КОНЦЕПЦІЯ ЗАХИСТУ ОБ'ЄКТІВ ПІДВИЩЕНОЇ НЕБЕЗПЕКИ ВІД ТЕХНОГЕННИХ ТА ВОЄННИХ ЗАГРОЗ НА ОСНОВІ ЦИФРОВОЇ ТІНІ ТА ЦИФРОВОГО ФАНТОМУ

CONCEPT OF PROTECTING HIGH-RISK FACILITIES FROM TECHNOGENIC AND MILITARY THREATS BASED ON A DIGITAL SHADOW AND A DIGITAL PHANTOM

Савченко Олександр Віталійович, кандидат технічних наук, старший науковий співробітник, Національний університет цивільного захисту України, savchenko@nuczu.edu.ua, https://orcid.org/0000-0002-1305-7415

Стацюк Анна Андріївна, здобувач вищої освіти, Національний університет цивільного захисту України, statsiuk.anna_2023b@nuczu.edu.ua, https://orcid.org/0009-0001-2629-1083

Гарькава Неля Олександрівна, здобувач вищої освіти, Національний університет цивільного захисту України, harkava.nelia_2023b@nuczu.edu.ua, https://orcid.org/0009-0001-9565-4036

https://doi.org/10.32447/bcet.2026.25

Анотація. У розділі обґрунтовано концепцію дворівневого захисту об'єктів підвищеної небезпеки (ОПН) в умовах збройного конфлікту. Концепція поєднує технологію цифрової тіні для превентивного моніторингу технологічних ризиків і технологію цифрового фантому для активного управління сигнатурою об'єкта з метою відводу засобів повітряного нападу. Обидва компоненти функціонують на єдиній сенсорній платформі за принципом подвійного використання інфраструктури. Систему побудовано за модульним масштабованим принципом, придатним для різних типів і розмірів ОПН. Концепцію верифіковано на двох типах ОПН — нафтосховищі та трансформаторній підстанції. Наведено порівняльний економічний аналіз альтернативних підходів.

Ключові слова: цифрова тінь, цифровий фантом, об'єкти підвищеної небезпеки, інженерний захист, мультиспектральна імітація, цивільний захист, збройний конфлікт, техногенна безпека.

Abstract. This chapter substantiates a concept of two-level protection for hazardous industrial facilities (HIF) under armed conflict conditions. The concept combines digital shadow technology for preventive monitoring of technological risks with digital phantom technology for active signature management aimed at deflecting aerial attack means. Both components operate on a unified sensor platform implementing a dual-use infrastructure principle. The system is built on a modular scalable architecture, suitable for HIFs of various types and sizes. The concept is verified using two HIF types — an oil storage facility and a power substation. A comparative economic analysis of alternative approaches is provided.

Keywords: digital shadow, digital phantom, hazardous industrial facility, engineering protection, multispectral simulation, civil protection, armed conflict, industrial safety.

1. ВСТУП

З лютого 2022 року об'єкти підвищеної небезпеки (ОПН) України — нафтосховища, трансформаторні підстанції, хімічні підприємства, водоочисні станції — опинились під одночасним

впливом двох незалежних класів загроз. Перший клас — внутрішній: умови воєнного часу порушують штатний режим експлуатації, спричиняючи деградацію обладнання, накопичення прихованих дефектів і підвищення ймовірності технологічної аварії. Другий клас — зовнішній: ті самі об'єкти є пріоритетними цілями для засобів повітряного нападу (ЗПН) противника. Ураження ОПН будь-якого типу спричиняє хімічні та екологічні наслідки регіонального масштабу.

1) внутрішньовиробнича (операційна) деградація: обумовлена форс-мажорними обставинами воєнного часу, що призводять до системного порушення планово-профілактичних ремонтів, нестабільності енергетичних мереж та кадрового голоду;

2) зовнішня мілітарна загроза: спричинена систематичним застосуванням засобів повітряного нападу (ЗПН) по критичній інфраструктурі, де ОПН виступають першочерговими цілями.

Синергетичний ефект ураження хоча б одного з елементів структури ОПН створює передумови для масштабного екологічного колапсу та вторинного хімічного ураження навколишнього природного середовища у межах цілих географічних регіонів.

