

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

**Навчально–науковий Інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей**

«На правах рукопису»

УДК 621.391

До захисту допущено

Завідувач кафедри

_____ Анатолій МАКАРЕНКО

«__» _____ 20__ р.

Дипломна робота

на здобуття ступеня магістра

**за освітньо-професійною програмою «Системи електронних
комунікацій та Інтернету речей»**

зі спеціальності 172 «Електронні комунікації та радіотехніка»

**на тему: «Розробка типового рішення системи відеоспостереження для
логістичних об'єктів»**

Виконав:

студент II курсу, групи ЦС–41

Колісник Даніїл Олександрович _____

Керівник:

Старший викладач каф. ЕКІР, к.т.н.

Новіков Валерій Іванович _____

Рецензент:

Професор кафедри ТК, д.т.н., професор

Лисенко Олександр Іванович _____

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.

Студент (–ка) _____

Київ – 2025 року

**Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально–науковий Інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей**

Рівень вищої освіти – другий (магістерський)

Спеціальність – 172 Електронні комунікації та радіотехніка

Освітня програма – «Системи електронних комунікацій та інтернету речей»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Анатолій МАКАРЕНКО

«__» _____ 20__ р.

ЗАВДАННЯ

на дипломну роботу студенту

Коліснику Даніїлу Олександровичу

1. Тема роботи «Розробка типового рішення системи відеоспостереження для логістичних об'єктів», керівник роботи Новіков Валерій Іванович, кандидат технічних наук, затверджені наказом по університету від «03» листопада 2025 р. №4773-с.

2. Термін подання студентом дисертації 05.12.2025

3. Зміст роботи

1. Теоретичні основи побудови системи відеоспостереження для логістичних об'єктів

2. Аналіз об'єкта та визначення вимог до системи

3. Дослідження методів та технологій систем відеоспостереження

4. Перелік ілюстративного матеріалу

1. Вступ, актуальність, мета

2. Об'єкт та предмет дослідження

3. Задачі дослідження

4. Теоретичні відомості систем відеоспостереження

5. Аналіз об'єкта
6. Впровадження системи відеонагляду на логістичний об'єкт
7. Дослідження та порівняння технологій CCTV
8. Загальні висновки.

5. Дата видачі завдання 01.03.2025

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1.	Аналіз літературних джерел та визначення актуальності дослідження	01.03.2025 – 30.03.2025	виконано
2.	Визначення вимог для забезпечення безпеки на логістичних об'єктах	01.05.2025 – 31.05.2025	виконано
3.	Вивчення теоретичних відомостей по системам відеоспостереження	01.06.2025 – 30.06.2025	виконано
4.	Вивчення існуючих впровадження CCTV	01.07.2025 – 31.07.2025	виконано
5.	Вивчення використання методів обробки потоку за допомогою відеоаналітики	01.08.2025 – 29.08.2025	виконано
6.	Оновлення існуючої системи відеоспостереження на реальному об'єкті	01.09.2025 – 31.09.2025	виконано
7.	Оформлення та підготовка дипломної роботи до захисту	01.10.2025 – 31.10.2025	виконано

Студент

Керівник

Даніїл КОЛІСНИК

Валерій НОВІКОВ

РЕФЕРАТ

Робота містить 104 сторінки, 37 рисунків, 3 таблиці. Було використано 45 джерел інформації.

Актуальність роботи. Сучасні логістичні комплекси працюють у режимі високої інтенсивності, де переміщення товарів, техніки і персоналу відбувається безперервно, та будь-яка помилка, затримка або інцидент може призвести до суттєвих фінансових втрат. Зі зростанням обсягів операцій та підвищенням вимог до прозорості процесів зберігання та обліку товарів значно зросла потреба у впровадженні ефективних систем відеоспостереження, які здатні забезпечити постійний контроль критичних зон, знизити рівень ризиків та підвищити безпеку персоналу.

Актуальність даної роботи визначається тим, що традиційні системи контролю, а саме: точки реєстрації, охоронні патрулі, фотофіксація – більше не відповідають реаліям сучасної логістики. Вони не дозволяють оперативно виявляти інциденти, контролювати великі площі чи гарантувати збереження матеріальних цінностей у складних виробничих умовах. До того, відсутність централізованої системи керування відеонаглядом, робить неможливим аудит операцій та прийняття рішень у реальному часі.

