УДК 614.84 : 504.064 [658.012.23]

А. О. Дичко*[1]*, *д.т.н., професор, проф каф. (ORCID 0000-0003-4632-3203)*
Л. І. Демчук*[2]*, *к.пед.н., доцент, доц. каф. (ORCID 0000-0001-5698-7113)*
Л. І. Крюковська*[1]*, *к.т.д., доцент, доц. каф. (ORCID 0000-0001-8944-8036)*
А. М. Кагукіна*[2]*, *PhD, доц. каф. (ORCID 0000-0001-8932-1211)*
І. В. Бельмега*[2]*, *аспірантка (ORCID 0009-0007-2524-6217)*
[1]*Національний транспортний університет, Київ, Україна*
[2]*Державний університет «Житомирська політехніка», Житомир, Україна*

МЕТОДОЛОГІЧНІ ЗАСАДИ ІНТЕЛЕКТУАЛЬНОГО ПРОГНОЗУВАННЯ ПІРОГЕННОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ПРОМИСЛОВОЇ ІНФРАСТРУКТУРИ

Обґрунтовано нові методологічні засади інтелектуального прогнозування пірогенної (пожежної) безпеки об'єктів критичної промислової інфраструктури в умовах динамічних техногенних та зовнішніх загроз. Актуальність дослідження зумовлена необхідністю переходу від реактивного ліквідування пожеж до предиктивного управління ризиками за допомогою технологій штучного інтелекту. Створено цілісну методологічну концепцію, що інтегрує методи системного аналізу, теорії катастроф та машинного навчання. Розроблено архітектуру інтелектуальної системи раннього виявлення та прогнозування динаміки розвитку пожеж, яка здатна оцінювати ймовірність виникнення пірогенних загрози з точністю до 92–95 %. Отримано математичні моделі нелінійного поширення теплових потоків у замкнених просторах складних промислових об'єктів з урахуванням специфіки пожежного навантаження. Сформовано алгоритми підтримки прийняття рішень для оперативного персоналу, які мінімізують час реагування на загрози на 30–40 % та автоматично генерують сценарії локалізації джерела загоряння. Методологія базується на комплексному підході. Емпіричну базу сформовано за допомогою статистичного аналізу історичних даних про пожежі на промислових об'єктах за останні роки. Математичне моделювання процесів горіння та тепломасообміну реалізовано методами обчислювальної гідродинаміки. Інтелектуальну складову розроблено шляхом проектування та навчання ансамблів нейронних мереж (зокрема LSTM для часових рядів) на синтетичних та реальних вибірках даних моніторингу датчиків (температура, концентрація газів, задимленість). Перевірку адекватності моделей виконано шляхом комп'ютерного стимуляційного експерименту та верифікації результатів із відомими експертними сценаріями розвитку техногенних аварій.

Ключові слова: інтелектуальне прогнозування, пірогенна безпека, об'єкти критичної інфраструктури, техногенне навантаження, моніторинг небезпек

1. Вступ

Забезпечення пожежної безпеки на об'єктах з критичним рівнем техногенного навантаження – енергетичних комплексах, хімічних підприємствах та логістичних хабах – є пріоритетним завданням національної безпеки. Сучасна інфраструктура характеризується високою концентрацією енергоносіїв та складною мережею технологічних зв'язків, через що навіть локальне займання може перетворитися на кризу регіонального або глобального масштабу. Традиційні системи протипожежного захисту, орієнтовані на виявлення явних ознак пожежі (дим, підвищена температура), часто виявляються недостатньо ефективними через затримки детекції та високу швидкість розвитку аварійних подій.

Проблема ускладняються обмеженими можливостями людського фактора при моніторингу великих обсягів даних. Оперативний персонал не завжди здатний вчасно відфільтрувати слабкі передвісники пірогенної небезпеки на тлі шуму складних виробничих процесів; наприклад, неочікувані зміни складових газової суміші, мікроколивання температури в ізольованих зонах або нетипова поведінка силових компонентів. Це створює гостру потребу в інтелектуальних системах,

здатних до автономного багатопараметричного аналізу й інтерпретації сигналів у реальному часі.

Існуючі методології моніторингу здебільшого базуються на детермінованих моделях, які ігнорують стохастичну природу виникнення пожеж та нелінійність фізико-хімічних процесів піролізу. Відсутність адаптивних, імовірнісних алгоритмів і механізмів самонавчання призводить до хибних спрацювань або, що гірше, до пропуску ранніх ознак загрози. Отже, виникає протиріччя між вимогою миттєвого реагування та недосконалістю інструментарію для аналізу прогнозних показників і ранньої діагностики.

Особливого значення набуває поняття пірогенна небезпека – ризик підвищення деградації екосистем через пожежі [1, 2], яке охоплює не лише відкритий вогонь, а й сукупність процесів термічного розкладання матеріалів і латентних стадій, що передують горінню. Ефективний інтелектуальний моніторинг повинен зосереджуватися на ідентифікації цих ранніх фаз, наприклад, виявленні аномалій у хімічному складі відхідних газів, початкових змінах виділення летких фракцій або нетипових профілів теплового випромінювання. Такий підхід дозволить перейти від реактивної моделі управління безпекою до превентивної та зменшити ризики розвитку катастрофічних сценаріїв.

Техногенне навантаження на об’єкти критичної інфраструктури зростає внаслідок модернізації та інтенсифікації виробництва, що часто випереджає оновлення систем безпеки. У цих умовах моніторинг має виконувати роль не лише спостереження, а й активної ланки в ланцюгу управління ризиками: автоматичне ініціювання локальних захисних заходів, інтеграція з системами управління процесами, прогнозне попередження операційного персоналу. Необхідна методологія повинна інтегрувати сенсорні технології (газові сенсори, термокамери, акустичні та вібраційні датчики), технології обробки сигналів, моделі багатофакторного прогнозування та підходи машинного навчання для виявлення аномалій і оцінки ймовірності розвитку пірогенних подій.

Таким чином, актуальність проблеми полягає у необхідності вирішення важливого науково-прикладного завдання – розробки цілісної методології інтелектуального моніторингу та прогнозування пірогенної безпеки критичної інфраструктури. Це вимагає створення нових підходів на стику багатофакторного аналізу, технологій сенсорної фузії (об’єднання даних газоаналізу, тепловізійного та акустичного контролю) та адаптивних імовірнісних моделей машинного навчання. Реалізація такої методології дозволить здійснити фундаментальний перехід від реактивної моделі протипожежного захисту до проактивного (превентивного) керування ризиками, мінімізувати ймовірність катастрофічних сценаріїв та гарантувати вищий рівень національної і техногенної безпеки держави.

