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
ДЕРДЮК Юрій Сергійович
_____
(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

ДЕРДЮКУ Юрію Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: *Проектування інформаційної системи охорони периметра спеціального полігону (комплексна робота з Садовим М. О.)*

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: *План полігону спеціального для перевантаження ядерних відходів. IAEA Nuclear Security Series No. 13 (INFCIRC/225/Rev.5). ISO/IEC 27001. ISO/IEC 27002. НП 306.8.126-2006. НП 306.8.175-2011. ДСТУ EN 50131. ДСТУ IEC 62676. ДБН В.2.5-56:2014. Інша науково-технічна література за тематикою дослідження.*

4. Зміст розрахунково-пояснювальної записки (перелік питань, що потрібно розробити): *Анотація. Вступ. Розділ 1. Аналітичний огляд стану предметної області. 1.1 Характеристика об'єкту проектування. 1.2 Огляд нормативно-правової бази та стандартів. 1.3 Порівняльний аналіз технологій та підходів до побудови ІСОП. 1.4 Обґрунтування вибору архітектури та шляхів реалізації ІСОП. 1.5 Постановка завдань на кваліфікаційну роботу бакалавра. Розділ 2. Обґрунтування вибору засобів та методів реалізації. 2.1 Вибір елементної бази підсистем виявлення. 2.2 Обґрунтування вибору засобів оптико-електронного спостереження та тепловізійного моніторингу. 2.3 Вибір програмно-апаратної платформи центру обробки даних. 2.4 Методи та алгоритми інтелектуальної обробки сигналів і відеоаналітики. 2.5 Обґрунтування підсистем інженерного забезпечення, безперебійного живлення та заземлення. Розділ 3. Практична реалізація. Загальні висновки та рекомендації. Список використаних джерел. Додатки*

5. Перелік графічного (ілюстративного) матеріалу: *Презентація на 12 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 _____ (Дердюк Ю. С.)
(підпис)

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

АНОТАЦІЯ

Дердюк Ю. С. Проектування інформаційної системи охорони периметра спеціального полігону (комплексна робота з Садовим М. О.). 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 аналітичному огляді стану предметної області, нормативно-правовій базі та стандартах надійності у сфері проєктування систем безпеки об’єктів стратегічного призначення, а також проведено порівняльний аналіз сучасних технологій і підходів до побудови інформаційних систем охорони периметра. Обґрунтовано вибір елементної бази підсистем виявлення, засобів біспектрального оптико-електронного та тепловізійного моніторингу, а також програмно-апаратної платформи центру обробки даних та елементів інженерного забезпечення й безперебійного живлення. Описано методи й алгоритми інтелектуальної обробки сигналів, нейромережевого фільтрування кліматичних перешкод, а також математичні підходи до просторово-часової крос-кореляції подій. У практичній частині деталізовано особливості монтажу периферійного обладнання та побудови кабельної інфраструктури в складних умовах місцевості. Розроблено й конфігуровано топологію відмовостійкої магістральної мережі з налаштуванням кільцевого резервування за протоколом ERPS.

Ключові слова: інформаційна система, охорона периметра, полігон, відеоаналітика, тепловізійний моніторинг, нейромережа, крос-кореляція подій, алгоритм Байєса, кільцеве резервування, ERPS, платформа PSIM.

ANNOTATION

Derdiuk Yu. Designing an information system for physical perimeter security at a special training ground (comprehensive work with Sadovyi M.). 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 an analytical review of the subject area, the regulatory framework, and reliability standards in the field of designing security systems for strategic facilities, alongside a comparative analysis of modern technologies and approaches to constructing perimeter security information systems. The selection of the component base for detection subsystems, bispectral optoelectronic and thermal imaging monitoring equipment, as well as the hardware-software platform for the data center and elements of engineering support and uninterruptible power supply is substantiated. Methods and algorithms for intelligent signal processing, neural network filtering of environmental interference, and mathematical approaches to spatial-temporal cross-correlation of events are described. The practical section details the specific features of peripheral equipment installation and cable infrastructure construction under challenging terrain conditions. The topology of a fault-tolerant backbone network has been developed and configured with the deployment of ring redundancy using the ERPS protocol.

Keywords: information system, perimeter security, proving ground, video analytics, thermal imaging monitoring, neural network, cross-correlation of events, Bayesian algorithm, ring redundancy, ERPS, PSIM platform.

ЗМІСТ

ВСТУП

Еволюційним стартом інженерії технічної безпеки стало розгортання класичних аналогових систем на базі радіальних шлейфів, які тривалий час виступали базовим інструментом для контролю цілісності меж об’єктів.

На сьогодні розробники профільних рішень активно інтегрують передові мікропроцесорні компоненти та мережеві інтерфейси, що дозволяє адаптувати комплекси захисту під специфіку конкретних зон моніторингу. Спектр розгортання таких засобів є універсальним: від локальних житлових до критично важливих просторів. Подібні системи демонструють високу ефективність в управлінні, стабільність та живучість під час експлуатації завдяки впровадженню інтеграційних технологій, резервуванню каналів передачі даних та автоматизації процесів верифікації.

Пріоритетним напрямком розвитку цієї галузі є масштабування комплексів класу PSIM та впровадження нейромережевих алгоритмів відеоаналітики, які функціонують в межах відмовостійких кільцевих топологій. Такий підхід гарантує перманентний аудит стану ліній зв’язку, дозволяє гнучко проводити конфігурацію параметрів, нівелювати вплив природних завад і забезпечувати безпрецедентну точність ідентифікації загроз відповідно до критеріїв Grade 4.

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

Предмет дослідження – процеси функціонування, топологічні аспекти проєктування кабельної інфраструктури, методики інтеграції, налаштування та програмно-апаратні алгоритми крос-кореляції подій.

Мета кваліфікаційної роботи – проєктування та програмно-апаратна реалізація комплексної інформаційної системи охорони периметра спеціального полігону для забезпечення мінімізації ризиків несанкціонованого проникнення.

РОЗДІЛ 1
АНАЛІТИЧНИЙ ОГЛЯД СТАНУ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Характеристика об’єкту проектування

Спеціальний полігон (рис. 1.1), призначений для перевантаження ядерних відходів, є критично важливим інфраструктурним об’єктом, який вимагає найвищого рівня фізичної безпеки та радіаційного захисту.

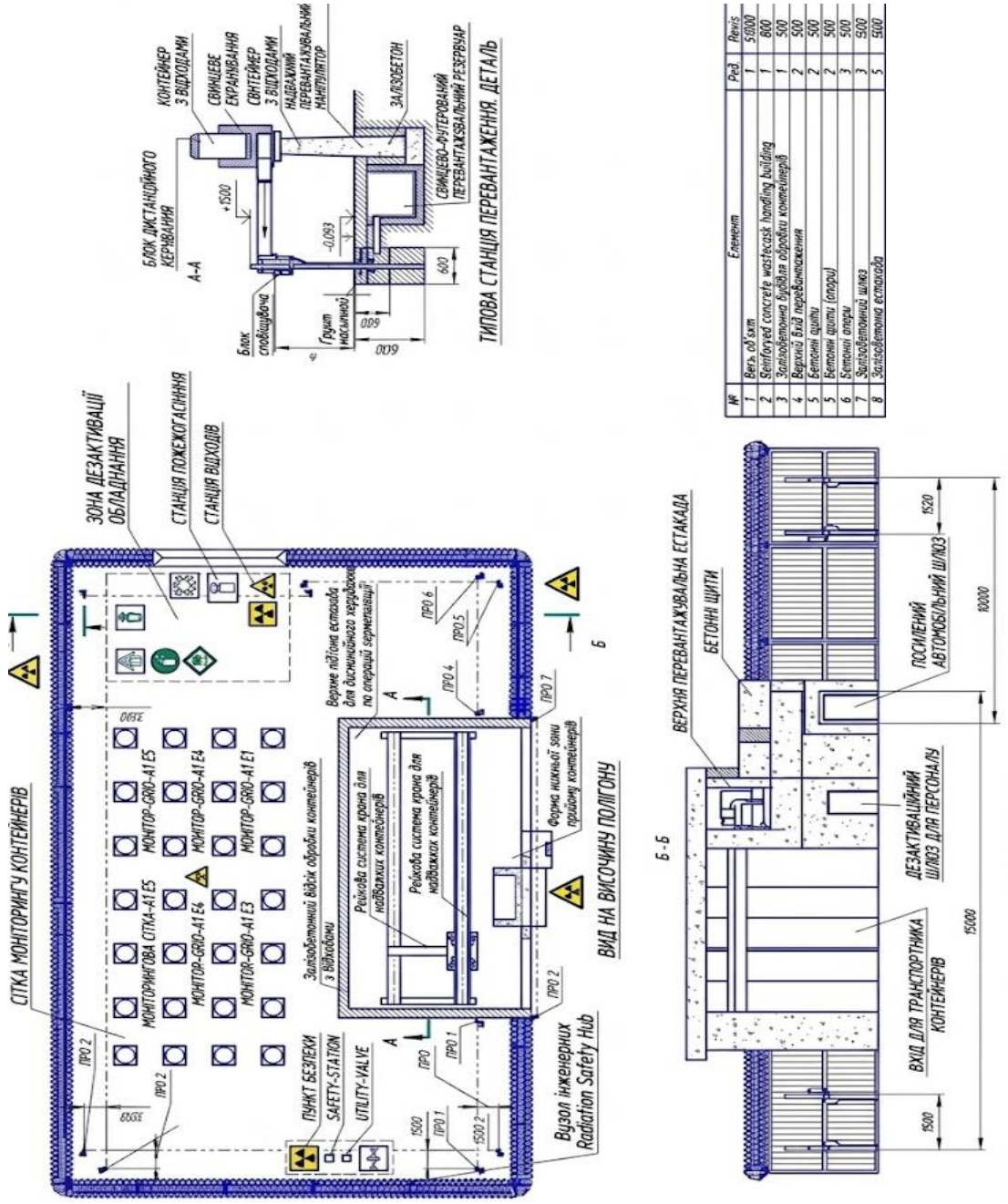

Рисунок 1.1 – Полігон спеціальний для перевантаження ядерних відходів

З точки зору капітального будівництва та інженерії, сам об’єкт проєктування – це складний технологічний вузол, який поєднує у собі логістичний термінал, закриті складські потужності та високозахищені інженерні споруди. Основним технологічним ядром об’єкта прийнято вважати будівлю для перевантаження ядерних відходів – це герметичний залізобетонний комплекс із масивним біологічним захистом, який оснащено дистанційно-керованими крановими системами, шлюзовими камерами для автомобільного транспорту, а також автоматизованими комплексами для перевантаження відходів із транспортних пакувальних комплектів у стаціонарні або довгострокові контейнери зберігання.

До суміжних елементів інфраструктури входять майданчики для тимчасового та довгострокового зберігання контейнерів, пункти дезактивації спецтехніки, лабораторії радіаційного моніторингу, а також автономні системи життєзабезпечення: резервні джерела живлення, система водопостачання та спецвентиляція із багатоступеневими фільтрами тонкого очищення повітря.

З огляду геопросторового та інженерно-геологічного проєктування, то об’єкт розташовується у лісовому масиві на значній відстані від населених пунктів (рис. 1.2), чим створює вигідний природний екран та мінімізує ризики випадкового техногенного впливу на цивільне населення. Проте специфіка локації вимагає закладення додаткових інженерних рішень: помірно-континентальний клімат із високою вологістю, частими туманами та значними сезонними коливаннями температур змушує використовувати обладнання та зовнішні електронні компоненти в антикорозійному виконанні (IP67/IP68).

Рівнинний рельєф суттєво спрощує вертикальне планування майданчика, прокладання підземних комунікацій та зведення фундаментів глибокого закладення, які здатні витримувати надважкі статичні та динамічні навантаження від кранового обладнання та захисних контейнерів. Оточення майданчика лісом також вимагає інженерно-технічної підготовки території – створення навколо об’єкта мінералізованих смуг відчуження шириною щонайменше 50-100 метрів без жодної рослинності, що дозволяє ліквідувати

сліпі зони для оптико-електронних систем та виконує роль протипожежного бар’єру у випадку лісових пожеж.

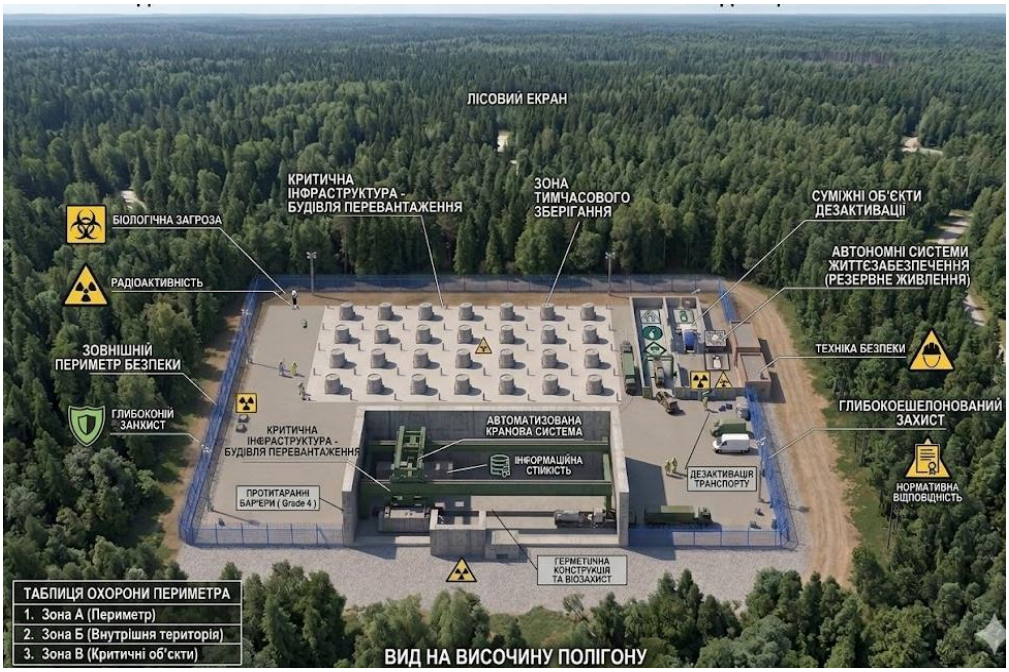

Рисунок 1.2 – Геопросторове розташування полігона спеціального для перевантаження ядерних відходів (згенеровано ШІ)

Розрахунок комплексної безпеки об’єкта базується на матриці потенційних інженерних, диверсійних та природних загроз, які класифікують за рівнем критичності:

– перша група – це ризики несанкціонованого проникнення з метою крадіжки радіоактивних матеріалів, вандалізму чи/або побутового проникнення сторонніх осіб;

– друга група – це спрямовані диверсійні атаки на критичні вузли інфраструктури;

– третя група – це шпигунство та інженерно-технічна розвідка, які здійснюють за допомогою оптичних засобів, засобів радіоперехоплення або дистанційного зондування.

Для нівелювання цих загроз у проєкті необхідно реалізувати концепцію глибокоешелонованого (багаторівневого) інженерного захисту, яка б дозволила поділити об’єкт проєктування на чіткі фізичні зони відповідальності.

Зона А (зовнішній периметр) – являє собою першу лінію оборони і повинна складатись з подвійного або потрійного контуру фізичних бар'єрів (сітчасті та капітальні загородження із протитаранними властивостями), які, зазвичай, обладнують тривожною сигналізацією, вібраційними давачами, тепловізійними камерами та радіолокаційними системами сканування периметра. Особливу увагу слід приділити геометрично вразливим точкам – кути та згини огорожі, де зони видимості камер перекриваються, а також транспортним воротам та контрольно-пропускним пунктам, які є основними точками таранного або силового прориву, а тому оснащуються автоматичними боллардами, шлюзами та детекторами вибухових і радіоактивних речовин.

Зона Б (внутрішня технологічна територія) – фокусується на моніторингу простору між периметром та безпосередніми спорудами; тут розгортається мережа стаціонарних постів радіаційного контролю, автоматизовані системи освітлення та сектори для патрулювання мобільних груп охорони.

Зона В – охоплює виключно критичні об'єкти (будівлю перевантаження та сховища). Вона проєктується у вигляді повністю ізольованого бункерного контуру із строгим біометричним контролем доступу, шлюзовими системами блокування дверей, броньованим склінням, сейсмостійкими стінами та дубльованими пультами управління.