З огляду на ці фактори, побудова сучасної системи відеоспостереження на базі мережевих камер та VMS платформи Milestone XProtect є критично важливою для підвищення ефективності управління логістичними процесами. Вона дозволяє не лише покривати ключові зони об'єкта – периметр, зони приймання та відвантаження, внутрішні склади, робочі ділянки персоналу – а й забезпечує повний відеоархів для подальшого аналізу, контролю та оптимізації.

У межах проєкту було виконано реконструкцію існуючої системи, встановлено нові камери, модернізовано інфраструктуру та проведено розрахунок серверної частини, що дозволило перейти до більш продуктивної, масштабованої та надійної архітектури. Таким чином, актуальність роботи

полягає в необхідності створення комплексної відеосистеми, здатної забезпечити безпеку, контроль логістичних процесів та підвищення загальної ефективності управління складським об'єктом.

Мета роботи. Метою роботи є проєктування, обґрунтування та впровадження комплексної системи відеоспостереження на об'єкті складського типу, включно з підбором обладнання, розробкою схеми розміщення камер, прокладанням кабельної інфраструктури та розрахунком серверних потужностей для системи управління відео Milestone VMS. Робота спрямована на підвищення рівня безпеки, оптимізацію контролю товарних потоків та забезпечення надійного зберігання відеоданих.

Завдання дослідження. Основним завданням дослідження було обґрунтувати та реалізувати проєкт сучасної системи відеоспостереження для складського комплексу. Для цього необхідно було проаналізувати територію та внутрішні приміщення, визначити критичні зони контролю й підібрати оптимальні типи IP-камер для кожної з них. Окремим завданням стало розроблення схеми розміщення камер з урахуванням реальних сценаріїв руху персоналу та товару, а також мінімізації «мертвих зон». У межах дослідження також потрібно було спроектувати кабельну інфраструктуру: визначити маршрути прокладання кабелів, вибрати комутаційне обладнання та організувати підключення всіх вузлів до серверної. Важливою частиною роботи був розрахунок серверних ресурсів для системи Milestone – обсяг сховища, навантаження від камер, необхідна продуктивність і можливість подальшого масштабування.

Завдання завершувалося формуванням комплексного технічного рішення, яке поєднує вибір обладнання, мережеву інфраструктуру, розрахунки та кінцеву логіку роботи системи.

Об'єкт дослідження. Система відеоспостереження складського комплексу, включно з інженерною інфраструктурою, серверною підсистемою та комплексом мережевого устаткування.

Предмет дослідження. Методи та технічні засоби побудови сучасної системи відеоспостереження на основі IP–технологій, особливості вибору камер, принципи організації мережевої та серверної інфраструктури, а також підходи до забезпечення надійного збереження відеоінформації.

Ключові слова. Відеоспостереження, IP–камери, Milestone, сервер відеозапису, кабельна інфраструктура, UTP, мережеве обладнання, складський об’єкт, система безпеки, проєктування CCTV, відеоаналітика, бітрейт, PoE, комутація.

ABSTRACT

The work contains 104 pages, 37 figures, 3 tables, 45 sources of information were used.

Relevance of work. Modern logistics complexes operate in a high-intensity environment, where the movement of goods, machinery and personnel occurs continuously, and any mistake, delay or incident can lead to significant financial losses. As the volume of operations increases and the requirements for transparency and accuracy of storage and inventory processes grow, the need for efficient video surveillance systems has become substantially more important. Such systems must provide constant monitoring of critical areas, reduce operational risks and improve the safety of personnel.

The relevance of this work is driven by the fact that traditional control methods – registration points, security patrols, manual photo documentation – no longer meet the demands of modern logistics. They do not allow timely detection of incidents, do not provide adequate coverage of large areas and cannot guarantee the preservation of material assets under complex operational conditions. In addition, the absence of a centralized video management system makes it impossible to perform proper audits of operations or make real-time decisions based on actual visual data.

Considering these factors, the development of a modern video surveillance system based on network cameras and the Milestone XProtect VMS platform is essential for improving the efficiency of logistics processes. Such a system enables comprehensive coverage of key areas of the facility – the perimeter, loading and unloading zones, internal warehouse spaces and operational working areas – while also providing a complete video archive for future analysis, control and optimization.