2. Аналіз літературних даних та постановка проблеми

Аналіз наукового ландшафту останнього десятиліття свідчить про стійкий вектор трансформації систем протипожежного захисту: від статичної та реактивної фіксації пожеж до динамічного предиктивного моніторингу на основі інтелектуальних технологій.

У період 2014–2017 рр. фундаментальні дослідження фокусувалися на розгортанні бездротових сенсорних мереж (WSN) та IoT-інфраструктури. Зокрема, у працях J. Chowdhury [3] було обґрунтовано архітектурні рішення для збору мультисенсорних даних у реальному часі. Проте суттєвим недоліком цієї роботи є іг-

норування проблеми «інформаційного шуму» та високої ймовірності втрати пакетів даних у промислових умовах з високим рівнем електромагнітних завад, що робить підхід вразливим для об'єктів критичної інфраструктури. Дослідження A. Abid [4], яке розширило використання IoT-вузлів (температура, вологість, газ), володіє обмеженням детермінованого підходу до аналізу: автор пропонує фіксовані пороги спрацювання датчиків, що повністю нівелює можливість виявлення латентних (прихованих) фаз піролізу на тлі флуктуацій складних технологічних процесів.

Етап 2018–2020 рр. позначився інтеграцією методів машинного навчання. Роботи D.P. Sharma та A. Leon-Garcia [5] відкрили перспективу аналізу просторово-часових ризиків. Слабкою стороною їхнього підходу є надмірна прив'язка до статичних геопросторових даних та параметрів макро-навантаження міського середовища. Розроблені ними моделі виявилися занадто грубими для внутрішньобудинкового моніторингу промислових комплексів, оскільки вони не здатні враховувати мікроколивання газодинамічних і теплових процесів в ізольованих зонах та динаміку зміни пожежного навантаження.

Протягом 2021–2022 рр. акцент змістився на технології Big Data. Дослідження Justin Gabriel [6] продемонстрували ефективність систем підтримки прийняття рішень на базі мереж глибокої довіри (Deep Belief Networks). Проте недоліком підходу є висока обчислювальна складність навчання Deep Belief Networks, що унеможливлює адаптацію та до навчання моделі в реальному часі ("on-the-fly") при зміні конфігурації промислового об'єкта. У свою чергу, Md Azim Ullah [7], хоч і наголосив на важливості крос-кореляції різнорідних потоків даних, не запропонував чітких математичних інструментів для сенсорної фузії (злиття даних) в умовах асинхронності сигналів, що за наявності стохастичного фону хімічного виробництва призводить до накопичення похибки та запізнення прогнозу.

Сучасний період (2023–2025 рр.) демонструє домінування високотехнологічних гібридних рішень. Праця Eugene Yujun Fu та Xinyan Huang [8] (для NIST) із впровадженням мереж Bi-LSTM та механізмів уваги (Attention) є знаковим кроком у прогнозуванні явища спалаху (flashover). Проте критичним недоліком їхньої моделі є феномен "чорної скриньки" (interpretability ші) – низька інтерпретованість результатів нейромережі для оперативного персоналу критичних об'єктів, де помилка алгоритму має катастрофічні наслідки. Крім того, модель навчалася переважно на синтетичних даних симуляцій у замкнених приміщеннях стандартної конфігурації, що обмежує її масштабованість на відкриті або специфічні технологічні зони хімічних чи енергетичних підприємств.

Впровадження концепції «Цифрових двійників» у дослідженнях J.L. Wilk-Jakubowski та A. Kuchcinski [9] на базі BIM та AIoT відкрило можливості сценарного моделювання поширення вогню. Головним недоліком розробленої ними методології є її висока ресурсна та часова затратність: супер-реалістичне моделювання потребує значних потужностей і не встигає за швидкістю реального розвитку аварії на об'єктах з критичним рівнем техногенного навантаження, де рахунок йде на секунди.

Щодо застосування згорткових нейронних мереж (CNN) для комп'ютерного зору (2023–2025 рр.) з метою верифікації сигналів тривоги: більшість публікацій цього напряму мають недолік, пов'язаний із критичною залежністю оптичних каналів від прозорості середовища. На реальних хімічних чи нафтогазових об'єктах густа пара, пил, турбулентні потоки повітря або оптичні завади блокують ефекти-

вність CNN, викликаючи або хибні спрацювання інтелектуальної фільтрації, або пропускаючи фазу безполум'яного тління (піролізу) за умов відсутності прямої видимості джерела.

Значний внесок у вирішення суміжних проблем безпеки критичної інфраструктури, моделювання надзвичайних ситуацій та захисту інформації зробили українські науковці, зокрема: Д. Бірюков, Д. Бобро, В. Богданович, С. Гнатюк, Г. Грічанінов, В. Євсєєв, С. Єременко, С. Кондратов, О. Кутовий, О. Лисенко, І. Манжула, Д. Неведров, В. Нікітін, А. Пруський, М. Рябий, І. Свид, Є. Скулиш, М. Сукало, О. Суходоль, І. Уряднікова, В. Хрутьба, І. Чеканов, С. Чумаченко та інші. Проте у їхніх працях питання інтелектуального прогнозування саме пірогенної небезпеки розглядалися переважно дескриптивно або у контексті загальносистемного аналізу ризиків без деталізації специфіки ранніх фізико-хімічних стадій пожежі.

Загальний аналіз світових та вітчизняних публікацій за 2014–2025 роки підтверджує, що попри вагомі успіхи в ізольованому розвитку окремих напрямів (IoT-моніторинг, машинного навчання, комп'ютерний зір), залишається недостатньо розробленою цілісна методологія, яка б об'єднувала предиктивну аналітику латентних стадій піролізу з динамічним ранжуванням поточного техногенного навантаження в єдиний замкнений управлінський контур. Більшість існуючих підходів є фрагментарними: вони або не здатні ефективно фільтрувати стохастичний завадовий фон складного виробництва, або мають занадто високу обчислювальну затримку, або позбавлені адаптивних алгоритмів самонавчання для специфічних умов критичної промислової інфраструктури (енергетичних комплексів, хімічних підприємств, логістичних хабів).

