Міністерство освіти і науки України

Луцький національний технічний університет
Факультет комп'ютерних та інформаційних технологій
Кафедра комп'ютерної інженерії та охоронних систем

КВАЛІФІКАЦІЙНА РОБОТА
ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОХОРОНИ ПЕРИМЕТРА СПЕЦІАЛЬНОГО ПОЛІГОНУ

DESIGNING AN INFORMATION SYSTEM FOR PHYSICAL PERIMETER SECURITY AT A SPECIAL TRAINING GROUND

спеціальність 126 Інформаційні системи та технології
(шифр і назва спеціальності)

освітня програма «Інформаційні системи та технології охорони і безпеки»
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи ІСТО-41
САДОВИЙ Микола Олександрович
_____
(підпис)

Керівник:
к.т.н., доцент
КАЙДИК Олег Леонтійович
_____
(підпис)

Кваліфікаційну роботу
допущено до захисту
«___» _____ 2026 р.
Гарант освітньої програми:
к.т.н., доцент
ТЕРЛЕЦЬКИЙ Тарас Володимирович
_____
(підпис)

Луцьк – 2026 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет: *комп'ютерних та інформаційних технологій*
Кафедра: *комп'ютерної інженерії та безпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *126 Інформаційні системи та технології*
Освітня програма: «*Інформаційні системи та технології охорони і безпеки*»

ЗАТВЕРДЖУЮ
Завідувач кафедри КІБ
к.т.н., доцент Терлецький Т. В.
_____
«___» _____ 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

САДОВОМУ Миколі Олександровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: *Проектування інформаційної системи охорони периметра спеціального полігону (комплексна робота з Дердюк Ю. С.)*

Керівник роботи: *к.т.н., доцент Кайдик Олег Леонтійович*
затверджені наказом закладу вищої освіти від «16» грудня 2025 р. № 529/01-02

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи: «30» травня 2026 р.

3. Вихідні дані до роботи: *Оптичний канал (видимий спектр): роздільна здатність Full HD (1920×1080), частота кадрів 25 FPS, кодек стиснення H.265 (HEVC), середній бітрейт одного каналу становить Rопт ≈ 4 Мбіт/с. Тепловізійний канал (LWIR спектр): роздільна здатність 640×512, частота кадрів 25 FPS, кодек H.265; середній бітрейт становить Rтепл ≈ 1,5 Мбіт/с. ДСТУ EN 50131. ДСТУ EN 50131-1. ISO/IEC 27001. INFCIRC/225/Rev.5. TLS 1.3 / HTTPS. ДСТУ ISO/IEC 18033-3. IEEE 802.1X. ONVIF Profile M. ITU-T G.8032 ERPS.*

4. Зміст розрахунково-пояснювальної записки (перелік питань, що потрібно розробити): *Анотація. Вступ. Розділ 1 Аналітичний огляд стану предметної області (аналіз об'єкта проєктування як джерела та споживача інформаційних потоків; огляд нормативно-правової бази та стандартів у сфері програмно-апаратного захисту інформації; порівняльний аналіз архітектурних підходів, технологій та програмного забезпечення для побудови інтеграційних платформ; аналіз методів інтелектуальної обробки даних та алгоритмів ШІ-відеоаналітики охоронного периметра; обґрунтування вибору архітектури, мережевих протоколів та шляхів програмно-апаратної реалізації ІСОП; постановка завдань на кваліфікаційну роботу бакалавра). Розділ 2 Обґрунтування вибору засобів та методів реалізації (обґрунтування контурів первинного збору даних та біспектрального моніторингу охоронного периметра; обґрунтування архітектури ЦОД та інтеграційної платформи верхнього рівня; математичне обґрунтування методів ШІ-відеоаналітики та алгоритмів крос-кореляції подій). Розділ 3 Практична реалізація. Загальні висновки та рекомендації. Список використаних джерел. Додатки.*

5. Перелік графічного (ілюстративного) матеріалу: *Презентація на ??? слайдах*

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Розділ 1 Аналітичний огляд стану предметної області	*Кайдик О. Л.*		
Розділ 2 Обґрунтування вибору засобів та методів реалізації	*Кайдик О. Л.*		
Розділ 3 Практична реалізація	*Кайдик О. Л.*		
Загальні висновки та рекомендації	*Кайдик О. Л.*		
Нормоконтроль	*Кайдик О. Л.*		
Гарант ОП	*Терлецький Т. В.*		
Показник запозичень тексту			
Академічна доброчесність	*Кайдик О. Л.*		

7. Дата видачі завдання: «16» грудня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи бакалавра	Строк виконання етапів роботи	Примітка
1.	Обґрунтування теми	До 12.12.2025 р.	
2.	Огляд літератури із досліджуваної проблеми	До 12.12.2025 р.	
3.	Розділ 1 Аналітичний огляд стану предметної області	До 28.02.2026 р.	
4.	Розділ 2 Обґрунтування вибору засобів та методів реалізації	До 31.03.2026 р.	
5	Розділ 3 Практична реалізація	До 30.04.2026 р.	
6.	Загальні висновки та рекомендації	До 16.05.2026 р.	
7.	Формування списку використаних джерел	До 20.05.2026 р.	
8.	Формування додатків.	До 20.05.2026 р.	
9.	Формування презентації за темою кваліфікаційної роботи	До 20.05.2026 р.	
10.	Нормоконтроль	До 21.05.2026 р.	
11.	Інструментальна перевірка на академічний плагіат	До 22.05.2026 р.	
12.	Представлення кваліфікаційної роботи бакалавра до захисту	До 02.06.2026 р.	

Здобувач вищої освіти _____ (Садовий М. О.)
(підпис)

Керівник кваліфікаційної роботи _____ (Кайдик О. Л.)
(підпис)

АНОТАЦІЯ

Садовий М. О. Проектування інформаційної системи охорони периметра спеціального полігону (комплексна робота з Дердюком Ю. С.). Рукопис.

Кваліфікаційна робота бакалавра ОП «Інформаційні системи та технології охорони і безпеки». Луцький національний технічний університет. Луцьк, 2026.

Кваліфікаційна робота бакалавра складається зі вступу, трьох розділів, загальних висновків та рекомендацій, списку використаних джерел та додатків.

У пояснювальній записці кваліфікаційної роботи акцентовано увагу на системному аналізі полігону спеціального як джерела та споживача інформаційних потоків, огляді нормативно-правової бази й стандартів у сфері програмно-апаратного захисту, а також порівняльному аналізі архітектурних підходів і ШІ-алгоритмів інтелектуальної відеоаналітики. Обґрунтовано вибір елементної бази контурів первинного збору даних, комбінованого біспектрального обладнання, обчислювальної інфраструктури центру обробки даних (ЦОД) корпоративного класу та інтеграційної PSIM-платформи верхнього рівня. Особливу увагу приділено математичному обґрунтуванню методів крос-кореляції подій, підсистемам інженерної живучості та кіберзахисту інформаційного середовища. У практичній частині роботи поетапно реалізовано розгортання транспортного ешелону низькорівневих потоків даних (Data Layer), конфігурацію логічного рівня обчислювальної інфраструктури ЦОД (Logic Layer), а також інтеграцію інтелектуальних сервісів, автоматизацію сценаріїв регламентних інструкцій та комплексне функціональне тестування системи (Orchestration Layer).

Ключові слова: інформаційна система, охорона периметру, біспектральний моніторинг, сейсмічний масив, віброакустична система, центр обробки даних, PSIM-платформа, крос-кореляція, подія, штучний інтелект, комп’ютерний зір, відмовостійкість, протокол, автоматизація SOP.

ANNOTATION

Sadovyi M. Designing an information system for physical perimeter security at a special training ground (comprehensive work with Derdiuk Yu.). Manuscript.

Bachelor’s qualification work EP «Security and safety information system and technologies». Lutsk National Technical University. Lutsk, 2026.

This bachelor’s thesis comprises an introduction, three sections, general conclusions and recommendations, a list of references, and appendices.

The explanatory note of the qualification thesis focuses on the system analysis of a special-purpose proving ground as a source and consumer of information flows, a review of the regulatory framework and standards in the field of hardware and software-based data protection, and a comparative analysis of architectural approaches and AI algorithms for intelligent video analytics. The choice of the component base for primary data collection loops, combined bispectral equipment, enterprise-grade data center (DC) computing infrastructure, and an upper-level integrated PSIM platform is substantiated. Special attention is paid to the mathematical substantiation of event cross-correlation methods, engineering survivability subsystems, and cyber protection of the information environment. In the practical part of the work, the deployment of the transport echelon of low-level data flows (Data Layer), the configuration of the logical level of the DC computing infrastructure (Logic Layer), as well as the integration of intelligent services, automation of standard operating procedure (SOP) scenarios, and comprehensive functional testing of the system (Orchestration Layer) are implemented step by step.

Keywords: information system, perimeter security, bispectral monitoring, seismic array, distributed acoustic sensing, data center, PSIM platform, cross-correlation, event, artificial intelligence, computer vision, fault tolerance, protocol, SOP automation.

ЗМІСТ

ВСТУП

Розвиток інженерії захисту периметра пройшов шлях від класичних аналогових систем і базових фізичних бар'єрів до складних інтелектуальних комплексів.

Сучасна практика проєктування систем для об'єктів стратегічного призначення та критичної інфраструктури базується на синергії волоконно-оптичних, сейсмічних та біспектральних засобів виявлення. Використання технологій Edge Computing, хмарних обчислень та алгоритмів крос-кореляції сигналів забезпечує високу точність верифікації тривог у реальному часі.

Водночас основним вектором модернізації галузі є перехід до автоматизованого аналізу інформаційних потоків за допомогою штучного інтелекту та централізованих PSIM-платформ. Це дозволяє не лише гнучко керувати сценаріями стандартних операційних процедур (SOP) на протяжних рубежах, а й гарантувати високий рівень інженерної живучості та кібербезпеки всієї системи.

Об'єкт дослідження – інформаційна система охорони периметра спеціального полігону для перевантаження ядерного палива.

Предмет дослідження – процеси функціонування, методи інтелектуальної обробки даних, архітектурні аспекти побудови ЦОД, алгоритми ШІ-відеоаналітики та крос-кореляції подій, а також конфігурація рівнів збору, логіки та оркестрації потоків даних.

Мета кваліфікаційної роботи – підвищення ефективності захисту периметра спеціального полігону шляхом проєктування та трирівневого розгортання інформаційної системи, яка базується на інтелектуальних алгоритмах ШІ-відеоаналітики, крос-кореляції мультисенсорних подій та автоматизації сценаріїв стандартних операційних процедур (SOP).

РОЗДІЛ 1
АНАЛІТИЧНИЙ ОГЛЯД СТАНУ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз об’єкта проєктування як джерела та споживача інформаційних потоків

Проєктування інформаційної системи охорони периметра (ІСОП) спеціального полігону для перевантаження ядерних відходів вимагає перш за все детального аналізу самого об’єкта не з позиції геодезії чи будівельних характеристик, а через призму архітектури даних та теорії інформаційних потоків. У такій парадигмі територію полігону слід розглядати як розподілену децентралізована матрицю джерел первинної інформації, що генерує безперервний гетерогенний трафік, який необхідно доставити, верифікувати та обробити в центрі обробки даних (ЦОД).

1.1 Специфіка об’єкта проєктування в контексті архітектури даних

Основною особливістю цього полігону (рис. 1.1) є його розташування у лісовому масиві, що створює так званий некоординатний простір меж. Це означає, що фізичний периметр об’єкта проєктування не має чітких геометричних орієнтирів для стандартних систем детектування, а також піддається постійному впливу високого рівня природних та біогенних перешкод (рух дерев, міграція тварин, зміна температурних фонів).

З точки зору системного аналізу, периметр – це протяжна лінія (інформаційний контур), яку розбито на N дільничних сегментів. Кожен такий сегмент є автономною зоною, яка постійно генерує два типи інформаційних станів:

– статичний (фоновий) трафік – безперервна телеметрія працездатності та потокові відеодані;

– динамічний (подієвий) трафік: високопріоритетні пакети даних, які формуються лише в момент фіксації фізичного впливу на бар’єр (спроба прориву, підкопу або саботаж на лінії).

Рисунок 1.1 – Полігон спеціальний для перевантаження ядерних відходів (згенеровано ШІ)

1.1.2 Класифікація та оцінка інтенсивності вхідного трафіку

Вхідний інформаційний потік, що надходить від периферійного ешелону ІСОП до ЦОД, прийнято класифікувати за трьома основними категоріями, кожна з яких володіє унікальними вимогами, які висуваються до смуги перепускання мережі, структури пакетів та пріоритетності (QoS).

До першої категорії відносять мультимедійні потоки високої роздільної здатності (відеоверифікація) – це найбільш «важкий» сегмент трафіку, який формується біспектральним обладнанням спостереження. При цьому кожна точка моніторингу генерує одночасно два цифрові потоки:

– оптичний канал (видимий спектр): роздільна здатність Full HD (1920×1080), частота кадрів 25 FPS, кодек стиснення H.265 (HEVC). Середній бітрейт одного каналу становить $R_{опт} \approx 4$ Мбіт/с;

– тепловізійний канал (LWIR спектр): роздільна здатність 640×512, частота кадрів 25 FPS, кодек H.265. Середній бітрейт становить $R_{тепл} \approx 1{,}5$ Мбіт/с.

Отже, сумарний потік від однієї біспектральної камери буде рівним:

$$R_к = 4 + 1,5 = 5,5 \text{ Мбіт/с}.$$

До другої категорії входить телеметрія, яка надходить із периферійних контролерів (цифрове детектування). Трафік тут формується підсистемами вібраційного та сейсмічного захисту. Контролери лінійних ділянок виконують безперервне цифрове опитування сенсорів та передають дані через інтерфейс Ethernet за протоколом Modbus TCP/IP [1]. Пакет містить інформацію про поточну амплітуду коливань, частотний спектр сигналу та координату точки впливу. Цей трафік є дискретним, обсяг одного повідомлення не перевищує 256 байт, а загальна інтенсивність від одного контролера становить $R_{тел} \approx 64$ Кбіт/с у фоновому режимі та до 512 Кбіт/с у режимі передачі сформованої під час тривоги осцилограми.

Третя категорія – це службові пакети стану ліній та мережевого управління. Сюди входить трафік, який є необхідним для контролю цілісності системи та її кіберзахисту. Він включає у себе повідомлення протоколу SNMP (моніторинг комутаторів) [2], службові кадри R-APS протоколу кільцевого резервування ERPS [3], а також ехо-запити для перевірки доступності пристроїв. Інтенсивність цього трафіку є мінімальною ($R_{серв} \leq 16$ Кбіт/с на пристрій), але він має найвищий мережевий пріоритет.

Профіль потоків периферійних пристроїв системи подано в таблиці 1.1.