Within the project, the existing system was reconstructed, new cameras were installed, the infrastructure was upgraded, and the server subsystem was recalculated. These measures made it possible to transition to a more productive, scalable and reliable architecture. Therefore, the relevance of this work lies in the need to create a

comprehensive video surveillance system capable of ensuring safety, improving process control and increasing the overall operational efficiency of the warehouse facility.

Purpose of the Work. The purpose of this work is to design, justify and implement an integrated video surveillance system for a warehouse-type facility. This includes selecting the appropriate equipment, developing a detailed camera placement scheme, designing the cable infrastructure and calculating the server capacity required for the Milestone VMS video management system. The work aims to enhance security, optimize the control of goods flow and ensure reliable storage of video data.

Objectives of the study. The main objective of the study was to justify and implement the design of a modern video surveillance system for a warehouse complex. To achieve this, it was necessary to analyze the facility's territory and interior spaces, identify critical monitoring zones and select optimal types of IP cameras for each area. An important part of the task was to develop a camera deployment plan that reflects real scenarios of personnel and goods movement and minimizes blind spots.

The research also required the design of the cable infrastructure: determining cable routing paths, selecting switching equipment and organizing the connection of all nodes to the server room. A key component of the work was calculating the required server resources for Milestone – including storage capacity, camera load, system performance and future scalability.

The final stage of the work involved forming a comprehensive technical solution that brings together equipment selection, network infrastructure, system calculations and the overall operational logic of the CCTV system.

Object and subject of research. The object of our research is the video surveillance system of a warehouse complex, including its engineering infrastructure, server subsystem and network equipment.

The subject of our research is methods and technical tools for building a modern video surveillance system based on IP technologies, including camera selection criteria, principles of network and server infrastructure design and approaches to ensuring reliable storage of video information.

Keywords: video surveillance, IP cameras, Milestone, video recording server, cable infrastructure, UTP, network equipment, warehouse facility, security system, CCTV design, video analytics, bitrate, PoE, switching.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ	12
ВСТУП.....	14
1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ЛОГІСТИЧНИХ ОБ’ЄКТІВ	16
1.1 Джерела та нормативна база для аналізу вимог до систем технічної безпеки.....	16
1.2 Технології IP–відеоспостереження	17
1.2.1 Технологія WDR (Wide Dynamic Range)	19
1.2.2 Інфрачервона підсвітка.....	20
1.2.3 PoE	21
1.3 Відеокодеки	24
1.3.1 Кодек H.264	25
1.3.2 Кодек H.265	26
1.3.3 Кодек MJPEG – технічний опис	27
1.4 Протоколи передачі даних у CCTV.....	28
1.4.1 RTSP.....	29
1.4.2 HTTP та HTTPS у системах IP–відеоспостереження	31
1.4.3 ONVIF.....	32
1.5 Принцип роботи систем керування відео (VMS) на прикладі Milestone XProtect.....	34
1.5.1 Склад серверних компонентів Milestone Xprotect	35
1.5.2 Логіка потоків даних, запису і зберігання відео.....	38

1.5.3 Масштабованість, відмовостійкість, резервування і розподілені системи	39
1.6 Загальні принципи роботи відеоаналітики та AI	41
1.6.1 Типи відеоаналітичних задач у логістиці та транспортній інфраструктурі.....	43
1.7 Висновки з розділу 1	46
2 АНАЛІЗ ОБ'ЄКТА ТА ВИЗНАЧЕННЯ ВИМОГ ДО СИСТЕМИ	48
2.1 Розроблення структурної та функціональної схеми системи.....	51
2.2 Схема трас силових/UTP кабелів	77
2.3 Калькуляція сервера.....	80
2.4 Висновки з розділу 2.....	82
3 АНАЛІЗ СУЧАСНИХ ТЕНДЕНЦІЙ РОЗВИТКУ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ.....	84
3.1 Порівняння брендів камер відеоспостереження: Axis, Hanwha проти китайських виробників	85
3.2 Порівняння серверної і бортової аналітики	88
3.3 Підходи до проектування топології інфраструктури відеоспостереження	92
3.4 Аналіз життєвого циклу системи відеоспостереження та вплив довгострокових витрат на вибір архітектури.....	93
3.5 Висновки з розділу 3.....	95
ВИСНОВКИ.....	97
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	99