Стабільність та безвідмовність усього комплексу має забезпечуватись за допомогою фундаментальних інженерних принципів автоматизації, резервування та автономності. Усі критично важливі системи – включаючи електропостачання, цифрові магістралі зв'язку, контури охолодження та відеоспостереження повинні володіти стовідсотковим «гарячим» резервуванням (схема N+1 або 2N), що гарантує миттєве перемикання на альтернативне джерело у разі аварії чи/або диверсії. Автоматизація технологічних процесів та алгоритмів безпеки дозволяє звести до мінімуму людський чинник: під час виявлення загрози система здатна самостійно заблокувати гермодвері, активувати системи автоматичного пожежогасіння та перевести об'єкт проєктування у режим ізоляції. Розроблена концепція

завершується постійною готовністю воєнізованої фізичної охорони, наявністю підземних захищених командних пунктів, регулярним проведенням інструментального тестування інженерних систем на відмовостійкість і безперервним автоматизованим аналізом потенційних вразливостей конструкцій об’єкта.

1.2 Огляд нормативно-правової бази та стандартів

Проєктування інформаційної системи охорони периметра (ІСОП) спеціального полігону для перевантаження ядерних відходів є складним інженерно-технічним завданням, реалізація якого неможлива без жорсткого дотримання чинних правових норм, технічних регламентів та стандартів безпеки. Оскільки об’єкт проєктування належить до категорії критичної інфраструктури підвищеної небезпеки, будь-які проєктні рішення щодо його фізичного захисту та інформаційної стійкості мають безперечний пріоритет національної безпеки й підлягають державному та міжнародному регулюванню.

Предметом розгляду виступають три основні рівні нормативної документації:

– міжнародні рекомендації у сфері поводження з радіоактивними матеріалами;

– національне законодавство України щодо захисту об’єктів критичної інфраструктури;

– відомчі будівельні, електротехнічні та інформаційні стандарти.

Базовим міжнародним орієнтиром у цій сфері прийнято вважати рекомендації Міжнародного агентства з атомної енергії (МАГАТЕ), зокрема IAEA Nuclear Security Series No. 13 (INFCIRC/225/Rev.5) «Ядерна безпека: Рекомендації щодо фізичного захисту ядерних матеріалів та ядерних установок» [1], який закладає фундаментальний принцип глибокоешелонованого захисту, вимоги до часових показників виявлення порушника та обов’язкові вимоги до створення декількох рубежів охорони.

Додатково, у контексті захисту цифрових даних, мережевої інфраструктури та каналів зв’язку ІСОП від кіберзагроз, проєкт спирається на положення міжнародних стандартів інформаційної безпеки серії ISO/IEC 27001 [2] та ISO/IEC 27002 [3].

На рівні національного законодавства правове поле формується законами України «Про використання ядерної енергії та радіаційну безпеку» [4], «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» [5] та «Про критичну інфраструктуру» [6]. Ці законодавчі акти визначають юридичну відповідальність оператора за забезпечення недоторканності об’єкта, покладають на розробника обов’язок інтеграції системи фізичного захисту в єдиний комплекс та встановлюють критерії безперервності й стійкості функціонування систем безпеки за умов виникнення гібридних чи/або диверсійних загроз.

Технічна конкретизація цих законів відображена у відомчих нормативно-правових актах Державної інспекції ядерного регулювання України (ДЯРУ), серед яких ключовими є НП 306.8.126-2006 «Правила фізичного захисту ядерних установок та ядерних матеріалів» [7] та НП 306.8.175-2011 «Вимоги до комплексу інженерно-технічних засобів системи фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» [8]. Відповідно до цих документів, для зовнішнього периметра (Зона А) обов’язковим є проєктування щонайменше двох рубежів сповіщення, які будуть функціонувати за різними фізичними принципами, повне перекриття засобами відеоспостереження (CCTV) підступів до об’єкта без сліпих зон, а також резервування живлення та автоматичне ведення протоку подій.

Практична інженерна реалізація, монтаж обладнання та побудова кабельних трас регламентуються системою національних стандартів України та державними будівельними нормами. Зокрема, вимоги до надійності та стійкості периметральної сигналізації визначаються стандартами серії ДСТУ EN 50131

«Системи тривожної сигналізації. Системи охоронної сигналізації» [9], за якими для об’єктів ядерного циклу все обладнання повинно відповідати найвищому класу безпеки Grade 4, що передбачає протидію зловмисникам із професійними навичками та спеціальним інструментарієм.

Проєктування та розгортання оптико-електронних засобів і систем інтелектуальної відеоаналітики здійснюється на основі стандартів серії ДСТУ IEC 62676 «Системи відеоспостереження охоронного призначення» [10], які встановлюють чіткі критерії роздільної здатності для виявлення та ідентифікації цілей у несприятливих метеорологічних умовах.

З огляду на розташування полігону в лісовому масиві та високу пожежну небезпеку, архітектура ІСОП інтегрується з вимогами ДБН В.2.5-56:2014 «Системи протипожежного захисту» [11], які зобов’язують використовувати вогнестійкі кабельні лінії (класу FLAME-X) та передбачає взаємодію із автоматичними системами локалізації загорянь.

Електротехнічна безпека, захист від блискавок, організація контурів заземлення та безперебійного живлення першої категорії надійності реалізуються у суворій відповідності до «Правил улаштування електроустановок» [12].

1.3 Порівняльний аналіз технологій та підходів до побудови ІСОП

Сучасний ринок інженерно-технічних засобів охорони пропонує широкий спектр технологічних рішень для захисту протяжних периметрів, проте проєктування інформаційної системи охорони периметра спеціального полігона для перевантаження ядерних відходів, вимагає безкомпромісного аналізу експлуатаційних параметрів кожної підсистеми.

Специфіка локації об’єкта (лісовий масив із помірно-континентальним кліматом, частими туманами, грозовою активністю та високою вологістю повітря) накладає жорсткі обмеження на використання багатьох комерційних технологій. Реалізація концепції глибокоешелонованого захисту [13] потребує

комбінування та інтеграції різнотипних сповіщувачів, які працюють за різними фізичними принципами роботи, для нівелювання «сліпих зон» та взаємного перекриття недоліків окремих технологій.

Перший технологічний рівень ешелонованої оборони становлять периметральні системи загороджувального типу, які монтують безпосередньо на фізичну огорожу і реагують на механічні спроби подолання бар'єра (перелаз, перекушування сітки, руйнування полотна). У цій групі виділяються три базові технології [14-16]:

– трибоелектричні системи;

– вібраційні системи;

– волоконно-оптичні системи.

Трибоелектричні системи використовують коаксіальний кабель, у якому, під час механічної деформації, за рахунок тертя провідника об діелектрик, виникає електричний заряд. Незважаючи на його доступну вартість, трибоелектричний кабель володіє високою схильність до формування хибних спрацювань за умови сильних вітрів та шквалів, які характерні для лісистої місцевості, а також піддається впливу сильних електромагнітних перешкод від грозових розрядів.

Вібраційним системам, які працюють на базі п'єзоелектричних або електромагнітних сенсорів, притаманна вища точність завдяки можливості детального спектрального аналізу частоти коливань огорожі, що дозволяє відфільтровувати дрібних тварин або поривів вітру, проте вони також чутливі до промислових та атмосферних перешкод.

Найбільш прогресивним рішенням для критичної інфраструктури є волоконно-оптичні системи (ВОС). Принцип їх роботи базується на реєстрації зміни інтерференційної картини лазерного випромінювання у коаксіальному світловоді під час найменших геометричних мікродеформаціях кабелю (рис. 1.3). Волокно – це повністю пасивний елемент системи, що не потребує підведення електричного живлення вздовж усього периметра, має абсолютну стійкість до електромагнітних імпульсів, наводок, блискавок і корозії в умовах

високої вологості. Завдяки програмному розділенню кабелю на віртуальні зони та використанню алгоритмів штучного інтелекту, ВОС забезпечують точність локалізації місця прориву до кількох метрів за мінімального рівня хибних тривог, що виправдовує їхню високу початкову вартість.

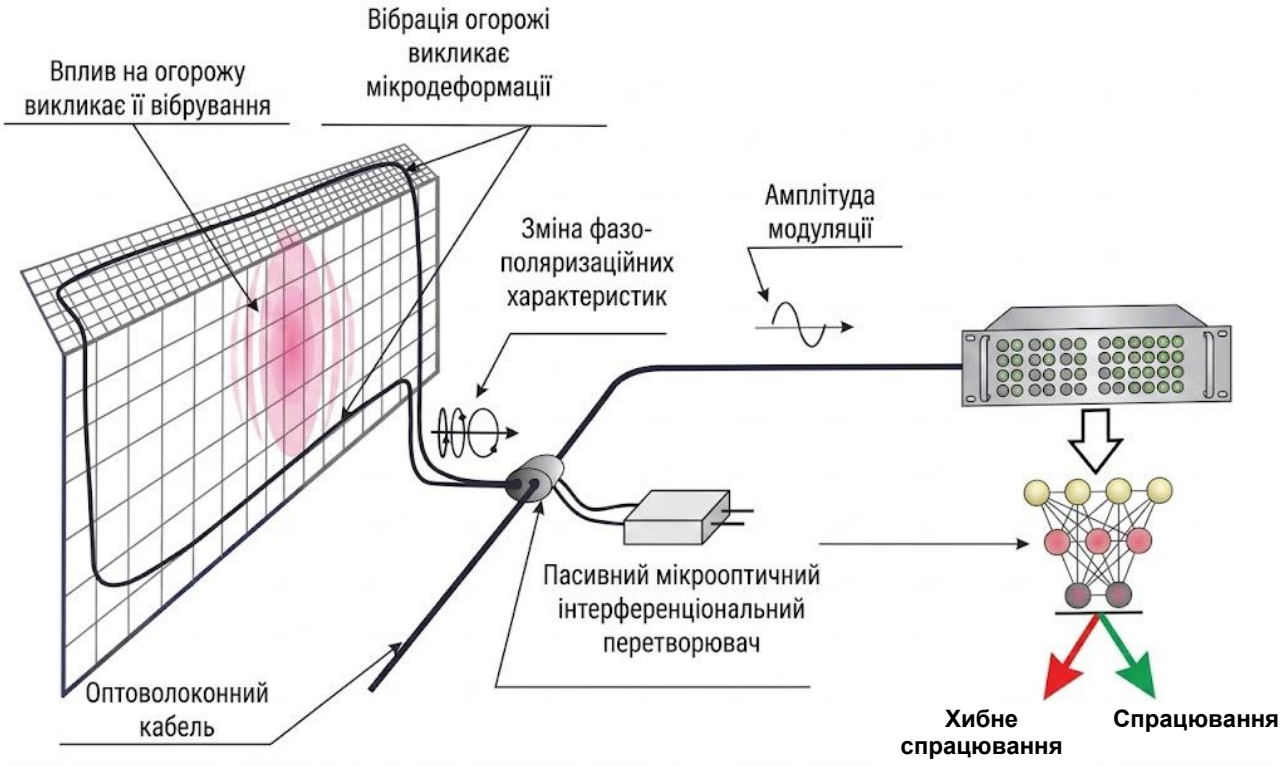

Рисунок 1.3 – Принцип роботи оптоволоконного засобу виявлення [16]

Другий рівень ешелонованого захисту базується на об’ємних і зональних системах виявлення, які контролюють смугу відчуження навколо огорожі та підступи до неї. До цього класу відносять такі сповіщувачі [14-16]:

– радіохвильові;

– інфрачервоні;

– сейсмічні.

Радіохвильові (радіолокаційні та лінійні двопозиційні) давачі формують об’ємну зону виявлення у вигляді еліпсоїда між приймачем і передавачем за рахунок формування високочастотного електромагнітного поля (рис. 1.4). Вони вкрай ефективні для реєстрації швидких та силових спроб прориву, проте їх

стабільність критично залежить від геометрії зони відчуження: наявність рослинності, дерев або високої трави у лісовому масиві призводить до критичного зростання хибних спрацювань через рух гілок/трави.

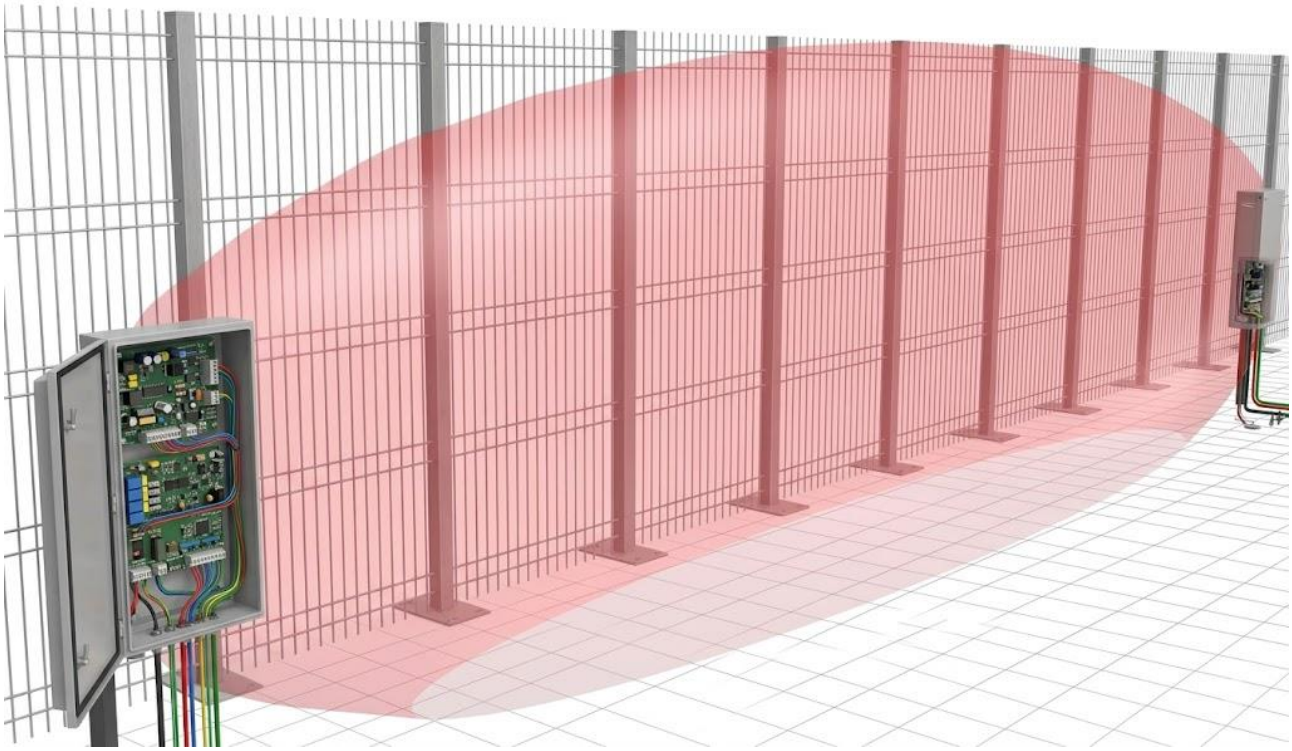

Рисунок 1.4 – Зона виявлення радіохвильового засобу виявлення [16]

Активні інфрачервоні (ІЧ) бар’єри працюють за принципом фіксації переривання лінійних оптичних променів між стійками-випромінювачами (рис. 1.5). Пасивні ІЧ-давачі здатні реєструвати зміну теплового контрасту під час руху об’єкта в зоні огляду. Спільною критичною вразливістю обох типів ІЧ-систем у цих кліматичних умовах є висока схильність до блокування або втрати чутливості під час густих туманів, затяжних злив та снігопадів, коли оптична прозорість атмосфери падає нижче критичної межі, що робить охоронний рубіж тимчасово непридатним.

Сейсмічні системи виявлення, які монтуються безпосередньо в ґрунті вздовж периметра, здатні реєструвати акустичні коливання та пружні геофізичні хвилі, які генеруються кроками людини або рухом транспортних засобів (рис. 1.6). Сейсмічні давачі забезпечують максимальний рівень

прихованості монтажу, їх неможливо виявити візуально або заблокувати засобами радіоелектронної боротьби, проте коріння дерев навколишнього лісу, яке коливається від вітру та передає вібрацію в ґрунт, вимагає застосування складних цифрових сигнальних процесорів (DSP – Digital Signal Processor) для фільтрування корисного сигналу від природного фону.

Рисунок 1.5 – Однопроменевий активний ІЧ-сповіщувач [16]

Рисунок 1.6 – Зона виявлення сейсмічного сповіщувача [16]

Третім, найважливішим координаційним рівнем ешелонованого захисту сучасної ІСОП є підсистема верифікації тривог та інтелектуального моніторингу, яка базується на інтеграції цифрового відеонагляду високої роздільної здатності, тепловізійної техніки та ШІ-аналітики (рис. 1.7).

