly focused either on the legal status of subjects of public relations, or on individual areas and conditions of their functioning. This raises the question that existing studies, mainly, tend to limit their scope of interest, not fully covering the aspects of security at critical infrastructure facilities. This requires the introduction of new methods of modelling the conditions of critical infrastructure functioning, and also emphasises the importance of further research in this area and the relevance of the chosen topic of the article.*

Research results. *A cognitive model of the functioning of critical infrastructure facilities under the influence of various threats has been developed, where the key components of the system are divided into three groups. The components of everyday functioning consider the relationships between indicators of the level of financing, resource provision, the state of technological equipment, product quality, as well as the number and qualifications of personnel. The components of external and internal threats combine different types of risks (financial, natural, man-made, social, the use of unmanned aerial vehicles, the use of firearms, information, fire, etc.) and take into account the degree of their impact on the level of normal functioning of the facility. The consequences of these dangers combine social, material and environmental losses.*

Research novelty. *The proposed method describes a novel approach to assessing the negative impact of the most significant threats on the security level of critical infrastructure facilities. The use of fuzzy cognitive maps is first applied in assessing the consequences of fire threats, attacks using unmanned aerial vehicles, and terrorist acts using firearms.*

Theoretical and practical significance. *The results obtained have practical significance for building adaptive critical infrastructure security management systems at the city, regional and state levels. The model can be integrated into the existing unified state civil protection system, increasing the efficiency of its functional and territorial subsystems in emergency and martial law regimes.*

Conclusion and future work. *The results obtained provide a scientific basis for conducting scenario modelling of the impact of implementing an acoustic monitoring system at a critical infrastructure facility to detect and identify fire threats, attacks using unmanned aerial vehicles, and terrorist acts using firearms.*

Keywords: *cognitive modelling, fuzzy cognitive maps, critical infrastructure facilities, fire threats, threats of drones, threats of firearms.*