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

IP — Internet Protocol

PoE — Power over Ethernet

UTP — Unshielded Twisted Pair

Cat6 — Category 6

VMS — Video Management System

NVR — Network Video Recorder

WDR — Wide Dynamic Range

IR / ІЧ — Infrared

FPS — Frames per Second

RTSP — Real Time Streaming Protocol

ONVIF — Open Network Video Interface Forum

ACAP — AXIS Camera Application Platform

LPR / ANPR — License Plate Recognition / Automatic Number Plate Recognition

FR — Face Recognition

Edge — Edge Processing

CPU — Central Processing Unit

RAM — Random Access Memory

HDD — Hard Disk Drive

SSD — Solid State Drive

RAID — Redundant Array of Independent Disks

GbE — Gigabit Ethernet

TCP/IP — Transmission Control Protocol / Internet Protocol

HTTP — HyperText Transfer Protocol

HTTPS — HTTP Secure

UPS — Uninterruptible Power Supply

QoS — Quality of Service

LAN — Local Area Network

WAN — Wide Area Network

ROI — Region of Interest

SDK — Software Development Kit

API — Application Programming Interface

PTZ — Pan-Tilt-Zoom

ВСТУП

У сучасних умовах розвитку логістики, дистрибуції та складської інфраструктури системи відеоспостереження стала одним із ключових інструментів забезпечення безпеки, контролю операцій та оптимізації внутрішніх процесів. Зростання обсягів товарообігу, підвищення вимог до прозорості логістичних операцій та необхідність запобігання крадіжкам чи ненавмисним помилкам персоналу роблять системи відеонагляду не просто елементом охорони, а повноцінною частиною бізнес-процесів. Сучасні CCTV системми об'єднують мережеві камери, інтелектуальні алгоритми та розвинені платформи керування відео, що дозволяє отримувати не лише зображення, а й аналітичну інформацію у режимі реального часу.

Особливу роль у таких системах відіграють мережеві технології та серверна інфраструктура, оскільки саме вони визначають стабільність роботи, якість відеоархіву та можливість масштабування. Вибір топології мережі, методів стиснення відео, протоколів передачі, архітектури зберігання даних та логіки роботи відеоаналітики безпосередньо впливають на ефективність усієї системи. Програмні платформи класу VMS, зокрема Milestone XProtect, дозволяють інтегрувати обладнання різних виробників, налаштовувати складні сценарії моніторингу та забезпечувати надійне управління великими обсягами відеоданих.

Актуальність дослідження підсилюється тим, що складські об'єкти мають специфічні умови експлуатації: великі площі, зональний поділ, рух транспортних засобів, постійну зміну товарних позицій та необхідність контролю доступу персоналу. Це потребує комплексного підходу до проектування системи відеоспостереження – від аналізу ризиків до моделювання покриття та оцінки навантаження на мережу та сервери. Для побудови надійної системи необхідно дослідити характеристики камер, принципи роботи сучасних відеокодеків, методи оптимізації бітрейту,

механізми відеоаналітики та правила взаємодії між апаратними та програмними компонентами.

У цій роботі буде проведено детальний аналіз сучасних методів проектування та побудови IP-систем відеоспостереження, розглянуто принципи функціонування мережевих камер, протоколів передачі даних та платформ управління відео. Окрема увага приділяється методам моделювання систем за допомогою інструментів Axis Site Designer, Hanwha Toolbox та Milestone Calculator, а також підходам до розрахунку серверної інфраструктури для забезпечення надійного запису та зберігання відеоархіву. Крім того, буде досліджено застосування відеоаналітики для логістичних об'єктів – контроль зон доступу, моніторинг транспортних засобів, оцінка руху персоналу та інші практичні сценарії.

Метою даного дослідження є систематизація знань про сучасні технології IP-відеоспостереження та розроблення комплексної моделі роботи відеосистеми для логістичного об'єкта, що включає аналіз обладнання, мережевих компонентів, методів стиснення відео, аналітичних модулів та вимог до серверної частини. Результати роботи дозволяють визначити оптимальні рішення та перспективні напрямки розвитку систем відеоспостереження у сфері логістики та складської інфраструктури

1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ЛОГІСТИЧНИХ ОБ'ЄКТІВ

1.1 Джерела та нормативна база для аналізу вимог до систем технічної безпеки

Для проведення аналізу нормативних вимог до систем відеоспостереження було використано міжнародні стандарти та технічні документи, що регламентують побудову та експлуатацію сучасних систем технічної безпеки. Основу нормативної бази становлять стандарти серії ІЕС 62676, які визначають загальні принципи побудови систем відеоспостереження, вимоги до обладнання, параметрів зображення, умов експлуатації та протоколів передавання даних.