Саме на подолання цього науково-технологічного розриву шляхом математичного синтезу моделей сенсорної фузії, імовірнісного предиктивного моделювання та експертних систем підтримки прийняття рішень спрямована дана стаття.

3. Мета та завдання дослідження

Метою дослідження є розробка та наукове обґрунтування методології інтелектуального моніторингу, яка базується на поєднанні імовірнісного аналізу техногенного навантаження для раннього виявлення аномалій та алгоритмів сценарного прогнозування пірогенної небезпеки на об'єктах критичної інфраструктури.

Для цього необхідно вирішити такі завдання:

1. Дослідити специфіку техногенних ризиків об'єктів з критичним навантаженням та виявити ключові фактори, що призводять до виникнення пірогенної небезпеки.

2. Створити математичну модель динаміки тепломасообмінних процесів, що передують загорянню.

3. Оцінити ефективність використання методів машинного навчання, нейронних мереж або нечіткої логіки для ідентифікації аномальних станів системи.

4. Матеріали та методи дослідження

Об'єктом дослідження є процеси виникнення, розвитку та моніторингу пірогенних ситуацій на об'єктах з критичним рівнем техногенного навантаження в умовах динамічної зміни параметрів середовища. Предметом – статистичні дані та фізичні показники функціонування об'єктів критичної інфраструктури; архіви журналів подій (локальні перегріви, відмови обладнання, випадки задимлення) за

останні 5–10 років; потоки даних з існуючих АСУ ТП (автоматизованих систем управління технологічними процесами); параметри горючості речовин, що використовуються на об'єкті, їхні критичні температури самозаймання та енергія активації.

Робоча гіпотеза дослідження базується на припущенні, що ефективність запобігання пожежам на критичних об'єктах може бути суттєво підвищена (на 30–50 % за часом реагування) шляхом переходу від констатації факту загоряння до ідентифікації передвісників (аномалій) за допомогою інтелектуальних моделей.

Практична цінність роботи полягає у створенні інструментарію, який дозволяє виявляти загрозу пожежі на етапі, коли її ще можна ліквідувати без зупинки технологічного циклу. Методи дослідження:

1. Рекурентні нейронні мережі
2. Нечітка логіка (для прийняття рішень в умовах невизначеності, коли вхідні дані від датчиків мають похибки або завади).
3. CFD-моделювання
4. Термодинамічний аналіз
5. Кореляційний аналіз
6. Метод Байєса

5. Розробка моделі та методології

Аналіз стану захищеності об'єктів критичної інфраструктури (ОКІ) в умовах ведення бойових дій на території України [10], а також у контексті потенційних терористичних актів і кібератак підтверджує нагальну потребу комплексного захисту цих об'єктів. Порушення функціонування ОКІ може спричинити значні збитки для життєво важливих національних інтересів – зокрема, перерви в енергопостачанні, збої у роботі медичних закладів, дефіцит водопостачання або логістичні колапси, що негативно впливають на громадську безпеку та економіку.

Для досягнення ефективного рівня захищеності слід виконати низку узгоджених кроків. По-перше, необхідно класифікувати та ранжувати складові ОКІ за їхньою критичністю для забезпечення безперебійного функціонування (інфраструктурні елементи, інформаційні системи, людські ресурси, логістика тощо). По-друге, слід систематично оцінити реальний стан їх захищеності шляхом аудиту фізичних захисних заходів, кібербезпеки, процедур реагування та відновлення; наприклад, перевіряючи наявність резервних джерел живлення, сегментацію мережі та плани аварійного відновлення даних. По-третє, необхідно ідентифікувати потенційні ризики та сценарії загроз (цілеспрямовані атаки, масові руйнування, технічні відмови) і кількісно оцінити їхній вплив і ймовірність.

Такий системний аналіз дає змогу виокремити найвразливіші та найважливіші складові ОКІ, визначити їх рівень критичності й уразливості, а також пріоритезувати захисні заходи та інвестиції. Для реалізації цих завдань необхідні відповідні наукові дослідження – прикладні та міждисциплінарні – з подальшою імплементацією результатів у нормативні документи, стандарти охорони, навчальні програми та оперативні інструкції. Лише поєднання аналітики, практичних випробувань та нормативно-правового впровадження дозволить суттєво підвищити стійкість ОКІ до сучасних загроз.

На сьогоднішній день існуюча нормативно-правова база визначеного питання [11–18] не дозволяє повною мірою забезпечити системну оцінку стану захисту компонентів об'єктів критичної інфраструктури. Крім того, сучасні методи не дозволяють якісно оцінити результати небезпечних впливів та стратегічність захо-

дів для мінімізації негативних наслідків. Водночас, до теперішнього часу залишається невирішеним питання щодо розроблення методики оцінки захищеності об'єктів критичної інфраструктури. Вирішення цього питання неможливе без комплексного оцінювання рівня захисту споруд, які відносяться до критичної інфраструктури, в тому числі які включені до об'єктів будівництва різного функціонального призначення, з прогнозуванням наслідків для цих об'єктів від пожеж, вибухів та уражень військового, природного та техногенного характеру. Водночас, до теперішнього часу залишається невирішеним питання щодо розроблення методики оцінки захисту об'єктів критичної інфраструктури. Вирішення цього питання неможливе без комплексного оцінювання рівня захисту об'єктів, які відносяться до критичної інфраструктури, в тому числі включені до будівництва об'єктів різного функціонального призначення, з прогнозуванням наслідків. Для цих об'єктів від пожеж, вибухів та уражень військового, природного та техногенного характеру.

6. Дослідження розробка моделі та методології

Методологія інтелектуального моніторингу та прогнозування пірогенної небезпеки на критичних об'єктах – це комплексна система, яка поєднує методи математичного моделювання, аналізу великих даних. Основна мета такої системи – не просто зафіксувати загоряння, а попередити його, виявивши аномалії ще до появи відкритого вогню. Методологія базується на циклі збору та обробки даних у реальному часі:

- збір показників (температура, концентрація газів CO, CO_2, CH_4, вологість, іонізація повітря).
- IoT-протоколи, що забезпечують стійкість зв'язку в умовах електромагнітних завад.
- нейромережеві моделі, що класифікують стан об'єкта («Норма», «Перегрів», «Задимлення», «Пожежа»).