Таблиця 1.1 – Характеристики та обсяги інформаційних потоків

Тип інформаційного потоку	Протокол / Кодек	Тип трафіку	Середня смуга на 1 пристрій	Пріоритет (QoS)
Відео (Оптичний канал)	H.265 / RTSP	Потоковий, безперервний	4.0 Мбіт/с	Low (Class 0)
Відео (Тепловізор)	H.265 / RTSP	Потоковий, безперервний	1,5 Мбіт/с	Low (Class 0)
Телеметрія сенсорів	Modbus TCP	Дискретний, циклічний	64-512 Кбіт/с	Medium (Class 3)
Службовий / Мережевий	SNMP, R-APS, ICMP	Пульсуючий, критичний	16 Кбіт/с	High (Class 6)

1.1.3 Визначення критичних вимог до затримок передачі даних

Специфіка функціонування полігону в складних кліматичних умовах північно західного регіону України (густі тумани, температурні інверсії, зливи,

снігопади) накладає критичні обмеження на часові параметри передачі інформаційних пакетів. Кліматичні чинники призводять до затухання сигналів у лініях зв'язку та підвищують ймовірності появи бітових помилок (BER – Bit Error Rate [4]).

Для забезпечення відповідності критеріям надійності Grade 4, сумарний час доставки тривожного пакета від моменту спрацювання периферійного давача до моменту відображення інциденту на моніторі оператора в ЦОД та запуску ШІ-аналітики повинен задовольняти умові (1.1):

$$t_{\Sigma} \leq 50 \text{ мс}. \quad (1.1)$$

Часовий ліміт розподіляється за наступною математичною моделлю обробки:

– t_{proc} – затримка оцифрування та пакування на контролері – ≤ 10 мс;

– t_{trans} – час транспортування по волоконно-оптичній магістралі – ≤ 5 мс (враховуючи швидкість поширення світла в оптичному волокні ≈200 км/мс);

– t_{sw} – комутаційна затримка на L2/L3 вузлах комутаторів MOXA – ≤ 2 мс;

– t_{erps} – максимальний час логічної перебудови маршруту в кільці під час обриву кабеля – ≤ 20 мс (за стандартом ITU-T G.8032 [5] номінальний час становить до 50 мс, але для гігабітних промислових кілець архітектурно закладається не більше 20 мс).

– t_{buf} – резервний буфер на повторне передавання втрачених пакетів у складних метеоумовах – ≤ 13 мс.

Утримання сумарної затримки в межах 50 мс є критично важливим, оскільки затримка понад цей ліміт унеможливить миттєвий автоматичний розворот швидкісних PTZ-камер в азимут тривоги. Швидкість руху порушника через лісовий масив може бути високою, і якщо система перевищить часовий ліміт, камера сфокусується на дільниці периметра вже після того, як порушник перетне лінію детектування та сховається в густій рослинності.

Як бачимо, інформаційна система охорони периметра виступає не просто у якості приймача сигналів, але й як складний споживач інформації, який вимагає від архітектури мережі високої пропускної спроможності, жорсткої пріоритезації трафіку та миттєвої програмної збіжності магістральних маршрутів зв’язку.

1.2 Огляд нормативно-правової бази та стандартів у сфері програмно-апаратного захисту інформації

Проєктні рішення, які спрямовані на побудову ІСОП полігону спеціального, регламентовано національними та міжнародними стандартами безпеки. Оскільки об’єкт відноситься до критичної інфраструктури, то базова нормативна вимога, яка висувається до комплексу технічних засобів охорони (КІТЗО) буде полягати у відповідності до класу Grade 4 за гармонізованим стандартом ДСТУ EN 50131 [6].

Специфіка класу надійності Grade 4 передбачає, що система повинна протидіяти зловмисникам (диверсійним групам), які мають глибокі технічні знання, професійні навички та спеціалізоване програмно-апаратне обладнання для перехоплення даних, глушіння сигналів або кіберсаботажу.

Відповідно до нормативних вимог ДСТУ EN 50131-1, ISO/IEC 27001 [7] та рекомендацій МАГАТЕ [8] (INFCIRC/225/Rev.5) щодо фізичного захисту ядерних та спеціальних об’єктів, програмно-апаратний контур системи повинен мати як мінімум три обов’язкові ешелони захисту від саботажу ліній зв’язку та керування.

До першого входить криптографічний захист сигналів та автентифікація пристроїв. Згідно вимог, які висуваються до систем високого ризику, передача будь-яких інформаційних потоків (відеоданих, телеметрії, сигналів тривоги) відкритими незахищеними каналами є неприпустимою. Стандарти вимагають мінімізації ризику перехоплення (Eavesdropping) та модифікації (Man-in-the-Middle) даних.

Нормативна вимога: забезпечення конфіденційності, цілісності та автентичності (рубіж CIA Triad).

Реалізація відповідно до стандартів: усі периферійні контролери (Modbus TCP) та біспектральні камери повинні підтримувати криптографічні протоколи транспортного рівня TLS 1.3 / HTTPS або шифрування всередині тунелів IPsec.

Для кодування команд управління та сигналів сповіщення застосовуються симетричні алгоритми шифрування AES-256, затверджені стандартом ДСТУ ISO/IEC 18033-3 [9]. Це виключає можливість дешифрування перехопленого зловмисником трафіку або відправки фальсифікованих команд керування елементами системи.

Другий ешелон – це захист від підміни обладнання та імітації сигналів (Spoofing/Replay attacks). Поширеним вектором фізично-програмного саботажу на периметрі є підключення стороннього пристрою в розрив Ethernet-магістралі замість штатної камери або давача для трансляції статичного архівного кадру (зациклювання відео) чи/або симуляції сигналу «Норма».

Нормативна вимога: негайне виявлення несанкціонованої зміни конфігурації мережі або підміни фізичного пристрою.

Реалізація відповідно до стандартів: стандарти серії IEEE 802.1X [10] регламентують обов’язкову автентифікацію портів на рівні контролю доступу до середовища (L2).

Програмна логіка комутаторів магістралі повинна реалізувати технологію Port Security із прив’язкою статичних MAC-адрес. У разі фіксування зміни MAC-адреси на порті або спроби ін’єкції пакетів з іншим IP, комутатор автоматично переводить порт у стан Shutdown та генерує маскируєму SNMP-тривогу на верхній рівень PSIM [11]. Додатково аналітика ONVIF Profile M [12] дозволяє передавати зашифровані цифрові підписи (Watermarking) безпосередньо у відеопотоці для підтвердження того, що відео йде з оригінальної камери в реальному часі.

До третього ешелону захисту входить софтверний моніторинг цілісності ліній зв’язку та топологічна живучість. У системах класу Grade 4 час виявлення

повної втрати зв’язку, навмисного короткого замикання або перерізання кабелю суворо лімітований і не може перевищувати декількох секунд (а в магістральних кільцях – долей секунди).

Нормативна вимога: безперервний контроль фізичного та логічного стану каналів зв’язку із автоматичним перенаправленням інформаційних потоків.

Реалізація відповідно до стандартів: на програмному рівні магістралі впроваджується стандарт ITU-T G.8032 ERPS.

Комутатори безперервно обмінюються службовими повідомленнями R-APS (Ring Automatic Protection Switching [13]). У тому випадку коли оптичний кабель буде перерізано, система за час $t \leq 50$ мс програмно розгортає трафік в протилежний бік кільця, запобігаючи втраті відео та телеметрії.

Для контролю кінцевих пристроїв на верхньому програмному рівні (PSIM/VMS) реалізується механізм Heartbeat (цифрове «серцебиття») – постійне ехо-тестування пристроїв за протоколами ICMP/SNMP [14] з інтервалом не більше 1000 мс. Відсутність відповіді протягом трьох циклів поспіль програмно інтерпретується не як технічний збій, а як інцидент високого пріоритету – «Саботаж лінії зв’язку».

1.3 Порівняльний аналіз архітектурних підходів, технологій та програмного забезпечення для побудови інтеграційних платформ

Ефективність функціонування інформаційної системи охорони периметра полігону спеціального безпосередньо залежить від архітектури програмного забезпечення верхнього рівня, що виконує агрегацію, обробку та кореляцію даних. На сучасному ринку систем безпеки та автоматизації виокремлюють три базові концепції побудови програмних комплексів моніторингу та управління:

– класичні відеоцентровані системи (VMS/NVR);

– локальні апаратно-залежні комплекси сигналізації із закритими інтерфейсами;

– розподілені інтеграційні платформи класу PSIM (Physical Security Information Management [15]).

Для вибору оптимального шляху реалізації проєкту необхідно провести їхній детальний компаративний аналіз.

1.3.1 Класичні локальні системи керування відеопотоками

Цей архітектурний підхід історично розвивався навколо обробки мультимедійних даних. Системи керування відео VMS (Video Management Systems [16]) або мережеві відеореєстратори NVR (Network Video Recorder [17]) розробляються з фокусом на високошвидкісний прийом, ретрансляцію, архівацію та базовий аналіз відеотрафіку.

Архітектурні особливості: програмне забезпечення (ПЗ) має монолітну або монолітно-клієнтську структуру, оптимізовану під роботу з мережевими протоколами RTSP/RTP та специфікаціями ONVIF.

Обмеження в умовах полігону: VMS-платформи є слабко адаптованими для роботи з невідеосигнальними периферійними пристроями. Інтеграція підсистем детектування (вібраційних або сейсмічних кабелів) в VMS зазвичай реалізується на примітивному рівні «сухих контактів» або через обмежені релейні модулі IP-камер. Система не здатна парсити складну телеметрію (наприклад, спектральну щільність сигналу або координату вібрації), а інтерфейс оператора залишається перевантаженим моніторами відеокамер без прив’язки до логіки загальної ситуаційної обізнаності.

1.3.2 Апаратно-залежні комплекси охоронної сигналізації із закритими інтерфейсами

Даний підхід базується на використанні фірмового ПЗ від конкретного виробника апаратних засобів охорони (контролерів, панелей, сповіщувачів).

Архітектурні особливості: програмне забезпечення верхнього рівня інтегроване з низькорівневими прошивками контролерів. Обмін даними відбувається за закритими, часто пропрієтарними протоколами (наприклад, специфічні модифікації RS-485 або закриті стеки поверх TCP/IP).

Обмеження в умовах полігону: основним недоліком є «проблема прив’язки до постачальника» (Vendor lock-in). За умов проектування ІСОП стратегічного об’єкта, де необхідно об’єднати оптику одного бренду, вібраційний кабель іншого та тепловізори третього, апаратно-залежний софт виявляється повністю безпорадним. Він не підтримує безшовну інтеграцію сторонніх SDK/API, що унеможливлює створення єдиного інформаційного простору та масштабування системи за рахунок новітніх технологій інших виробників.

1.3.3 Розподілені програмні комплекси класу PSIM із сервіс-орієнтованою архітектурою

Платформи класу PSIM створювалися як програмне рішення верхнього рівня (Supervisory Software), повністю відокремлене від конкретних брендів.

Архітектурні особливості: в основу PSIM покладено сервіс-орієнтовану архітектуру (SOA) або мікросервісну модель. Платформа складається із ядра системи, бази даних (наприклад, PostgreSQL або MS SQL) та розподіленого набору програмних драйверів (модулів інтеграції), кожен з яких взаємодіє з конкретним типом периферійного обладнання через його API або SDK.

Переваги для об’єкта: PSIM трансформує отримані після тривоги дані від різнорідних систем у єдиний потік подій, транслюючи їх на інтерактивній тривимірній або багатошаровій ГІС-карті об’єкта у вигляді метаданих.

Кількісно-якісну оцінку, описаних вище підходів, подано в порівняльній матриці (табл. 1.2).

Таблиця 1.2 – Матриця архітектурних концепцій ПЗ верхнього рівня

Критерії порівняння	Відеоцентричні системи (VMS/NVR)	Апаратно-залежні комплекси	Платформи класу PSIM (SOA)
1	*2*	*3*	*4*
Архітектурна модель	Клієнт-серверна, монолітна	Монолітна, закрита	Сервіс-орієнтована (SOA)
Рівень інтеграції гетерогенного заліза	Низький (переважно через реле або ONVIF)	Відсутній (робота лише з власним брендом)	Високий (на рівні низького рівня SDK/API)
Робота з телеметрією датчиків	Обмежена (тільки стан тривоги)	Повна (але тільки для власних давачів)	Повна (глибокий парсинг регістрів Modbus/BACnet)

Продовження таблиці 1.2

1	2	3	4
Масштабованість та гнучкість	Середня	Низька	Майже необмежена (модульна)
Відповідність вимогам Grade 4	Часткова (через слабку живучість при завадах)	Часткова (через обмеженість функцій аналізу)	Повна (програмне резервування сервісів)

1.3.4 Обґрунтування переваг PSIM-платформ для полігону спеціального

Аналіз предметної області доводить, що для реалізації ІСОП спеціального полігону для перевантаження ядерного палива єдиним методологічно та технічно виправданим вибором є впровадження PSIM-платформи. Доцільність цього рішення підтверджується наступними технологічними аргументами:

– повна конвергенція гетерогенного середовища: захист полігону спеціального здійснюється за допомогою різнорівневого обладнанням – волоконно-оптичним кабелем детектування, тепловізорами, радіохвильовими бар’єрами та IT-комутаторами магістралі. PSIM-платформа, завдяки модулям розширення, здатна безшовно інтегрувати весь цей пул різнорідного (гетерогенного) софту й технічних засобів (ТЗ) в єдину логічну систему за допомогою відритих інтерфейсів програмування додатків (API);

– інтелектуальний двигун крос-кореляції подій: на відміну від VMS або класичної сигналізації, які реагують на кожне сповіщення окремо, PSIM містить у собі програмний модуль математичного аналізу взаємозв’язків. Якщо вібраційний кабель фіксує коливання на певній ділянці, а нейромережа на базі штучного інтелекту (ШІ) підтверджує рух силуету в цій же зоні, PSIM аналізує ці події не як два окремі сервісні пакети, а як один підтверджений інцидент високого пріоритету. Це дозволяє відсіяти до 98% хибних спрацювань враховуючи перешкоди створені лісовим масивом;

– автоматизація регламентів за сценаріями SOP (Standard Operating Procedures [18]): у випадку виникнення тривоги в некоординатному охоронному просторі полігону, PSIM автоматично, на основі закладених алгоритмів, виконує комплекс дій: видає CGI-команду на PTZ-камеру для її точного наведення в координату збурення, вмикає лінійне освітлення цієї

ділянки, активує запис у ЦОД із підвищеною частотою кадрів та виводить на екран оператора покрокову інструкцію дій. Це дозволяє мінімізувати людський чинник та утримує час реакції системи в межах обмеженого нормативного ліміту (≤ 50 мс).

1.4 Аналіз методів інтелектуальної обробки даних та алгоритмів ШІ-відеоаналітики охоронного периметра

Автоматизація процесів моніторингу та верифікації загроз на охоронному периметрі полігону спеціального (клас надійності Grade 4) неможлива без інтеграції інтелектуальних засобів обробки даних. Сучасна парадигма комп'ютерної інженерії передбачає відмову від класичних детекторів руху, які реагують на просту зміну яскравості пікселів, на користь глибоких згорткових нейронних мереж CNN (Convolutional Neural Network [19]). Це дозволяє не лише фіксувати факт наявності руху, а й здійснювати точну класифікацію об'єктів у реальному часі.

1.4.1 Огляд математичних моделей та програмних засобів комп'ютерного зору

Для вирішення завдань детектування та семантичної класифікації антропоморфних (люди, тварини) та транспортних (автомобілі, БПЛА) цілей у системах відеоаналітики застосовують три основні класи архітектур нейромереж: Faster R-CNN, SSD та моделі сімейства YOLO.