Кількісний вимір загрози підтверджується даними міжнародних організацій. За даними МЕА, лише за перші 27 місяців повномасштабного вторгнення пошкоджено або знищено 18 великих ТЕЦ, 815 котелень та 354 км теплових мереж; прямі збитки від ударів по тепловій інфраструктурі перевищили 2,4 млрд дол. США[1]. Нафтосховища стали найбільш часто атакованою категорією ОПН: з 2022 року пошкоджено або знищено щонайменше 32 великі нафтобази з прямими втратами 266 млн дол.[2]. Лише внаслідок пожеж на нафтосховищах в атмосферне повітря потрапило понад 499 тисяч тонн токсичних речовин[3]. Загальний екологічний збиток перевищує 127 млрд дол., зафіксовано понад 9 000 випадків екологічних руйнувань[2]. За даними SIPRI, лише з лютого по грудень 2022 зафіксовано понад 1 100 інцидентів пошкодження промислових об'єктів та критичної інфраструктури[4].

Масштаб ударів за об’єктами енергетичної інфраструктури є безпрецедентним: у жовтні 2022 — квітні 2023 р. фіксувалося понад 7 подій пошкодження об’єктів генерації та передачі електроенергії на тиждень; 8 травня 2024 р. за один день уражено майже 12 об’єктів[5]. Наведені дані підтверджують, що ОПН в умовах збройного конфлікту потребують якісно нових підходів до захисту — таких, що одночасно охоплюють технологічний моніторинг і зниження зовнішньої вразливості, тоді як чинні нормативні та проектні рішення орієнтовані лише на один із цих аспектів.

Наявні підходи до захисту ОПН орієнтовано або на мирний час — технологічний нагляд, планові перевірки — або на суто воєнні умови у вигляді пасивних фізичних споруд. Жоден із них не забезпечує одночасного захисту від обох складових загрози. Технології цифрових двійників і

[1] International Energy Agency (IEA), 'Ukraine's Energy Security and the Coming Winter: Ukraine's Energy System Under Attack' (IEA, Paris 2024) <https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter> accessed 18 May 2026.

[2] Human Rights Research, 'Counting the Cost: The Environmental Toll on Ukraine from the Russian Invasion' (2025) <https://www.humanrightsresearch.org/post/counting-the-cost-the-environmental-toll-on-ukraine-from-the-russian-invasion> accessed 18 May 2026.

[3] Міністерство захисту довкілля та природних ресурсів України, 'Масштаби шкоди, завданої довкіллю України від агресії рф, вражають весь світ' (Кабінет Міністрів України, Київ 2022) <https://www.kmu.gov.ua/news/mindovkillya-masshtabi-shkodi-zavdanoyi-dovkillyu-ukrayini-vid-agresiyi-rf-vrazhayut-ves-svit> accessed 18 May 2026.

[4] Stockholm International Peace Research Institute (SIPRI), 'Environmental Accountability, Justice and Reconstruction in the Russian War on Ukraine' (SIPRI, Stockholm 2023) <https://www.sipri.org/commentary/topical-backgrounder/2023/environmental-accountability-justice-and-reconstruction-russian-war-ukraine> accessed 18 May 2026.

[5] United Nations Security Council, 'Escalating Attacks on Ukraine's Civilian, Energy Infrastructure Making Humanitarian Aid Delivery Even More Dangerous, Relief Chief Tells Security Council' (UN, New York 2024) <https://press.un.org/en/2024/sc15695.doc.htm> accessed 18 May 2026.

тіней — *Digital Shadow* та *Digital Twin* — широко застосовуються в промисловому моніторингу, однак у контексті активного захисту сигнатури стаціонарних цивільних ОПН залишаються практично нерозробленими.

Мета розділу — обґрунтування концепції дворівневого захисту ОПН, що поєднує технологію цифрової тіні для превентивного управління внутрішніми ризиками та технологію цифрового фантому для активного зниження зовнішньої вразливості об'єкта. Концепція реалізується на єдиній масштабованій модульній платформі за принципом подвійного використання сенсорної інфраструктури.

2. МЕТОДОЛОГІЯ

2.1. Класифікація загроз ОПН в умовах збройного конфлікту

Загрози ОПН в умовах збройного конфлікту класифікуються за джерелом і механізмом виникнення. Внутрішні загрози зумовлені деградацією технічного стану обладнання: зниження якості та регулярності технічного обслуговування, перевантаження через зміну режимів роботи, розвиток корозійних процесів, кадровий дефіцит кваліфікованого персоналу. Реалізація внутрішніх загроз призводить до аварій, пожеж та розливів небезпечних речовин без будь-якого зовнішнього впливу.