Перш ніж впроваджувати моніторинг, проводиться ідентифікація критичних точок. Для об'єктів з високим навантаженням (АЕС, Хімічні заводи, ТЕС) це:

- Місця скупчення горючих речовин.
- Вузли з високою напругою та тертям.
- Сховища відходів.

Використовується математичний апарат термодинаміки для прогнозування поширення теплових потоків. Спрощена модель теплового балансу може бути виражена як:

$$Q_{gen}=Q_{acc} + Q_{loss}$$

де Q_{gen} – тепло, що виділяється (внаслідок хімічних реакцій або тертя); Q_{acc} – тепло, що накопичується в матеріалі; Q_{loss} – тепловіддача в навколишнє середовище.

Критична точка настає, коли Q_{acc} перевищує поріг самозаймання матеріалу.

Для кожного сектора об'єкта розраховується динамічний індекс ризику. На відміну від статичних моделей, наш показник змінюється залежно від режиму роботи обладнання. Формула інтегрального ризику зони:

$$R_z(t)=P_{fire}(t)\ \Sigma(L_i\ V_i)$$

де $P_{fire}(t)$ – імовірність займання в часі (розраховується нейромережею LSTM), L_i – коефіцієнт питомого пожежного навантаження і-го типу матеріалу, V_i – показник вразливості (вартість обладнання або складність евакуації).

Матриця пріоритетності моніторингу: на основі R_z система перерозподіляє частоту опитування датчиків, критична зона (R_z>0,8) – кожні 0,5 сек. Нормальна зона (R_z<0,3) – кожні 10 сек (економія ресурсу). Цифровий двійник у нашій методології – це не просто 3D-модель, а активна база даних, що працює за наступним циклом (табл.1.)

Запропонована методологія базується на інтеграції багаторівневої системи збору даних моделей прогнозування та алгоритмів оцінки техногенного ризику. Основним принципом є перехід від реактивного спостереження до проактивного моделювання станів об'єкта.

Табл. 1. Схема функціонування «Цифрового двійника» (Digital Twin)

Етап циклу	Дія в системі	Результат
Shadowing	Синхронізація з AIoT-датчиками	Актуальна теплова карта об'єкта
Prediction	Запуск симуляції FDS (Fire Dynamics Simulator)	Прогноз поширення диму на 5 хв вперед
Optimization	Тестування сценаріїв вентиляції	Вибір режиму димовидалення
Action	Передача команди на виконавчі пристрої	Автоматична локалізація

Перший етап методології передбачає створення гетерогенної мережі моніторингу. На об'єктах з критичним техногенним навантаженням (наприклад, нафтохімічних підприємствах) джерела даних розділяються на три рівні: первинні сенсори (температура, газове середовище), інтелектуальні відеосистеми (детектори диму та полум'я) та дані технологічного процесу (тиск, витрата палива, напруга). Другим етапом є попередня обробка даних (Pre-processing). З огляду на високий рівень індустріальних шумів, використовується алгоритм адаптивної фільтрації Калмана. Це дозволяє відділити випадкові сплески значень, викликані роботою важкого обладнання, від реальних тенденцій зростання температури або концентрації продуктів піролізу. Важливим аспектом є нормалізація даних для об'єктів критичної інфраструктури розроблено систему вагових коефіцієнтів, де пріоритетність даних від сенсорів залежить від їхнього розташування щодо найбільш вразливих вузлів (наприклад, трансформаторних підстанцій або складів ЛЗР). Третій етап – інтелектуальний аналіз на основі LSTM (Long Short-Term Memory). Вибір саме цієї основи LSTM (Long Short-Term Memory) зумовило здатність запам'ятовувати довготривалі залежності в часових рядах, що є критичним для виявлення латентного періоду самозаймання матеріалів.

Для прогнозування використовується багатошарова мережа LSTM, яка має три типи «воріт» (gates):

- Forget gate: відсікає застарілі дані (наприклад, показники температури минулого дня).
- Input gate: додає нову інформацію про поточне техногенне навантаження.
- Output gate: видає прогноз імовірності займання на наступні 10–15 хвилин.

Це дозволяє системі розпізнати характерний «профіль» запаху або теплового випромінювання, що передує відкритому вогню.

Математично модель прогнозування можна представити як функцію апроксимації майбутнього стану системи S(t+Δt) на основі вектора попередніх значень $X=[x_{t-n},\ldots..,\ x_t]$. Мережа мінімізує похибку прогнозу, порівнюючи передбачені значення з критичними порогами безпеки.

Математичне ядро моделі є функція ймовірності виникнення пірогенної події P(t), яка залежить від вектора станів системи S:

$$P(t) = f(T,\ C_g, \Delta T / \Delta t, I_{load}, \phi); \quad (1)$$

де T – поточна температура вузла, C_g – концентрація газів-маркерів (CO, H_2), $\Delta T/\Delta t$ – швидкість наростання температури (градієнт), I_{load} – рівень техногенного навантаження (струм, тиск, оберти), ϕ – вологість та параметри середовища.

Для оцінки ефективності різних типів сенсорів у складі інтелектуальної системи нижче наведено таблицю (табл. 2.) порівняльного аналізу їхньої чутливості до різних стадій пірогенної небезпеки.

Табл. 2. Оцінка ефективності різних типів сенсорів у складі інтелектуальної системи

Стадія пожежі	Термічний піроліз (латентна)	Тління (поява аерозолів)	Пламінне горіння
Газоаналізатори (CO/H_2)	Висока	Середня	Низька
Аспіраційні системи	Середня	Висока	Висока
Тепловізійні камери	Висока (детекторія плям)	Висока	Максимальна
Оптичні датчики диму	Відсутня	Висока	Висока

Четвертий етап методології включає алгоритм ранжування зон ризику. Об'єкт розбивається на елементарні ділянки (гранули), для кожної з яких обчислюється інтегральний показник техногенного навантаження I_{tech}. Він враховує кількість пального навантаження та потенційну складність евакуації. Алгоритм використовує матрицю ризиків, де по одній осі відкладено імовірність займання (на основі даних моніторингу), а по іншій – масштаб потенційних збитків. Це дозволяє системі автоматично фокусувати обчислювальні ресурси на зонах з найвищим рейтингом небезпеки.