Стандарт ІЕС 62676–1–1:2013 [1] містить узагальнені вимоги до систем відеоспостереження, включаючи класифікацію систем, технічні параметри камер, вимоги до якості відео та критерії спостереження залежно від задачі (детекція, розпізнавання, ідентифікація).

Стандарт ІЕС 62676–2–1:2013 [2] регламентує мережеві інтерфейси, протоколи передавання відеоданих, вимоги до сумісності та інтеграції ІР–обладнання. Документ визначає принципи побудови систем на основі відкритих протоколів, що є критично важливим для великих об'єктів логістичного сектору.

Документ ІЕС 62676–4:2025 [3] містить рекомендації щодо практичного проектування систем відеоспостереження: параметри розміщення камер, вимоги до освітленості, оглядовості, вибору типів об'єктів, а також принципи формування інформаційної безпеки відеомереж.

Оскільки системи відеоспостереження на логістичних об'єктах часто інтегруються до корпоративних ІТ–інфраструктур, при аналізі вимог враховано положення стандарту **ISO/IEC 27001**, який визначає політики кіберзахисту, вимоги до контролю доступу, ведення журналів подій та сегментації мереж [5].

Додаткову цінність для аналізу становить BS EN 62676–2–2, де докладно описуються аспекти реалізації мережевих протоколів, використання HTTP/REST–інтерфейсів, а також вимоги до забезпечення сумісності відеосистем із програмними платформами керування (VMS) [4].

У сукупності ці документи формують комплексну нормативну основу, яка дозволяє оцінити технічні, функціональні та безпекові вимоги до систем відеоспостереження, що впроваджуються на логістичних об'єктах.

1.2 Технології IP–відеоспостереження

У цій частині розділа було детально розглянуто концептуальні основи функціонування систем IP–відеоспостереження, які сьогодні є базовим технологічним підходом для побудови сучасних комплексів технічної безпеки. З урахуванням тенденцій розвитку безпеки на логістичних, промислових та інфраструктурних об'єктах, IP відеоспостереження розглядається як ключовий елемент цифрової інженерної інфраструктури, що забезпечує не лише фіксацію візуальної інформації, але й глибоку аналітичну обробку подій у реальному часі. Також було проаналізовано, що перехід від аналогових систем до IP–технологій змінив підхід до проектування, експлуатації та масштабування систем відеонагляду. На відміну від попередніх рішень, де кожна камера була прив'язана до конкретного фізичного входу на відеореєстратор, сучасні мережеві пристрої працюють як повноцінні мережеві компоненти, здатні передавати дані у будь-яку точку IP мережі. Такий підхід забезпечує мобільність, можливість розподілу навантаження, резервування каналів, а також спрощує інтеграцію з іншими системами безпеки.

У теоретичній частині було приділено увагу структурній гнучкості IP–архітектури. Було відзначено, що її основою є стандартна мережа Ethernet, яка забезпечує одночасне передавання відео, службових команд, журналів, подій та метаданих. У рамках аналізу було розглянуто концепцію рівнів системи –

включно з рівнем пристроїв, рівнем мережевої інфраструктури, обчислювальним рівнем, а також рівнем сервісів відеоаналітики та централізованого управління. Також було визначено, що мережеві системи дозволяють створювати складні топології: від простих локальних мереж, у рамках одного складу, до ієрархічних багаторівневих структур, що охоплюють десятки територіально віддалених вузлів.

У ході аналізу розглянуто важливість логічної сегментації мережі, ізоляції службового трафіку, балансування навантаження між комутаторами та застосування механізмів пріоритезації критичних потоків. Особлива увага була приділена питанням стабільності та відмовостійкості — включно з використанням резервних ліній, дублювання мережевих шляхів та застосування методів мережевого моніторингу.