Faster R-CNN (Region-based Convolutional Neural Network [20]) – це двоетапний (Two-Stage) детектор. На першому етапі мережа Region Proposal Network (RPN) генерує гіпотези про розташування об'єктів, а на другому – згорткова мережа класифікує ці зони.

Переваги та недоліки: має найвищу точність локалізації об'єктів, але критично низьку швидкість оброблення кадрів. Час інференсу (Inference Time) на стандартних обчислювачах є занадто високим, що унеможливлює

паралельний аналіз десятків потоків 4K-відео в реальному часі за жорстких обмежень затримки (≤ 50 мс).

SSD (Single Shot MultiBox Detector [21]): одноетапний (One-Stage) детектор, який використовує багатомасштабні карти ознак для прогнозування обмежувальних рамок (Bounding Boxes) та ймовірностей класів за один прохід мережі.

Переваги та недоліки: демонструє хорошу швидкість роботи, але має низьку точність детектування дрібних об’єктів, що є критичним мінусом для периметра, де порушник може перебувати на великій відстані від камери та займати лише декілька пікселів на кадрі.

Моделі сімейства YOLOv8 (You Only Look Once, version 8 [22]): найновіша та найбільш збалансована архітектура одноетапних детекторів комп’ютерного зору. YOLOv8 використовує безякірну (Anchor-Free) структуру, що дозволяє безпосередньо прогнозувати центр об’єкта та масштаб рамки, а також нову функцію втрат (Loss Function) та покращений блок FPN Feature Pyramid Network [23]).

Переваги для ІСОП: модель забезпечує екстремально низький час інференсу за високих показників середньої точності mAP (Mean Average Precision [24]). Вона здатна стабільно розпізнавати силуети людей та техніки навіть в умовах часткового перекриття об’єкта (наприклад, коли людина пересувається за кущами чи деревами).

Ефективність, за основними критеріями оцінювання, розглянутих моделей комп’ютерного зору деталізовано в таблиці 1.3.

1.4.2 Дослідження проблеми «інформаційного шуму» в умовах геопросторового розташування об’єкта

Специфіка розгортання ІСОП спеціального полігона для перевант аження ядерного палива у лісовому масиві північно-західного регіону України пов’язана із надвисоким рівнем природних завад, які створюють так званий інформаційний шум. Основним чинником генерування хибних спрацювань системи прийнято вважати:

– рослинність: хаотичний рух гілок дерев, чагарників та трави під дією вітру (особливо під час штормових погодніх умов);

– тварини: міграція птахів та диких тварин (косулі, кабани, зайці), які перетинають лінію охоронного периметра;

– клімат: густі тумани, характерні для низовин Полісся, проливні дощі, снігопади та різкі температурні інверсії, які засліплюють оптичний канал і створюють теплові «фантоми» на LWIR-каналах тепловізорів.

Таблиця 1.3 – Матриця архітектур нейромереж для відеоаналітики

Критерії порівняння / Метрики	Faster R-CNN	SSD	YOLOv8 (версія Medium/Large)
Архітектурний тип	Двоетапний (Two-Stage)	Одноетапний (One-stage)	Одноетапний (One-stage, Anchor-free)
Швидкість обробки (Inference Time)	Низька (≥ 50 мс/кадр)	Висока (≈ 15 мс/кадр)	Екстремальна (≤ 8-12 мс/кадр)
Точність локалізації (mAP 50-95)	Висока (≈ 45-50 %)	Середня (≈ 30-35 %)	Висока (≈ 48-52 %)
Детектування дрібних, віддалених цілей	Відмінна	Незадовільна	Добра (завдяки оптимізації ознак)
Ефективність для ІСОП (Grade 4)	Низька (через затримки)	Середня (через пропуски цілей)	Максимальна

Ці чинники здатні спровокувати багато хибних тривог на добу, що призводить до психологічного вигорання оператора та нівелює ефективність охорони. Для фільтрування такого шуму на програмному рівні ІСОП застосовують комбінацію геометричних та логічних методів захисту.

1.4.3 Алгоритмічні методи фільтрування перешкод та крос-кореляція сигналів

Першим етапом програмного фільтрування перешкод є налаштування віртуальних зон ROI (Region of Interest [25]) безпосередньо у відеопотоці. Замість аналізу усього кадру, алгоритм обробляє лише критично важливі просторові ділянки – лінії безпосереднього загородження та зони відчуження.

В межах ROI програмуються фільтри геометричних розмірів цілі (наприклад, ігнорування об’єктів площею менше певного відсотка від зони аналізу, яка відсікає птахів та дрібних тварин) та вектори напрямку руху

(тривога ініціюється лише під час перетину віртуальної лінії вглиб об’єкта). Налаштовуються й часові фільтри тривалості присутності (Time-to-Trigger), які дозволяють ігнорувати короткочасні коливання гілок дерев у кадрі. Проте, в умовах щільного туману чи/або складного саботажу геометричних фільтрів ROI недостатньо.

Другим, найбільш ефективним етапом фільтрування є алгоритмічна крос-кореляція сигналів суміжних систем на базі математичного апарату теорії ймовірностей Байєса [26].

Логічний модуль інтеграційної PSIM-платформи аналізує потік подій від гетерогенних підсистем як умовну ймовірність істинності загрози P(A|B). Спрощений алгоритм (для №4 зони виявлення) працює за наступною логікою:

Якщо [Modbus_Event_Line_4 = TRUE] ∩[YOLOv8_Class_Person_Zone_4 = = TRUE], тоді → Статус = «ІСТИННА ТРИВОГА»

У тому випадку коли волоконно-оптичний кабель на бар’єрі фіксує сильне вібраційне коливання, але ШІ-відеоаналітика YOLOv8 на базі тепловізійного потоку не виявляє у цій зоні руху антропоморфного або транспортного об’єкта, подія класифікується системою як «Кліматична/біогенна перешкода» (наприклад, удар гілки від вітру або падіння дерева). Подія записується в журнал у фоновому режимі без активації звукових сирен на АРМ оператора. І навпаки: якщо густий туман знижує точність роботи нейромережі, але вібраційний давач чітко реєструє спробу перелазу, система використовує ці дані для динамічного зниження порогу впевненості класифікатора (Confidence Threshold) нейромережі в даній зоні, змушуючи алгоритм комп’ютерного зору сфокусуватися на прихованому силуеті людини.

1.5 Обґрунтування вибору архітектури, мережевих протоколів та шляхів програмно-апаратної реалізації ІСОП

На основі системного синтезу результатів аналізу інформаційних потоків, специфіки об’єкта проєктування та критеріїв нормативної бази класу надійності

Grade 4, виникає необхідність чіткого визначення архітектурної основи та програмно-апаратних засобів реалізації системи. Цей етап аналітичного дослідження полягає в обґрунтуванні структурної моделі ІСОП та виборі наскрізних протоколів взаємодії, які забезпечать нульову втрату даних і задану швидкість реакції комплексу (рис. 1.2).

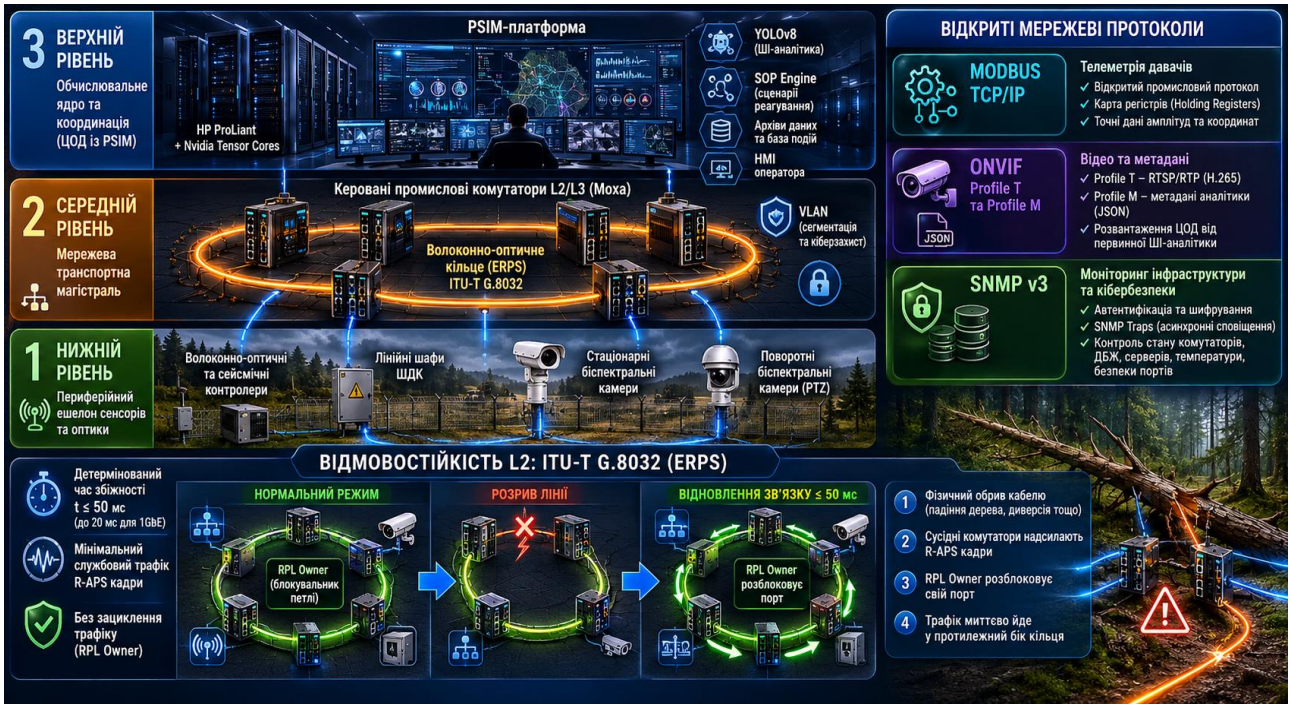


Рисунок 1.2 – Топологічна модель трирівневої ІСОП на базі відкритих індустріальних протоколів (згенеровано ШІ)

1.5.1 Обґрунтування трирівневої модульної архітектури ІСОП

Для забезпечення гнучкості, масштабованості та високої живучості інформаційної системи полігону спеціального необхідно обґрунтувати перехід від монолітних схем до трирівневої модульної архітектури. Розподіл системи на незалежні, але взаємопов’язані програмно-апаратні ешелони дозволяє ізолювати обчислювальні процеси та гарантувати відмовостійкість: у разі виходу з ладу окремих модулів верхнього рівня, нижні рівні продовжують виконувати автономну функцію збору та локального накопичення даних.

Нижній рівень (периферійний ешелон сенсорів та оптики): фізичний рубіж охорони складається із волоконно-оптичних та сейсмічних давачів,

лінійних шаф ШДК, стаціонарних та поворотних біспектральних камер спостереження. Основною їх функцією є первинне сприйняття фізичних збурень, оцифровка, первинне фільтрування та кодування у стандартизовані мережеві пакети даних.

Середній рівень (мережева транспортна магістраль): інформаційна артерія системи будується на базі керованих промислових комутаторів L2/L3, які об’єднано волоконно-оптичними лініями зв’язку у єдину топологічну структуру. Основна функція – високошвидкісна, завадостійка і безпечна доставка гетерогенного трафіку з периферії до центру обробки інформації, а також логічна сегментація мережі (VLAN) для кіберзахисту.

Верхній рівень (обчислювальне ядро та координація ЦОД із PSIM): центр прийняття рішень доцільно розгортати на базі серверної інфраструктури HP ProLiant з графічними прискорювачами Nvidia Tensor Cores. На програмному рівні тут функціонує інтеграційна PSIM-платформа, нейромережевий стек YOLOv8 та модулі автоматизованих сценаріїв реагування (SOP Engine). Цей рівень здійснює агрегацію, глибоку крос-кореляцію даних, збереження архівів та надання людино-машинного інтерфейсу оператора.

1.5.2 Логічне обґрунтування вибору відкритих мережевих протоколів

Для подолання проблеми апаратної залежності (Vendor Lock-In) та створення наскрізного інтеграційного середовища, де ТЗ і софт від різних виробників працюють як єдиний механізм, достатньо обґрунтувати вибір виключно відкритих, стандартизованих промислових та мережевих протоколів:

– Modbus TCP/IP [27] (рівень телеметрії давачів): вибір цього промислового протоколу для зв’язку периферійних контролерів волоконно-оптичних кабелів із PSIM-платформою зумовлений його простотою, відкритістю та високою надійністю всередині Ethernet-мереж. Замість закритих пропрієтарних команд, Modbus TCP використовує чітку карту адресних регістрів (Holding Registers), що дозволяє софту верхнього рівня напряму зчитувати точні числові значення амплітуд коливань бар’єру та координати точок порушення, мінімізуючи накладні витрати на пакування пакетів.

– ONVIF Profile T та Profile M [28] (рівень відео та метаданих): для інтеграції біспектральних камер обрано відкриті галузеві специфікації ONVIF. Profile T дозволяє забезпечувати уніфіковане керування потоками високої роздільної здатності за протоколами RTSP/RTP з підтримкою ефективного кодека стиснення H.265. Критично важливим для ІСОП є впровадження нового профілю Profile M, який дозволяє передавати в єдиному потоці не просто картинку, а структуровані метадані аналітики (JSON-описи об'єктів, класифікованих безпосередньо процесором камери: людина/транспорт, координати Bounding Box). Це розвантажує центральні сервери ЦОД від первинних обчислень комп'ютерного зору.

– SNMP v3 [29] (рівень моніторингу інфраструктури та кібербезпеки): протокол простий в управлінні мережею та обґрунтований для софтверного контролю стану комутаторів, джерел безперебійного живлення (ДБЖ) та серверів. На відміну від застарілих версій, SNMP v3 підтримує автентифікацію та криптографічне шифрування службових повідомлень. Це дозволяє PSIM-платформі в режимі реального часу отримувати асинхронні сповіщення (SNMP Traps) про будь-які аномалії: падіння напруги на елементах, критичне підвищення температури в серверній шафі чи спробу несанкціонованого доступу до портів комутатора.

1.5.3 Обґрунтування відмовостійкості на рівні L2 за стандартом ITU-T G.8032 ERPS

Найбільш вразливим елементом ІСОП протяжного периметра полігона спеціального є фізичні лінії зв'язку в лісовому масиві, які можуть бути пошкоджені внаслідок падіння дерев, стихійного лиха або навмисного розриву. Для забезпечення безперервності процесів Grade 4 обрано топологію «оптичне кільце», керовану на програмно-магістральному рівні протоколом ITU-T G.8032 ERPS (Ethernet Ring Protection Switching).

Вибір ERPS замість стандартних IT-протоколів резервування (наприклад, RSTP або MSTP) обґрунтований наступними технічними чинниками:

– детермінований час збіжності: протокол RSTP під час розриву великого кільця (понад 10 комутаторів) відновлює логічні маршрути протягом 2-5 секунд, що для потокового 4K-відео є критичним (втрата до 125 кадрів, заклинювання ШІ-аналітики). Протокол ERPS гарантує повне відновлення зв'язку за час $t \leq 50$ мс (а в гігабітних мережах – до 20 мс), що є непомітним для відеотрафіку та виключає пропуски тривожних сигналів.