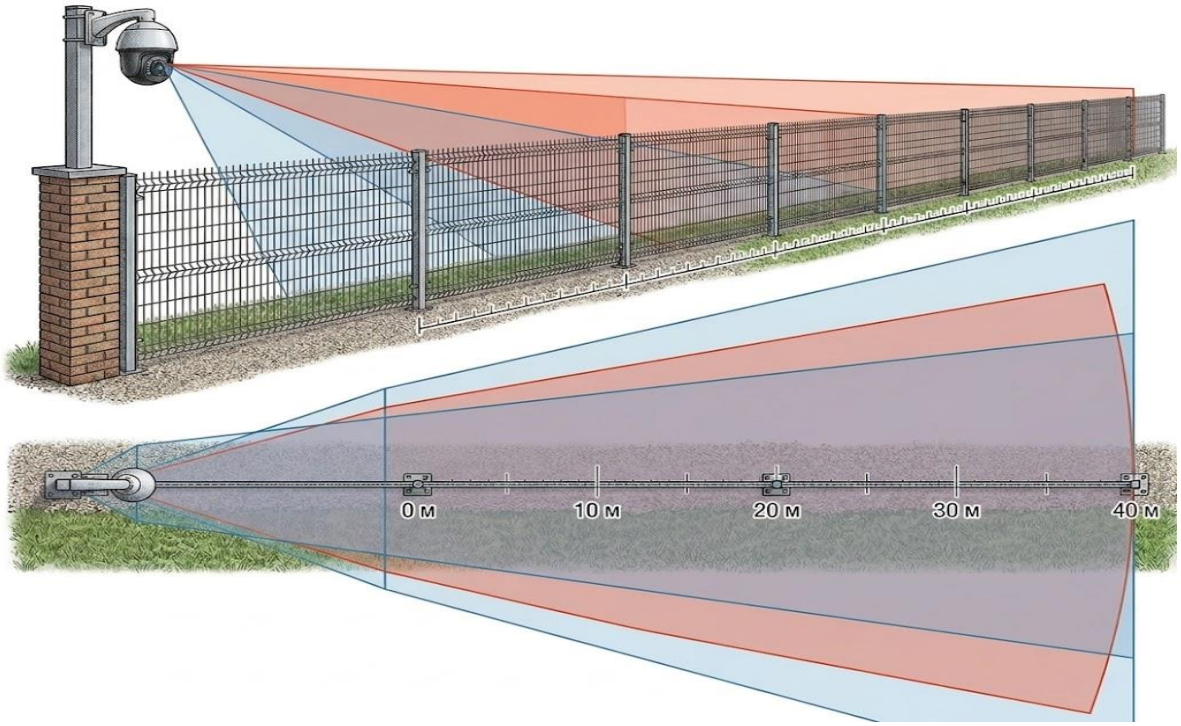

Рисунок 1.7 – Підсистема верифікації тривог [16]

Звичайні оптичні камери, які експлуатуються в лісовій місцевості у нічний час або за наявності туманну втрачають свою ефективність. Інтеграція довгохвильових інфрачервоних тепловізорів (LWIR – Long-Wave Infrared) повністю розв’язує цю проблему, оскільки вони фіксують власне теплове випромінювання об’єктів, забезпечуючи, при цьому, чітку видимість порушника крізь густий туман, дим, дощ чи маскувальний одяг на фоні холодного лісового масиву. Впровадження нейромережевої відеоаналітики (AI – Artificial Intelligence) на рівні серверної платформи або безпосередньо на «борту» камери (Edge AI) дозволяє системі не лише фіксувати рух, але й проводити класифікацію цілей, чітко розрізняючи людину, автомобіль, дику тварину чи коливання гілок дерев. Це радикально знижує навантаження на

оператора пульта охорони, зводячи частоту хибних тривог майже до нуля, та автоматично підсвічує траєкторію руху порушника для мобільних груп реагування.

Для узагальнення техніко-економічних й експлуатаційних характеристик розглянутих технологій та обґрунтування їх вибору для проєкту спеціального полігону перевантаження ядерних відходів, нижче наведено порівняльну таблицю (табл. 1.1).

Таблиця 1.1 – Порівняльна характеристика технічних засобів виявлення для систем охорони периметра

Тип технології	Переваги	Недоліки	Відносна вартість	Стійкість до хибних спрацювань
1	*2*	*3*	*4*	*5*
Трибоелектричні системи	Низька ціна матеріалів; простий монтаж на гнучких типах парканів	Чутливість до вітру та ЕМ-перешкод; високе зношування кабелю	Низька	Низька (залежить від погодних умов)
Вібраційні системи	Можливість частотного фільтрування сигналів; точна локалізація зон на жорстких типах парканівх	Потребують регулярного калібрування; чутливі до граду та сильного дощу	Середня	Середня
Волоконно-оптичні системи	Абсолютна стійкість до гроз, ЛЕП, ЕМП; пасивність; довжина зон до десятків кілометрів; довговічність	Складність зварювання оптоволокна під час монтажу; висока вартість контролерів	Висока	Дуже висока (за умови використання ШІ-фільтрування)
Радіохвильові давачі	Надійне виявлення об’ємних цілей; стійкість до туману та опадів	Вимагають ідеально розчищеної смуги відчуження без трави та дерев	Середня	Середня (критична до наявності рослинності)
Інфрачервоні бар’єри (активні/пасивні)	Чітка лінійна межа виявлення; низька ціна; швидка інтеграція	Повне блокування сигналу під час туманів, завірюх та задимлень лісу	Низька	Низька в умовах високої вологості
Сейсмічні давачі	Прихований підземний монтаж; неможливість саботажу; захист від вітру та опадів	Складність монтажу в каменистий або промерзлий ґрунт; вплив коріння дерев	Висока	Висока (при належній DSP-фільтрації)

Продовження таблиці 1.1.

1	2	3	4	5
ШІ-відеонагляд та тепловізори	Верифікація 24/7; класифікація цілей; робота в тумані; автоматичний трекінг	Залежність від обчислювальної потужності серверів; висока ціна тепловізійних матриць	Дуже висока	Максимальна (найкращий інструмент для верифікації)

Проаналізувавши, у контексті проєктування ІСОП спеціального полігону, параметри порівняльної таблиці стає очевидним, що жодна із технологій не може бути використана як єдиний рубіж захисту. Для забезпечення класу безпеки Grade 4 оптимальним інженерним рішенням стає побудова комбінованого комплексу. У якості першого рубежа охорони доцільно використати волоконно-оптичну систему через її стійкість до погодних та електромагнітних чинників. Другий рубіж (смуга відчуження) повинен формуватися на основі сейсмічних давачів (захищених ґрунтом від зовнішнього впливу) та радіохвильових бар'єрів на прямих ділянках. Обов'язковим елементом системи виступає інтегрований контур тепловізійного спостереження з використанням ШІ-аналітики, який виконує роль основного інструменту автоматичної верифікації та дублювання тривожних сповіщень, що повністю виключає людський фактор та забезпечує безперебійний захист об'єкта критичної інфраструктури.

1.4 Обґрунтування вибору архітектури та шляхів реалізації ІСОП

Побудова високонадійної інформаційної системи охорони периметра для спеціального полігону перевантаження ядерних відходів базується на комплексному інженерному синтезі апаратних модулів, середовища передачі сигналів та керуючого програмного ядра. Для забезпечення безперебійного функціонування об'єкта класу Grade 4 в агресивних кліматичних умовах Полісся традиційні лінійні підходи незадовільні. Оптимальним вибором для критичної інфраструктури підвищеної небезпеки є трирівнева модульно-

кластерна архітектура з розподіленою логікою обробки даних. Така концепція передбачає поділ системи на:

– периферійний рівень (польові контролери, які проводять первинну фільтрацію сигналів, які надходять від датчів);

– проміжний рівень (секторні концентратори та комутатори агрегації);

– центральний рівень (дубльовані сервери баз даних та відеоаналітики).

Модульний принцип організації на кожному з цих рівнів гарантує високу живучість комплексу: локальне пошкодження одного з кабельних сегментів або вихід з ладу секторного контролера не викликає каскадного збою суміжних зон, повністю нівелюючи ризик наявності єдиної точки відмови (Single Point of Failure [17]).

Визначення топології та фізичного середовища комунікаційного контуру ІСОП підпорядковується жорстким вимогам завадостійкості та захисту від саботажу. Використання бездротових радіоканалів у якості магістральних ліній є недопустимим через високу ймовірність їх навмисного придушення засобами радіоелектронної боротьби, а також через критичне згасання високочастотного сигналу в умовах густого лісу та щільних туманів. Мідні кабельні лінії (вита пара, коаксіальні траси) також мають жорсткі обмеження внаслідок вразливості до сильних грозових розрядів та електромагнітних наводок. Відповідно, єдино правильним інженерним рішенням для магістралі ІСОП є розгортання волоконно-оптичних ліній зв’язку (ВОЛЗ) за топологією «подвійного резервованого кільця» (протоколи RSTP/ERPS [18]), де кабель слід вкладати під землею у захищених промислових коробах за двома географічно рознесеними маршрутами. Оптоволокно забезпечує повну гальванічну ізоляцію, високу пропускну здатність для трансляції багатопотокового тепловізійного зображення та абсолютну захищеність від дистанційного знімання інформації порушником. Підключення давачів, на локальних ділянках, до польових контролерів здійснюється за допомогою екранованого кабелю який інсталюють металевий рукав через завадостійкі промислові інтерфейси RS-485 або Industrial Ethernet.

Для об’єднання периферійного обладнання та ліній зв’язку у єдину інформаційну екосистему обґрунтовано впровадження спеціалізованого програмного забезпечення класу PSIM (Physical Security Information Management [19]) на базі захищеної операційної системи сімейства «Linux». Платформа PSIM буде виконувати роль інтелектуального диспетчера, який реалізує автоматичні крос-системні сценарії реагування без участі людини. Програмний комплекс у реальному часі зіставляє дані від волоконно-оптичної сигналізації, сейсмосенсорів та радарів, автоматично здійснюючи просторове наведення PTZ-тепловізорів на координати зони прориву, увімкнення охоронного освітлення та активацію загороджувальних боллардів на КПП.

Вбудовані нейромережеві алгоритми відеоаналітики (Edge та Server AI) здійснюють миттєву класифікацію рухомих об’єктів, що зводить до мінімуму частоту хибних спрацювань через природні шуми лісу. Безпека самого програмного ядра досягається за рахунок повного шифрування трафіку (AES-256 [20]), резервування баз даних за принципом Active-Active та розгортання дублюючого пульта управління в захищеному приміщенні полігону.

Для системного узагальнення та технічного обґрунтування обраних інженерних рішень наведемо матрицю вибору архітектурних та технологічних шляхів реалізації ІСОП спеціального полігону (табл. 1.2).

Таблиця 1.2 – Обґрунтування архітектурної та програмно-апаратної моделі ІСОП

Компонент / Рівень ІСОП	Розглянуті альтернативи	Обране інженерне рішення	Техніко-економічне та безпекове обґрунтування вибору
1	*2*	*3*	*4*
Архітектурна концепція системи	Модульна / централізована / багаторівнева	Гібридна багаторівнева модульно-кластерна архітектура	Розділення логіки на 3 автономні рівні ліквідує «єдину точку відмови». Модульність дозволить гарантувати живучість системи Grade 4 під час пошкодження окремих секторів
Середовище магістральної передачі даних	Захищений радіоканал / мідні лінії (вита пара) / волоконно-оптичні лінії	Подвійне резервоване підземне кільце ВОЛЗ (протоколи RSTP/ERPS)	Повна стійкість до ЕМП, блискавок, РЕБ-придушення. Гарантує гігабітну швидкість для тепловізійного відео та збереження зв’язку під час одноразового фізичного розриву магістралі

Продовження таблиц 1.2

1	2	3	4
Локальні інтерфейси периферії	Бездротовий зв’язок (Wi-Fi/LoRa) / промислові дротові шини	Екрановані кабелі в металорукавах (RS-485/Modbus, Industrial Ethernet)	Висока стійкість до перешкод на коротких відстанях, захист ліній від механічних пошкоджень, гризунів та вологи (виконання IP67/IP68)
Платформа програмного забезпечення	Стандартні VMS-системи / спеціалізоване програмне забезпечення класу PSIM	Кросплатформена PSIM-платформа на базі Linux із ШІ-відеоаналітикою	Забезпечення нативної інтеграції різнорідних підсистем, автоматичні сценарії наведення камер за координатами тривоги, класифікація цілей нейромережами та захист від кібератак
Стійкість та резервування керування	Локальний сервер / хмарна архітектура / кластерне «гаряче» резервування	Кластеризація Active-Active з географічно дубльованим пультом	Забезпечення безперервності моніторингу полігону та збереження журналів подій (AES-256) за умови повного руйнування або захоплення наземного центрального поста охорони

Систематизована в таблиці 1.2 конфігурація ІСОП, заснована на багаторівневому модульному принципі, волоконно-оптичних магістралях зв’язку та інтелектуальній PSIM-платформі, повною мірою відповідає жорстким критеріям живучості та інформаційної стійкості. Такий архітектурний підхід дозволить створити монолітний контур безпеки критичного об’єкта, мінімізуючи вплив складного геопросторового розташування та людського чинника на загальний рівень захищеності об’єкта проектування.

1.5 Постановка завдань на кваліфікаційну роботу бакалавра

Ефективність сучасних інформаційних систем охорони периметра стратегічних об’єктів напряму залежить від детального аналізу ландшафтно-географічних особливостей місцевості, виявлення потенційних векторів та шляхів несанкційонованого проникнення, а також правильного вибору технологічного стеку. Проєктування комплексу безпеки для полігону спеціального вимагає синергії між надійною гетерогенною апаратною

інфраструктурою, відмовостійким мережевим ешелоном та гнучким програмним забезпеченням верхнього рівня, що дозволяє забезпечити стабільне його функціонування в умовах складних динамічних та експлуатаційних навантажень лісового масиву.

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

– проаналізувати просторово-геометричні характеристики об’єкту проєктування, змоделювати потенційні загрози диверсійної діяльності та визначити найбільш вразливі зони й ділянки охоронного периметра;

– провести порівняльний аналіз сучасних технологій периметрального виявлення та методів інтелектуального моніторингу з точки зору доцільності впровадження біспектральних засобів і відкритих промислових протоколів зв’язку;

– розрахувати та спроєктувати відмовостійку топологію магістральної кабельної мережі ліній, обґрунтувати параметри системи безперебійного живлення, заземлення та виконати перевірочні інженерні розрахунки ємності буферних АКБ;

– здійснити програмно-апаратну інтеграцію периферійних засобів виявлення, оптико-електронного спостереження та засобів автоматизації на базі центральної платформи класу PSIM;

– розробити та параметризувати програмні алгоритми інтелектуальної обробки сигналів для автоматизації сценаріїв реагування на АРМ оператора.

РОЗДІЛ 2
ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ ТА МЕТОДІВ РЕАЛІЗАЦІЇ

2.1 Вибір елементної бази підсистем виявлення

Реалізація трирубіжного контуру охорони периметра полігону спеціального для перевантаження ядерного палива потребує переходу від концептуальних рішень до вибору конкретних апаратних засобів виявлення. Для забезпечення високої живучості системи класу Grade 4 в умовах географічного регіону Полісся необхідно провести порівняльний аналіз ринкових пропозицій та сформувати кінцеву специфікацію елементної бази.

Перший рубіж охорони орієнтований на реєстрацію механічних впливів (перелаз, перекушування, руйнування полотна). З метою визначення оптимального типу сповіщувача виконано порівняльну оцінку (табл. 2.1) лінійних радіохвильових, вібраційних трибоелектричних та волоконно-оптичних систем за ключовими техніко-експлуатаційними критеріями.