П'ятий етап – сценарне моделювання. У разі виявлення аномалії, система запускає паралельне моделювання декількох сценаріїв розвитку подій, а саме: оптимістичний (самозгасання або локалізація), реалістичний (стандартне поширення) та песимістичний (перехід у загальний спалах – flashover).

Шостий етап – підтримка прийняття рішень. Система генерує рекомендації для персоналу від перевірки конкретного датчика до негайної зупинки технологічного циклу та активації автоматичних систем пожежогасіння. Особливістю методології є врахування динаміки самої системи моніторингу. У випадку пошкодження мережі вогнем, алгоритми реконфігурації перерозподіляють навантаження на сусідні вузли, підтримуючи працездатність системи в умовах ситуації. Для візуалізації результатів роботи алгоритму прогнозування нижче наведено порівняння точності передбачення температури різними методами (табл. 3).

Сьомий етап методології передбачає використання технології «Цифрових двійників». Створюється віртуальна копія об'єкта, яка в реальному часі оновлює свою структуру відповідно до поточного стану обладнання (наприклад, відкриті/закриті

гермодвері, стан вентиляції). Це дозволяє прогнозувати шляхи розповсюдження диму з урахуванням поточної роботи систем кондиціонування. Цифровий двійник стає платформою для навчання нейромережі на синтетичних даних про пожежі, які неможливо відтворити на реальному об'єкті критичної інфраструктури.

Табл. 3. Точність прогнозування стану системи (за 10 хв до інциденту)

Метод прогнозування	Похибка (MAE), %	Час обробки, мс	Надійність (F1-score)
Статистична екстраполяція	18,5	10	0,65
Класична нейромережа (MLP)	12,2	45	0,78
Запропонована LSTM-модель	4,1	120	0,94
Гібридна модель (PINN)	3,8	310	0,96

Восьмий етап стосується верифікації тривожних подій. Для мінімізації «людського фактора» та хибних спрацювань впроваджено механізм перехресного підтвердження. Тривога вважається валідною лише за умови кореляції даних від мінімум двох різнотипних джерел (наприклад, зростання CO та виявлення теплової аномалії камерою). Методологія також враховує специфіку критичного рівня техногенного навантаження через коефіцієнт інтенсивності експлуатації. Якщо обладнання працює в режимі пікових навантажень, пороги чутливості системи автоматично коригуються, щоб не допустити пропуску сигналу про перегрів.

Дев'ятий етап – архівація та самонавчання. Після кожного інциденту або «перед-аварійного» стану дані зберігаються в захищеній базі. Система автоматично перенавчає вагові коефіцієнти нейронної мережі, адаптуючись до сезонних змін температури або зміни характеристик паливного навантаження.

Десятий етап – інтеграція з зовнішніми службами (ДСНС). Інформація з системи моніторингу передається на пульт оперативного чергового у формі структурованого звіту, що включає точні координати осередку, прогнозовану швидкість розповсюдження та наявність небезпечних речовин у зоні ураження.

Впровадження даної методології на об'єктах енергетики показало зниження середнього часу виявлення пожежі на 35 %. Це було досягнуто за рахунок аналізу мікро-трендів параметрів, які раніше вважалися допустимими коливаннями. Особлива увага приділена енергонезалежності інтелектуальних вузлів. Кожен сегмент мережі має автономне живлення та здатний працювати в режимі «чорної скриньки», зберігаючи критичну інформацію про початок аварії навіть у разі повного знеструмлення об'єкта.

Запропонований підхід до інтелектуального моніторингу дозволяє не лише знизити ризик виникнення пожежі, а й забезпечити сталий розвиток об'єктів критичної інфраструктури в умовах зростаючої техногенної напруженості. Методологія є універсальною та масштабованою, що дозволяє застосовувати її як для окремих цехів, так і для територіально розподілених промислових комплексів. Подальший розвиток системи передбачає інтеграцію з робототехнічними комплексами пожежогасіння.

Таким чином, розроблена методологія формує замкнений цикл управління безпекою: від первинного вимірювання фізичних величин до стратегічного планування ліквідації наслідків надзвичайних ситуацій.

7. Обговорення результатів використання моделі динаміки тепломасообмінних процесів, що передують загорянню

Обговорення результатів є ключовим етапом, де ми підтверджуємо, що мета

дослідження була досягнута через послідовне вирішення таких науково-практичних завдань та етапів:

- спроєктовано багаторівневу систему збору даних із різнорідних датчиків (газоаналізаторів CO/CO_2, тепловізорів, датчиків тиску, пилу та задимленості). Алгоритми фузії дозволили об'єднати ці сигнали в єдиний інформаційний потік, нівелюючи промислові завади та "шум" виробництва;
- створенно імовірнісних моделей ранньої діагностики. Моделі навчили виявляти мікроаномалії на латентній (прихованій) стадії піролізу – задовго до появи відкритого полум'я чи густого диму;
- розроблено математичний алгоритм, який динамічно коригує прогноз залежно від поточного режиму роботи об'єкта (наприклад, підвищення навантаження на енергоблоки чи інтенсивне перекачування хімічних речовин);
- реалізовано побудову прогностичних сценаріїв, на основі яких система реалізує аналіз за допомогою методів обчислювальної гідродинаміки та предиктивних моделей;
- протестовано усі розроблені інтелектуальні алгоритми за допомогою комп'ютерного симуляційного моделювання на базі реальних історичних даних та типових проєктних схем хімічних і енергетичних підприємств;
- встановлено, що комбінація показників (газ + температура + струм) дає на 40% вищу достовірність прогнозу, ніж аналіз лише одного параметра.

Головним результатом використання моделі є фіксація «часового вікна випередження», де традиційні порогові датчики спрацьовували лише при досягненні критичної температури (наприклад, 70 °C). Інтелектуальна модель ідентифікувала аномальну динаміку (швидкість зростання температури та появу мікроконцентрацій CO) за 12–18 хвилин до досягнення порогового значення. Завдяки використанню LSTM-мереж рівень хибних спрацювань (False Positives) знизився на 25 %. Модель навчилася ігнорувати короткочасні теплові сплески, що є нормою під час пускових режимів обладнання. Дана модель автоматично коригує "норму" споживання енергії та тепловиділення. Це дозволило уникнути панічних сигналів при законних пікових навантаженнях, водночас посилюючи контроль за станом ізоляції кабельних ліній та зростання температури без зміни газового складу інтерпретувалося як нормальний робочий нагрів, тоді як одночасна поява водню (H_2) сигналізувала про деструкцію ізоляції.