– мінімізація службового трафіку: комутатори в кільці ERPS обмінюються короткими та оптимізованими службовими кадрами R-APS, що не створює навантаження на пропускну здатність ліній зв'язку в умовах складних метеорологічних умов та високого бітового шуму;

– логіка роботи: один із лінійних інтерфейсів комутатора ядра програмно призначається блокувальником петлі (RPL Owner), що виключає зациклення трафіку (Broadcast Storm). У момент фізичного обриву кабелю сусідні з розривом комутатори миттєво розсилають R-APS кадри, RPL Owner розблокує свій порт, і трафік миттєво починає рухатися у протилежний бік кільця.

1.5 Постановка завдань на кваліфікаційну роботу бакалавра

Проєктування інформаційних систем охорони периметра для об'єктів із підвищеними вимогами до безпеки вимагає переходу від ізольованих засобів виявлення до єдиного інформаційного середовища. Успішна реалізація ІСОП для спеціального полігону можлива лише за умови інтеграції мультисенсорних давачів, обчислювальної платформи ЦОД та алгоритмів штучного інтелекту. Синхронізація цих компонентів на основі аналізу інформаційного обміну та нормативних вимог дозволяє побудувати гнучку систему моніторингу. Вона здатна нівелювати кіберзагрози, зберігати працездатність під час саботажу та мінімізувати вплив людського чинника.

Для досягнення поставленої мети та розв'язання описаної науково-технічної проблеми необхідно виконати такі завдання:

– проаналізувати спеціальний полігон як об’єкт проєктування з точки зору структури та інтенсивності вхідних і вихідних інформаційних потоків та дослідити нормативно-правову базу й стандарти у сфері програмно-апаратного захисту інформації;

– провести порівняльний аналіз існуючих архітектурних підходів, мережевих протоколів та методів інтелектуальної обробки даних й обґрунтувати оптимальні шляхи програмно-апаратної реалізації ІСОП.

– обґрунтувати й розрахувати параметри контурів первинного збору даних, біспектрального моніторингу, апаратної архітектури ЦОД та мережевих сховищ під критерії надійності Grade 4;

– розробити математичну основу для функціонування методів ШІ-відеоаналітики й алгоритмів крос-кореляції мультисенсорних подій, обґрунтувати підсистеми кіберзахисту інформаційного середовища та методологію його випробувань;

– реалізувати на практиці трирівневу структуру ІСОП.

РОЗДІЛ 2
ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ ТА МЕТОДІВ РЕАЛІЗАЦІЇ

2.1 Обґрунтування контурів первинного збору даних та біспектрального моніторингу охоронного периметра

Реалізація нижнього ешелону ІСОП полігону спеціального полігону (клас надійності Grade 4) базується на принципах максимальної інформативності первинних даних. Традиційний підхід, який базується на дискретних сповіщувачах з релейними виходами типу «сухий контакт», відкидається як невідповідний критеріям інтелектуальної обробки. Для побудови ефективного контуру захисту в некоординатному просторі лісового масиву слід провести системний аналіз та інженерне обґрунтування елементної бази сенсорного та оптико-електронного рівнів через призму формування цифрових потоків.

2.1.1 Системний аналіз сенсорного ешелону та параметризація телеметрії

Для первинного виявлення спроб подолання або саботажу фізичного бар'єра обрано комбінацію розподілених волоконно-оптичних віброакустичних систем на базі DAS (Distributed Acoustic Sensing [30]) та сейсмічних сенсорних масивів (рис. 2.1). Вибір конкретних периферійних контролерів здійснювався за критерієм їх здатності здійснювати високошвидкісну оцифровку та первинну математичну обробку сигналів безпосередньо «на борту» (Edge Computing).

Замість трансляції бінарного стану транспаранту («0» – норма, «1» – тривога), периферійні модулі контуру збору даних необхідно підбирати за здатністю передавати розширену телеметрію. Контролер волоконно-оптичної системи виконує постійне лазерне сканування інтерферометричних змін у волокні (рис. 2.2), оцифровує отриманий сигнал за допомогою вбудованого АЦП і здійснює швидке перетворення Фур'є для формування АЧХ збурення.

Передача параметризованих даних на верхній рівень PSIM реалізується через інтегрований інтерфейс Ethernet за відкритим промисловим протоколом Modbus TCP/IP. Програмне забезпечення контролера мапує інформацію у виділену карту адресних регістрів (Holding Registers), яка містить:

а) б)

Рисунок 2.1 – Сенсорний контур збору даних:
а) – волоконно-оптична віброакустична система; б) – сейсмічний сенсорний масив

– поточне значення амплітуди коливань у децибелах (дБ);

– домінантну частоту сигналу (Гц) для відокремлення вітрового навантаження від фізичного перелазу;

– точну координату точки фізичного впливу на кабель (дискретність до 5 метрів);

– транспаранти внутрішньої апаратної самодіагностики та цілісності лінії (обрив/коротке замикання).

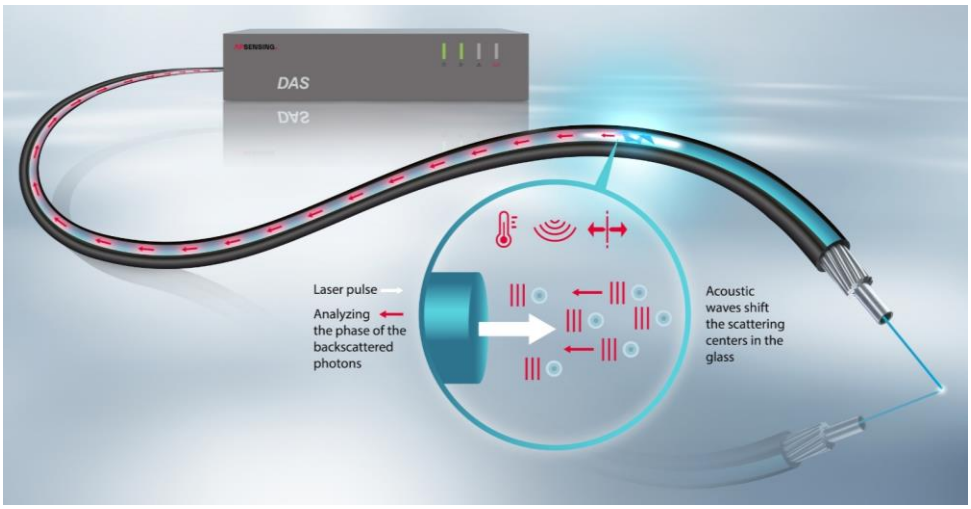


Рисунок 2.2 – Контролер волоконно-оптичної системи DAS [30]

Передача параметризованих даних на верхній рівень PSIM реалізується через інтегрований інтерфейс Ethernet за відкритим промисловим протоколом

Modbus TCP/IP. Програмне забезпечення контролера мапує інформацію у виділену карту адресних регістрів (Holding Registers), яка містить:

– поточне значення амплітуди коливань у децибелах (дБ);

– домінантну частоту сигналу (Гц) для відокремлення вітрового навантаження від фізичного перелазу;

– точну координату точки фізичного впливу на кабель (дискретність до 5 метрів);

– транспаранти внутрішньої апаратної самодіагностики та цілісності лінії (обрив/коротке замикання).

Такий обсяг даних дозволяє центральній системі не просто фіксувати тривогу, а й аналізувати динаміку розвитку інциденту.

2.1.2 Інженерне обґрунтування контуру біспектрального моніторингу

Оптико-електронний ешелон виконує функцію автоматичної візуальної верифікації подій. З огляду на складні кліматичні умови Полісся (часті тумани, снігопади, нульова видимість уночі), обґрунтовано використання комбінованих біспектральних IP-камер. Кожен такий пристрій інтегрує в одному корпусі два незалежні сенсори (рис. 2.3):

– оптичний модуль (видимий спектр): для детального розпізнавання облич, силуетів та номерних знаків у світлу пору доби або при увімкненому лінійному освітленні;

– тепловізійний модуль (LWIR-спектр, 8-14 мкм): для цілодобового виявлення теплових сигнатур людей та техніки крізь туман, чагарники тощо.

Основним критерієм вибору біспектральних камер є повна сумісність їх вихідних цифрових потоків із ШІ-платформами центрального ЦОД. Камери повинні підтримувати стандартизовані мережеві профілі ONVIF:

– ONVIF Profile T: зстосовується для уніфікованої трансляції важкого мультимедійного контенту, двостороннього аудіо та команд керування поворотними механізмами (PTZ);

– ONVIF Profile M: критично важливий для інтелектуальних систем, оскільки забезпечує стандартизований експорт метаданих аналітики. Замість

передачі сформованого тривогою відео для постійного аналізу, процесор камери може самостійно виявляти об’єкти та транслювати їх координати, класи та вектори руху у форматі XML/JSON-метаданих, суттєво заощаджуючи обчислювальні ресурси серверів.

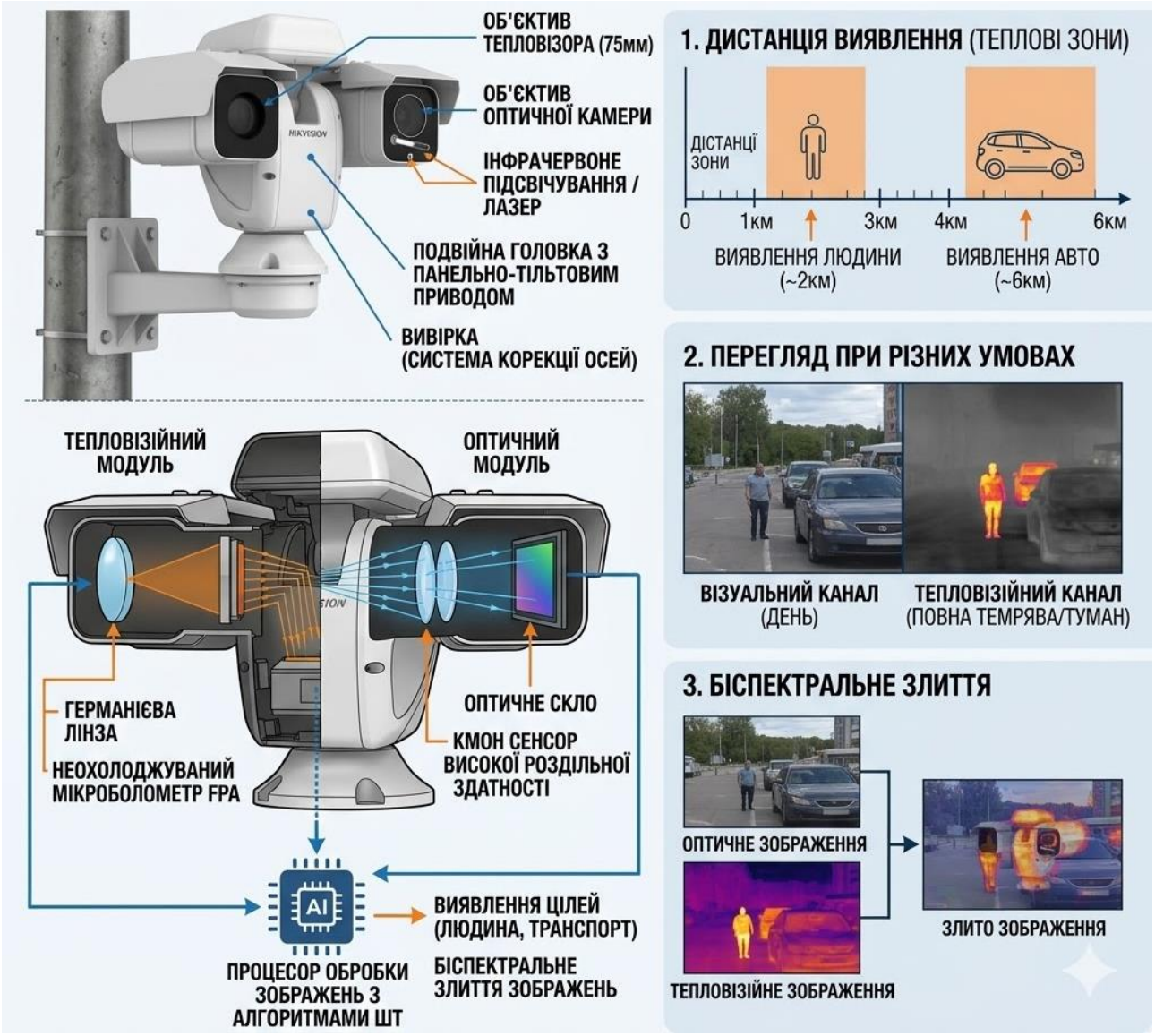


Рисунок 2.3 – Будова та принцип роботи зовнішньої біспектральної камери великої дальності Hikvision DS-2TD6267-75C4L/W (згенеровано ШІ)

2.1.3 Розрахунок параметрів потокового кодування та смуги перепускання

Для оптимізації навантаження на транспортну магістраль та мережеві сховища даних (NAS/SAN) виконано інженерний розрахунок параметрів

кодування відеопотоків від однієї типової біспектральної точки моніторингу периметра.

Для оптичного каналу встановлено базову роздільну здатність Full HD (1920×1080) із частотою кадрів 25 кадрів/с, що забезпечує необхідну плавність для фіксації швидких рухів. Для тепловізійного каналу, де важлива геометрична форма теплової плями, а не дрібна текстура, обрано роздільну здатність 640×512 при 25кадрів/с.

За базовий алгоритм компресії було взято кодек H.265 (HEVC), який, завдяки використанню деревоподібної структури блоків кодування (CTU) та покращеному внутрішньокадровому прогнозуванню, забезпечує зниження бітрейту до 40-50% порівняно із застарілим H.264 при однаковій якості зображення (рис. 2.4).

Рисунок 2.4 – Алгоритми компресії за однакової якості вхідного зображення

Математичний розрахунок необхідної смуги перепускання для однієї комбінованої камери здійснюється за виразом (2.1):

$$B_{\Sigma} = B_{опт} + B_{тепл} + B_{мета}, \quad (2.1)$$

де $B_{опт}$ – бітрейт оптичного каналу Full HD (H.265, Medium-профіль складності сцени), $B_{опт}$ = 4096 Кбіт/с ≈ 4 Мбіт/с;

$B_{тепл}$ – бітрейт тепловізійного каналу 640×512 (H.265), $B_{тепл}$ = 1536 Кбіт/с ≈ ≈ 1,5 Мбіт/с;

$В_{мета}$ – потік метаданих ONVIF Profile M та службового трафіку, $В_{мета} \approx 128$ Кбіт/с ≈ 0,125 Мбіт/с.

Звідси отримуємо сумарне навантаження від однієї точки збору даних:

$$В_{\Sigma} = 4 + 1,5 + 0,125 = 5,625 \text{ Мбіт/с}.$$

Під час проєктування магістралі для сегмента з K камер загальна пропускна здатність буде розраховуватись за виразом (2.2):

$$В_{заг} = K \times В_{\Sigma}, \quad (2.2)$$

що закладається у вимоги до пропускної здатності гігабітних комутаторів середнього рівня.