Таблиця 2.1 – Порівняльний аналіз систем виявлення для першого рубежу охорони

Параметр порівняння	Радіохвильовий кабель	Вібраційні трибоелектричні давачі	Волоконно-оптична система (FFT Secure Fence)
Принцип роботи	Реєстрація зміни ЕМП навколо кабелю	Фіксація електричних зарядів під час тертя мідних жил	Лазерна інтерферометрія (зміна фази світла у волокні)
Точність локалізації	Низька (в межах зони/сектора 100-200 м)	Середня (до 50 метрів)	Висока (дискретність до 5-10 метрів)
Електромагнітна стійкість	Вразлива до промислових завад та ЛЕП	Вразлива до близьких розрядів блискавок	Абсолютна інертність (відсутній струм у лінії)
Вплив погоди (зливи, туман)	Середній (потребує постійного підлаштування)	Низький (за якісної герметизації муфт)	Відсутній (герметичний пасивний кабель)
Живучість лінії	Вихід з ладу кабелю паралізує увесь сектор	Потребує ремонту мідної жили, чутлива до вологи	Зберігає працездатність під час розриву (двостороннє сканування)
Висновок	Не рекомендовано для об’єктів Grade 4	Рекомендовано у якості резервного варіанта	Рекомендовано у якості базового рішення

Відповідно до висновків системного аналізу, для першого лінійного рубежу, який розгортається безпосередньо на металевій огорожі із панельної сітки за ДСТУ EN 10223-4-2001 [21] (рис. 2.1), обрано розподілену волоконно-оптичну систему виявлення на базі контролера моделі FFT Aura Ai-2 (рис. 2.2). Дана система використовує пасивний волоконно-оптичний сенсорний кабель LT024-SM-ADSS-3kN [23], який кріпиться до полотна огорожі за допомогою пластикових або металевих стяжок [24].

Рисунок 2.1 – Металева огорожа із панельної сітки

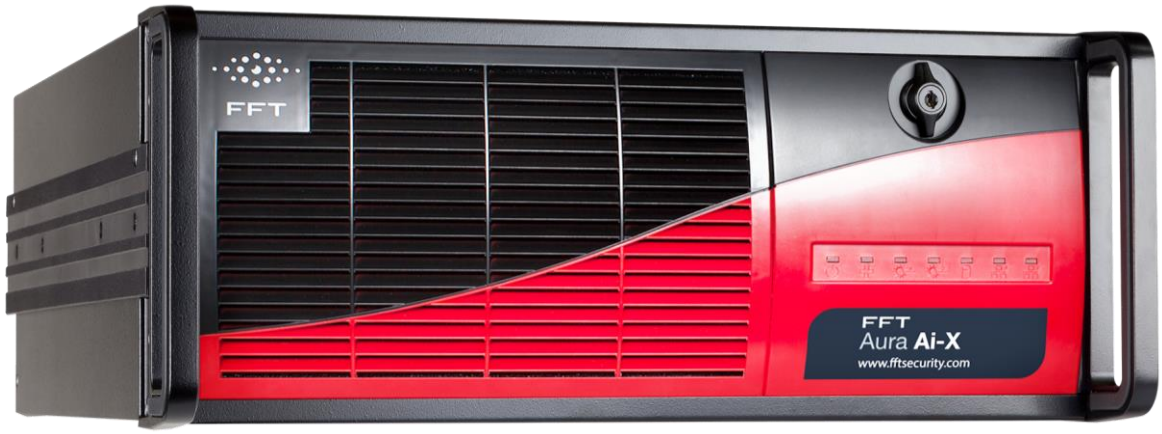

Рисунок 2.2 – Контролер охоронної оптоволоконної системи детекції FFT Aura Ai-2 [22]

Принцип роботи контролера базується на лазерній інтерферометрії: будь-який механічний вплив на паркан (перелаз, перекушування дроту, руйнування

секції) викликає мікродеформацію оптичного волокна, що миттєво змінює фазові та інтерференційні характеристики світлового променя. Основною інженерною перевагою системи є її здатність здійснювати точну локалізацію місця порушення з точністю від 5 до 10 метрів за довжини одного оптичного плеча до 40 км. Центральний процесорний блок обробки сигналів забезпечує частоту дискретизації до 10 кГц та використовує ШІ-алгоритми для розпізнавання сигнатури завад.

Сенсорний кабель повинен бути абсолютно герметичним, робочий діапазон температур від -40 до +70°C та не піддаватись впливу блискавок, що вкрай важливо для грозової активності. Оскільки в кабелі відсутній електричний струм, то він володіє нульовим пожежним та вибухонебезпечним випромінюванням, повністю відповідає вимогам які відносяться до об’єктів ядерного циклу.

Для другого рубежу охорони запроєктовано комбінацію з підземних сейсмічних давачів та лінійних радіохвильових бар’єрів. Специфікацію цього обладнання, із зазначенням його експлуатаційних характеристик, які задовольняють кліматичні вимоги IP67/IP68 наведено у таблиці 2.2.

Для організації прихованого наземного виявлення обрано сейсмоакустичну систему на базі сейсмічної системи охорони ARCTIUM (рис. 2.3), яка складається із ланцюга інтелектуальних грунтових геосенсорів.

Таблиця 2.2 – Специфікація та тактико-технічні характеристики обраної елементної бази підсистем виявлення

Рубіж / Тип сповіщувача	Конкретна модель обладнання	Ключові тактико-технічні характеристики (ТТХ)	Клас захисту (IP) та кліматичне обґрунтування вибору
1	*2*	*3*	*4*
1-й рубіж / волоконно-оптична система, яка розташована на паркані	Волоконно-оптичний сенсорний кабель LT024-SM-ADSS-3kN Контролер FFT Aura Ai-2	– довжина оптичного плеча: до 40 км; – точність локалізації: ±5-10 м; – частота дискретизації лазера: 10 кГц; – алгоритми обробки: ШІ-класифікація сигна-тур подій	IP68 (пасивна частина). Сенсорний кабель не містить металевих елементів та не схильний до корозії, захищений від наводок під час ударів блискавок в паркан

Продовження таблиці 2.2

1	2	3	4
2-й рубіж / підземний сейсмоакустичний комплекс	Сейсмічна система охорони ARCTIUM	– смуга частот: від 1 до 500 Гц; – радіус детектування суб'єкта виявлення: від 15 до 20 м; – аналіз сигналів: вбудований DSP-процесор; – джерело живлення: літієві елементи з ресурсом до 5 років	IP68 (повна герметичність). Корпус геосенсорів розрахований на тривале перебування у вологому ґрунті та болотистих низинах, зберігає ТТХ під час промерзання верхнього шару землі
2-й рубіж / двопозиційний мікрохвильовий бар'єр	Мікрохвильовий детектор Forteza FMC 24-300	– робоча частота: 24,15 ГГц; – довжина ділянки: до 300 м; – ширина/висота зони: 2,0/1,8 м; – кількість частотних каналів: 8 (унеможливлює взаємний вплив)	IP67 (ударостійкий полікарбонат). Частота 24 ГГц забезпечує вузьку зону детектування, що є критичним в лісистій місцевості. Захист від злив та туману

Рисунок 2.3 – Сейсмічна система охорони ARCTIUM [25]

До ТТХ цієї системи варто віднести смугу реєстрованих частот від 1 до 500 Гц, радіус зони виявлення поодиноких суб'єктів виявлення від 15 до 20 метрів на один давач, та здатність їх працювати в умовах повного затоплення або промерзання ґрунту. Повністю герметичний корпус грунтових модулів за стандартом IP68 унеможливлює проникнення підземних вод, характерних для заболоченої місцевості. Вбудований у кожен давач цифровий сигнальний процесор аналізує амплітудно-частотну характеристику пружних геофізичних хвиль ґрунту, що дозволяє системі математично відокремлювати кроки людини

або рух колісної техніки від акустичних шумів, викликаних коливанням коріння дерев за шквального вітру.

Для захисту протяжних прямих ділянок у межах другого ешелону охорони закладено двопозиційний радіохвильовий сповіщувач Forteza серії FMC 24 Pro (рис. 2.4), який працює на робочій частоті 24 ГГц (К-діапазон). Вибір цієї частоти зумовлений її високою стійкістю до атмосферних явищ у порівнянні із стандартними 10-гігагерцовими аналогами.

Рисунок 2.4 – Мікрохвильовий детектор Forteza FMC 24 Pro [26]

Комплект складається з передавача та приймача, що утворюють об’ємну зону виявлення у формі еліпсоїда обертання довжиною до 300 метрів. До ключових ТТХ належать: висота зони виявлення – до 1,8 м, ширина зони виявлення – до 2,0 м, швидкість руху суб’єкта виявлення – 0,1 до 10 м/с. Корпус приладів виготовлено із ударостійкого полікарбонату з рівнем захисту IP67, що забезпечує повну пилонепроникність та стійкість до сильних струменів води під час злив. Застосування частоти 24 ГГц забезпечує вузьку зону відчуження, зменшуючи вплив дрібної рослинності на краях смуги охорони, а наявність 8 незалежних частотних каналів виключає взаємні наводки (взаємовплив) сусідніх сповіщувачів за послідовного монтажу по периметру.

Кліматична стійкість обраної елементної бази повністю відповідає стандарту ДСТУ IEC 60529 [27]. Окрім того, усі периферійні блоки інтегрують у собі внутрішні елементи підігріву електронних плат, що виключає дрейф

робочих параметрів під час критичнонизьких температур та нівелює вплив льодової кірки на працездатність системи охорони периметра.

2.2 Обґрунтування вибору засобів оптико-електронного спостереження та тепловізійного моніторингу

Підсистема оптико-електронного спостереження та тепловізійного моніторингу виконує функцію другого контуру верифікації тривог. Її основне завдання – це автоматичне або автоматизоване підтвердження факту порушення, зафіксованого першим (волоконно-оптичним) або другим (сейсмічним/радіохвильовим) рубежами охорони. Враховуючи географічне розташування об’єкта проєктування та його специфіку, де пряма видимість обмежена лісовим масивом, а щільні тумани унеможливлюють використання виключно класичного оптичного діапазону, основу цієї підсистеми буде формувати комбінація стаціонарних біспектральних камер та швидкісних поворотних (PTZ) комплексів.

2.2.1 Специфікація та конфігурація обладнання

Для безперервного моніторингу лінійних ділянок периметра вздовж паркану обрано стаціонарні біспектральні камери моделі Hikvision DS-2TD2167-25/PI (рис. 2.5). Даний пристрій поєднує у собі:

– тепловізійний модуль: неохолоджувана матриця на основі оксиду ванадію із роздільною здатністю 640 × 512 пікселів, фокусною відстанню об’єктива 25 мм та температурною чутливістю NETD < 35 Мк;

– оптичний модуль: цифрова камера роздільної здатності 4 Мп (2688 × 1520) з матрицею 1/1,8 Progressive Scan CMOS та технологією DarkFighter для роботи в умовах глибоких сутінків.

Камери встановлюються стаціонарно на кутових та проміжних опорах периметра на висоті 4,5-5 метрів й спрямовуються назустріч одна одній для перекриття «сліпих зон» безпосередньо під самими опорами.

Рисунок 2.5 – Тепловізійна IP-камера циліндричного типу Hikvision DS-2TD2167-25/PI [28]

Для верифікації тривог у глибині території об’єкта проєктування та на складних ділянках рельєфу лісового масиву запроєктовано швидкісні поворотні біспектральні PTZ-комплекси моделі Hikvision DS-2TD6267-75C4L/W (рис. 2.6). Фокусна відстань тепловізора 75 мм, оптичне збільшення до 50× та вбудовані ШІ-алгоритми супроводу цілі (Smart Tracking). За умови спрацюванні будь-якого лінійного давача охорони, PTZ-камера автоматично розгортається в координати точки тривоги для детальної ідентифікації цілі.

Рисунок 2.6 – Зовнішня біспектральна камера великої дальності Hikvision DS-2TD6267-75C4L/W [29]

2.2.2 Математичний розрахунок зон виявлення

З метою унеможливлення появи неконтрольованих ділянок («сліпих зон») у лісистій місцевості розрахунок геометрії огляду камер слід вести за критеріями Джонсона (ДСТУ EN 62676-4 [30]). Для забезпечення надійного автоматичного ШІ-аналізу щільність пікселів на фоні цілі має відповідати критерію «Виявлення» для тепловізора та «Розпізнавання» для оптичної камери.

Математичний розрахунок зон виявлення для стаціонарної тепловізійної камери Hikvision DS-2TD2167-25/PI проводять за наведеною нижче методикою.

Кути огляду тепловізійної матриці (640 × 512, розмір пікселя q = 17 мкм) визначають з виразу (2.1) та (2.2):

$$\alpha = 2 \cdot \arctan[W_{m\alpha} / (2 \cdot f)]; \quad (2.1)$$

$$\beta = 2 \cdot \arctan[W_{m\beta} / (2 \cdot f)], \quad (2.2)$$

де: $W_{m\alpha}$ – вертикальний розмір матриці ($W_{m\alpha} = 640 \cdot 17 = 10{,}88$ мм);

$W_{m\beta}$ – горизонтальний розмір матриці ($W_{m\beta} = 512 \cdot 17 = 8{,}71$ мм);

f – фокусна відстань (f = 25 мм).

Тоді кути огляду тепловізійної камери будуть рівні:

$\alpha = 2 \cdot \arctan[10{,}88 / (2 \cdot 25)] \approx 24{,}5°$, $\beta = 2 \cdot \arctan[8{,}71 / (2 \cdot 25)] \approx 19{,}7°$.

Для стабільної роботи ШІ-аналітики із виявлення людини (граничний розмір H = 1,8 м) необхідно, щоб її силует на екрані займав щонайменше 6 пікселів матриці. Максимальну дальність виявлення розраховують з виразу (2.3):

$$L_{max} = (H \cdot f) / (N \cdot q) = (1{,}8 \cdot 0{,}025) / (6 \cdot 17 \cdot 10^{-6}) \approx 441 \text{ м}. \quad (2.3)$$

Враховуючи специфіку географічного розташування полігона спеціального для перевантаження ядерних відходів (ризик поглинання ІЧ-

випромінювання щільним туманом чи дрібною мрякою), доцільно ввести коефіцієнт послаблення середовища $k_п = 0,75$. Тоді ефективна дальність ШІ-детектування суб'єкта доступу буде рівна:

$$L_e = 441 \cdot 0,75 \approx 330 \text{ м}.$$

Оскільки камера встановлена на висоті h = 5 м під нахилом до горизонту ($\gamma = 12°$), під нею утворюється «сліпа зона», і відповідно кут огляду не буде її захоплювати. Довжину «сліпої зони» визначають з виразу (2.4):

$$L_{сз} = h / [\tan(\gamma + \beta/2)] = 5 / [\tan(12 + 19,7/2)] \approx 12,4 \text{ м}. \quad (2.4)$$

Для того, щоб повністю нівелювати «сліпу зону» довжиною 12,4 м необхідно щоб зустрічна камера, яка монтується на протилежній опорі, перекривала цю ділянку. Зважаючи на те, що ефективна дальність роботи тепловізора становить 330 м, а довжина прямих лінійних ділянок загородження не перевищує 250-300 метрів, крок розстановки опор із камерами приймається рівним 250 метрів. Це гарантує 100% взаємне перекриття і дублювання оптичних каналів, повністю виключаючи «мертві зони» вздовж усього лісового масиву.

Специфікація та основні ТТХ запроєктованого оптико-електронного та тепловізійного обладнання зведено у таблиці 2.3.

Таблиця 2.3 – Зведена специфікація засобів оптико-електронного моніторингу

Тип пристрою	Місце та задача розгортання	Режим роботи / Оптика	Ступінь захисту (IP) та стійкість
Стаціонарний біспектральний комплекс Hikvision DS-2TD2167-25/PI	Опори по периметру (крок 250 м). Безперервний контроль лінії загородження	– тепловізор 25 мм (ШІ-детекція до 330 м); – оптика 4 Мп (Dark Fighter); – сталитй кут: 24,5°	IP67 / IK10. Захист від прямих струменів води під час злив, грозозахист TVS 6000V. Вбудований обігрівач скла
Поворотний біспектральний PTZ-комплекс Hikvision DS-2TD6267-75C4L/W	Висотна вежа по центру полігону. Верифікація за координатами та супровід цілей	– тепловізор 75 мм (детекція до 1000 м); – оптика 4 Мп з 50× зумом; – огляд: 360° безпе-рервно	IP67 / Корозійна стійкість. Герметичний корпус з очищувачем скла для видалення крапель дощу та туману

Впровадження цієї конфігурації забезпечить цілодобову верифікацію лінійних тривог у складних метеорологічних умовах та мінімізує вплив людського чинника завдяки первинній фільтрації подій засобами бортової комп’ютерної аналітики камери.

2.3 Вибір програмно-апаратної платформи центру обробки даних

Уніфікація інформаційних потоків, автоматизована обробка сигналів тривоги та управління комплексами інженерно-технічних засобів охорони полігону спеціального для перевантаження ядерного палива реалізується на базі трирівневої архітектури збирання, передавання та аналізу даних. Надійна робота інтелектуального моніторингу в умовах лісистої місцевості забезпечується застосуванням промислового мережевого обладнання з підтримкою протоколів швидкого кільцевого резервування, відмовостійких серверних кластерів та спеціалізованого програмного забезпечення класу PSIM.