Окремим аспектом було розглянуто можливість інтеграції IP відеоспостереження з цифровими платформами управління безпекою. Сучасні системи відеоспостереження не функціонують у відриві від інших підсистем — зокрема, контролю доступу, охоронної сигналізації, систем ідентифікації транспортних засобів та пожежної автоматики. Було підкреслено, що мережевий характер IP-систем дозволяє легко організовувати двосторонній обмін подіями, формувати складні автоматизовані сценарії реагування та створювати централізовані ситуаційні центри. Важливим компонентом огляду стала масштабованість IP рішень. Було розглянуто, що для логістичних об'єктів, які постійно розширюються і часто змінюють конфігурацію складських зон, здатність швидко додавати або переміщувати камери є критичною. IP архітектура дозволяє проводити нарощування системи без перебудови кабельної інфраструктури, а також включає підтримку PoE, що дає можливість жити камери та інші пристрої одним кабелем, що зменшує витрати на монтаж. Також було проаналізовано питання централізованого управління системою. IP-підхід передбачає можливість повного адміністрування через спеціалізовані програмні платформи: конфігурація

камер, оновлення мікропрограм, управління користувачами, контроль подій та інцидентів можуть виконуватися віддалено та централізовано, що значно спрощує технічну експлуатацію. Особливо це важливо для логістичних компаній, де на одному серверному вузлі може зберігатися відео з десятків складів або вантажних терміналів.

1.2.1 Технологія WDR (Wide Dynamic Range)

Технологія WDR – це механізм, що дозволяє камері захоплювати зображення з високим контрастом, тобто коли в кадрі є як дуже світлі, так і дуже темні ділянки [6]. У таких умовах без WDR камера або «висвітлить» яскраві частини, або «затемнить» тіні, втрачаючи деталі там, де вони важливі. Принцип роботи WDR полягає в тому, що камера робить декілька кадрів або «експозицій» з різними налаштуваннями витримки: один кадр з короткою витримкою – щоб захопити яскраві області, інший – з більшою витримкою – щоб «побачити» темні ділянки. Потім ці кадри комбінуються в один фінальний кадр, в якому вирівнюється освітлення: світлі ділянки не «згоряють», а темні стають більш читабельними (Рис.1).

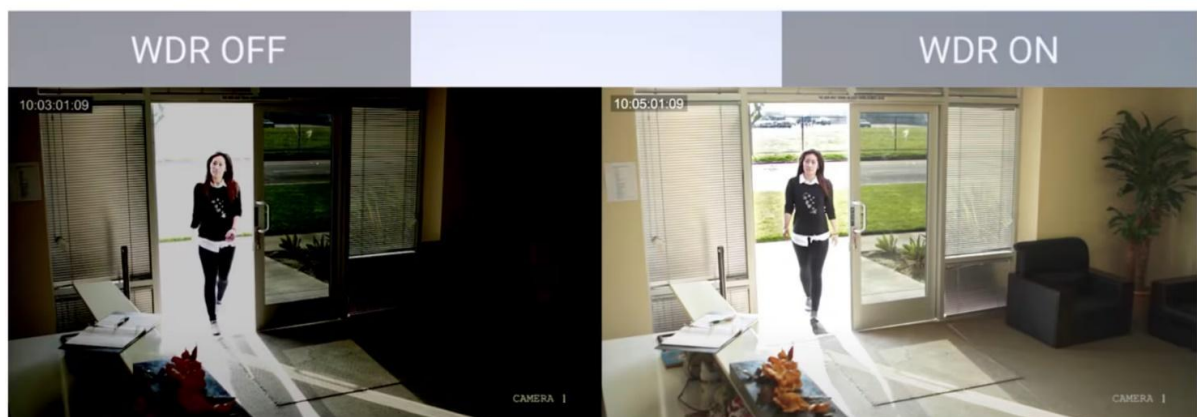


Рисунок 1.1 - Приклад роботи технології WDR

1.2.2 Інфрачервона підсвітка

Інфрачервона підсвітка є однією з ключових технологій, що забезпечує коректну роботу IP-камер відеоспостереження в умовах низького або повністю відсутнього освітлення, що особливо актуально для логістичних об'єктів, де значна частина діяльності відбувається вночі або у зонах зі складними умовами освітлення. Принцип роботи IR-підсвітки базується на використанні інфрачервоного випромінювання, зазвичай у діапазоні 850 або 940 нм (Рис. 2), яке практично непомітне для людського ока, але добре сприймається сучасними CMOS-сенсорами [7].