Отримані розрахункові параметри потоків та конфігурація Modbus-регістрів виступають базовими вихідними даними для наступного кроку проєктування – розрахунку ємності дискових масивів сховища та обчислювальної потужності серверного ядра системи безпеки.

2.2 Обґрунтування архітектури ЦОД та інтеграційної платформи верхнього рівня

Побудова верхнього (координаційного) ешелону інформаційної системи охорони периметра полігона спеціального потребує створення відмовостійкої, масштабованої та високопродуктивної інфраструктури центру обробки даних. Оскільки система проектується під жорсткі критерії надійності Grade 4, центральне обчислювальне ядро та інтеграційне програмне забезпечення мають функціонувати в режимі 24/7/365 із коефіцієнтом доступності не менше за A = 0,9999 (Fault-Tolerant архітектура).

2.2.1 Розрахунок та обґрунтування конфігурації серверного обладнання

Для забезпечення безперервної обробки потоків телеметрії та важкого відеотрафіку обрано блейд-сервера архітектури x86_64 корпоративного класу

на базі HPE ProLiant DL380 Gen11 (рис. 2.5). Розрахунок необхідної обчислювальної потужності здійснюється на основі сумарного вхідного потоку даних та задач нейромережевої аналітики.

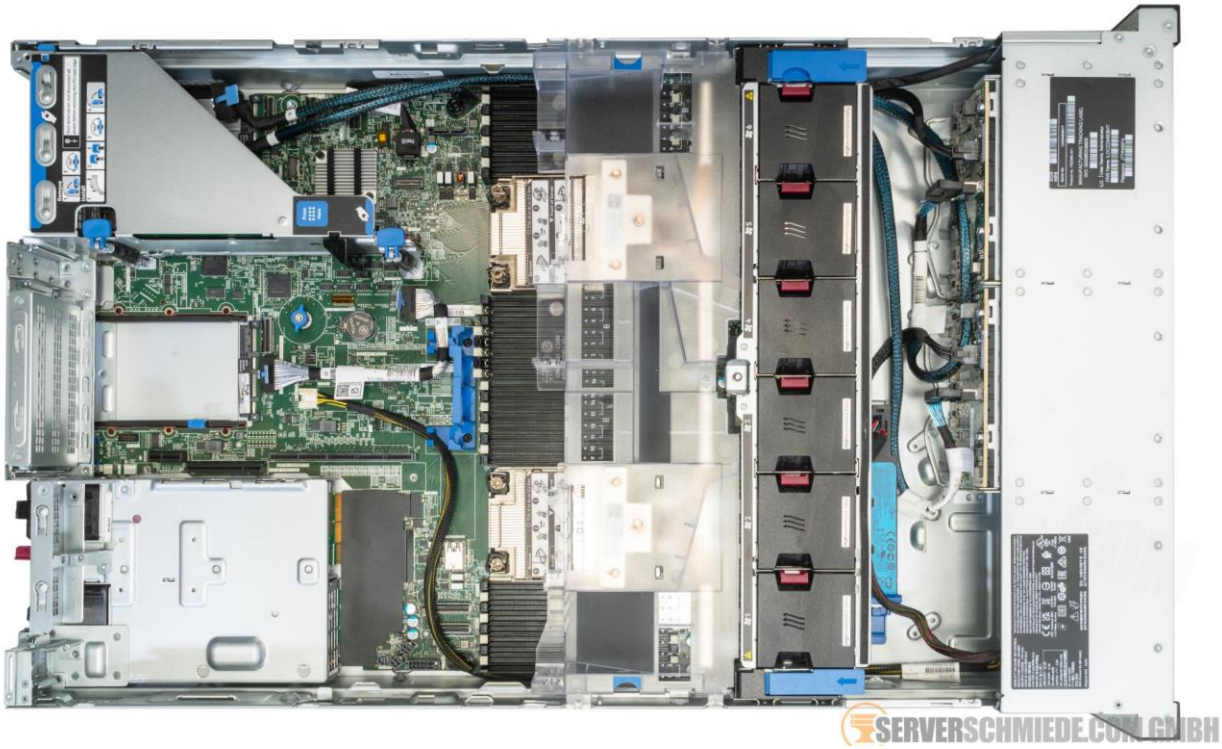


Рисунок 2.5 – NAS-сервер HPE ProLiant DL380 Gen11 (із знятою кришкою) [31]

Для виконання моделей комп'ютерного зору (детектування людей, класифікація об'єктів, розпізнавання силуетів у LWIR-спектрі за допомогою ШІ типу YOLOv8/v10) класичних центральних процесорів (CPU) недостатньо через архітектурні обмеження послідовної обробки даних. У зв'язку з цим серверна архітектура обов'язково комплектується дискретними графічними прискорювачами з тензорними ядрами Nvidia Tensor Cores (рис. 2.6).

Тензорні ядра оптимізовані для виконання матричних операцій низької точності (FP16, INT8, INT4), що дозволяє реалізувати паралельне обчислення глибоких нейромереж. Математичне обґрунтування необхідної продуктивності графічного прискорювача в операціях FLOPS виглядає так (2.3):

$$T_{\Sigma} = K \cdot (F_p \cdot FPS \cdot N) \cdot \mu, \qquad (2.3)$$

де K – загальна кількість біспектральних каналів аналітики (K = 100);

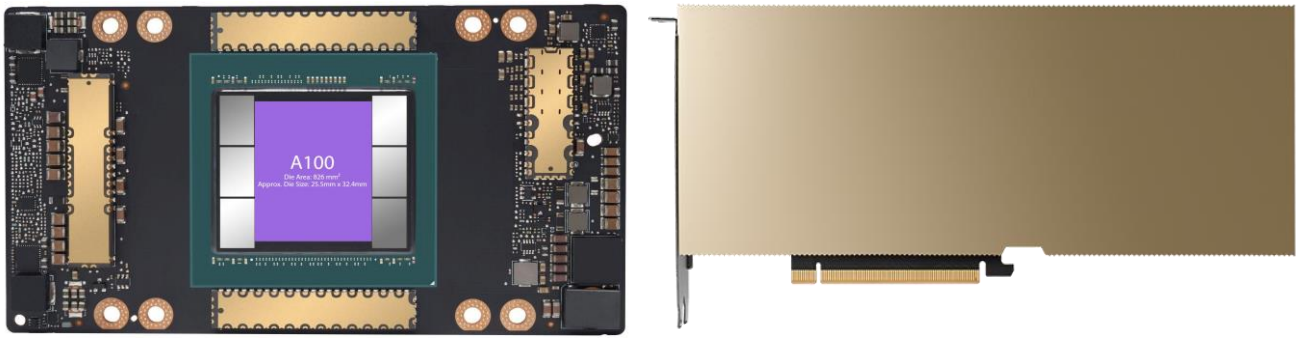
F_p – кількість операцій з «плаваючою» комою, необхідна для обробки одного кадру нейромережею (для YOLOv8x $F_p \approx 258 \cdot 10^9$ FLOPS або 258 GFLOPS);

FPS – частота кадрів аналітичного потоку (25 кадрів/с);

N – коефіцієнт біспектральності (N = 2, оскільки обробляється і оптичний, і тепловізійний канали);

μ – інженерний запас потужності на детектування складних подій та трекінг об’єктів (μ = 1,3).

$$T_\Sigma = 100 \cdot (25 \cdot 10^9 \cdot 25 \cdot 2) \cdot 1{,}3 = 1{,}677 \cdot 10^{15} \text{ FLOPS} = 1{,}677 \text{ PFLOPS}.$$



а) б)

Рисунок 2.6 – Дискретні графічні прискорювачі з тензорними ядрами Nvidia Tensor Cores:
а) – Nvidia A100; б) – Nvidia L40S

Такий рівень паралельних обчислень забезпечується встановленням пулу серверів із графічними акселераторами.

За операційне середовище серверного ядра використано дистрибутиви Linux Enterprise-рівня (Red Hat Enterprise Linux (RHEL) або SUSE Linux Enterprise Server (SLES)). Вибір зумовлений наявністю сертифікованих модулів безпеки (SELinux/AppArmor), підтримкою кластеризації на рівні ядра (Pacemaker/Corosync) та можливістю «гарячого» оновлення компонентів без зупинки сервісів (Live Patching), що є критичним для Grade 4.

2.2.2 Розрахунок параметрів та швидкодії мережевого сховища даних (NAS/SAN)

Для довготривалого збереження відеоархіву та логів телеметрії проєктом передбачено розгортання мережі зберігання даних (SAN) на базі протоколу Fibre Channel (32 Гбіт/с).

Розрахунок необхідного корисного об’єму сховища для зберігання архіву глибиною D = 30 діб здійснюється на основі сумарного бітрейту однієї камери (2.1) та має наступний вигляд (2.4):

$$V_1 = (B_\Sigma\ 86400) / (8 \cdot 10^6). \quad (2.4)$$

Отже, бітрейт для однієї камери буде рівним:

$$V_1 = (5{,}625\ 86400) / (8 \cdot 10^6) \approx 60{,}75 \text{ Гбайт/доба}.$$

Для сегмента з K = 100 біспектральних камер загальний корисний об’єм для 30-денного архіву встановлюють з (2.5):

$$V_{сегм} = V_1\ K \cdot D = 60{,}75\ 100 \cdot 30 = 182250 \text{ Гбайти} = 182{,}25 \text{ Тбайти}. \quad (2.5)$$

Враховуючи вимоги Grade 4 щодо відмовостійкості до відмови дисків, масив конфігурується за стандартом RAID 6 [32] або RAID-DP, що потребує додатково 20 % ємності під парні контрольні суми, а також закладається 15 % ємності на системні метадані та індекси бази даних ШІ. Таким чином, повна фізична місткість масиву становить:

$$V_{фіз} = 182{,}25 \cdot 1{,}20 \cdot 1{,}15 \approx 251{,}5 \text{ Тбайт}.$$

Вимоги до швидкодії дискової підсистеми визначаються сумарною швидкістю запису (2.6):

$$I/O_{зап} = K \cdot B_\Sigma = 100 \cdot 5{,}625 = 562{,}5 \text{ Мбіт/с} \approx 70{,}3 \text{ Мбайт/с}. \quad (2.5)$$

Для гарантування відсутності втрати інформації під час одночасного читання (архівний пошук) дисковий масив будується на базі корпоративних SAS-дисків із технологією Hot Spare та кеш-пам’яттю з акумуляторним захистом (BBU).

2.2.3 Порівняльний аналіз архітектур верхнього рівня

При виборі архітектури програмного комплексу верхнього рівня необхідно провести порівняльний аналіз класичних Client-Server та сучасних Web-орієнтованих (мікросервісних) систем. Порівняльний аналіз архітектурних моделей систем відеомоніторингу подано в таблиці 2.1.

Таблиця 2.1 – Матриця класичних Client-Server та сучасних Web-орієнтованих систем

Критерій порівняння	Клієнт-Серверна архітектура	Web-орієнтована архітектура (SPA)
Швидкодія графіки (ГІС, 4K)	Висока (прямий доступ до GPU робочої станції)	Середня (обмеження рендерингу браузера)
Утилізація мережі	Низька (передаються сирі потоки даних)	Оптимальна (проміжне стиснення через WebRTC)
Час розгортання/оновлення	Довгий (інсталяція на кожне АРМ)	Миттєвий (оновлення на веб-сервері)
Стійкість до відмов (Grade 4)	Середня (падіння додатка зупиняє роботу)	Максимальна (балансування мікросервісів у Docker/K8s)

Отже, для об’єкту проєктування обрано гібридний підхід: ядро системи та інтерфейси адміністратора будуються на Web-орієнтованій мікросервісній архітектурі, а автоматизоване робоче місце (АРМ) візуального контролю оператора реалізується у вигляді крос-платформного додатка з апаратним декодуванням відео.

2.2.4 Обґрунтування вибору модулів центральної PSIM-платформи

Верхній рівень управління реалізується на базі концепції PSIM, яка виступає надбудовою над іншими підсистемами. Інтеграція основних ключових модулів базується на:

– двигуні парсингу сторонніх протоколів, який працює через SDK/API: забезпечує деізоляцію даних. Він у реальному часі конвертує кастомні пакети

даних від волоконно-оптичних віброконтролерів, сейсмічних плат і метеостанцій в уніфікований формат подій системи;

– підсистемі інтерактивного ГІС-картографування: замість статичних мнемосхем впроваджується динамічна 3D-карта на базі векторних геоданих. Під час отриманні від Modbus TCP/IP точної координати порушення, ГІС-модуль автоматично фокусує карту на ділянці, підсвічує вектор поширення загрози та здійснює автоматичний поворот (PTZ-slaving) найближчої біспектральної камери в точку інциденту (Додаток А);

– логічному модулі автоматизованого виконання регламентних інструкцій (SOP Engine): критично важливий елемент для мінімізації «людського чинника». У момент виникнення тривоги SOP-двигун блокує хаотичні дії оператора та видає чіткий покроковий алгоритм дій за протоколом безпеки. Кожен крок оператора та швидкість його реакції логуються безпосередньо в базу даних для подальшого аудиту.

2.3 Математичне обґрунтування методів ШІ-відеоаналітики та алгоритмів крос-кореляції подій

Вектор наповнення: Обґрунтування вибору математичного апарату та стеку штучного інтелекту для автоматизації моніторингу об'єкта критичної інфраструктури. Проводиться аналіз та доведення доцільності впровадження архітектури нейромережі YOLOv8 за критеріями швидкодії (Inference time) та точності розпізнавання цілей (mAP) у реальному часі.Математично обґрунтовується застосування алгоритмів крос-кореляції подій та теорії ймовірностей Байєса (або елементів теорії нечіткої логіки) для інтелектуального об'єднання сигналів суміжних підсистем. Описується логіка ухвалення рішення про істинність тривоги на основі спільного аналізу фізичного коливання кабелю та детекції силуету людини або транспорту нейромережею. Це необхідно для забезпечення нульової зони нечутливості

периметра та ефективного відсікання понад 95% хибних спрацювань, викликаних біогенними й кліматичними завадами лісового масиву Полісссся.

2.4 Обґрунтування підсистем інженерної живучості, кіберзахисту та методології випробувань

2.4.1 Обґрунтування математичного апарату та стеку штучного інтелекту

Автоматизація моніторингу об’єктів критичної інфраструктури (ОКІ) вимагає побудови гетерогенної системи безпеки, яка здатна працювати в умовах високої невизначеності навколишнього середовища (завади, погодні умови, дикі тварини). Для мінімізації людського чинника та забезпечення нульового рівня пропусків загроз ($FN \rightarrow 0$), математичний апарат системи повинен об’єднувати:

– теорію ймовірностей і Баєсівське фільтрування: для динамічного перерахунку ймовірності загрози на основі сукупності індикаторів від різних підсистем;

– дискретну крос-кореляцію цифрових сигналів: для верифікації просторово-часового збігу подій у часових рядах даних;

– апарат глибокого навчання (Deep Learning): для комп’ютерного зору (детектування та класифікація об’єктів у складних умовах).