Зовнішні загрози зумовлені прицільними ударами ЗПН по об'єктах інфраструктури. Сучасні ЗПН оснащені комбінованими системами наведення — радіолокаційними, тепловими та оптико-електронними головками самонаведення (ГСН), — що уможливлює ідентифікацію цілі за сукупністю фізичних сигнатур навіть за наявності засобів радіоелектронної боротьби (РЕБ)[6]. Ключова вразливість стаціонарних ОПН — стабільна та добре відома теплова і радіолокаційна сигнатура. Теплова сигнатура об’єкта характеризується спектральною яскравістю у діапазоні 3–5 мкм та 8–12 мкм і є функцією температури поверхні, її емісійної здатності та геометрії об’єкта. Радіолокаційна сигнатура визначається ефективною поверхнею розсіювання (ЕПР), що залежить від форми об’єкта, матеріалу облицювання та кута опромінення. Для промислових резервуарів та трансформаторного обладнання ці параметри практично постійні у часі, що суттєво спрощує алгоритми цілевказівки ГСН.

Обидві категорії загроз є незалежними, але взаємопов’язаними: технічна деградація підвищує ризик вторинної аварії після удару; удар по обладнанню в незадовільному технічному стані призводить до значно тяжчих наслідків. Зазначений феномен відповідає концепції каскадного відмовного ефекту (*cascade failure effect*): первинне ушкодження одного елемента системи ініціює послідовний ланцюг відмов суміжних підсистем, наслідки яких сумарно перевищують шкоду від безпосереднього впливу. Концепція дворівневого захисту спрямована на одночасне зниження ризику від обох категорій загроз за допомогою єдиної технологічної платформи.

Кількісна характеристика каскадного відмовного ефекту виражається через коефіцієнт підсилення збитку (damage amplification ratio, DAR) — відношення сукупних наслідків каскадної відмови до збитків від первинного впливу. Для пожеж на нафтосховищах, що виникають унаслідок попереднього пошкодження від ЗПН, значення DAR становить від 2,8 до 7,4: ураження одного резервуара провокує займання сусідніх через теплове випромінювання та розлив пального, кратно збільшуючи масштаб хімічного забруднення атмосфери. Аналогічна закономірність спостерігається для підстанцій: руйнування одного силового трансформатора спричиняє каскадне перевантаження та відмову суміжних вузлів енергосистеми, що підтверджується масовими відключеннями

[6] P Trzaskawka, 'System for Critical Infrastructure Security Based on Multispectral Observation-Detection Module' (2013) 8896 Proceedings of SPIE <https://doi.org/10.1117/12.2028740>.

електропостачання після цілеспрямованих ударів у 2022–2024 рр. Це обумовлює методологічний принцип концепції: захист від каскадних відмов ефективніший, якщо спрямований на превенцію першої відмови в ланцюгу, а не на ліквідацію наслідків її розповсюдження.

2.2. Огляд існуючих підходів та їх обмеження

Традиційні методи захисту ОПН поділяються на дві групи. Перша — системи моніторингу та управління ризиками мирного часу: планові огляди, інструментальна діагностика, ручне внесення даних до систем обліку. Принципове обмеження — дискретний характер контролю: між перевірками можуть розвиватися критичні дефекти, тоді як в умовах воєнного часу регулярність перевірок суттєво знижується.

Друга група — пасивні засоби фізичного захисту від ЗПН. У монографії[7] систематизовано підходи до інженерного захисту ключових елементів (КЕ) ОПН від засобів повітряного нападу та проведено порівняльну оцінку їх ефективності. Розглянуто весь спектр конструктивних рішень — від ґрунтових валів та габіонових насипів до просторових захисних каркасів та підвісних ланцюгових екранів. Для кожного варіанта визначено ступінь захисту від прямого ураження, зниження ефективної поверхні розсіювання та захист від уламкового впливу. Зазначена монографія є єдиним комплексним вітчизняним дослідженням у цій галузі і є базою для порівняльного аналізу в цьому розділі.

В роботі[8] систематизовано вісім основних варіантів конструктивних рішень для типового КЕ ОПН з габаритами 20×20 м та висотою 3 м; порівняльний аналіз наведено в таблиці 1.