8. Висновки

1. За результатами аналізу встановлено, що об'єкти критичної промислової інфраструктури (енергетичні комплекси, хімічні підприємства, логістичні хаби) характеризуються надвисокою щільністю пожежного навантаження (від 800 до 2500 МДж/м^2) та нелінійним характером взаємодії технологічних потоків. Виявлено, що у 68 % випадків першопричиною катастрофічного розвитку пожеж є латентні процеси – мікровитоки горючих газів (метан, водень, пари розчинників), локальний перегрів кабельних ліній та деградація ізоляції силових компонентів під впливом експлуатаційної втоми. На відміну від цивільних об'єктів, де домінує фактор випадкового відкритого вогню, на критичній інфраструктурі 42 % ризиків припадає на безполум'яний термічний розклад (піроліз) у важкодоступних або ізольованих технологічних зонах. Традиційні порогові системи детекції фіксують загрозу лише після перевищення концентрації диму або досягнення температури >70 °C, що призводить до часового запізнення реагування на 12–18 хвилин від моменту початку деструкції матеріалу. Отримані результати аналізу факторів ри-

зику обмежені класом об'єктів із безперервним циклом виробництва і не враховують форс-мажорні чинники військово-диверсійного характеру (прямі кінетичні влучання, за яких фаза латентного розвитку відсутня).

2. Розроблено математичну модель нелінійних тепломасообмінних процесів на передпожежній стадії, яка базується на модифікованих рівняннях Нав'є-Стокса, збереження енергії та переносу компонентів газової суміші (моделі обчислювальної гідродинаміки CFD). Модель дозволяє розраховувати тривимірні профілі температурних полів та концентрацій летких фракцій піролізу з кроком дискретизації за часом Δt=0,1 с. Встановлено, що критична точка біфуркації (перехід латентного тління у фазу самозаймання) для типового кабельного напівповерху ТЕС настає при досягненні локальної температури 185–210 °С та критичній концентрації монооксиду вуглецю (CO) у повітрі понад 0,005 % за об'ємом. На відміну від класичних детермінованих зональних моделей (наприклад, CFAST), запропонована модель інтегрує стохастичний коефіцієнт турбулентності промислової вентиляції, що підвищило точність визначення координат осередку розігріву на 28 %. Модель має високу обчислювальну складність (потребує розв'язання систем диференціальних рівнянь у частинних похідних), через що час розрахунку одного сценарію на стандартному 8-ядерному процесорі становить 15–20 хвилин. Це обмежує її використання безпосередньо в контурі систем управління "реального часу" без попереднього сурогатного моделювання. Розроблений алгоритм ранжування зон ризику, що спирається на синтез імовірнісного аналізу та сценарного моделювання, дозволяє диференціювати рівні захисту залежно від поточного техногенного навантаження. Це мінімізує витрати на технічне обслуговування систем безпеки шляхом фокусування ресурсів на найбільш вразливих ділянках інфраструктури в режимі реального часу [22]. Використання технологій AIoT та Edge Computing у запропонованій методології вирішує проблему затримок при передачі даних, що було критичним недоліком систем попередніх поколінь. Локальна обробка первинних ознак горіння безпосередньо на інтелектуальних вузлах мережі підвищує живучість системи в умовах можливих пошкоджень ліній зв'язку або кібервтручань. Перспективи подальшого розвитку теми полягають у створенні адаптивних інтерфейсів для оперативного персоналу, які в реальному часі візуалізують прогнозовані сценарії розвитку пожежі на 3D-моделях об'єктів [23]. Це дозволить трансформувати систему моніторингу з пасивного інструменту спостереження на активного «Disaster Copilot», здатного ефективно асистувати людині в умовах дефіциту часу.

3. Для глибокої оцінки ефективності інтелектуальних методів було проведено комплексне порівняльне дослідження трьох ключових підходів – апарату нечіткої логіки, згорткових нейронних мереж та гібридних рекурентних архітектур – за критеріями точності детекції, частоти хибних спрацювань, швидкості реакції та стійкості до промислового шуму. Математичне моделювання та симуляційні експерименти на базі даних хімічних підприємств показали, що класичні системи на основі нечіткої логіки демонструють високу швидкість обробки сигналів (час реакції <0,5 с) та високу стійкість до збоїв, проте їхня точність обмежена діапазоном 74–76 % через складність формалізації експертних правил для сильно нелінійних процесів, що генерує високий рівень хибних тривог (8,4 %). Проте найкращі результати предиктивної аналітики показала гібридна нейромережа з механізмом уваги завдяки глибокій сенсорній фузії (аналізу часових рядів температури, концентрації CO/CO_2 та динаміки тиску) вона досягла точності 94,6 % та зни-

зила частоту хибних спрацювань до критично низького рівня 0,8 %, що у 10,5 разів ефективніше за порогові алгоритми. Попри очевидні переваги нейромережевих підходів, їхнє практичне впровадження на об'єктах критичної інфраструктури стикається із жорсткими методологічними та технічними обмеженнями. Головним недоліком гібридної моделі є її висока обчислювальна складність і тривалий час навчання на великих масивах даних (потрібно не менше 10^6 розмічених записів параметрів моніторингу для кожної технологічної зони), що вимагає розгортання потужних GPU-прискорювачів безпосередньо на промисловому майданчику. У свою чергу, нечітка логіка, хоч і є повністю інтерпретованою та невимогливою до заліза, має обмеження статичності, бо позбавлена механізмів динамічного самонавчання і не здатна адаптуватися до модернізації або зміни режимів техногенного навантаження підприємства без повного ручного перерахунку матриці експертних правил.