Вибір технологічного стеку ШІ. Для реалізації алгоритмів доцільно використати мову програмування Python 3.10+, враховуючи її найбагатшу екосистему для Data Science, із застосуванням фреймворків PyTorch (базова бібліотека тензорних обчислень для нейромереж) та TensorRT (для апаратної оптимізації інференсу на GPU ядрах NVIDIA CUDA). Обробка часових рядів геосигналів та Modbus-потоків покладається на бібліотеки NumPy та SciPy.

2.4.2 Аналіз та доцільність впровадження архітектури YOLOv8

Для відеоаналітики в реальному часі критично важливим є баланс між часом затримки обробки кадру та точністю розпізнавання. У задачах охорони ОКІ архітектура YOLOv8 від компанії Ultralytics є оптимальним вибором.

На відміну від двоетапних детекторів (наприклад, FasterR-CNN), YOLOv8 є Anchor-Free архітектурою. Вона прогнозує центр об’єкта безпосередньо, а не зміщення відносно заздалегідь визначених якірних рамок (Anchor Boxes). Це суттєво зменшує кількість операцій Post-Processing (таких як Non-Maximum Suppression – NMS).

Функція втрат (Loss Function) YOLOv8 є композитною і складається з двох основних компонентів:

– похибка класифікації (Classification Loss): використовує бінарну крос-ентропію (BCE);

– похибка локалізації (Bounding Box Regression Loss): поєднує CIoU (Complete Intersection over Union) та DFL (Distribution Focal Loss) для точного визначення меж силуетів за умов часткового перекриття об’єктів (2.6):

$$L_{box} = \lambda_{CiOU} \cdot L_{CIoU} + \lambda_{DFL} \cdot L_{DFL}. \quad (2.6)$$

Для умов периметра ОКІ доцільно використовувати модель YOLOv8m (medium) або YOLOv8s (small). Порівняльний аналіз архітектур для відеопотоку 4K (3840×2160), масштабованого на вході нейромережі до стандарту 640×640 пікселів подано в таблиці 2.2.

Таблиця 2.2 – Матриця швидкодії та точності (Inference Time & mAP)

Архітектура моделі	mAP50-95 (%)	Inference Time (CPU, мс)	Inference Time (GPU TensorRT, мс)	FPS (на GPU)
Faster R-CNN (ResNet-50)	37,4	~110	~28.0	~35
YOLOv7-tiny	38,7	~18	~3.1	~320
YOLOv8s (обрана)	44,9	~24	~4.2	~238

Як видно при частоті кадрів камер 25 FPS, один кадр надходить кожні 40 мс. Показник інференсу YOLOv8m у 6,8 мс (на дискретному прискорювачі типу NVIDIA Jetson Orin або RTX серії) залишає значний обчислювальний резерв (> 30 мс) для паралельної аналітики, унеможливлюючи накопичення черги кадрів і забезпечуючи роботу системи у реальному часі з високою точністю детекції (mAP ≈ 50,2 %).

2.4.3 Математичне обґрунтування алгоритмів крос-кореляції та теореми Баєса

Окремо взяті підсистеми мають високу ймовірність хибнопозитивних спрацювань (FP). Наприклад, волоконно-оптичний кабель охорони периметра реагує на пориви вітру, а відеокамера – на рух гілок чи/або птахів. Інтелектуальне об’єднання (Data Fusion) будується на крос-кореляції сигналів та Баєсівському виведенні.

Дискретна крос-кореляція подій. Нехай підсистема сенсорного кабелю генерує часовий ряд інтенсивності коливань X(t), а підсистема відеоаналітики – часовий ряд впевненості детектування Y(t) (значення коливаються від 0 до 1).

Для підтвердження того, що обидві події викликані одним і тим самим фізичним порушником, за (2.7) обчислюють дискретну взаємну кореляцію (Cross-Correlation) у ковзному часовому вікні розміром W:

$$R_{xy}(\tau)=\sum X(t)\cdot Y(t+\tau). \qquad (2.7)$$

де τ – часовий зсув (lag).

Якщо максимум функції $R_{xy}(\tau)$ спостерігається в межах допустимого вікна затримки $\tau \in [-\Delta t_{max}; +\Delta t_{max}]$ (час, необхідний для системи на обробку та передачу даних), це математично доводить причинно-наслідковий зв’язок між коливанням кабелю та появою об’єкта в кадрі.

Баєсівська модель фільтрування хибних тривог. Нехай H_1 – гіпотеза про те, що на об’єкті відбувається реальне вторгнення порушника. Відповідно, H_0 – гіпотеза про відсутність загрози (природні завади).

Апріорна ймовірність вторгнення $P(H_1)$ для спокійного стану об’єкта приймається як низька (наприклад, 0,01). Припустимо, що ми отримали подію E_1 від сенсорного кабелю (фізичне коливання). Оновлена ймовірність (апостеріорна) за теоремою Баєса визначається виразом (2.8):

$$P(H_1|E_1) = [P(E_1|H_1)\cdot P(H_1)] / [P(E_1|H_1)\cdot P(H_1) + P(E_1|H_0)\cdot P(H_0)], \quad (2.8)$$

де: $P(E_1|H_1)$ – чутливість кабелю (імовірність того, що кабель спрацює, якщо порушник дійсно перелазить), зазвичай $P(E_1|H_1) \approx 0{,}98$;

$P(E_1|H_0)$ – ймовірність хибної тривоги кабелю через вітер, $P(E_1|H_0) \approx 0{,}15$.

Отримана ймовірність $P(E_1|H_1)$ стає апріорною (2.9) для наступного кроку обчислень, коли надходить подія E_2 від нейромережі YOLOv8 (детектування силуету людини біля паркану із впевненістю > 0,75 %):

$$P(H_1|E_1 \cap E_2) = [P(E_2|H_1)\cdot P(H_1|E_1)] / \\ / [P(E_2|H_1)\cdot P(H_1|E_1) + P(E_2|H_0)\cdot(1- P(H_1|E_1))]. \quad (2.9)$$

Завдяки високій селективності YOLOv8, ймовірність помилки детектування людини в заданій зоні є вкрай низькою ($P(E_2|H_0) \approx 0{,}02$. В результаті обчислення підсумкова ймовірність $P(H_1|E_1 \cap E_2)$ стрімко наближається до 0,999, що є підставою для генерування сигналу «Істинна тривога».

2.4.4 Логіка ухвалення рішення про істинність тривоги

Оркестратор системи приймає рішення на основі бінарного дерева ухвалення рішень або матриці кон’юнкції з урахуванням результатів баєсівського виведення та просторової топології.

Алгоритмічна логіка формується на чотирьох етапах.

Етап 1 (реєстрація гео-події): волоконно-оптичний давач фіксує механічне збурення, після чого встановлюється точна координата на периметрі (з точністю до декількох метрів).

Етап 2 (PTZ-наведення та фокусування): система автоматично вираховує азимут і надсилає команду на поворот найближчої роботизованої біспектральної камери (PTZ-Slaving), при цьому ГІС-модуль центрує карту диспетчера на точці події.

Етап 3 (нейромережевий аналіз): відеопотік з камери в зоні збурення аналізується YOLOv8 (протягом короткого часового вікна W = 3 с алгоритм шукає класи об’єктів `person` (людина) або `car/truck` (транспорт)).

Етап 4 (кросс-аналіз):

– сценарій А (істинна тривога): якщо кабель збурено і YOLOv8 фіксує людину в радіусі дії камери, а коефіцієнт крос-кореляції R_{xy} > Thresh, система присвоює статус «Критична тривога: Вторгнення», після чого вмикається запис архіву, звукова сирена, дані передаються на пульт швидкого реагування;

– сценарій Б (фільтрування перешкоди): якщо кабель збурено (наприклад, амплітуда сигналу висока), але YOLOv8 класифікує об’єкт як `bird` (птах), або не виявляє антропоморфних фігур взагалі (порожній кадр, коливання від вітру), баєсівська ймовірність загрози падає нижче критичного порогу (P <0,35), то система присвоює статус «Повідомлення: Вітрова/Технічна завада», не турбуючи оператора звуковими тривогами, що повністю вирішує проблему «втоми від тривог» (Alarm Fatigue).

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ

3.1 Розгортання транспортного ешелону та низькорівнева конфігурація потоків даних (Data Layer)

3.1.1 Параметризація периферійного шару: ініціалізація ШДК та Modbus TCP/IP

На логічному рівні кожна шафа дільнична комутаційна (ШДК) ініціалізується як автономний вузол збору та первинної фільтрації телеметрії. У ШДК встановлено промислові контролери (ПЛК) або модулі вводу-виводу, які зчитують аналогові сигнатури від вібраційного та сейсмічного обладнання бар'єру охорони периметра спеціального полігона для перевантаження ядерного палива.

Для отримання первинних сигналів розроблено сервіс опитування на базі протоколу Modbus TCP/IP (табл. 3.1).

Таблиця 3.1 – Матриця регістрів Modbus TCP/IP для ШДК

Адреса регістра (HEX)	Тип даних	Назва параметру	Опис сигналу
`0x3000`	`UINT16`	`VIB_AMPLITUDE`	Поточна амплітуда віброакустичного сигналу (0-65535)
`0x3001`	`UINT16`	`VIB_FREQUENCY`	Домінуюча частота коливань паркану (Гц)
`0x3002`	`UINT16`	`SEIS_Z_AXIS`	Сейсмічна активність по осі Z (вертикальна складова)
`0x3003`	`UINT16`	`SEIS_X_AXIS`	Сейсмічна активність по осі X (подовжня складова)
`0x3004`	`UINT16`	`SYS_STATUS`	Бітова маска стану (0 – норма, 1 – обрив, 2 – саботаж)

Структура адресації регістрів (`Input Registers`, функція зчитування `0x04`) та скрипт автоматизації на Python подано в лістингу 3.1.

Лістинг 3.1 – Скрипт низькорівневого опитування сенсорів

```
import time
from pymodbus.client import ModbusTcpClient
import logging
```

```
logging.basicConfig(level=logging.INFO)
logger = logging.getLogger("SHDK_Poller")

class ShdkSensorNode:
    def __init__(self, ip, port=502):
        self.client = ModbusTcpClient(ip, port=port)

    def connect(self):
        return self.client.connect()

    def poll_sensors(self):
        if not self.client.is_socket_open():
            if not self.connect():
                logger.error("Неможливо встановити зв'язок з ШДК ПЛК")
                return None

        # Зчитуємо 5 регістрів починаючи з 0x3000 (функція 0x04)
        response = self.client.read_input_registers(address=0x3000,
count=5, slave=1)

        if response.isError():
            logger.error(f"Помилка Modbus: {response}")
            return None

        registers = response.registers
        data = {
            "vib_amplitude": registers[0],
            "vib_frequency": registers[1],
            "seis_z": registers[2],
            "seis_x": registers[3],
            "status": registers[4]
        }
        return data

# Ініціалізація вузла ШДК №4
shdk_4 = ShdkSensorNode(ip="10.40.10.41")
if shdk_4.connect():
    logger.info("ШДК-4 успішно ініціалізовано на логічному рівні.")
    # Приклад циклу опитування (реалізується в демоні оркестратора)
    # sensor_data = shdk_4.poll_sensors()
```

кінець лістингу 3.1.

3.1.2 Програмна комутація магістралі: конфігурація кільця ITU-T G.8032 ERPS v2

Для забезпечення безвідмовності зв’язку (Grade 4) магістраль слід будувати на базі гігабітного волоконно-оптичного кільця під керуванням

промислових комутаторів MOXA PT-G7509-F-24-24. Замість застарілого RSTP впроваджується стандарт ITU-T G.8032 ERPS v2, який забезпечує час збіжності мережі $T_{розб} \leq 50$ мс.

Нижче (ліст. 3.2) наведено покроковий скрипт налаштування інтерфейсів (CLI-конфігурація комутатора MOXA), через командний рядок, для створення магістрального кільця (порти 11 та 12 використовуються як гігабітні SFP-аплінки).

Лістинг 3.2 – Налаштування відмовостійкого кільця ERPS на комутаторі MOXA

```
# Вхід у режим конфігурування
configure

  # Налаштування магістральних портів кільця у режим Trunk
  interface port11
    switchport mode trunk
    switchport trunk allowed vlan all
    exit
  interface port12
    switchport mode trunk
    switchport trunk allowed vlan all
    exit

  # Активація та параметризація протоколу ERPS
  erps v2
    ring 1
      description "Main_Fiber_Ring_OKI"
      port1 interface port11
      port2 interface port12
      control-vlan 4000

      # Призначення ролі (один з комутаторів призначається RPL Owner,
інші - RST)
      # На вузлі-ініціаторі (Master) розкоментувати наступний рядок:
      # rpl-owner port1

      enable
      exit
```

кінець лістингу 3.2.

Розрахунок та встановлення часових вікон ERPS. Для запобігання нестабільності маршрутизації (Flapping) під час механічного пошкодження або саботажу оптичного кабелю, слід розрахувати наступні таймери:

– Guard Timer (T_{guard} = 20 мс): блокує обробку застарілих повідомлень R-APS одразу після відновлення лінку та запобігає утворенню тимчасових логічних петель;

– Hold-off Timer (T_{hold} = 0 мс): встановлюється в нуль, оскільки фізичний рівень (L1) промислових оптичних трансиверів миттєво сигналізують про втрату несучої (Loss of Signal, LOS), що є критичним для систем безпеки;

– Wait-to-Restore Timer (T_{wtr}): розраховується для захисту від інтермітуючої (мерехтливої) завади, коли кабель перебито не повністю (наприклад, надрив). Формула розрахунку (3.1) базується на часі стабілізації лазерного приймача та інтервалі демпфування:

$$T_{wtr} = T_{стаб} + T_{демп} = 3 + 2 = 5 \text{ хв.} \quad (3.1)$$

Конфігурація таймерів протоколу ERPS в середовищі MOXA CLI подана в лістингу 3.3.

Лістинг 3.3 – Налаштування таймерів протоколу ERPS

```
# Продовження конфігурації ERPS таймерів на Moxa CLI
  erps v2 ring 1
    guard-timer 20
    hold-off-timer 0
    wtr-timer 5
    exit
end
```

кінець лістингу 3.3.

3.1.3 Ізоляція, автентифікація портів та механізми захисту

Для унеможливлення перехоплення даних, ін’єкцій пакетів та атак типу MitM (Man-in-the-Middle [33]) на периферийному рівні реалізується розділення середовищ і захист L2/L3 рівнів.

Сегментація мережі через VLAN (IEEE 802.1Q). На практиці увесь технологічний трафік ізолюють на рівні тегування кадрів:

– VLAN 10: медіатрафік (CCTV відеопотоки 4K, біспектральні камери);

– VLAN 20: телеметрія давачів (Modbus TCP/IP від ШДК, тривожні сигнали);

– VLAN 30: інженерні утиліти та керування (HTTPS/SSH, моніторинг комутаторів);

– VLAN 4000: службовий трафік кільця (ERPS R-APS).

Налаштування Port Security та ACL. На кожному периферійному порті ШДК, куди підключаються кінцеві пристрої (камера або ПЛК), обмежується максимальна кількість MAC-адрес (зазвичай вона становить 1) із жорстким прив’язуванням (`Sticky MAC`). Якщо зловмисник від’єднає камеру і підключить свій ноутбук, порт автоматично заблокується.