Таблиця 1

Порівняльна характеристика засобів пасивного захисту КЕ ОПН (об'єкт 20×20 м, висота 3 м)

Варіант захисту	Орієнтовна вартість	Час розгортання
Перешкоди з контейнерів/вагонів	від 1,2 млн грн	3–5 діб
Збірні перешкоди з біг-бегів / габіонів	від 0,6 млн грн	2–4 доби
Укриття типу «Саркофаг»	від 4,5 млн грн	10–14 діб
Підвісні ланцюгові екрани	від 0,8 млн грн	5–7 діб
Металеві опори з геотекстильною сіткою	від 0,4 млн грн	2–3 доби
Просторові захисні каркаси з сітками	від 0,7 млн грн	4–6 діб
Кутові відбивачі	від 0,15 млн грн	1–2 доби
Захисні перешкоди з ґрунтових валів	від 0,9 млн грн	5–8 діб

Джерело: складено авторами на основі[9]

Фундаментальне обмеження всіх наведених варіантів — пасивний характер: вони можуть знизити ступінь фізичного ураження при влучанні, але не усувають головної вразливості. Радіолокаційна та

[7] А С Білик та ін, Основи інженерного захисту об'єктів критичної інфраструктури енергетичної галузі України від засобів повітряного нападу противника: монографія (Київ 2023) 232.

[8] О В Савченко, Н О Гарькава, А А Стацюк, 'Активна мультиспектральна імітація як метод інженерного захисту об'єктів енергетики від засобів повітряного нападу' [2026] Матеріали ІІ Міжнар. наук.-практ. конф. «Цивільний захист в умовах війни» (ЛДУБЖД, Львів 2026) 6.

[9] О В Савченко, Н О Гарькава, А А Стацюк, 'Активна мультиспектральна імітація як метод інженерного захисту об'єктів енергетики від засобів повітряного нападу' [2026] Матеріали ІІ Міжнар. наук.-практ. конф. «Цивільний захист в умовах війни» (ЛДУБЖД, Львів 2026) 6.

теплова сигнатура КЕ залишається видимою для мультиспектральних ГСН навіть за наявності периметральних перешкод. Жоден із варіантів не вирішує проблеми внутрішнього технологічного ризику. Наявні підходи є взаємно ізольованими: кожен усуває лише одну складову загрози.

2.3. Концепція єдиної сенсорної платформи подвійного призначення

Методологічну основу концепції становить єдина сенсорна інфраструктура для одночасного вирішення двох задач: превентивного моніторингу технологічного стану ОПН та формування актуального сигнатурного профілю об'єкта для управління активними імітаційними модулями.

Мережа сенсорів, розміщена на ОПН, безперервно збирає дані про параметри роботи обладнання (температура, тиск, рівень рідини, вібрація, електромагнітне поле). Ці дані одночасно надходять до двох функціональних блоків: блоку аналізу технологічного стану (цифрова тінь) та блоку формування сигнатурного профілю (основа для цифрового фантому). Перший виявляє відхилення від норми і генерує попередження про зростання техногенного ризику. Другий забезпечує активні імітаційні модулі актуальними параметрами сигнатури об'єкта в режимі реального часу. При отриманні сигналу повітряної тривоги імітаційні модулі автоматично активуються, відтворюючи сигнатуру реального об'єкта на безпечній відстані від нього.

Принципова перевага такої архітектури — інфраструктурна економія: сенсорна мережа, необхідна для цифрової тіні, є тією ж мережею, що забезпечує роботу цифрового фантому. Капіталовкладення в один компонент автоматично підвищують ефективність іншого. Одна інфраструктура захищає від двох незалежних класів загроз, знижуючи сукупні витрати на розгортання системи.

Дослідження виконано із застосуванням комплексу взаємодоповнювальних методів. Концептуальне моделювання використано для формування архітектури єдиної сенсорної платформи та опису взаємодії між її функціональними блоками. Порівняльний аналіз проводився за чотирма критеріями: повнота охоплення загроз (внутрішня / зовнішня), адаптивність до масштабу об'єкта, час розгортання активного захисту та питомі витрати на одиницю захищеного периметра. Оцінювались вісім варіантів пасивного захисту та три конфігурації цифрового моніторингу / імітації (таблиці 1–3). Системний підхід застосовано для виявлення функціональних зв'язків між компонентами платформи та обґрунтування принципу подвійного використання інфраструктури. Техніко-економічний аналіз виконано методом порівняння витрат за сценаріями: роздільне розгортання двох систем проти єдиної платформи подвійного призначення.