2.3.1 Організація лінійно-кабельної інфраструктури та польових вузлів комутації

Периферійний рівень системи складається з шаф дільничних контурних (ШДК), які рівномірно розподіляються за периметром об’єкта проєктування. На ШДК (рис. 2.7) покладено функцію локальних вузлів комутації, у них відбувається первинний збір даних, які надходять з волоконно-оптичних контролерів, радіохвильових бар’єрів, сейсмодавачів та біспектральних камер.

Основою ШДК є керовані промислові комутатори другого рівня (рис. 2.8) або еквівалентне обладнання промислового класу. Ці пристрої підтримують технологію Turbo Ring / Turbo Chain (час відновлення зв’язку < 20 мс за повної відмови магістрального кабелю) та стандарт ITU-T G.8032 ERPS [33]. Це гарантує, що у разі навмисного пошкодження або обриву волоконно-оптичної магістралі на будь-якій ділянці лісового масиву, передавання тривожного відеопотоку та сигналів детектування миттєво перенаправиться у протилежний бік кільця, виключаючи втрату зв’язку з центром обробки даних (ЦОД).

Рисунок 2.7 – Шафа вулична навісна ЦМО ШТВ-Н (ШТВ-Н-15.6.3-4ААА) [31]

Рисунок 2.8 – Комутатор MOXA PT-G7509-F-24-24 [32]

Кожна польова кросова шафа повинна відповідати класу захисту не нижче IP66 [27], виготовляється з нержавіючої сталі та комплектується системою мікроклімату, що унеможливлює формування конденсату.

2.3.2 Апаратний комплекс центру обробки даних та ядра PSIM

Центральним елементом архітектури ІСОП є ЦОД, де розгортається програмно-апаратний комплекс інтеграційної платформи PSIM. Ця платформа виконує роль верхнього рівня управління: зводить в один інтерфейс топологічну карту периметра, інтегрує відеонагляд, тепловізори, СКУД і охоронну сигналізацію, а також автоматично пропонує оператору сценарії реагування на тривоги (Standard Operating Procedures [34]).

Для забезпечення безперебійного функціонування ядра аналітики та збереження баз даних у реальному часі, обчислювальний комплекс ЦОД

будується на відмовостійкому серверному рішенні моделі HPE ProLiant DL380 Gen11 6526Y Server (рис. 2.9) у виконанні 2U. З огляду на необхідність паралельної обробки ШІ-відеоаналітики (класифікація об’єктів та верифікація біспектральних потоків), сервер комплектується спеціалізованим графічним процесором обчислення нейромереж.

Рисунок 2.9 – NAS-сервер HPE ProLiant DL380 Gen11 6526Y Server [35]

Для організації автоматизованих робочих місць (АРМ) операторів служби безпеки запроєктовано високопродуктивну графічну станцію HP Z4 G5 Tower (рис. 2.10) та відеостіну Samsung 4×55″ (рис. 2.11) для безперервного виведення інтерактивної карти полігону та візуальних вікон тривожної верифікації.

Рисунок 2.10 – Робоча станція HP Z4 G5 Tower [36]

Рисунок 2.11 – Відеостіна Samsung 4×55″(221855-K) [37]

Зведені технічні характеристики та конфігурація обладнання ЦОД, лінійних комутаційних вузлів та інтеграційного програмного забезпечення (ПЗ) класу PSIM подано у таблиці 2.4.

Таблиця 2.4 – Конфігурація та експлуатаційні параметри серверного, комутаційного та диспетчерського обладнання

Компонент системи	Конкретна модель обладнання / ПЗ	Ключові тактико-технічні характеристики (ТТХ) та конфігурація	Інженерне обґрунтування вибору підзадачі Grade 4 та ШІ-моніторингу
1	*2*	*3*	*4*
Магістральний промисловий комутатор	MOXA PT-G7509-F-24-24	– 9 Full Gigabit портів (оптичні SFP слоти); – підтримка кольоро-вих протоколів: ERPS (G.8032), Turbo Ring; – робоча температу-ра: від -40 до +85°C (без вентиляторів); – клас стійкості: EMC Level 4, Grade 4 сертифі-кація	Забезпечує миттєве кільцеве резервування мережі (< 20 мс) під час саботажу або пошкодженні кабелю. Стійкий до грозових наводок у лісовій зоні

Продовження таблиці 2.4

1	2	3	4
Центральний сервер обробки та ШІ-аналітики	HPE ProLiant DL380 Gen11 6526Y Server	– 2× процесори Intel Xeon Scalable (по 32 ядра); – ОЗУ: 256 GB DDR5 SmartMemory; – графічний прискорювач: 2× Nvidia Tensor Core H100 (або A100/L4) для ШІ-аналізу; – дисковий масив: RAID 6 (НЖМД SAS 12G Hot Plug); – джерела живлення: 2× 1600W (резервування)	Необхідний для одночасної безперебійної роботи нейромережевих алгоритмів біспектральної аналітики з 20+ каналами периметра та підтримки бази даних PSIM без затримок
Робоче місце оператора	Графічна станція HP Z4 G5 Workstation	– процесор Intel Xeon W-line (8-12 ядер); – відеокарта: Nvidia RTX A4000 (4× DisplayPort 1,4); – ОЗУ: 32 GB; – накопичувач: 1 ТБ NVMe M.2 SSD; – монітори Samsung: 4× 55" Full HD IPS (безрамкові)	Забезпечує паралельне плавне виведення 24 відеопотоків високої роздільної здатності, інтерактивної 3D-карти об’єкта проєктування та швидку реакцію інтерфейсу PSIM під час тривоги
Програмне забезпечення верхнього рівня	ПЗ класу PSIM (WinGuard від Advancis / Milestone XProtect Expert)	– відкрита архітектура інтеграції через SDK/API; – модуль ШІ-класифікації та менеджменту інцидентів; – клієнт-серверна архітектура з гарячим дублюванням серверів (Failover cluster).	Об’єднує усі підсистеми в єдиний інтелектуальний комплекс. Автоматизує процес верифікації, виключаючи людський чинник під час оцінки тривоги

Кліматичне та апаратне виконання обраної платформи ЦОД та мережевого лінійного рівня повністю задовольняє критеріям відмовостійкості об’єктів стратегічного призначення. Завдяки дублюванню магістральних каналів за допомогою оптичного кільця волоконно-оптичних ліній зв’язку та використанню промислових керованих комутаторів Моха з грозозахистом,

побудована мережева інфраструктура здатна витримувати екстремальні погодні та техногенні навантаження.

Обчислювальний потенціал серверної групи з апаратною підтримкою тензорних ядер гарантує мінімальний час відгуку системи на аналіз завадової обстановки та забезпечує нульовий рівень пропуску цілей типу «людина» на фоні складних природних перешкод лісового масиву.

2.4 Методи та алгоритми інтелектуальної обробки сигналів і відеоаналітики

Ефективність функціонування комплексу інженерно-технічних засобів охорони в умовах лісистої місцевості критично залежить від математичного та програмного забезпечення верхнього рівня. Для мінімізації коефіцієнта хибних спрацювань (FAR), викликаних природними завадами (рух гілок дерев, пориви вітру, міграція дрібних тварин), та забезпечення нульового рівня пропускання цілей (FRR) запроваджено дворівневу систему інтелектуальної обробки: локальний нейромережевий аналіз відеопотоків та системну крос-кореляцію сигналів у єдиному PSIM-просторі.

2.4.1 Нейромережева архітектура оброблення біспектральних даних та фільтрування перешкод

Для автоматичного виявлення, класифікації та супроводу об’єктів у реальному часі застосовується комбінація згорткових нейронних мереж (CNN) архітектури YOLOv8 (You Only Look Once [38]), оптимізованих під обчислення на тензорних ядрах графічних процесорів серверної платформи.

Математична задача детектування об’єкта зводиться до мінімізації багатокомпонентної функції втрат, яка повинна враховувати похибку локалізації обмежувальної рамки (Bounding Box) та помилку класифікації (2.5):

$$L_{tot} = \lambda_{box} \cdot L_{box}(b, b') + \lambda_{cls} \cdot L_{cls}(c, c'), \qquad (2.5)$$

де b та $b^{/}$ – реальні та прогнозовані координати рамки порушника;

c, $c^{/}$ – реальний та розподілений нейромережею вектори ймовірностей класів;

λ_{box} та λ_{cls} – регуляризуючі вагові коефіцієнти.

Для відсіювання перешкод біогенного походження та гідрометеорологічних явищ нейромережа навчена на специфічному датасеті з використанням операцій просторового та часового фільтрування (рис. 2.12).

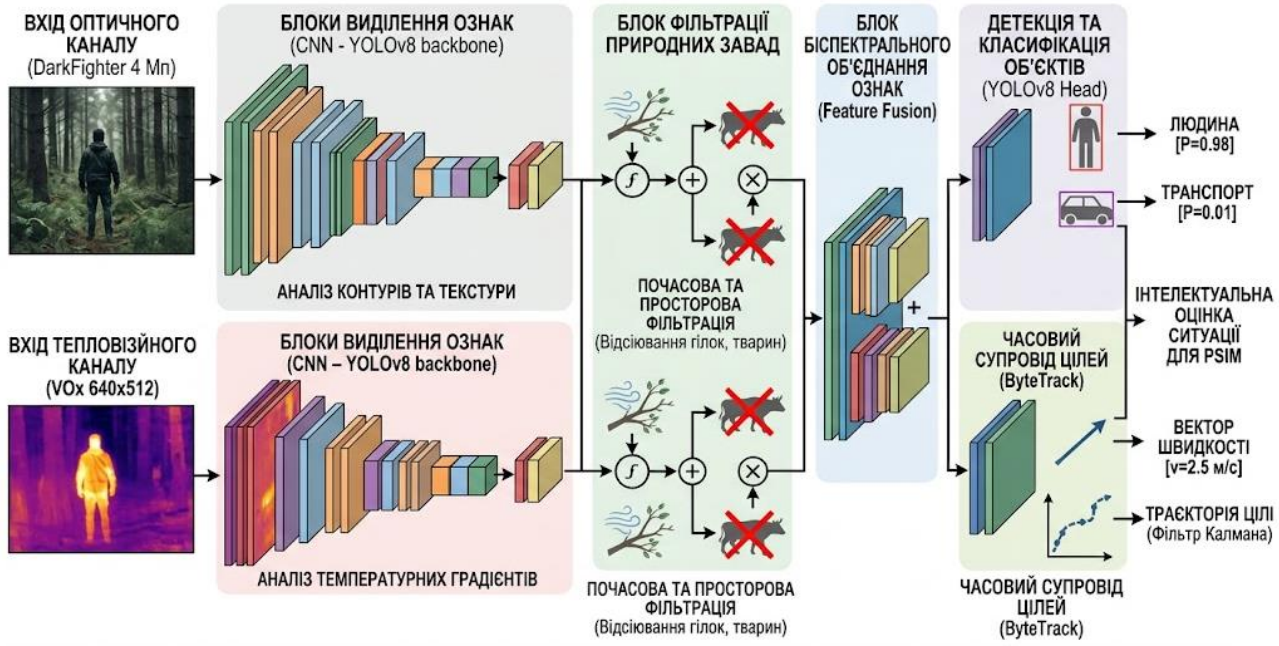

Рисунок 2.12 – Нейромережева архітектура обробки біспектральних даних та фільтрування перешкод

Просторове фільтрування (Spatial Filtering) – згорткові шари мережі виділяють високорівневі текстурні та геометричні ознаки цілі (співвідношення сторін антропоморфного силуету людини 1:3 та характерні теплові контрасти кінцівок). Гілки дерев відсіюються на етапі аналізу карт ознак через хаотичність структури та відсутність замкнутих контурів з високим градієнтом яскравості.

Часове фільтрування – після первинного детектування об’єкта його координати передаються на алгоритм ByteTrack [39], який використовує фільтр

Калмана для прогнозування траєкторії руху. Класифікація «людина» підтверджується лише за умови стабільного вектора швидкості протягом 0,5 с, тоді як коливальні рухи кущів навколо фіксованої точки мають нульовий результуючий вектор і маркуються як «шум середовища».

2.4.2 Алгоритми інтеграції та крос-кореляції подій у PSIM-просторі

Верхній ієрархічний рівень системи функціонує як шина обміну даними у реальному часі, об’єднуючи гетерогенне обладнання за допомогою стандартизованих промислових та безпекових протоколів:

– ONVIF (Profile S, G, T): для отримання біспектральних відеопотоків, керування PTZ-приводами та трансляції метаданих ШІ-аналітики з камер;

– Modbus TCP / OPC UA: для низькорівневого збору телеметрії, сигналів тривог від контролерів ВОС та діагностики стану шаф ШДК;

– BACnet / IP: інтеграція із системами життєзабезпечення ЦОД.

Математична логіка верифікації тривог у PSIM-просторі базується на апараті булевої алгебри та теорії ймовірностей Байєса. Замість лінійного реагування на один давач, система реалізує алгоритм просторово-часової крос-кореляції (Multi-sensor Data Fusion [40]). Тривожний сигнал генерується на основі логічної функції вищих порядків (2.6):

$$S_{тр} = (S_{опт} \cap S_{тепл}) \cup (S_{ВОС} \cap [S_{опт} \cup S_{сейсм}]), \quad (2.6)$$

де $S_{ВОС}$ – бінарний сигнал, який надходить від лінійного волоконно-оптичного сенсора на паркані;

$S_{сейсм}$ – сигнал, який формується геосенсором;

$S_{опт}$ та $S_{тепл}$ – ШІ-детекування «людина» оптичною та тепловізійною камерою відповідно.

Якщо кабель ВОС фіксує вібрацію паркану ($S_{ВОС} = 1$), PSIM-платформа автоматично обчислює апостеріорну ймовірність істинного прориву за виразом Байєса (2.7):

$$P(A|B) = [(P(B|A)\cdot P(A)] / P(B), \quad (2.7)$$

де: P(A) – апріорна ймовірність вторгнення на конкретній ділянці;

P(B|A) – ймовірність того, що ШІ-аналітика камери підтвердить ціль за умови реального вторгнення.

Одночасно з цим PSIM видає команду на поворотну PTZ-камеру для наведення в географічну координату спрацювання. Якщо протягом $\lambda = 3$ с нейромережа підтверджує наявність антропоморфної цілі в зоні ($S_{тепл} = 1$ або $S_{опт} = 1$), ймовірність P(A|B) наближається до 99,8 %, і на АРМ оператора миттєво активується сценарій картки інциденту (SOP) з виведенням відеотіні та маршруту висування тривожної групи. Якщо підтвердження від ШІ-аналітики відсутнє, а амплітуда сигналу кабеля відповідає сигнатурі вітрового навантаження, подія автоматично архівується як «низькопріоритетна технічна подія», що розвантажує оператора та зводить людський чинник до мінімуму.

2.5 Обґрунтування підсистем інженерного забезпечення, безперебійного живлення та заземлення

Надійність функціонування комплексу інженерно-технічних засобів охорони полігону спеціального для перевантаження ядерних відходів в умовах автономної роботи та грозової активності Полісся забезпечується проєктуванням інженерної інфраструктури відповідно до вимог ДСТУ EN 50131 (для систем Grade 4) та ДСТУ EN 62305-1:2012 [41]. Електропостачання комплексу відноситься до I категорії, що вимагає наявності двох незалежних взаєморезервованих джерел змінного струму та третього (особлива група) – автономного джерела живлення на базі акумуляторних батарей (АКБ) та дизель-генераторної установки (ДГУ).

2.5.1 Розрахунок параметрів безперебійного живлення та ємності АКБ

Для забезпечення безперервного моніторингу периметра під час повного

знеструмленні об’єкта, підсистема безперебійного живлення повинна підтримувати працездатність усіх польових пристроїв, мережевих засобів та ЦОД протягом деякого часу, який буде необхідним для запуску ДГУ або ліквідування аварії. Відповідно до вимог Grade 4, мінімальний час автономної роботи від АКБ становить 4 години (у режимі очікування) + 1 година (у режимі повної тривоги з увімкненим освітленням та PTZ-камерами).