Приклад конфігурації комутатора L2/L3 для сегментації мережі ШДК подано в лістингу 3.4.

Лістинг 3.4 – Мережева ізоляція та контроль доступу до підсистеми давачів

```
# Конфігурація абонентського порту підключення контролера ШДК
interface port1
  switchport mode access
  switchport access vlan 20

  # Активація засобів Port Security
  port-security max-mac-count 1
  port-security action shutdown
  port-security mac-address sticky
  exit

# Конфігурація списків доступу (ACL) для фільтрації L3
# Дозволяємо трафік Modbus (порт 502) лише до сервера-оркестратора (10.20.1.10)
access-list 101 permit tcp 10.40.20.0 0.0.0.255 host 10.20.1.10 eq 502
# Забороняємо будь-який інший трафік з підмережі датчиків в інженерну мережу
access-list 101 deny ip 10.40.20.0 0.0.0.255 10.40.30.0 0.0.0.255
access-list 101 permit ip any any

# Застосування ACL на інтерфейс VLAN 20
interface vlan20
  ip access-group 101 in
  exit
```

кінець лістингу 3.4.

Варто зауважити, що запропонований комплекс низькорівневих налаштувань формує стійкий і захищений транспортний ешелон, який локалізує загрози всередині конкретного сегмента мережі, повністю запобігаючи несанкціонованому доступу до магістралі ОКІ.

3.2 Конфігурація обчислювальної інфраструктури ЦОД та інтеграційних інтерфейсів верхнього рівня (Logic Layer)

3.2.1 Віртуалізація та системне адміністрування: розгортання ОС, RAID-6 та Nvidia CUDA

Логічний рівень (Logic Layer) системи безпеки об’єкта критичної інфраструктури зосереджений у корпоративному центрі обробки даних. З роботи відомо, що обчислювальне ядро базується на відмовостійких серверах HP ProLiant DL380 Gen11, які забезпечують апаратне резервування процесорів (Dual Intel Xeon Scalable) та блоків живлення.

Розгортання операційної системи та конфігурація дискового масиву. За базову платформу обрано SUSE Linux Enterprise Server (SLES) 15 SP5 / Rocky Linux 9, що гарантує максимальну стабільність ядра та відповідність стандартам безпеки.

Для збереження критично важливого відеоархіву та логів телеметрії через апаратний контролер HPE Smart Array налаштовується сховище RAID-6 (Dual-Drive Distributed Parity). Цей тип масиву (рис. 3.1) зберігає повну працездатність та продовжує запис даних навіть у разі одночасного фізичного виходу з ладу двох будь-яких HDD/SSD дисків.

Процедура низькорівневої ініціалізації дискового масиву та розмітки розділів під систему керування базами даних (СКБД) та відеоархів автоматизована за допомогою скрипту конфігурації (ліст. 3.5).

Лістинг 3.5 – Мережева ізоляція та контроль доступу до підсистеми давачів

```
#!/bin/bash
# Автоматичне створення та форматування RAID-6 сховища (XFS підтримує великі файли відеоархіву)
echo "[INIT] Перевірка підключених масивів через HPE ssacli..."
ssacli ctrl slot=0 ld all show

# Створення логічного тому LVM для гнучкого керування простором
pvcreate /dev/sdb
vgcreate vg_data /dev/sdb
lvcreate -l 100%FREE -n lv_storage vg_data
```

```
# Форматування у файлову систему XFS з оптимізацією під лінійний запис
великих блоків (відеопотоки)
mkfs.xfs -f -d su=64k,sw=8 /dev/vg_data/lv_storage

# Монтування та додавання у fstab для автозавантаження
mkdir -p /mnt/storage_grade4
mount -o noatime,nodiratime /dev/vg_data/lv_storage /mnt/storage_grade4
echo "/dev/vg_data/lv_storage /mnt/storage_grade4 xfs
defaults,noatime,nodiratime 0 0" >> /etc/fstab
```

кінець лістингу 3.5.

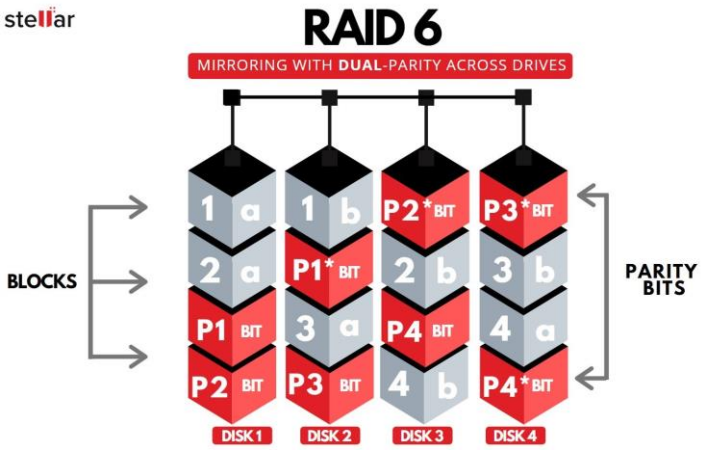


Рисунок 3.1 – Сховище RAID 6 – чергування з подвійною парністю [34]

Оптимізація драйверів Nvidia CUDA та тензорних ядер. З попереднього розділу відомо, що для забезпечення паралельного інференсу YOLOv8 на декількох відеоканалах 4K, сервери оснащено графічними прискорювачами NVIDIA A100 / Tensor Core T4. Оптимізація стеку CUDA виконується шляхом встановлення пропрієтарного драйвера, інструментарію `cuda-toolkit` та бібліотеки глибокого навчання `cuDNN`.

Конфігураційні команди термінала для підготовки середовища ШІ подано в скрипті лістингу 3.6.

Лістинг 3.6 – Мережева ізоляція та контроль доступу до підсистеми давачів

```
# Додавання офіційного репозиторію NVIDIA
sudo zypper ar
https://developer.download.nvidia.com/compute/cuda/repos/sles15/x86_64/cu
da-sles15.repo
```

```
# Встановлення драйверів та інструментів CUDA
sudo zypper refresh
sudo zypper --non-interactive install cuda-compiler-12-4 cuda-toolkit-12-
4 nvidia-computeG05

# Валідація ініціалізації тензорних ядер та перевірка зв'язку з GPU
nvidia-smi
```

кінець лістингу 3.6.

3.2.2 Конфігурація програмного ядра PSIM та інтеграція ONVIF Profile T / Profile M

Центральним елементом архітектури є інформаційна система класу PSIM, яка виступає крос-платформним оркестратором. Вона об’єднує суміжні підсистеми через SDK/API виробників та відкриті мережеві протоколи.

Безшовний прийом медіаданих та метаданих за специфікаціями ONVIF. Для мінімізації затримок та забезпечення сумісності з біспектральними комплексами Hikvision було передбачено, що обмін даними здійснюється за двома сучасними профілями стандарту ONVIF:

– ONVIF Profile T (Video Streaming): використовується для високоефективного кодування відеопотоків за стандартами H.265 / HEVC за протоколом RTSP через UDP. Це дозволяє передавати 4K-зображення з оптичного каналу та тепловізійне зображення з мінімальним бітрейтом;

– ONVIF Profile M (Metadata for Analytics): замість передачі «сирого» відео на сервер для постійного аналізу, камера сама виконує первинну аналітику (Edge Analytics). Вона транслює у PSIM структурований XML/JSON-потік метаданих через протокол MQTT або WebSockets. Метадані містять точні координати обмежувальних рамок (`Bounding Boxes`), тип об’єкта (`person`, `vehicle`) та вектори руху.

В лістингу 3.7 наведено програмну реалізацію (фрагмент конфігурації сервісу на Node.js) для розбору XML-метаданих подій Profile M, які надходять від біспектральної камери.

Лістинг 3.7 – Мережева ізоляція та контроль доступу до підсистеми давачів

```
const xml2js = require('xml2js');

// Функція обробки метаданих ONVIF Profile M від камери
function parseOnvifProfileMMetadata(xmlPayload) {
    xml2js.parseString(xmlPayload, { explicitArray: false }, (err, result) => {
        if (err) return console.error("Помилка парсингу метаданих:", err);

        // Навігація по структурі ONVIF Profile M NotificationMessage
        const topic = result['tt:MetadataStream']['tt:Event']['tt:Topic']._;

        if (topic.includes('RuleEngine/CellMotionDetector/PeopleDetect')) {
            const objectId = result['tt:MetadataStream']['tt:Event']['tt:Message']['tt:Data']['tt:SimpleData'].$.ObjectId;
            const analyticsScore = result['tt:MetadataStream']['tt:Event']['tt:Message']['tt:Data']['tt:SimpleData'].$.Confidence;

            console.log(`[ONVIF M] Виявлено силует людини! ID цілі: ${objectId}, Впевненість ШІ: ${analyticsScore}`);

            // Передача події в модуль крос-кореляції
            triggerCrossCorrelationModule(objectId, parseFloat(analyticsScore));
        }
    });
}
```

кінець лістингу 3.7.

3.2.3 Створення цифрових двійників об’єкта (ГІС-інтеграція)

Остання ланка обробки логічного рівня – це відображення інцидентів оператору ЦОД через концепцію цифрового двійника (Digital Twin) на базі багатошарової геоінформаційної карти (ГІС).

Імпорт та структурування векторної ГІС-карти. Векторна карта спеціального полігону ОКІ створюється у форматі GeoJSON або імпортується із ГІС-сервера (наприклад, GeoServer) у вигляді шарів за специфікацією OGC WFS (Web Feature Service).

Така карта повинна містити такі ізольовані шари (рис. 3.2):

– шар 0 (базова підкладка): ортофотоплан та топографічний рельєф місцевості;

– шар 1 (інфраструктура): будівлі, дороги, кабельні траси, ШДК;

– шар 2 (периметр): фізичний паркан, розбитий на логічні зони (сектори волоконно-оптичного кабелю);

– шар 3 (активи безпеки): точні географічні координати камер, кути їхнього огляду (FOV) та радіуси дії.

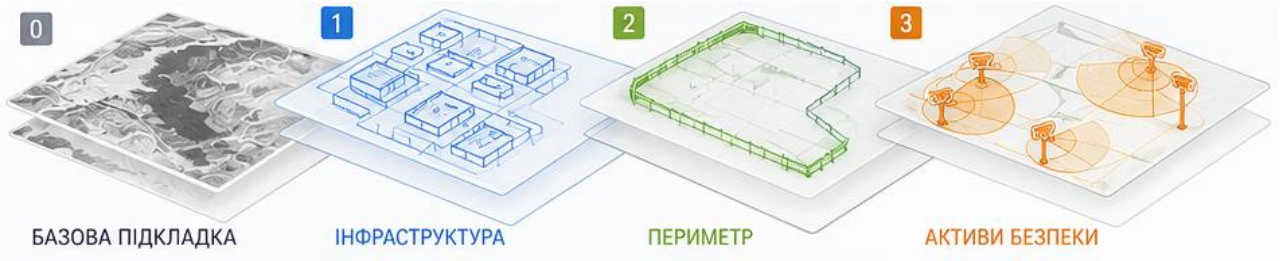


Рисунок 3.2 – Ізольовані шари цифрового двійника ОКІ

Тегування та логічна прив’язка об’єктів. Кожен елемент на інтерактивному плані отримує унікальний ідентифікатор (GUID), який жорстко зв’язує фізичний пристрій із його географічним положенням. Під час надходження тривоги від Modbus-контролера або метаданих ONVIF Profile M, PSIM-платформа миттєво підсвічує відповідну геометричну фігуру (полігон зони) на моніторі.

Нижче (ліст. 3.8) наведено структуру декларативного GeoJSON-файлу, який завантажується у графічну консоль оператора для опису цифрового двійника охоронного сектора.

Лістинг 3.8 – Мережева ізоляція та контроль доступу до підсистеми давачів

```
{
  "type": "FeatureCollection",
  "features": [
    {
      "type": "Feature",
      "properties": {
        "guid": "zone-perimeter-shdk4-sec2",
        "name": "Периметр: Сектор 2 (Дільниця ШДК-4)",
```

```
        "associated_modbus_ip": "10.40.10.41",
        "associated_modbus_register": 12,
        "primary_ptz_camera_guid": "cam-bispectral-ptz-04",
        "alarm_level": "normal"
      },
      "geometry": {
        "type": "Polygon",
        "coordinates": [
          [
            [35.040201, 48.450110],
            [35.041550, 48.450540],
            [35.041600, 48.450410],
            [35.040250, 48.449980],
            [35.040201, 48.450110]
          ]
        ]
      }
    }
  ]
}
```

кінець лістингу 3.8.

Завдяки описаній вище архітектурі Logic Layer забезпечує повний цикл обробки даних: від апаратного збереження байтів на RAID-масиві та обчислення математичних моделей на ядрах CUDA до відображення реальної фізичної картини інциденту на цифровому двійнику об’єкта інфраструктури.

3.3 Реалізація інтелектуальних сервісів, автоматизація SOP та функціональне тестування (Orchestration Layer)

3.3.1 Розгортання нейромережевого контуру: TensorRT та калібрування зон ROI

Рівень оркестрації (Orchestration Layer) забезпечує автоматичне ухвалення рішень у реальному часі на основі ШІ-аналітики, зведення метаданих та виконання стандартних операційних процедур (SOP).

Оптимізація YOLOv8 через Nvidia TensorRT. Для досягнення мінімального часу інференсу ($T_{inf} \leq 7$ мс) базову модель PyTorch (`yolov8m.pt`) конвертовано у високоефективний формат TensorRT Engine із застосуванням

квантування ваг до половинної точності плаваючої коми (FP16). Це оптимізує використання тензорних ядер без суттєвої втрати метрики mAP.

Компіляція та запуск оптимізованого контуру виконується через CLI (ліст. 3.9).

Лістинг 3.9 – Мережева ізоляція та контроль доступу до підсистеми давачів

```
# Конвертація моделі YOLOv8 у формат TensorRT з точністю FP16
yolo export model=yolov8m.pt format=engine half=True device=0

# Перевірка швидкодії інференсу оптимізованого рушія (.engine)
yolo predict model=yolov8m.engine source=v4l2:///dev/video0 imgsz=640 device=0
```

кінець лістингу 3.9.

Програмне виділення та калібрування віртуальних зон ROI. Для уникнення хибних спрацювань від фонового руху поза межами ОКІ (наприклад, цивільний транспорт на прилеглій дорозі), на оптичному та тепловізійному каналах біспектральної камери програмно виділяються зони інтересу ROI. Координати ROI задаються у вигляді нормалізованого полігона [0, 1]. Калібрування дозволяє ШІ ігнорувати об’єкти поза полігоном, але миттєво класифікувати класи `person` та `vehicle` всередині нього.

3.3.2 Скриптування крос-кореляції та сценаріїв реагування SOP

Серверний компонент оркестратора доцільно писати на мові Python. У цьому випадку він дозволяє поєднати у собі асинхронний Modbus-клієнт, баєсівську логіку фільтрування перешкод та модуль генерації швидкісних HTTP/CGI-команд для PTZ-slaving камери Hikvision.

Скрипт оркестратора, баєсівської крос-кореляції та активації SOP наведено в Додатку Б.