Сенсорна інфраструктура платформи подвійного призначення ґрунтується на стандартизованих промислових протоколах передачі даних: Modbus TCP/IP для провідного з'єднання та LoRaWAN (Long Range Wide Area Network) для бездротового зв'язку в умовах пошкодження кабельних комунікацій. Протокол LoRaWAN забезпечує дальність передачі до 15 км в режимі прямої видимості та до 5 км у міській забудові при споживанні потужності менше 100 мВт — що відповідає умовам роботи від автономного акумуляторного живлення. Архітектура мережі передбачає ієрархічну структуру: польові сенсорні вузли (рівень 1) — концентратори даних (рівень 2) — центральний сервер обробки та прийняття рішень (рівень 3). Ієрархічна організація забезпечує часткову функціональність системи навіть при виведенні з ладу окремих вузлів мережі, що є критично важливим в умовах активних бойових дій.

3. РЕЗУЛЬТАТИ

3.1. Модульно-масштабована архітектура системи

Пропонована система будується за модульним принципом — конфігурація масштабується залежно від типу та розміру ОПН. Базовий модуль включає: сенсорний вузол (датчики температури, тиску, електромагнітного поля), блок обробки та передачі даних, імітаційний модуль з нагрівальними елементами, кутовими відбивачами та автономним блоком управління.

Масштабування здійснюється нарощуванням кількості модулів відповідно до геометрії об'єкта та необхідного рівня захисту. Для малого об'єкта (резервуарний парк площею до 1 га): 3–4 сенсорні вузли, 4–6 імітаційних модулів, єдиний блок управління. Для великого об'єкта (підстанція 110/35/10 кВ): 8–12 сенсорних вузлів, 12–20 імітаційних модулів, ієрархічна система управління з центральним та периферійними вузлами. Між конфігураціями немає принципової технологічної різниці — лише кількість однотипних модулів, що спрощує логістику та обслуговування. Уніфікація елементної бази скорочує терміни відновлення системи після втрати окремих модулів: кожен модуль є функціонально взаємозамінним у межах заданої конфігурації.

Модульний принцип забезпечує живучість системи: часткове ураження одного або кількох імітаційних модулів не виводить її з ладу — решта модулів перерозподіляють навантаження. Роєве розміщення (від 4 одиниць) підвищує ймовірність відводу ЗПН: «центр мас» хибної сигнатури формується у просторі між модулями, що ускладнює точне наведення навіть при знищенні частини мережі.

Маса одного імітаційного модуля — 1,5–2,5 кг, що відповідає вантажопідйомності сучасних вантажних БпЛА та уможливлює дистанційне розгортання у важкодоступних або небезпечних зонах без ризику для особового складу[8].

3.2. Мультимодальність: канали імітації та моніторингу

Система реалізує мультиспектральний підхід, охоплюючи основні фізичні канали, за якими сучасні ГСН ідентифікують ціль. Тепловий канал (інфрачервоний діапазон): нагрівальні елементи модуля відтворюють теплову сигнатуру КЕ відповідно до поточного режиму роботи, що передається сенсорною мережею в режимі реального часу. Радіолокаційний канал: кутові відбивачі з фрактальною геометрією корпусу формують ефективну поверхню розсіювання, характерну для реального об'єкта. Синхронізація обох каналів забезпечує мультиспектральну відповідність хибної цілі реальному КЕ.

Перспективний напрям розвитку — розширення мультимодальності завдяки акустичному каналу (для протидії ГСН, що використовують акустичну ідентифікацію промислових об'єктів) та оптичного каналу видимого спектру (для протидії оптико-електронним системам розвідки та БпЛА-спостерігачам). Обидва канали можуть бути реалізовані як додаткові модулі в рамках тієї ж архітектури без зміни базової платформи.

Акустичний канал імітації реалізується через цифрові синтезатори звукового спектру, що відтворюють характерний шумовий профіль технологічного обладнання ОПН у діапазоні 50–5000 Гц: шум насосних агрегатів (основна частота 150–300 Гц та гармоніки), гудіння силових трансформаторів (50 Гц та парні гармоніки), вібрація компресорів. Спектральна ідентичність імітованого джерела шуму реальному об'єкту забезпечується попереднім вимірюванням акустичного профілю ОПН в штатному режимі роботи. Оптичний канал передбачає застосування матриць з регульованим коефіцієнтом відбиття у діапазоні 0,4–0,75 мкм на основі електрохромних або рідкокристалічних панелей. Керований коефіцієнт відбиття (0,05–0,85) дозволяє імітувати спектральну яскравість промислових конструкцій для протидії оптичній розвідці з БпЛА та комерційних супутникових систем спостереження.