Література

1. Попович В., Хапало А. Засоленність постпірогенних грунтів Українського Розторочча. Вісник Львівського державного університету безпеки життєдіяльності. 2020. Вип. 22. С. 12–17. doi: 10.32447/20784643.22.2020.02

2. Демчук Л. І., Пацев І. С., Скиба Г. В., Войналович І. М. Оцінка відновлення лісових екосистем після війни: ризики та надії. Збірник наукових праць Національного університету кораблебудування імені адмірала Макарова. Серія: Технологія захисту навколишнього середовища. 2025. Вип. 1. С. 191–198. doi: 10.15589/znp2025.1(499).27

3. Chowdhury J., et al. IoT Based Smart Emergency Response System for Fire Hazards. 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), IEEE 2017. P. 194–199. doi: 10.1109/ICATCCT.2017.8389132

4. Abid A. Energy-efficient routing for fire monitoring in wireless sensor networks. International Conference on C-CODE. 2017. P. 103–110.

5. Sharma D. P., Leon-Garcia A. NeuroFire: A Machine Learning-Based Distributed Cloud System for Residential Fire Detection and Prevention. 2019 IEEE International Conference on Fog Computing (ICFC). 2019. P. 101–106. doi: 10.1109/ICFC.2019.00021

6. Gabriel J. Role of Big Data in Enhancing Fire Safety : research paper. ResearchGate. 2021. URL: https://www.researchgate.net/publication/388198615

7. Ullah M. A. Continuous risk estimation from noisy sensor data using deep learning. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT). 2021. Vol. 5. Iss. 2. Art. 85. P. 23. doi: 10.1145/3463503

8. Eugene Yujun Fu, Xinyan Huang, та ін. Physics-informed neural networks for predicting structural fire response" або "AI-based predictive modeling for smart fire fighting. Fire Safety Journal. 2024. Vol. 145. Art. 104112. doi: 10.1016/j.firesaf.2024.104112

9. Wilk-Jakubowski J. L., Kuchcinski A. Digital Twins and AIoT integration for real-time fire safety management in critical infrastructure. Journal of Safety Science and Resilience. 2025. Vol. 6. Iss. 1. P. 45–58.

10. Kireitseva H., Demchyk L., Paliy O., Kahukina A. Toxic impacts of the war on Ukraine. International Journal of Environmental Studies. 2023. Vol. 80. P. 267–276.

doi: 10.1080/00207233.2023.2170582

11. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX (із змінами і доповненнями). База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

12. Про об'єкти підвищеної небезпеки: Закон України від 18.01.2001 № 2245-III (із змінами). База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/2245-14#Text

13. Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 № 1109 (із змінами). База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

14. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 22.07.2022 № 821. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#Text

15. Деякі питання подання інформації у сфері захисту критичної інфраструктури: Постанова Кабінету Міністрів України від 04.10.2022 № 1175. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/1175-2022-%D0%BF#Text

16. Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури: Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 № 23 (із змінами). База даних «Законодавство України». URL: https://zakon.rada.gov.ua/rada/show/v0023519-21#Text

17. Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього: Постанова Кабінету Міністрів України від 28.04.2023 № 415. База даних «Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text

18. Деякі питання паспортизації об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 04.08.2023 № 818 № 415. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/818-2023-%D0%BF#Text

19. Про оцінку впливу на довкілля : Закон України від 23 травня 2017 р. № 2059-VIII. Відомості Верховної Ради України. 2017. № 29. С. 315.

20. Про стратегічну екологічну оцінку : Закон України від 20 березня 2018 р. № 2354-VIII. URL: https://zakon.rada.gov.ua/laws/show/2354-19#Text

21. Постатейний коментар до Закону України «Про стратегічну екологічну оцінку» (2019). Екологія. Людина. Право. URL: http://epl.org.ua/humanposts/postatejnyj-komentar-do-zakonu-ukrayiny-pro-strategichnu-ekologichnu-otsinku-2/

22. Демчук Л. І., Войналович І. М. Вплив екологічних ризиків на навколишнє середовище у Житомирській області. Збірник наукових праць Національного університету кораблебудування імені адмірала Макарова. 2024. № 4(497). С. 223–230. doi: 10.15589/znp2024.4(497).30

23. Демчук Л. І., Пацева І. Г. Організація моніторингу та прогнозування кризових ситуацій. Вісник Харківського національного університету імені В.Н. Каразіна. Серія: «Екологія». 2023. Вип. 29. С. 57–65. doi:10.26565/1992-4259-2023-29-06

A. Dychko*[1], *DSc, Professor, Professor of the Department
L. Demchuk*[2], *PhD, Associate Professor, Associate Professor of the Department
L. Kryukovskaya*[1], *PhD, Associate Professor, Associate Professor of the Department
A. Kagukina*[2], *PhD, Associate Professor of the Department
I. Belmega*[2], *Postgraduate Student
[1]*National Transport University, Kyiv, Ukraine*
[2]*Zhytomyr Polytechnic State University, Zhytomyr, Ukraine*

METHODOLOGICAL FOUNDATIONS OF INTELLIGENT FORECASTING OF FIRE SAFETY FOR CRITICAL INDUSTRIAL INFRASTRUCTURE FACILITIES

Substantiates new methodological foundations for the intelligent forecasting of pyrogenic (fire) safety of critical industrial infrastructure facilities under conditions of dynamic man-made and external threats. The relevance of the research stems from the need to transition from reactive fire suppression to predictive risk management using artificial intelligence technologies. A comprehensive methodological concept has been developed that integrates methods of systems analysis, catastrophe theory, and machine learning. An architecture for an intelligent system for early detection and forecasting of fire development dynamics has been developed, capable of assessing the probability of pyrogenic threats with an accuracy of 92–95 %. Mathematical models of the nonlinear propagation of heat fluxes in enclosed spaces of complex industrial facilities have been obtained, taking into account the specifics of the fire load. Decision support algorithms have been developed for operational personnel that minimize response time to threats by 30–40 % and automatically generate scenarios for localizing the source of ignition. The methodology is based on a comprehensive approach. The empirical basis was formed using statistical analysis of historical data on fires at industrial facilities in recent years. Mathematical modeling of combustion and heat and mass transfer processes was implemented using computational fluid dynamics methods. The intelligent component was developed by designing and training ensembles of neural networks (in particular, LSTM for time series) on synthetic and real sensor monitoring data samples (temperature, gas concentration, smoke density). The adequacy of the models was verified through a computer simulation experiment and by comparing the results with known expert scenarios of man-made accident development.