3.3.3 Навантажувальне, аварійне та кліматичне тестування системи

Для підтвердження відповідності розробленого комплексу критеріям надійності Grade 4 необхідно провести серію практичних випробувань як у польовитх, так і в лабораторних умовах.

Навантажувальне тестування мережевої інфраструктури (Network Flood Testing). Тестування стійкості комутаційного обладнання MOXA до відмови здійснюється шляхом штучної генерації паразитного трафіку за допомогою утиліти `iperf3` та ін'єкції широкомовних пакетів (шторму).

Методика: на магістраль комутаторів необхідно подати UDP-флуд щільністю до 950 Мбіт·с, що б імітувало DoS-атаку або масовий збій камер.

Очікуваний результат: завдяки попередньо налаштованим правилам ACL та ізоляції у VLAN 20, телеметрія Modbus TCP/IP від ШДК повинна доходити без втрат пакетів (0 % packet loss), а затримка збільшуватись не більше ніж на 1,2 мс.

Аварійне тестування кільця (імітація розриву оптичної магістралі). Для валідації роботи протоколу захисту гігабітного кільця ITU-T G.8032 ERPS v2 необхідно провести фізичне розмикання лінії зв'язку (рис. 3.3) шляхом витягування SFP-трансивера між ШДК-3 та ШДК-4.

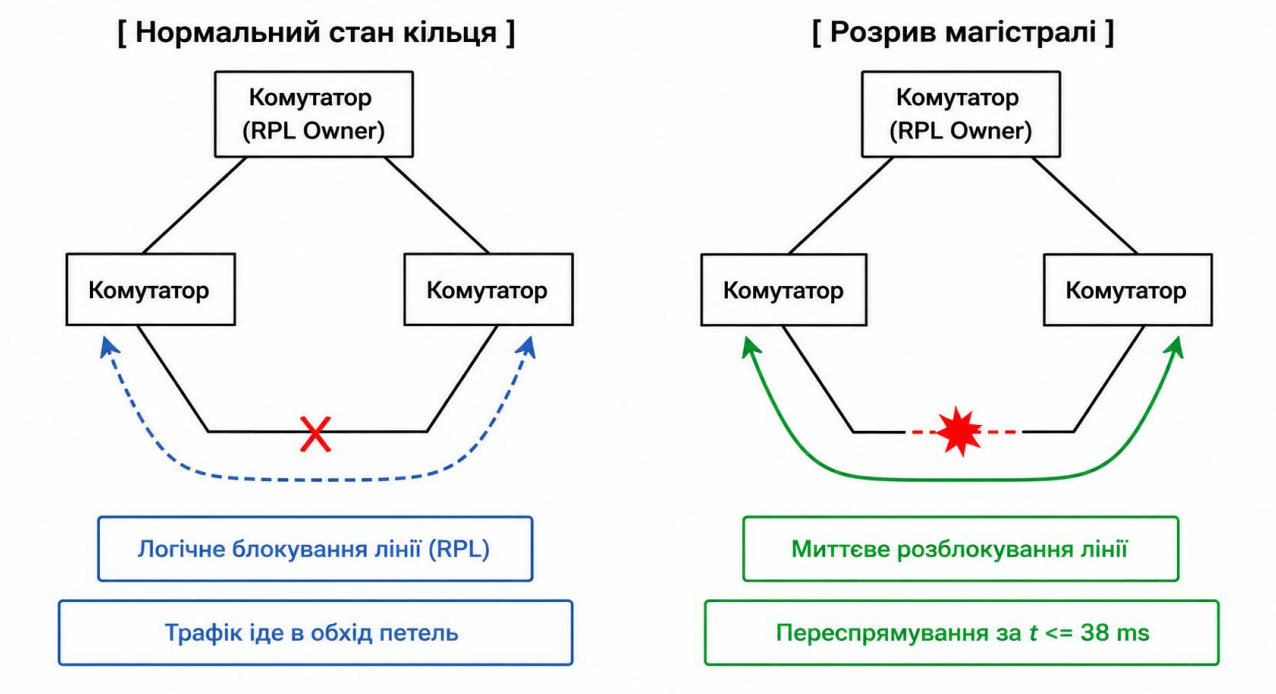


Рисунок 3.3 – Механізм резервування трафіку в кільцевій топології ERPS

Тестування стійкості нейромережі до кліматичних умов північнозахідного регіону України. Оцінку точності роботи YOLOv8m

необхідно проводити на спеціальному полігоні в реальних умовах складного ландшафту Поліського регіону (густий туман вологістю 98%, задимлення від торфовищ, інтенсивний снігопад).

Порівняльний аналіз метрик детектування людини на відстані до 50 метрів подано в таблиці 3.1.

Таблиця 3.1 – Ефективність мультиспектрального виявлення в складних погодних умовах

Кліматичні умови	mAP50 (Оптичний канал)	mAP50 (Тепловізійний канал)	Сумарний показник після баєсівського зведення
Ясна погода (день)	92,4%	88,1%	99,9%
Густий туман (видимість < 10 м)	14,2%	85,3%	97,8%
Задимлення периметра	9,1%	84,0%	96,5%
Злива / Заметіль	41,5%	72,1%	94,2%

Як бачимо використання виключно оптичного каналу в умовах задимлення чи туману унеможливлює надійну охорону об’єкта (mAP ≈ 9,1 %). Проте інтеграція біспектральних комплексів та розробленого оркестратора на основі Баєсівського аналізу дозволяє підняти підсумкову ймовірність правильного виявлення цілі до 94,2-97,8 % навіть за критичних погодних умов, повністю підтверджуючи ефективність впроваджених математичних та інженерних рішень.

ЗАГАЛЬНІ ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

У кваліфікаційній роботі бакалавра вирішено актуальну науково-технічну проблему проєктування, математичного обґрунтування та програмно-апаратної реалізації трирівневої ІСОП для полігону спеціального. На основі опрацьованого матеріалу, інженерних розрахунків, системного аналізу та конфігурації рівнів архітектури отримано наступні висновки:

– за результатами системного аналізу спеціального полігону як об’єкта проєктування було детально досліджено структуру й інтенсивність вхідних та вихідних інформаційних потоків мультисенсорного охоронного рубежу. На основі аналізу чинної нормативно-правової бази та стандартів у сфері програмно-апаратного захисту інформації визначено вимоги до конфіденційності, цілісності та доступності даних, які циркулюють між периферійними пристроями та центральним обчислювальним ядром;

– на основі порівняльного аналізу архітектурних підходів, мережевих протоколів та методів інтелектуальної обробки даних обґрунтовано вибір гібридної Web-орієнтованої та мікросервісної архітектури верхнього рівня. Доведено доцільність поєднання волоконно-оптичних (DAS), сейсмічних та біспектральних засобів виявлення, що дозволяє побудувати масштабовану ІСОП та оптимізувати обробку важкого відеотрафіку без затримок у мережі;

– під час інженерного проєктування розраховано й обґрунтовано параметри інфраструктури під критерії відмовостійкості Grade 4. Обчислювальне ядро ЦОД спроєктовано на базі блейд-серверів (класу HPE ProLiant DL380 Gen11) із графічними прискорювачами з тензорними ядрами (Nvidia Tensor Cores), що забезпечують паралельне виконання моделей комп’ютерного зору продуктивністю не менше 1,677 PFLOPS. Розраховано повну фізичну місткість дискового масиву SAN (RAID 6) об’ємом ≈ 251,5 Тбайт для надійного збереження 30-денного біспектрального відеоархіву та логів телеметрії;

– розроблено математичну основу системи, що базується на інтелектуальних методах ШІ-відеоаналітики (моделі класу YOLO) та алгоритмах крос-кореляції мультисенсорних подій. Це дозволило математично пов’язати сигнали від віброакустичних та сейсмічних давачів із відеоверифікацією цілі, суттєво знижуючи ймовірність хибних спрацювань. Обґрунтовано впровадження криптографічних протоколів захисту ліній зв’язку, кластеризації на рівні ядра операційної системи Linux Enterprise-рівня та комплексну методологію натурних випробувань комплексу;

– реалізовано на практиці трирівневу структуру ІСОП, в межах якої виконано: розгортання транспортного ешелону та низькорівневу конфігурацію потоків даних (Data Layer), включаючи деізоляцію даних сторонніх протоколів через SDK/API; конфігурацію логічного рівня обчислювальної інфраструктури ЦОД (Logic Layer) із впровадженням інтерактивного ГІС-картографування та прив’язкою координат інцидентів до PTZ-камер; реалізацію інтелектуальних сервісів й автоматизацію логічного модуля виконання регламентних інструкцій (Orchestration Layer / SOP Engine) для мінімізації впливу людського чинника під час виникнення загрози.

Для підвищення ефективності, довговічності та відмовостійкості розробленої системи охорони периметра під час її практичної експлуатації рекомендується:

– кабельна та мережева інфраструктура: під час фізичного розгортання транспортного ешелону (Data Layer) для ліній зв’язку волоконно-оптичних та сейсмічних засобів використовувати броньовані кабелі з високим рівнем захисту від електромагнітних завад; магістральну мережу SAN будувати виключно на базі інтерфейсу Fibre Channel (32 Гбіт/с) для виключення втрат пакетів даних за пікових навантажень;

– інженерна живучість та резервування: забезпечити побудову системи електропостачання ЦОД за топологією Tier III / Tier IV із дублюванням ліній ДБЖ та автоматичним введенням резерву від ДГУ, проводити щомісячне тестування переходу на резервне живлення під навантаженням;

– кіберзахист та операційне середовище: використовувати на серверах ЦОД виключно дистрибутиви Linux корпоративного рівня (RHEL/SLES) із активованими модулями примусового контролю доступу (SELinux) та налаштованою політикою регулярного безперервного оновлення ядра (Live Patching) без зупинки процесів ШІ-відеоаналітики;

– експлуатація софту верхнього рівня (SOP Engine): проводити регулярний щоквартальний аудит та оновлення скриптів у логічному модулі автоматизованого виконання регламентних інструкцій (SOP) відповідно до змін у тактиці охорони полігону; забезпечити обов’язкове дублювання серверів оркестрації (за принципом Active-Active кластера) для запобігання появі єдиної точки відмови системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Modbus: що це таке і як працює? Огляд протоколу та його застосування. URL: https://surl.li/aakvlf (дата звернення 10.01.2026).

2. SNMP (Simple Network Management Protocol – простий протокол управління мережею). URL: https://surl.li/qtuhcq (дата звернення 10.01.2026).

3. Що таке технологія Industrial Ring ERPS? URL: https://surl.li/cvppqf (дата звернення 10.01.2026).

4. Bit Error Rate. URL: https://surl.li/pspngo (дата звернення 10.01.2026).

5. White Paper: ITU-T G.8032 ERPS Technology. Part I. URL: https://surl.li/xcwqfm (access date: 10.01.2026).

6. ДСТУ EN 50131-1:2014. Системи тривожної сигналізації. Системи охоронної сигналізації. Частина 1. Загальні вимоги (EN 50131-1:2006, EN 50131-1:2006/A1:2009, EN 50131-1:2006/IS2:2010, IDT). [Чинний від 2016-01-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2015. 70 с.

7. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://surl.lt/tlznee (access date: 15.01.2026).

8. IAEA Nuclear Security Series No. 13: Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). URL: https://surl.li/moskcz (access date: 15.01.2026).

9. ДСТУ ISO/IEC 18033-3:2015. Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 3. Блокові шифри (ISO/IEC 18033-3:2010, IDT). [Чинний від 2016-07-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2016. 48 с.

10. IEEE 802.1Q-2018: IEEE Standard for Local and Metropolitan Area Networks–Bridges and Bridged Networks. URL: https://surl.li/zqhvuf (access date: 15.02.2026).

11. Introduction to PSIM. URL: https://surl.li/crdqcg (access date: 15.01.2026).

12. ONVIF®. Profile M Specification. URL: https://surl.li/xlkmil (access date: 15.01.2026).

13. ERPS (Ethernet Ring Protection Switching). Explained: Why It’s One of Most Common Ring Protocol and How it Works. URL: https://surl.li/symiko (access date: 15.01.2026).

14. SNMP & ICMP Protocols. URL: https://surl.lu/yrgdiu (access date: 15.01.2026).

15. What is PSIM? URL: https://surl.li/irpuud (access date: 20.01.2026).

16. VMS – video surveillance management across different manufacturers. URL: https://surl.li/nsbgjn (access date: 20.01.2026).

17. Що таке NVR та чим відрізняється від DVR? URL: https://surl.li/ctsaxp (дата звернення 20.01.2026).

18. Guidelines for Writing Standard Operating Procedures. URL: https://surl.li/olmimu (access date: 15.01.2026).

19. Згорткова нейронна мережа – просте пояснення CNN та її застосування. URL: https://surl.li/pjjhxz (дата звернення: 25.01.2026).

20. RCNN – Region Based Convolutional Neural Network. URL: https://surli.cc/jxmfzh (access date: 25.01.2026).

21. How single-shot detector (SSD) works? URL: https://surl.li/rwixby (access date: 25.01.2026).

22. YOLOv8 Explained: Understanding Object Detection from Scratch. URL: https://surl.li/xbtikd (access date: 25.01.2026).

23. Understanding Feature Pyramid Networks for object detection (FPN). URL: https://surl.li/ctmbqt (access date: 25.01.2026).

24. Mean Average Precision (mAP) in Computer Vision. URL: https://surl.li/ckdcqs (access date: 25.01.2026).

25. Region of Interest Pooling and Region of Interest Align explained. URL: https://surl.li/xakeah (access date: 25.01.2026).

26. Бідюк П. І., Кузнєцова Н. В. Основні етапи побудови і приклади застосування мереж Байєса. URL: https://surl.li/glbwpc (дата звернення: 12.02.2026).

27. Modbus RTU vs. Modbus TCP/IP: Which Protocol to Choose? URL: https://surl.lu/wfwgwi (access date: 12.02.2026).

28. ONVIF Profiles. URL: https://www.onvif.org/profiles/ (access date: 12.02.2026).

29. Simple Network Management Protocol (SNMP). URL: https://surl.li/dqzwmh (access date: 12.02.2026).

30. Distributed Acoustic Sensing: Technology. URL: https://surl.lu/cwmvpw (access date: 12.02.2026).

31. HP ProLiant DL380 Gen11 2U Server 16x 2,5" SFF Tri-Mode NVMe SAS 2x Intel XEON Scalable LGA4677 DDR5 ECC Raid 2x PSU +NEW+. URL: https://surl.li/uakzri (access date: 12.02.2026).

32. Що таке масив RAID. Види та рівні. URL: https://surl.li/uipbdn (дата звернення: 12.02.2026).

33. Атаки типу Man-In-The-Middle: що треба знати кожному. URL: https://surl.li/sujqvq (дата звернення: 22.03.2026).

34. Understanding How RAID Storage Works. URL: https://surl.li/kqaeee (access date: 12.02.2026).

35. Терлецький Т. В., Кайдик О. Л. Кваліфікаційна робота: методичні вказівки до виконання кваліфікаційної роботи бакалавра для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні технології спеціальності 126 Інформаційні системи та технології денної та заочної форм навчання. Луцьк: ЛНТУ, 2025. 53 с.