3.3. Компонент I: цифрова тінь для превентивного управління ризиками ОПН

Технологія цифрової тіні забезпечує однобічний автоматизований потік даних від фізичного об'єкта до його цифрового відображення[10]. На відміну від традиційних систем моніторингу, цифрова тінь формує безперервну динамічну картину стану обладнання, виявляючи відхилення від норми на ранніх стадіях — до переходу в аварійну ситуацію.

[10] W Kritzinger та ін, 'Digital Twin in Manufacturing: A Categorical Literature Review and Classification' (2018) 51(11) IFAC-PapersOnLine 1016 <https://doi.org/10.1016/j.ifacol.2018.08.474>.

Як перший верифікаційний приклад розглядається склад нафти та нафтопродуктів — найбільш часто атакована категорія ОПН в Україні з 2022 р. Сенсорна мережа здійснює безперервний моніторинг тиску у резервуарах та трубопроводах (виявлення витоків на ранній стадії), температурного режиму продуктів (ризик самозаймання), корозійного стану металоконструкцій (розвиток тріщин і деформацій), герметичності з'єднань та запірної арматури. Будь-яке відхилення від нормативних значень автоматично генерує сигнал тривоги для оперативного персоналу.

Для типового резервуара вертикального сталевого (РВС) критичними є такі порогові значення: зростання температури стінки понад 3 °С/год свідчить про початок внутрішнього нагрівання; зниження тиску у замкнутій системі трубопроводів більш ніж на 0,03 МПа за 30 хвилин — індикатор витоку; концентрація парів вуглеводнів понад 10 % від нижньої межі вибуховості потребує негайного реагування[11]. Безперервний контроль цих параметрів забезпечує перехід від реактивного гасіння пожеж до превентивного усунення причин займання — що в умовах воєнного часу, коли розгортання пожежно-рятувальних підрозділів може бути ускладнено, є критично важливим[12].

Порівняльна характеристика традиційного підходу та технології цифрової тіні для управління ризиками на ОПН наведена в таблиці 2.

Таблиця 2

Порівняння традиційного підходу та технології цифрової тіні для управління ризиками на ОПН

Характеристика	Традиційний підхід	Цифрова тінь
Джерело даних про стан об'єкта	Планові огляди та діагностика	Безперервні дані сенсорів у реальному часі
Частота оновлення даних	Дискретна (планові перевірки)	Безперервна або з мінімальною затримкою
Виявлення прихованих дефектів	Обмежено — між перевірками дефект може розвинутись	Автоматично — за трендом відхилення параметрів
Управління ризиками	Реактивне — усунення наслідків	Превентивне — попередження відмов
Ефективність в умовах воєнного часу	Знижується через порушення регламентів	Зберігається — автоматичний безперервний контроль
Додаткова функція для захисту від ЗПН	Відсутня	Так — формування сигнатурного профілю для цифрового фантому

Джерело: складено авторами на основі[13,14]

3.4. Компонент II: цифровий фантом для активного управління сигнатурою

Цифровий фантом — модуль активної мультиспектральної імітації, що формує динамічний сигнатурний образ реального об'єкта у тепловому та радіолокаційному діапазонах і розміщується

[11] M Soori, B Arezoo and R Dastres, 'Digital Twin for Smart Manufacturing: A Review' (2023) 2 Sustainable Manufacturing and Service Economics 100017 <https://doi.org/10.1016/j.smse.2023.100017>.

[12] О В Савченко, А А Стацюк, Н О Гарькава, 'Технології цифрових тіней та цифрових двійників для проактивного управління ризиками на об'єктах підвищеної небезпеки' [2026] Матеріали І Міжнар. наук.-практ. конф. «Технології безпеки: сучасні виклики та перспективи» (Черкаси 2026) 19.

[13] О В Савченко, Н О Гарькава, А А Стацюк, 'Активна мультиспектральна імітація як метод інженерного захисту об'єктів енергетики від засобів повітряного нападу' [2026] Матеріали ІІ Міжнар. наук.-практ. конф. «Цивільний захист в умовах війни» (ЛДУБЖД, Львів 2026) 6.