Розрахунок ємності акумуляторних батарей для центрального вузла та шаф ШДК виконується за виразом (2.8):

$$C_{АКБ} = [(P_{очік} \cdot t_{очік} + P_{трив} \cdot t_{трив}) \cdot k_{ез}] / (U_{напр} \cdot \eta \cdot k_{роз}), \quad (2.8)$$

де $P_{очік}$ – споживана потужність системи в режимі очікування (2400 Вт для ЦОД + магістраль);

$P_{трив}$ – споживана потужність у режимі тривоги (3600 Вт, враховуючи активацію прожекторів та приводів PTZ);

$t_{очік}$ та $t_{трив}$ – час роботи в режимах очікування (4 год) та тривоги (1 год);

$k_{ез}$ – коефіцієнт експлуатаційного запасу ($k_{ез}$ = 1,2 – враховує старіння АКБ);

$U_{напр}$ – номінальна напруга постійного струму шини джерела безперебійного живлення ($U_{напр}$ = 48 В);

η – коефіцієнт корисної дії інвертора джерела безперебійного живлення (η = 0,92);

$k_{роз}$ – коефіцієнт максимально допустимого розряду АКБ ($k_{роз}$ = 0,8 – для запобігання деградації пластин).

Визначимо загальну необхідну ємність центрального буфера:

$$C_{АКБ} = [(2400 \cdot 4 + 3600 \cdot 1) \cdot 1,2] / (48 \cdot 0,92 \cdot 0,8) \approx 448,36 \text{ А·год.}$$

Для забезпечення цієї ємності обираємо масив із герметизованих свинцево-кислотних акумуляторів типу AGM (Absorbent Glass Mat) Deep Cycle [42] напругою 12 В та ємністю 150 А·год кожен. Для формування шини 48 В

акумулятори з’єднуються послідовно в лінійки (по 4 блоки), а для досягнення цільової ємності лінійки підключаються паралельно.

Необхідна кількість блоків: 3 паралельні лінійки по 4 блоки в кожній, тобто 12 акумуляторів ємністю 150 А·год.

2.5.2 Комплексний блискавкозахист та заземлення комунікацій

Оскільки периметр проходить через лісисту місцевість з високою грозовою активністю, а сенсорні елементи (радіохвильові бар’єри, камери) встановлені на металевих опорах висотою до 5 м, існує високий ризик прямих ударів блискавки та вторинних електромагнітних наводок. Блискавкозахист реалізується як двокомпонентна система: зовнішня (пасивна) та внутрішня (активна).

Зовнішній блискавкозахист. Кожна опора з біспектральною камерою обладнується індивідуальним стрижневим блискавковідводом висотою 1,0 м, який виготовлено з оцинкованої сталі. Струмовідвід виконується сталевим дротом (каткою) діаметром не менше 8 мм, який прокладається по тілу опори та з’єднується з локальним заземлювачем.

Внутрішній блискавкозахист (ешелонований захист від імпульсних перенапруг). Для захисту електронних плат комутаторів MOXA та лінійних інтерфейсів давачів у кожній шафі ШДК встановлюють пристрої захисту від імпульсних перенапруг (ПЗІП) трьох класів:

– Клас 1 та Клас 2 (Тип 1 + Тип 2): встановлюють на вводах ліній живлення 220 В для гасіння енергії залишків струму блискавки;

– Клас 3 (Тип 3 / сигнальний): спеціалізовані модулі захисту для слабкострумових мереж та інтерфейсів (Ethernet PoE, RS-485). Для мідних ділянок кабелів зв’язку Ethernet (інтерфейси біспектральних камер) застосовуються ПЗІП з часом спрацювання $t_{спр} < 1$ нс.

Система заземлення. Контур заземлення кожної опори та шафи ШДК виконується за схемою «трикутник» (три вертикальні електроди з кутової сталі 50×50×5 мм довжиною 2,5 м, забиті в землю та з’єднані сталевою полосою 40×4 мм методом зварювання). Відповідно до вимог чинних нормативних

документів, імпульсний опір заземлення для систем зв’язку та безпеки в будь-яку пору року не повинен перевищувати $R_{заз} \leq 4$ Ом.

Основні експлуатаційні характеристики, конфігурація обладнання систем безперебійного живлення, ПЗІП та елементів контуру заземлення зведено до таблиці 2.5.

Таблиця 2.5 – Технічна специфікація підсистем інженерного забезпечення та живлення

Компонент інфраструктури	Модель обладнання / Матеріал	Основні технічні параметри	Призначення елемента в контурі Grade 4
Промислове джерело безперебійного живлення	APC Smart-UPS SRT 5000VA (або еквівалент)	– потужність: 4,5 кВт / 5,0 кВА; – топологія: подвійне перетворення (On-Line); – вихідна напруга: 230 В (чиста синусоїда)	Забезпечує нульовий час перемикання (0 мс) на роботу від АКБ під час зникнення основної мережі, захищає ЦОД від стрибків напруги
Акумуляторні батареї буфера	Ventura GPL 12-150 (AGM Deep Cycle)	– номінальна напруга: 12 В; – ємність: 150 А·год; – термін служби: від 10 до 12 років у буферному режимі	Формують відмовостійкий масив ємністю 450 А·год (при 48 В). Забезпечують 5 годин автономної роботи КІТЗО
Сигнальний захист Ethernet ліній	MOXA PT-G7509-F-24-24 (або Phoenix Contact)	– швидкість: 10/100 Мбіт/с; – максимальний струм розряду (I_{max}): 5 кА; – час відклику: < 1 нс	Захист портів комутаторів та біспектральних камер від наведених електромагнітних імпульсів під час близьких ударів блискавок
Контур заземлення та блискавковідвід	Сталь гарячого цинкування	– стрижневий приймач: Ø16 мм, l = 1,0 м; – опір контуру: Ø 4 Ом; – смуга заземлення: 40×4 мм.	Перенаправлення струму блискавки в землю, вирівнювання потенціалів між корпусами обладнання ШДК та землею.

Як бачимо, запропонована інженерна підсистема дозволяє гарантувати безперебійність збору та аналізу інформації з периметра за умов виникнення критичних дестабілізуючих чинників кліматичного або техногенного походження, що повністю задовольняє критеріям безпеки спеціальних об’єктів.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ

3.1 Монтаж периферійного обладнання та побудова кабельної інфраструктури

Практична реалізація інформаційної системи охорони периметра на полігоні спеціальному для перевантаження ядерних відходів вимагає врахування низки дестабілізуючих природних чинників. Серед основних варто виділити: висока вологість ґрунту, наявність розгалуженої кореневої системи дерев, сезонні підтоплення та підвищена грозова активність. Процес інженерного розгортання периферійного ешелону КІТЗО поділяється на три взаємопов’язані етапи: прокладання магістральних комунікацій, монтаж опорних конструкцій із дільничними шафами та улаштування локальних систем фізичного захисту й заземлення.

3.1.1 Специфіка прокладання волоконно-оптичного кабелю

Для забезпечення живучості системи класу Grade 4 магістральна мережа передавання даних реалізується шляхом комбінованого прокладання волоконно-оптичного кабелю (ВОК).

Підземне прокладання магістрального кільця. Основне відмовостійке кільце зв’язку прокладається в ґрунті на глибині не менше 0,9 м вздовж технологічної просіки охоронної зони периметра (рис. 3.1). Враховуючи специфіку лісового масиву, варто застосовувати лише спеціалізований кабель з бронею з гофрованою сталевою стрічкою та захисним шлангом із поліетилену високої щільності (ПівденКабель ОБгПо). На ділянках із підвищеним рівнем ґрунтових вод та переходах через заболочені місця кабель додатково затягується у гнучкі двостінні гофровані труби типу ПНД/ПВТ діаметром 40 мм. Для компенсації температурних розширень на кожні 100 метрів траси передбачається S-подібний запас кабелю довжиною від 1,5 до 2 метрів.

Прокладання розподільчої мережі по загородженню. Підключення лінійних давачів (волоконно-оптичного вібраційного сенсора) виконується

безпосередньо по полотну сітчастого загородження або плоского бар'єра безпеки (рис. 3.2). Кабель кріпиться за допомогою стійких до ультрафіолету та температурних коливань сталевих або пластикових стяжок із кроком від 25 до 30 см. Магістральний кабель піднімається зі шурфу до загородження виключно всередині сталевої захисної труби (антивандальний рукав) на висоту до 2,0 відносно рівня землі.

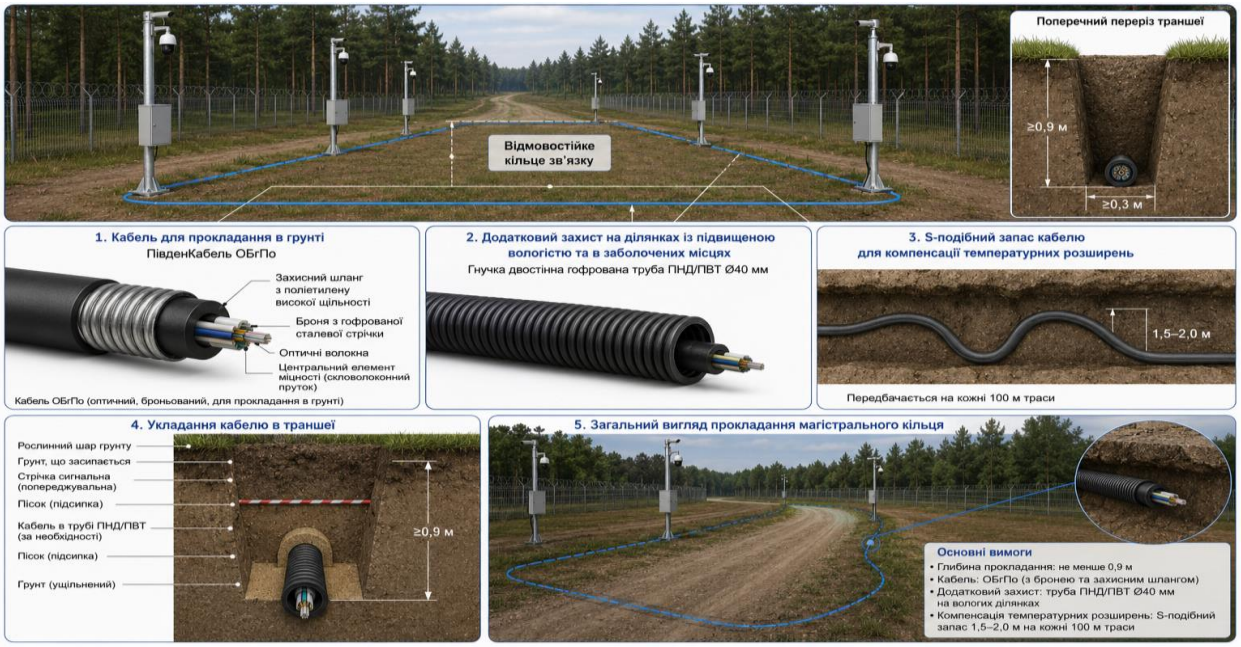

Рисунок 3.1 – Схема підземного прокладання магістрального кільця ВОК

Рисунок 3.2 – Монтаж розподільчої мережі та лінійних давачів

3.1.2 Монтаж опор під біспектральні камери та встановлення шаф ШДК

Розміщення засобів візуальної верифікації та комутаційних вузлів виконується на спеціально підготовлених точках периметра з дотриманням просторової геометрії.

Проміжні та кутові опори. Для встановлення біспектральних стаціонарних та PTZ-камер використовуються круглі конічні металеві опори висотою 5 м (рис. 3.3) із гарячим цинкуванням для захисту від корозії в умовах лісової вологості. Кутові опори, які зазнають підвищеного вітрового навантаження та натягу загородження, додатково посилюються ребрами жорсткості в основі.

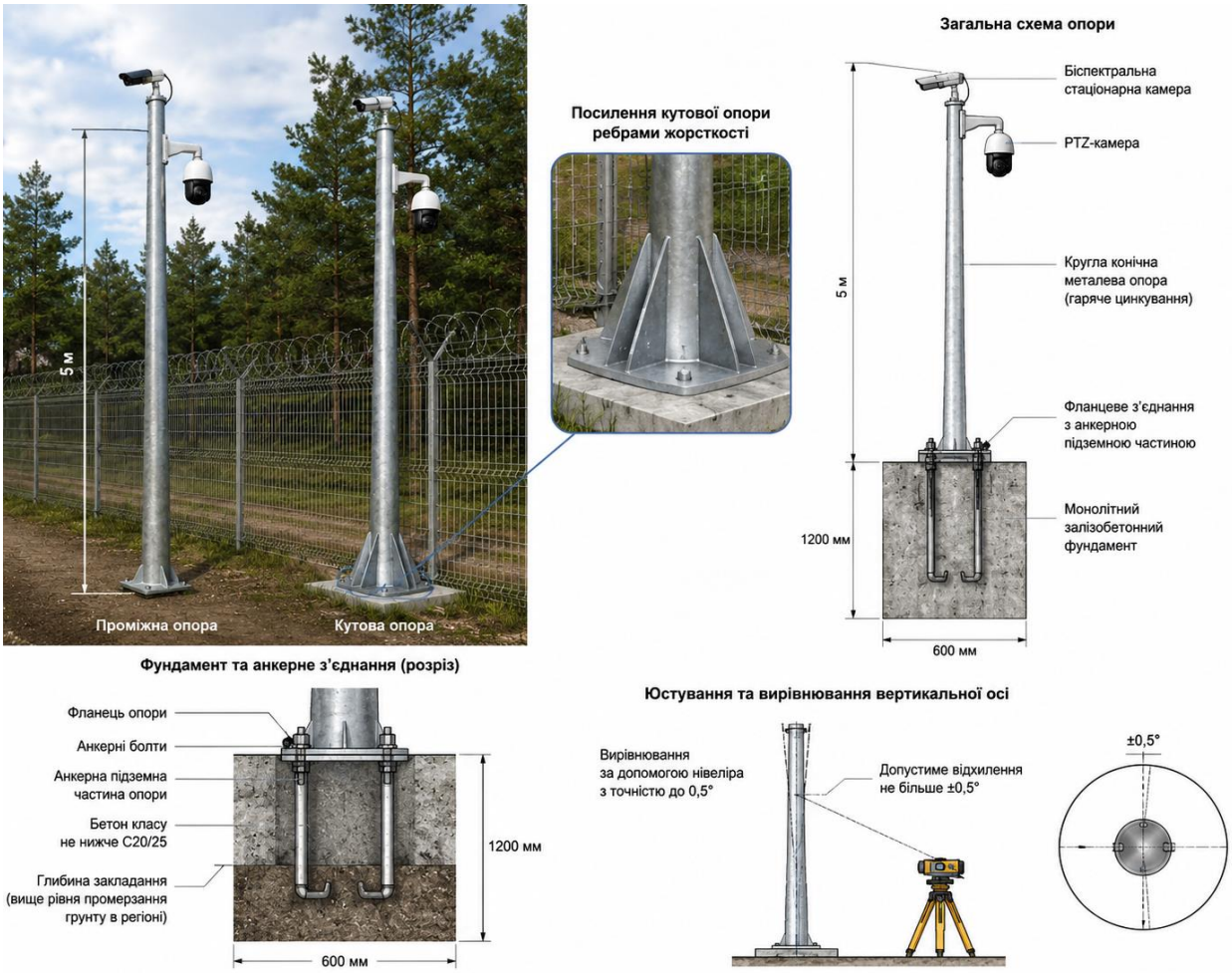

Рисунок 3.3 – Монтаж опор

Монтаж опор здійснюється на монолітний залізобетонний фундамент розміром 600×600×1200 мм (глибина закладання вища за рівень промерзання

ґрунту в регіоні). Опора фіксується на анкерну підземну частину за допомогою фланцевого з’єднання, що дозволяє проводити юстування та вирівнювання вертикальної осі за допомогою нівеліра з точністю до 0,5°.

Встановлення шаф ШДК. Кросові шафи дільничі контурні монтуються безпосередньо на тіло опорних металевих конструкцій (рис. 3.4) на висоті 1,5 м від поверхні землі (для зручності обслуговування та захисту від снігових заметів). Ввід кабельних трас (оптики та живлення ~220 В) в ШДК здійснюється виключно знизу через герметичні сальникові вводи (гермовводи) класу не нижче IP66. Всередині кожної шафи на DIN-рейку встановлюється промисловий комутатор MOXA, медіаконвертери, оптичний міні-крос (FOB), блок живлення та шина заземлення.