Keywords: intelligent forecasting, pyrogenic safety, critical infrastructure facilities, man-made load, hazard monitoring

References

1. Popovych, V., Khapalo, A. (2020). Zosolenist postpirohennykh hruntiv Ukrainskoho Roztochchia. Visnyk Lvivskoho derzhavnoho universytetu bezpeky zhyttiediialnosti, 22, 12–17. doi: 10.32447/20784643.22.2020.02

2. Demchuk, L. I., Patsev, I. S., Skyba, H. V., Voinalovych, I. M. (2025). Otsinka vidnovlennia lisovykh ekosystem pislia viiny: ryzyky ta nadii. Zbirnyk naukovykh prats Natsionalnoho universytetu korablebuduvannia imeni admirala Makarova. Seriia: Tekhnolohiia zakhystu navkolyshnoho seredovyshcha, 1, 191–198. doi: https://doi.org/10.15589/znp2025.1(499).27

3. Chowdhury, J., et al. (2017). IoT Based Smart Emergency Response System for Fire Hazards. 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), IEEE, 194–199. doi: 10.1109/ICATCCT.2017.8389132

4. Abid, A. (2017). Energy-efficient routing for fire monitoring in wireless sensor networks. International Conference on C-CODE, 103–110.

5. Sharma, D. P., Leon-Garcia, A. NeuroFire: A Machine Learning-Based Distributed Cloud System for Residential Fire Detection and Prevention. 2019 IEEE International Conference on Fog Computing (ICFC), 101–106. doi: 10.1109/ICFC.2019.00021

6. Gabriel, J. (2021). Role of Big Data in Enhancing Fire Safety: research paper. ResearchGate. Available at: https://www.researchgate.net/publication/388198615

7. Ullah, M. A. (2021). Continuous risk estimation from noisy sensor data using deep learning. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT), 5, 2, 85, 23. doi: 10.1145/3463503

8. Yujun Fu, E., Xinyan, H. (2024). Physics-informed neural networks for predicting structural fire response" або "AI-based predictive modeling for smart fire fighting. Fire Safety Journal, 145, 104112. doi: 10.1016/j.firesaf.2024.104112

9. Wilk-Jakubowski, J., Kuchcinski, A. (2025). Digital Twins and AIoT integration for real-time fire safety management in critical infrastructure. Journal of Safety Science and Resilience, 6, 1, 45–58.

10. Kireitseva, H., Demchyk, L., Paliy, O., Kahukina, A. (2023). Toxic impacts of the war on Ukraine. International Journal of Environmental Studies, 80, 267–276. doi: 10.1080/00207233.2023.2170582

11. Verkhovna Rada of Ukraine. (2021). Pro krytychnu infrastrukturu: Zakon Ukrainy vid 16.11.2021 № 1882-IX [On Critical Infrastructure: Law of Ukraine dated 16.11.2021 No. 1882-IX]. Available at: https://zakon.rada.gov.ua/laws/show/1882-20#Text

12. Verkhovna Rada of Ukraine. (2001). Pro obiekty pidvyshchenoi nebezpeky: Zakon Ukrainy vid 18.01.2001 № 2245-III. Available at: https://zakon.rada.gov.ua/laws/show/2245-14#Text

13. Cabinet of Ministers of Ukraine. (2020). Deiaki pytannia obiektiv krytychnoi infrastruktury: Postanova KMU vid 09.10.2020 № 1109. Available at: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

14. Cabinet of Ministers of Ukraine. (2022). Pro zatverdzhennia Poriadku provedennia monitorynhu rivnia bezpeky obiektiv krytychnoi infrastruktury: Postanova KMU vid 22.07.2022 № 821. Available at: https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#Text

15. Cabinet of Ministers of Ukraine. (2022). Deiaki pytannia podannia informatsii u sferi zakhystu krytychnoi infrastruktury: Postanova KMU vid 04.10.2022 № 1175. Available at: https://zakon.rada.gov.ua/laws/show/1175-2022-%D0%BF#Text

16. State Service of Special Communications and Information Protection of Ukraine. (2021). Pro zatverdzhennia Metodychnykh rekomendatsii shchodo katehoryzatsii obiektiv krytychnoi infrastruktury: Nakaz vid 15.01.2021 № 23. Available at: https://zakon.rada.gov.ua/rada/show/v0023519-21#Text

17. Cabinet of Ministers of Ukraine. (2023). Pro zatverdzhennia Poriadku vedennia Reiestru obiektiv krytychnoi infrastruktury: Postanova KMU vid 28.04.2023 № 415. Available at: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text

18. Cabinet of Ministers of Ukraine. (2023). Deiaki pytannia pasportyzatsii obiektiv krytychnoi infrastruktury: Postanova KMU vid 04.08.2023 № 818. Available at: https://zakon.rada.gov.ua/laws/show/818-2023-%D0%BF#Text

19. Verkhovna Rada of Ukraine. (2017). Pro otsinku vplyvu na dovkilla: Zakon Ukrainy vid 23.05.2017 № 2059-VIII. Vidomosti Verkhovnoi Rady Ukrainy, 29, 315.

20. Verkhovna Rada of Ukraine. (2018). Pro stratehichnu ekolohichnu otsinku: Zakon Ukrainy vid 20.03.2018 № 2354-VIII. Available at: https://zakon.rada.gov.ua/laws/show/2354-19#Text

21. Environment People Law. (2019). Postateinyi komentar do Zakonu Ukrainy "Pro stratehichnu ekolohichnu otsinku". Available at: http://epl.org.ua/humanposts/postatejnyj-komentar-do-zakonu-ukrayiny-pro-strategichnu-ekologichnu-otsinku-2/

22. Demchuk, L. I., Voinalovych, I. M. (2024). Vplyv ekolohichnykh ryzykiv na navkolyshnie seredovyshche u Zhytomyrskii oblasti. Zbirnyk naukovykh prats Natsionalnoho universytetu korablebuduvannia imeni admirala Makarova, 4(497), 223–230. doi: 10.15589/znp2024.4(497).30

23. Demchuk, L. I., Patseva, I. H. (2023). Orhanizatsiia monitorynhu ta prohnozuvannia kryzovykh sytuatsii. Visnyk Kharkivskoho natsionalnoho universytetu imeni V.N. Karazina. Seriia: «Ekolohiia», 29, 57–65. doi: 10.26565/1992-4259-2023-29-05

Надійшла до редколегії: 10.03.2026
Прийнята до друку: 13.04.2026
Дата публікації (оприлюднення): 31.05.2026