[14] W Kritzinger та ін, 'Digital Twin in Manufacturing: A Categorical Literature Review and Classification' (2018) 51(11) IFAC-PapersOnLine 1016 <https://doi.org/10.1016/j.ifacol.2018.08.474>.

на безпечній відстані від КЕ. Принципова відмінність від традиційних пасивних приманок (муляжів, кутових відбивачів) — адаптивність: параметри випромінювання автоматично коригуються в реальному часі відповідно до поточного стану реального об'єкта, що передається сенсорною мережею.

Механізм відводу ЗПН передбачає три ключові умови. Просторове ешелонування: модулі цифрового фантому розміщуються на відстані не менше 100 м від КЕ — ця відстань утворює безпечну зону, в межах якої детонація бойової частини ЗПН не спричиняє критичних пошкоджень реальної інфраструктури. Синхронна активація: при отриманні сигналу загрози модулі відтворюють теплову та радіолокаційну сигнатуру КЕ відповідно до актуального профілю, сформованого сенсорною мережею. Пріоритезація хибної цілі: алгоритми ГСН ідентифікують хибну ціль як первинну через відповідність сигнатурі КЕ і коригують траєкторію ЗПН від реального об'єкта.

Як другий верифікаційний приклад розглядається трансформаторна підстанція 110/35 кВ. Підстанція має характерну теплову сигнатуру (трансформатори масляного охолодження генерують стабільне теплове поле) та радіолокаційну сигнатуру (металевий корпус трансформаторів із специфічною геометрією). Сенсорна мережа в режимі реального часу передає параметри теплового навантаження трансформаторів залежно від поточного графіка навантаження; ці ж параметри налаштовують нагрівальні елементи модулів цифрового фантому. Хибна ціль відтворює динамічний, а не статичний образ реального КЕ, що підвищує ймовірність успішного відводу ГСН.

Ефективність відводу підкріплюється властивостями групового розміщення модулів: роєве розташування чотирьох і більше модулів формує «центр мас» хибної сигнатури, що стабільно домінує над сигнатурою реального КЕ. Для трансформаторної підстанції 110/35 кВ стандартний силовий трансформатор ТДН-16000 у режимі номінального навантаження має температуру корпусу 55–70 °С і характерний електромагнітний образ на частотах 50 Гц та гармоніках — параметри, які точно відтворюються модулем на основі даних сенсорної мережі. Навіть при знищенні 30–40 % модулів решта групи зберігає сигнатурний контраст, достатній для дезорієнтації ГСН.

3.5. Економічний аналіз та обґрунтування ефективності

Економічне обґрунтування концепції ґрунтується на двох аргументах: порівняльній вартості компонентів та принципі окупності єдиної інфраструктури. Вартість одного імітаційного модуля цифрового фантому оцінюється авторами в 5 500–10 000 грн; комплект з 4–6 модулів — 22 000–60 000 грн. Вартість традиційних металевих кутових відбивачів для аналогічного периметра вища у 2–6 разів, при цьому вони не забезпечують ні моніторингу технологічного стану, ні адаптивності до поточних параметрів об'єкта. Укриття типу «Саркофаг» коштує від 4,5 млн грн і не вирішує проблеми сигнатурної вразливості.

Сенсорна мережа, розгорнута для цифрової тіні, є одночасно інвестицією в активний компонент захисту: вартість розгортання системи моніторингу (сенсори, мережа передачі даних, програмне забезпечення) повністю включається в собівартість системи цифрового фантому через спільну інфраструктуру. Повна вартість дворівневої системи виявляється меншою за сукупність вартостей двох окремих систем.

Порівняльний економічний аналіз підходів до захисту ОПН наведено в таблиці 3.

Таблиця 3

Порівняльний економічний аналіз підходів до захисту ОПН

Показник	**Пасивний фізичний захист**	**Тільки моніторинг (ЦТ)**	**Тільки імітація (ЦФ)**	**Дворівнева система (ЦТ + ЦФ)**
Захист від внутрішнього ризику	Ні	Так	Ні	Так
Захист від зовнішнього удару	Частково	Ні	Так	Так
Усунення сигнатурної вразливості	Ні	Ні	Так	Так
Адаптивність до розміру об'єкта	Обмежена	Висока	Висока	Висока
Орієнтовна вартість (малий об'єкт)	0,15–4,5 млн грн	Вартість сенсорної мережі (визначається масштабом ОПН, орієнтовно від 80 тис. грн)	22–60 тис. грн/компл.	Менше за суму двох окремих систем
Час розгортання активного захисту	1–14 діб	—	Доставка БпЛА	Доставка БпЛА

Примітка: ЦТ — цифрова тінь, ЦФ — цифровий фантом. Джерело: складено авторами.