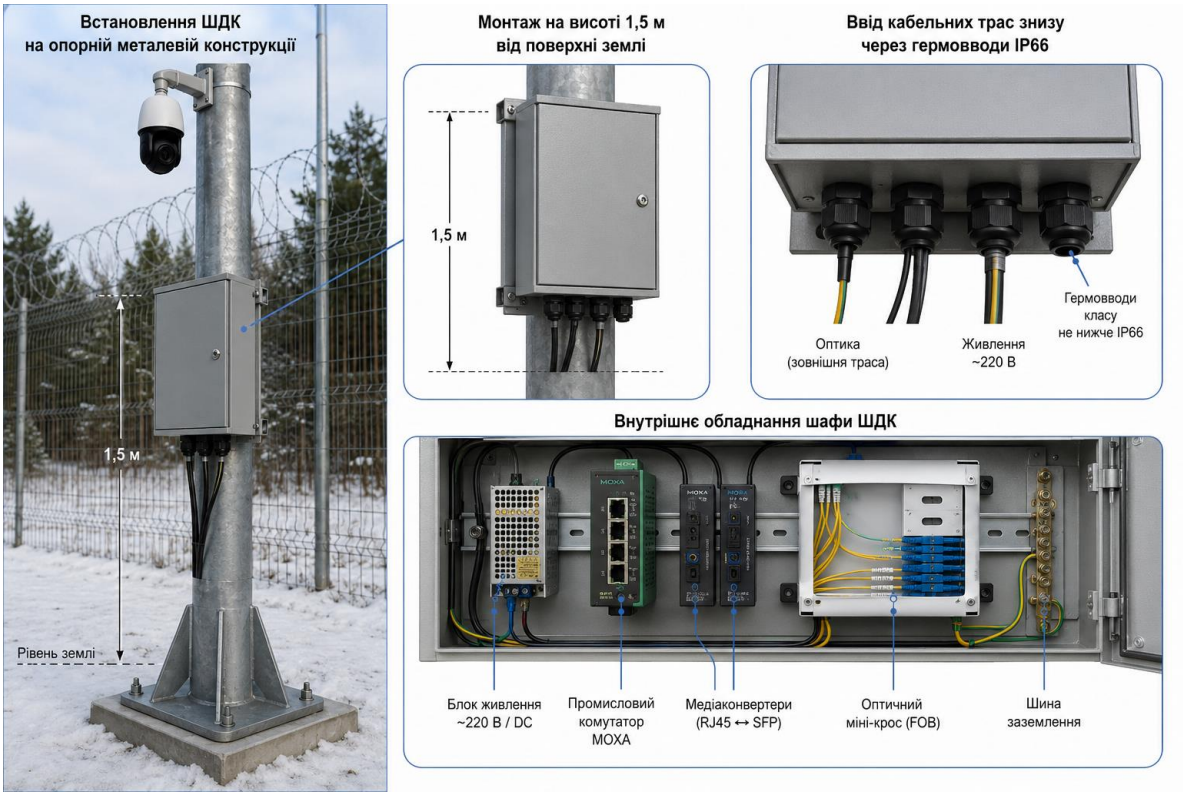

Рисунок 3.4 – Монтаж шаф ШДК

3.1.3 Організація локальних контурів заземлення та монтаж ПЗІП

Для мінімізації ризику виходу з ладу дорогої периферійної електроніки від наведених грозових потенціалів, кожна опора з ШДК перетворюється на самостійний захищений вузол.

Облаштування контуру заземлення. Біля основи кожного фундаменту опори облаштовується локальний заземлювач (рис. 3.5). За схемою «лінійний ряд» або «трикутник» у ґрунт забиваються три сталеві оцинковані стержні діаметром 16 мм та довжиною 2,5 м. Стержні з’єднуються між собою сталевою полосою 40×4 мм за допомогою різьбового з’єднання, оброблених антикорозійною бітумною мастикою. Вивід смуги підключається безпосередньо до болта заземлення на фланці опори. Завдяки високій природній вологості лісових ґрунтів регіону розташування об’єкта, опір розтікання струму кожного контуру має становити $R \leq 3{,}8$ Ом, що повністю задовольняє нормативні вимоги для систем зв’язку та відеоспостереження охоронного призначення.

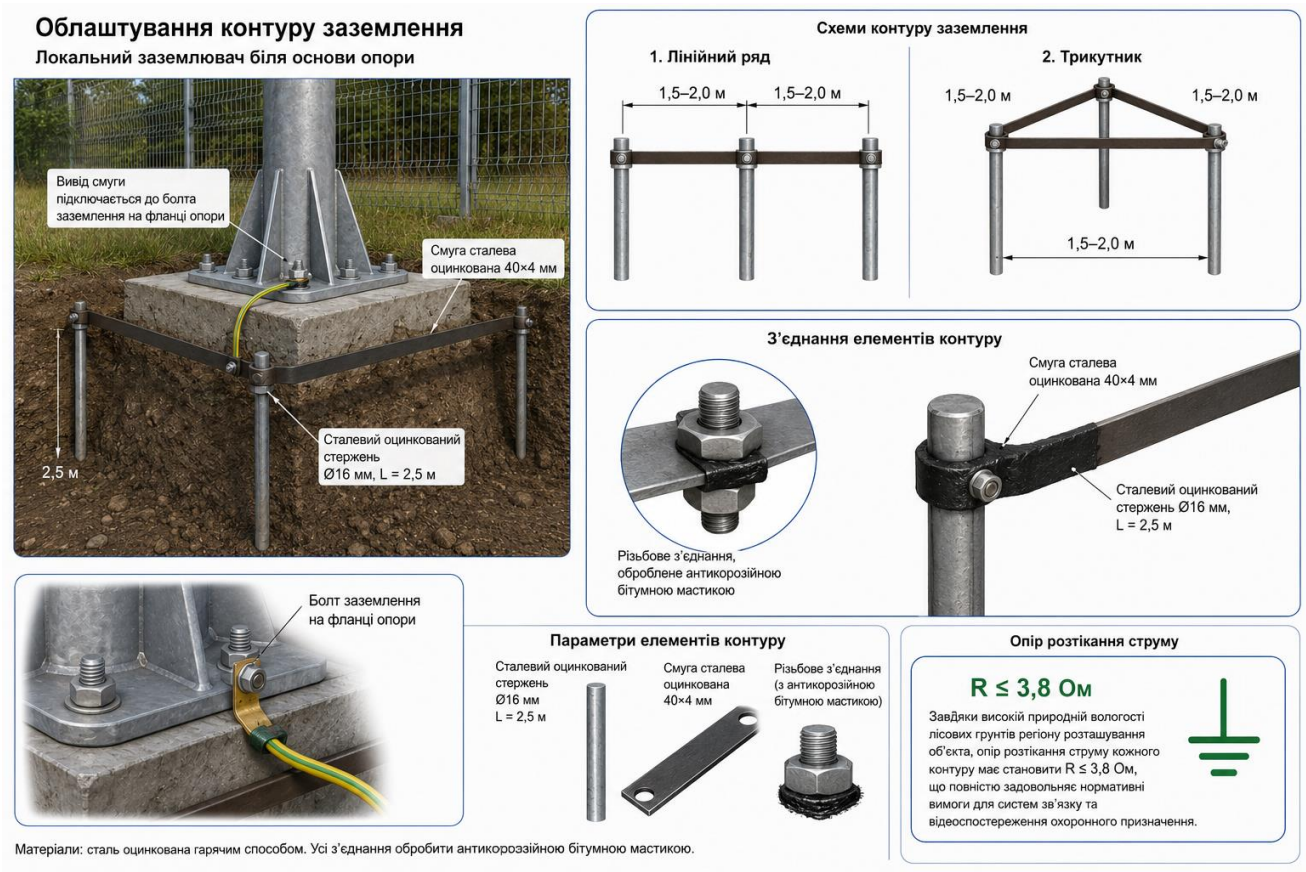

Рисунок 3.5 – Облаштування локального заземлювача

Монтаж модулів ПЗІП. Ешелонований захист електронних компонентів монтується безпосередньо в корпусі ШДК та на кронштейнах камер (рис. 3.6):

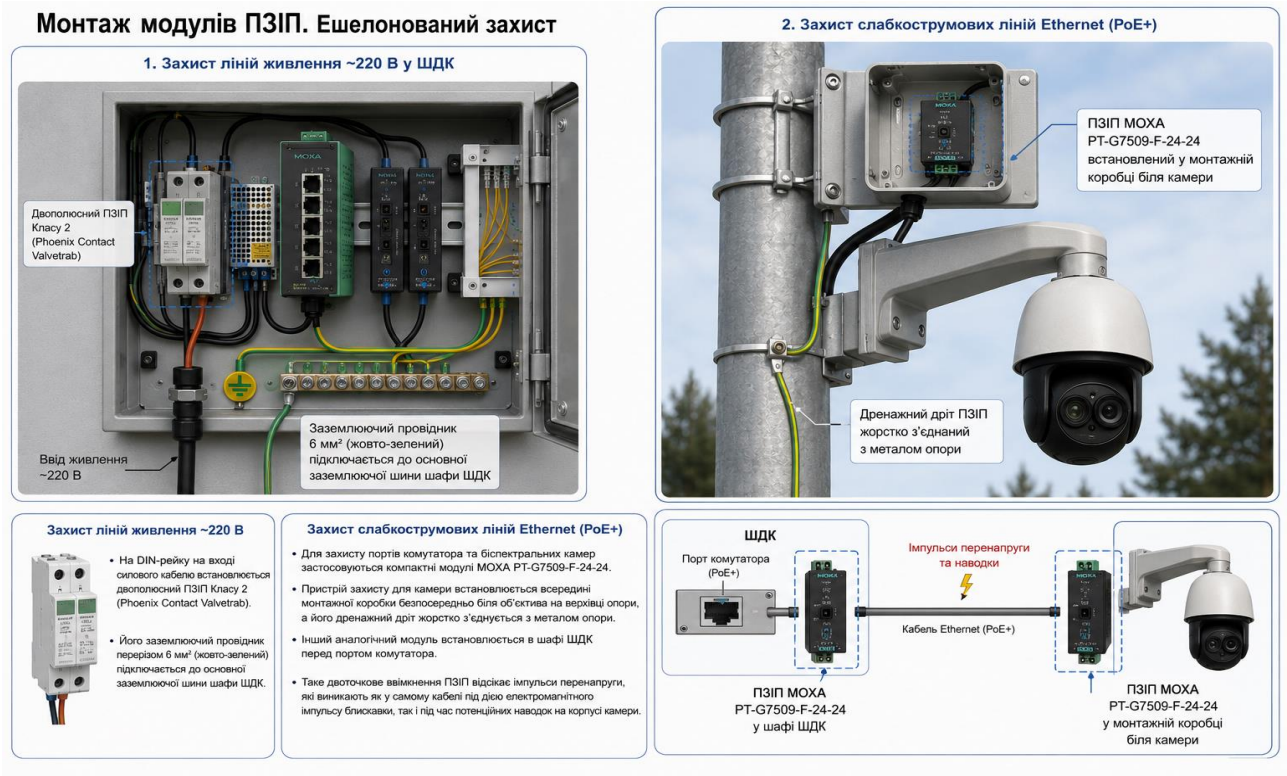

Рисунок 3.6 – монтаж пристроїв захисту від імпульсних перенапруг

– захист ліній живлення ~220 В: на DIN-рейку на вході силового кабелю встановлюється двополюсний ПЗІП Класу 2 (наприклад, Phoenix Contact Valvetrab), його заземлюючий провідник поперечним перетином 6 мм^2 (жовто-зелений колір) підключається до основної заземлюючої шини шафи ШДК;

– захист слабкострумових ліній Ethernet (PoE+): для захисту портів комутатора та біспектральних камер застосовуються компактні модулі MOXA PT-G7509-F-24-24; пристрій захисту для камери встановлюється всередині монтажної коробки безпосередньо біля об’єктива на верхівці опори, а його дренажний дріт жорстко з’єднується з металом опори, а інший аналогічний модуль встановлюється в шафі ШДК перед портом комутатора.

3.2 Конфігурація відмовостійкої магістральної мережі та налаштування кільцевого резервування

Практична реалізація мережевого ешелону комплексу інженерно-технічних засобів охорони полігону спеціального базується на розгортанні

високошвидкісного оптичного кільця зв’язку. Для об’єктів класу Grade 4 критично важливим є забезпечення мінімального часу відновлення мережі, за умови фізичного розриву, магістрального кабелю.

3.2.1 Схема комутації та фізичне об’єднання комутаторів в оптичне кільце

Магістральний ешелон формується з N дільничних комутаторів MOXA PT-G7509-F-24-24, розташованих у шафах ШДК по периметру, та одного центрального комутатора ядра в будівлі ЦОД.

Фізичне з’єднання елементів виконується за топологією «резервоване кільце» (Ring) з використанням гігабітних оптичних SFP-модулів (одномодове волокно, довжина хвилі 1310 нм, роз’єми LC). Комутація кожного лінійного вузла здійснюється за наступною схемою:

– оптичний кабель, який приходить з попереднього вузла (напрямок «Захід»), розварюється в оптичному кросі шафи ШДК і через патч-корд підключається до Порт 7 (SFP Slot 1) комутатора MOXA;

– оптичний кабель, який йде на наступний за контуром вузол (напрямок «Схід»), розварюється та підключається до Порт 8 (SFP Slot 2) цього ж комутатора.

Таким чином, порти 7 та 8 на кожному промисловому комутаторі призначаються фізичними носіями кільцевої магістралі (Ring Ports). Порти з 1 по 6 (мідні або PoE SFP) використовують для підключення локальної периферії: біспектральних камер, контролерів вібраційного кабелю та сейсмосенсорів.

3.2.2 Покрокове налаштування протоколу резервування ERPS (ITU-T G.8032)

Для запобігання утворенню широкомовних штормів (петляння трафіку) та забезпечення часу відновлення мережі ≤ 50 мс впроваджують міжнародний стандарт ITU-T G.8032 ERPS v2 [43]. На відміну від класичного STP/RSTP, ERPS оптимізований для промислових кілець великого радіуса.

Процес параметризації через веб-інтерфейс (або CLI) комутаторів MOXA складається із нижченаведених кроків.

Крок 1: призначення ролей у кільці. Один із комутаторів (зазвичай комутатор ядра в ЦОД) налаштовується як RPL Owner (Ring Protection Link Owner). Один із його магістральних портів (наприклад, Порт 8) програмно блокується в нормальному режимі роботи, що розриває логічну петлю. Усі інші комутатори в шафах ШДК конфігуруються у режимі RPL Node (звичайний вузол кільця).

Крок 2: активація ERPS в інтерфейсі MOXA. У меню `Communication Redundancy → Ethernet Ring Protection Switching (ERPS)` виставляються такі параметри:

– `ERPS Enable`: Checked;

– `Ring ID`: 1;

– `East Port`: Port 7 (напрямок «Схід»);

– `West Port`: Port 8 (напрямок «Захід»);

– `WTR Timer (Wait-to-Restore)`: 5 min (час очікування перед поверненням кільця в базовий стан після відновлення кабелю, щоб уникнути нестабільності зв’язку).

Крок 3: налаштування сигнальних VLAN (Control VLAN). Створюється виділений `Control VLAN` (наприклад, VLAN 100), яким комутатори обмінюються службовими R-APS (Ring Auto Protection Switching) повідомленнями про стан лінків. Передача користувацького трафіку через цей VLAN суворо заборонена.

3.2.3 Сегментація трафіку (VLAN) та захист від саботажу

Для захисту інформаційної системи від мережевих перевантажень, викликаних трансляцією важкого відеопотоку високої чіткості, а також для унеможливлення несанкціонованого доступу (саботажу) у разі фізичного розкриття лінійної шафи ШДК, застосовується чітке розділення мережі на віртуальні локальні мережі згідно зі стандартом IEEE 802.1Q [44].

Запроєктовані логічні контури системи наведено в таблиці 3.1.

До практичних заходів протидії саботажу відносять як блокування незадіяних портів, так і прив’язку до MAC-адрес (`Port Security`).

Таблиця 3.1 – Схема розподілу тегованого трафіку в магістралі КІТЗО

Ідентифікатор (VLAN ID)	Назва мережевого контуру	Тип тегування портів (802.1Q)	Пріоритет Qos (802.1p)	Опис та заходи безпеки контуру
VLAN 10	CCTV_Stream	Tagged (Магістраль) / Untagged (Порти камер)	5 (High)	Трансляція біспектральних відеопотоків (оптика + тепловізор) та ШІ-метаданих від камер до сервера ЦОД
VLAN 20	Sensors_Data	Tagged (Магістраль) / Untagged (Порти давачів)	6 (Critical)	Передавання тривожних сигналів і телеметрії від волоконно-оптичного кабелю та геосенсорів
VLAN 30	Mngmt_Network	Tagged (Магістраль) / Заблоковано на периферії	3 (Normal)	Доступ до веб-інтерфейсів та CLI комутаторів, ДБЖ, контролерів. Дозволено лише з АРМ адміністратора в ЦОД
VLAN 100	ERPS_Control	Tagged (Виключно магістральні порти 7, 8)	7 (Highest)	Службовий трафік протоколу G.8032 для миттєвої перебудови топології мережі під час аварій

У перших усі фізичні порти на комутаторах MOXA в шафах ШДК, які не використовуються для підключення проєктних пристроїв, програмно переводяться в стан Administrative Shutdown. А у других – на периферійних портах (з 1 по 6) активується функція Static MAC Address Binding. Якщо зловмисник відключить камеру і спробує під'єднати свій ноутбук до Ethernet-кабелю, комутатор зафіксує зміну MAC-адреси, миттєво заблокує цей порт (Disabling port) і надішле SNMP-trap тривогу «Саботаж лінії» на АРМ оператора через захищений контур VLAN 20.