References

1. Research. How russian shelling in October 2022 – January 2023 affected the migration of the Ukrainian population. [online], (2024). Available at: https://www.oporaua.org/viyna/doslidzhennya-yak-na-migraciyu-naselennya-ukrayini-vplinuli-rosiys-ki-obstrili-v-zhovtni-2022-sichni-2023-roku-25359 [Accessed : 05 September 2025]. **2. Russian strikes are destroying Ukraine's energy sector. What is the scale of the losses and what should be done?** [online], (2024). Available at: https://www.radiosvoboda.org/a/ruynuvannya-ukrayinskoyi-enerhetyky-pid-chas-viyny/33237255.html [Accessed : 05 September 2025]. **3. Russia has resumed strikes on Ukrainian energy facilities.** [online], (2025). Available at: https://suspilne.media/1047395-rosia-vidnovila-udari-po-energoobektah-ukraini-galusenko/ [Accessed : 05 September 2025]. **4. The destruction of the Kakhovka HPP is not only a crime against energy infrastructure, but also a large-scale ecocide.** [online], (2025). Available at: https://uhe.gov.ua/media_tsentr/novyny/ruynuvannya-kakhovskoyi-hes-tse-ne-lyshe-zlochyn-proty-enerhetychnoyi [Accessed : 05 September 2025]. **5. Anniversary of the disaster at the Kakhovka hydroelectric power station: chronology of the great disaster and what happens now to the territory.** [online], (2024). Available at: https://glavcom.ua/country/society/richnitsja-katastrofi-na-kakhovskij-hes-jak-vidreahuvav-svit-jaki-naslidki-ta-shcho-zaraz-iz-teritorijeju-vodoskhovishcha-1003838.html [Accessed : 05 September 2025]. **6. Kuleba spoke about the consequences of russian attacks on ports, ships and grain silos over the past three months.** [online], (2024). Available at: https://epravda.com.ua/news/2024/10/10/720438/ [Accessed : 05 September 2025]. **7. Russian attacks on Ukrainian ports: 300 facilities damaged, 79 civilians injured – Kuleba.** [online], (2024). Available at: https://latifundist.com/novosti/65760-ataki-rf-na-ukrayinski-porti-poshkodzheno-300-obyektiv-postrazhdalo-79-tsivilnih--kuleba [Accessed : 05 September 2025]. **8. August 2023: Night attacks on ports and construction of new elevators.** [online], (2023). Available at: https://elevatorist.com/blog/read/865-pidsumki-serpnya-2023-ataki-na-porti-ta-budivnitstvo-novih-elevatoriv [Accessed : 05 September 2025]. **9. Kuleba: Over the past three months, Russian forces have carried out almost 60 attacks on ports, civilian vessels and grain silos.** [online], (2024). Available at: https://www.radiosvoboda.org/a/news-ataky-rf-portova-infrastruktura-viyna/33154225.html [Accessed : 05 September 2025]. **10. 15 people injured, energy infrastructure hit: Zelenskyy shows consequences of russian attack.** [online], (2025). Available at: https://rubryka.com/2025/07/16/poraneni-15-lyudej-ye-vluchannya-po-energetychnij-infrastrukturi-zelenskyj-pokazav-naslidky-ataky-rf/ [Accessed : 05 September 2025]. **11. Ukraine restores critical infrastructure despite russian attacks.** [online], (2024). Available at: https://www.pap.pl/ua/ukrainian/news/ukraina-vidnovlyue-obekti-kritichnoi-infrastrukturi-nezvazhayuchi-na-rosiyski-ataki [Accessed : 05 September 2025]. **12. On National Security of Ukraine** [online], (2018). Zakon Ukrainy #2469-VIII, 21 June. Available at: http://zakon.rada.gov.ua/laws/show/2469-19 [Accessed : 05 September 2025]. **13. On critical infrastructure** [online], (2021). Zakon Ukrainy #1882-IX, 16 November. Available at: https://zakon.rada.gov.ua/laws/main/1882-20#Text [Accessed : 05 September 2025]. **14. On approval of the Procedure for monitoring the security level of critical infrastructure facilities** [online], (2022). Resolution of the Cabinet of Ministers of Ukraine dated #821, 22 July. Available at: https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#Text [Accessed : 05 September 2025]. **15. Regarding the improvement of the network of situational centers and the digital transformation of the sphere of national security and defense** [online], (2021). Decision of the National Security and Defense Council of Ukraine, 06 April. Enacted by Decree of the President of Ukraine #260/2021 dated 18 June. Available at: https://zakon.rada.gov.ua/laws/show/n0039525-21#Text [Accessed : 05 September 2025]. **16. Ruban, I. V., Tiutiunyk, V. V., Tiutiunyk, O. O.** (2021). Peculiarities of creating a support system for making anti-crisis decisions in conditions of uncertainty of input information in emergency situations. *Modern Information Technologies in the Sphere of Security and Defence*. 1(40), 75–84. DOI: https://doi.org/10.33099/2311-7249/2021-40-1-75-84.
17. Tiutiunyk, V. V., Yashchenko, O. A., Ruban, I. V., Tiutiunyk, O.O. (2022). Peculiarities of the functioning of the system of situational centers at different stages of the development of emergency situations. *Modern Information Technologies in the Sphere of Security and Defence*. 1(43), 41–52. DOI: https://doi.org/10.33099/2311-7249/2022-43-1-41-52.
18. Salieva, O. V., Yaremchuk, Y. E. (2020). Simplistic analysis of the structure of a cognitive model for studying the security of a critical infrastructure object. *Registration, storage and data processing*. 22, 3, 68–75. DOI: https://doi.org/10.35681/1560-9189.2020.22.3.218974.
19. Yevseyev, V. O. (2016). Possible ways to improve the protection of the critical infrastructure of Ukraine, taking into account the world experience. *Collection of scientific works of the Kharkiv National University of the Air Force*. 4, 168–172. [online] Available at: http://nbuv.gov.ua/UJRN/ZKhUPS_2016_4_35 [Accessed : 05 September 2025]. **20. Brezhnev, E. V., Fesenko, G. V., Kharchenko, V. S.** (2018). Methodological principles for assessing and ensuring the security of critical information infrastructure. *Radioelectronic and computer systems*. 4, 78–85. DOI: https://doi.org/10.32620/reks.2018.4.08.
21. Tiutiunyk, V. V., Usachov, D. V. (2025). Improving the Method of Preventing Local Emergencies Based on the Results of Acoustic Space Monitoring. *Social Development and Security*. 15(2), 153–164. DOI: 10.33445/sds.2025.15.2.12.

Рукопис надійшов до редакції *10.09.2025*
Рукопис прийнято до друку після рецензування *19.11.2025*
Дата публікації *30.12.2025*