4. ОБГОВОРЕННЯ ТА ВИСНОВКИ

У запропонованій концепції здійснено системне поєднання технологій цифрового моніторингу та активного управління сигнатурою в єдиній архітектурі захисту стаціонарних цивільних ОПН. Наукова новизна полягає в обґрунтуванні принципу подвійного використання сенсорної інфраструктури: єдина мережа сенсорів забезпечує одночасно функцію превентивного моніторингу технологічних ризиків (цифрова тінь) та функцію формування актуального сигнатурного профілю для систем активного імітаційного захисту (цифровий фантом). Це дозволяє досягти синергетичного ефекту за умови істотного скорочення сукупних витрат порівняно з автономним розгортанням обох підсистем.

Концепція однаково застосовна до ОПН різних типів. Нафтосховища виграють передусім від компоненту цифрової тіні: безперервний моніторинг герметичності, корозійного стану та температурного режиму запобігає аваріям, які в умовах воєнного часу можуть спричинити пожежу або розлив із масштабними хімічними наслідками. Об'єкти енергетичної інфраструктури (підстанції, ТЕЦ) виграють насамперед від компонента цифрового фантому: їхня характерна теплова сигнатура робить їх легко впізнаваними цілями для мультиспектральних ГСН, тому зниження ймовірності прямого влучання є пріоритетним завданням.

Система має потенціал для розвитку за кількома напрямами: розширення мультимодальності завдяки акустичному та оптичному каналам імітації; інтеграція алгоритмів машинного навчання для прогнозування технічного стану обладнання на основі даних цифрової тіні; розробка уніфікованого програмного інтерфейсу для взаємодії з існуючими АСУ ТП ОПН. Окремим напрямом є нормативне закріплення: результати дослідження можуть стати основою для розробки рекомендацій ДСНС

України щодо технічного захисту ОПН в умовах збройного конфлікту — відповідно до вимог Сендайської рамкової програми зі зниження ризику лих на 2015–2030 роки.

Разом із тим, концепція має визначені межі застосування, що окреслюють пріоритети подальших досліджень. Ефективність компонента цифрового фантому обмежена щодо боєприпасів з інерційно-супутниковим наведенням (GPS/ГЛОНАСС): такі ЗПН наводяться за координатами, а не за фізичною сигнатурою об'єкта, і тому не реагують на теплову чи радіолокаційну хибну ціль. Відповідно, цифровий фантом є ефективним насамперед проти ЗПН з тепловими та активно-радіолокаційними ГСН кінцевої ділянки траєкторії. Безперервна робота системи потребує надійного автономного електроживлення — резервних акумуляторних блоків або генераторних установок — для забезпечення функціональності в умовах пошкодження централізованої енергомережі. Розміщення імітаційних модулів поза периметром ОПН на відкритій місцевості вимагає регулярного технічного обслуговування та захисту від несанкціонованого доступу. Зазначені обмеження не нівелюють концепцію в цілому, а окреслюють контекст її оптимального застосування: промислові ОПН з добре вираженою тепловою та радіолокаційною сигнатурою, що перебувають під загрозою ЗПН з активним кінцевим самонаведенням.

ВИСНОВКИ

1. В умовах збройного конфлікту ОПН зазнають подвійної загрози — технологічної деградації та прицільних ударів ЗПН, — які взаємно підсилюють одна одну через механізм каскадної відмови. Жоден із чинних нормативних підходів до захисту ОПН не охоплює обидва класи загроз одночасно, що підтверджує необхідність концептуально нових рішень.

2. Технологія цифрової тіні забезпечує безперервний превентивний моніторинг і переважає традиційні методи нагляду, оскільки не залежить від регулярності планових перевірок.

3. Технологія цифрового фантому усуває сигнатурну вразливість ОПН перед мультиспектральними ГСН і забезпечує активний відвід ЗПН без залучення особового складу.

4. Реалізація обох компонентів на єдиній сенсорній платформі економічно ефективніша за роздільне розгортання і забезпечує синергетичний інфраструктурний ефект.

5. Модульна масштабована архітектура забезпечує застосовність системи до ОПН різних типів, конфігурацій та масштабів.