3.3 Розгортання програмного комплексу PSIM та параметризація алгоритмів ШІ-відеоаналітики

Фінальний етап побудови інформаційної системи охорони периметра полігону спеціального для перевантаження ядерних відходів полягає в

інтеграції гетерогенних підсистем нижнього та магістрального рівнів у єдиний інтелектуальний простір управління. Програмне забезпечення класу PSIM, розгорнуте на базі центрального сервера ЦОД, виступає як інтеграційна шина даних, яка не просто акумулює потоки інформації, а здійснює їх крос-кореляцію та автоматизує роботу оператора чергової зміни.

3.3.1 Інсталяція та налаштування серверної частини PSIM-платформи

Практична реалізація серверної архітектури виконується на базі обраного програмного комплексу з відкритими інтерфейсами інтеграції (SDK/API). Процес розгортання та базової конфігурації платформи складається з наступних технологічних кроків:

– ініціалізація відмовостійкого кластера (`Failover`): на серверній платформі HP ProLiant DL380 Gen11 під керуванням ОС Linux (Enterprise-рівня) розгортається ядро PSIM-сервера; для забезпечення вимог класу Grade 4 налаштовується архітектура гарячого резервування: основний сервер (Active) синхронізує базу даних конфігурації та подій у реальному часі з резервним сервером (Standby); час перемикання, у разі апаратного збою основного сервера, становить $\lambda \leq 2$ с із повним збереженням логів;

– інтеграція периферійних драйверів (`Southbound Interfaces`): через менеджер підключень до системи додають лінійні драйвери для зв’язку з комутаторами магістралі та кінцевими пристроями; збір телеметрії з кросових шаф та контролерів волоконно-оптичного вібраційного кабелю здійснюється шляхом опитування регістрів по протоколу `Modbus TCP` (порт 502); зв’язок із біспектральним телевізійними комплексами реалізується через протокол `ONVIF Profile T`, що дозволяє отримувати H.265-відеопотоки високої чіткості, координувати PTZ-приводи та зчитувати метадані ШІ-аналітики.

3.3.2 Практичне розгортання та завантаження інтерактивної карти об’єкта (ГІС/2D-План)

Для забезпечення просторової орієнтації оператора АРМ охорони, у модулі моніторингу PSIM здійснюється завантаження інтерактивної багатошарової карти полігону:

– прив’язка географічних координат: у систему імпортується векторна карта об’єкта у форматі DXF або спеціалізована підкладка ГІС (геоінформаційна система) з точними геодезичними координатами WGS-84;

– впровадження динамічних шарів: на карту наносяться шари інженерних споруд; кожен давач периметра, лінійне загородження та біспектральна камера розміщуються на плані у вигляді динамічних макрооб’єктів (відповідно до їх реальних координат та ID у мережі);

– конфігурація конусів огляду камери: для кожної стаціонарної біспектральної камери на мапі програмується векторний конус огляду, колір якого динамічно змінюється залежно від стану камери (зелений – норма, миготливий червоний – тривога в даній зоні, сірий – втрата зв’язку з вузлом).

3.3.3 Параметризація зон детектування та калібрування алгоритму YOLOv8

Локальний аналіз відеозображення здійснюється на тензорних ядрах графічних прискорювачів Nvidia сервера аналітики за допомогою нейромережевої моделі YOLOv8. Процес практичного налаштування алгоритму для кожної біспектральної камери містить наступні кроки:

– завдання віртуальних ліній та зон охорони (`Region of Interest`): через інтерфейс конфігурації камери поверх відеопотоку оптичного та тепловізійного каналів малюється закрита зона виявлення (зона відчуження безпосередньо перед загородженням) та тривожна лінія (віртуальний бар’єр на самому паркані); для кожної лінії задається вектор допустимого напрямку руху: тривога генерується лише під час руху суб’єкта виявлення вглиб охоронного об’єкта (напрямок «Вторгнення»);

– калібрування розмірів та геометрії цілей: для запобігання хибним спрацюванням від біогенних чинників (рух птахів біля об’єктива, міграція диких звірів) в алгоритмі YOLOv8 виставляються геометричні фільтри класифікатора; задаються мінімальні та максимальні лінійні розміри об’єктів (в пікселях) для класів «Людина» (співвідношення сторін силуету 1:3) та «Транспортний засіб»; об’єкти, які не відповідають критеріям (наприклад,

тварини низької посадки з горизонтальною орієнтацією тіла), маркуються алгоритмом як «Нерелевантний Шум» і фільтруються на етапі первинної обробки кадрів;

– налаштування порогу чутливості (`Confidence Threshold`): пороговий рівень впевненості нейромережі для генерації тривоги виставляється на рівні Conf=0,82, що гарантує стабільне розпізнавання антропоморфної цілі навіть в умовах задимлення, туману чи снігопаду через тепловізійний канал (LWIR-діапазон) із мінімальною ймовірністю пропуску порушника (FRR→0).

3.3.4 Програмування сценаріїв автоматичного реагування (SOP) під час крос-кореляції сигналів

Найвідповідальнішою частиною інтеграції є автоматизація логіки реагування системи за допомогою сценаріїв SOP (Додаток А). Замість відображення сотень хаотичних повідомлень, PSIM реалізує просторово-часову крос-кореляцію (кореляційний аналіз суміжних подій).

ЗАГАЛЬНІ ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

У цій роботі вирішено актуальну інженерно-технічну проблему проєктування, розробки та програмно-апаратної інтеграції високонадійної інформаційної системи охорони периметра спеціального полігону класу Grade 4. На основі опрацьованого матеріалу, інженерних розрахунків та програмно-апаратних конфігурацій отримано наступні висновки:

– за результатами аналізу ландшафтно-географічних особливостей місцевості об’єкта було вивчено просторову геометрію охоронного периметра в умовах лісового масиву та змодельовано потенційні вектори диверсійних загроз. Встановлено, що найбільш вразливими зонами є кутові ділянки загородження та просіки з обмеженою прямою видимістю. Відповідно до цього було розроблено стратегію ешелонованого захисту, яка поєднує периферійні фізичні засоби виявлення на бар’єрі з підсистемами біспектрального оптико-електронного та тепловізійного моніторингу;

– на основі порівняльного аналізу сучасних технологій периметрального виявлення обґрунтовано, що для захисту полігону спеціального найбільш доцільним є впровадження відкритих промислових протоколів зв’язку та біспектральних засіб спостереження. Цей підхід дозволяє інтегрувати гетерогенні підсистеми нижнього рівня в єдине інформаційне середовище, забезпечуючи високу інформативність та індивідуальний контроль кожного лінійного пристрою в мережі;

– під час інженерного проєктування було розраховано відмовостійку топологію магістральної кабельної мережі ліній. Застосування технології волоконно-оптичного кільця та промислових комутаторів дозволило досягти апаратного дублювання каналів зв’язку. Проведені перевірочні інженерні розрахунки ємності буферних акумуляторних батарей підтвердили, що масив із 12 AGM-блоків загальною ємністю 450 А·год (за напруги в шини 48 В) гарантує нормативну автономну роботу системи, під час повного знеструмлення об’єкта, протягом 5 годин.

– реалізовано програмно-апаратну інтеграцію периферійних засобів виявлення, відеонагляду та елементів інженерного забезпечення на базі центральної інтеграційної платформи класу PSIM. Застосування спеціалізованого програмного забезпечення верхнього рівня дозволяє здійснювати автоматичний збір телеметрії, логічно сегментувати тегований трафік за ізольованими контурами VLAN та відображати стан системи на багатошаровій інтерактивній ГІС-карті об’єкта, що суттєво підвищує точність локалізації інцидентів;

– розроблено та параметризовано програмні алгоритми інтелектуальної обробки сигналів на базі нейромережевої моделі YOLOv8 та теорії ймовірностей Байєса. Створено математичну логіку просторово-часової крос-кореляції подій, яка під час спрацювання лінійного давача забезпечує автоматичне наведення поворотної PTZ-камери в азимут події за 1,2 с та верифікує істинність загрози з точністю $P(A|B) \geq 99{,}8$ %. Це дозволяє успішно мінімізувати вплив біогенних та кліматичних завад регіону розташування об’єкту, автоматизувавши сценарії SOP на АРМ оператора.

Для підвищення ефективності та відмовостійкості ІСОП під час експлуатації рекомендується:

– кабельна інфраструктура: в землі прокладати виключно броньований оптичний кабель; всередині шаф ШДК розносити сигнальні та силові лінії на $\geq 0{,}2$ м, а вводи виконувати знизу через гермовводи IP66.

– резервування живлення: кожні шість місяців здійснювати тестування залишкової ємності АКБ типу AGM Deep Cycle для превентивного виявлення деградації елементів до моменту запуску ДГУ;

– заземлення та блискавкозахист: щороку перед грозовим сезоном перевіряти імпульсний опір заземлення опор ($R_{заз} \leq 4$ Ом) та контролювати цілісність дренажних провідників ПЗІП на інтерфейсах Ethernet камер;

– оптимізація нейромережі: за умов суттєвих сезонних змін ландшафту коригувати коефіцієнт впевненості (`Confidence Threshold`) алгоритму YOLOv8 для запобігання пропускам цілей та утримання вимог класу Grade 4.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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: 28.01.2026).

2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://surl.lt/tlznee (access date: 28.01.2026).

3. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. URL: https://surli.cc/nrzgvo (access date: 28.01.2026).

4. Закон України: Про використання ядерної енергії та радіаційну безпеку. URL: https://surl.li/shlmup (дата звернення: 30.01.2026).

5. Закон України: Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання. URL: https://surl.li/dzmjjw (дата звернення: 30.01.2026).

6. Закон України: Про критичну інфраструктуру. URL: https://surl.li/wbihpr (дата звернення: 30.01.2026).

7. НП 306.8.126-2006. Правила фізичного захисту ядерних установок та ядерних матеріалів. [Чинний від 2021-06-25]. Вид. офіц. Київ : ДЯРУ, 2021. 55 с.

8. НП 306.8.175-2011. Вимоги до комплексу інженерно-технічних засобів системи фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання. [Чинний від 2012-01-10]. Вид. офіц. Київ : ДЯРУ, 2011. 22 с.

9. 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.

10. ДСТУ IEC 62676-1-1:2017. Системи відеоспостереження охоронного призначення. Частина 1-1. Вимоги до систем. Загальні вимоги (IEC 62676-1-1:2013, IDT). [Чинний від 2017-12-15]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2015. 108 с.

11. ДБН В.2.5-56:2014. Системи протипожежного захисту. Зі Зміною № 1. [Чинний від 2019-11-01]. Вид. офіц. Київ : Мінрегіон України, 2015. 127 с.

12. ПУЕ. Правила улаштування електроустановок (перше переглянуте, перероблене, доповнене та адаптоване до умов України видання). [Чинний від 2017-08-21]. Вид. офіц. Київ : Міненерговугілля України, 2017. 617 с.

13. Глибокоешелонований захист. URL: https://surl.li/ihkhfi (дата звернення: 10.02.2026).

14. Design and Evaluation of Physical Protection. URL: https://surl.li/xosdlc (access date: 10.02.2026).

15. Physical Security Systems Assessment Guide. URL: https://surl.li/icyrpg (access date: 10.02.2026).

16. Кайдик О. Л., Терлецький Т. В. Системи охорони периметрів: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 (F) Інформаційні технології спеціальності 126 (F6) Інформаційні системи та технології денної та заочної форм навчання. Луцьк : ЛНТУ, 2026. 92 с.

17. What is a Single Point of Failure (SPOF)? URL: https://surl.lt/rbeciq (access date: 10.02.2026).

18. ERPS Vs RSTP: Topology Design, Ethernet Ring Protection And Spanning Tree Protocols. URL: https://surl.li/xxkguj (access date: 10.02.2026).

19. What is Physical Security Information Management (PSIM)? URL: https://surl.li/cspvwo (access date: 10.02.2026).

20. AES-256 Encryption – Everything You Need to Know. URL: https://lnk.ua/5wM1u1adR (access date: 28.02.2026).

21. ДСТУ EN 10223-4-2001. Дріт сталевий та дротяні вироби для огороджування. Частина 4. Сітка зі сталевого дроту зі зварними чарунками. Технічні умови (EN 10223-4:1998, IDT). [Чинний від 2003-01-01]. Вид. офіц. Київ : Держстандарт України, 2002. 54 с.

22. Охоронні оптоволоконні системи детекції. URL: https://surl.li/knsopz (дата звернення 28.02.2026).

23. ADSS Fiber Optic Cable. URL: https://surl.li/wjpenj (access date: 28.02.2026).

24. ДСТУ EN 62275:2015. Системи прокладання кабелів. Кабельні хомути для електричних установок (EN 62275:2009, IDT). [Чинний від 2016-01-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2018. 16 с.

25. Сейсмічний датчик – ARCTIUM. URL: https://surl.li/aoclxx (дата звернення: 06.03.2026).

26. Local Microwave Protective Detector Forteza FMC 24 Pro. URL: https://surl.li/dghhrt (access date: 06.03.2026).

27. ДСТУ IEC 60529:2019. Ступені захисту, забезпечувані корпусами (IP-код) (IEC 60529:2013, IDT). [Чинний від 2020-01-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2020. 50 с.

28. Thermal Network Bullet Camera DS-2TD2167-25/PI. URL: https://surl.li/sqpsvc (access date: 06.03.2026).

29. Thermal & Optical Bi-spectrum Network Positioning System DS-2TD6267-75C4L/W. URL: https://surl.li/ukdseu (access date: 06.03.2026).

30. ДСТУ EN 62676-4:2017. Системи відеоспостереження охоронного призначення. Частина 4. Правила застосування (EN 62676-4:2015, IDT). [Чинний від 2017-08-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2019. 78 с.

31. Шафа вулична навісна ЦМО ШТВ-Н (ШТВ-Н-15.6.3-4ААА). URL: https://surl.li/kfwxvb (дата звернення: 06.03.2026).

32. MOXA PT-G7509 Series. URL: https://surl.li/jnzxmt (access date: 06.03.2026).

33. ITU-T G.8032 / ERPS. URL: https://surl.li/zrnttb (access date: 06.03.2026).

34. What is a standard operating procedure (SOP)? URL: https://surl.li/rxpqnb (access date: 06.03.2026).

35. HPE ProLiant DL380 Gen11 6526Y Server. URL: https://surl.li/evlmyy (access date: 20.03.2026).

36. Робоча станція HP Z4 G5 Tower. URL: https://surl.li/avjstc (дата звернення: 20.03.2026).

37. Відеостіна Samsung 2×2 – 1,74 мм, 4×55″(221855-K). URL: https://surl.li/bnzzed (дата звернення: 20.03.2026).

38. You Only Look Once (YOLO). URL: https://surl.li/jwuphn (access date: 20.03.2026).

39. ByteTrack. URL: https://surli.cc/rugmjv (access date: 26.03.2026).

40. Multi-Sensor Data Fusion. URL: https://surl.li/mivjoo (access date: 28.12.2025).

41. ДСТУ EN 62305-1:2012. Захист від блискавки. Частина 1. Загальні принципи (EN 62305-1:2011, IDT). [Чинний від 2012-08-01]. Вид. офіц. Київ : Мінекономрозвитку України, 2012. 78 с.

42. Absorbed Glass Mat Batteries: What Are They? URL: https://surl.li/xiaoua (access date: 26.03.2026).

43. White Paper: ITU-T G.8032 ERPS Technology. Part I. URL: https://surl.li/xcwqfm (access date: 26.03.2026).

44. IEEE 802.1Q-2018: IEEE Standard for Local and Metropolitan Area Networks–Bridges and Bridged Networks. URL: https://surl.li/zqhvuf (access date: 26.03.2026).

45. 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.