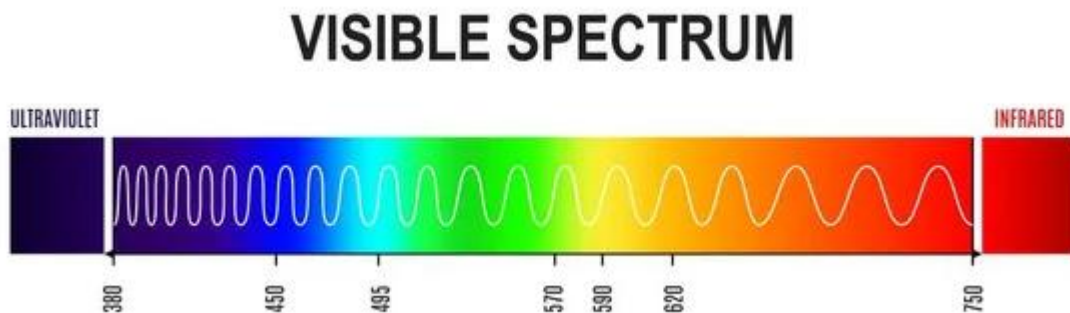


Рисунок 1.2 - Спектр електромагнітних хвиль видимого світла

У денному режимі камера працює через IR-cut фільтр, який відсікає інфрачервону складову світла та забезпечує правильну передачу кольору (рис.1.2). Коли рівень освітлення знижується, камера переходить у нічний режим, механічно прибираючи цей фільтр. У цей момент матриця стає максимально чутливою до інфрачервоного світла, і активується вбудована IR-підсвітка, що дозволяє отримувати чітке, контрастне чорно-біле зображення навіть у повній темряві. Правильно реалізована ІЧ-підсвітка особливо важлива для логістичних територій, таких як рампи, складські майданчики, зони завантаження та периметри, де транспортні засоби, стелажні конструкції, вантажні контейнери та інші елементи можуть створювати тіні, засвітлення або зони нерівномірного освітлення [8].

Розробники камер використовують різні типи IR-рішень, серед яких класичні світлодіодні модулі, діоди підвищеної потужності та технології на кшталт EXIR, що дозволяють формувати більш рівномірний світловий потік без характерної «гарячої точки» в центрі кадру. Значну роль відіграє також адаптивна IR-підсвітка, яка динамічно регулює потужність випромінення залежно від дистанції до об'єкта, запобігаючи пересвіченню облич або номерних знаків під час наближення транспорту до камери.

У практиці проектування систем спостереження на логістичних об'єктах важливо враховувати дальність дії ІЧ-підсвітки, кут її розсіювання, вплив середовища та відбиття від металевих поверхонь вантажівок чи контейнерів. Надмірно потужна підсвітка може створювати засвіт кадру, тоді як недостатня – призвести до втрати критичних деталей, що знижує ефективність як відеоконтролю, так і аналітики. Саме наявність достатньої IR-компенсації дозволяє алгоритмам розпізнавання номерних знаків, детекції людей або визначення несанкціонованих переміщень працювати стабільно і в темний час доби.

Таким чином, інфрачервона підсвітка є невід'ємним компонентом сучасної ІР-камери, забезпечуючи повноцінний відеоконтроль незалежно від умов освітлення. У контексті логістичних об'єктів її роль є критичною, оскільки саме від роботи ІР-модуля залежить можливість своєчасного виявлення загроз, контроль переміщень транспорту та вантажів, а також точність усіх систем аналітики, що застосовуються для підвищення безпеки та оптимізації операційних процесів [9].

1.2.3 PoE

Технологія PoE (Power over Ethernet) забезпечує одночасну передачу потрібного живлення та мережевих даних до ІР-камери через один кабель категорії UTP/FTP/STP, що дозволяє спростити монтаж, мінімізувати кількість

кабельних трас і підвищити надійність інженерної інфраструктури. Використання PoE стало стандартною практикою у професійних системах відеоспостереження, оскільки усуває потребу в локальних блоках живлення, що підвищує стійкість роботи та знижує ризики, пов'язані з перепадами напруги або неправильним підключенням сторонніх адаптерів [10]

Механіка роботи PoE базується на подачі постійної напруги 12–57 В по 2 парам Ethernet-кабелю, як зображено на рисунку 1.3.

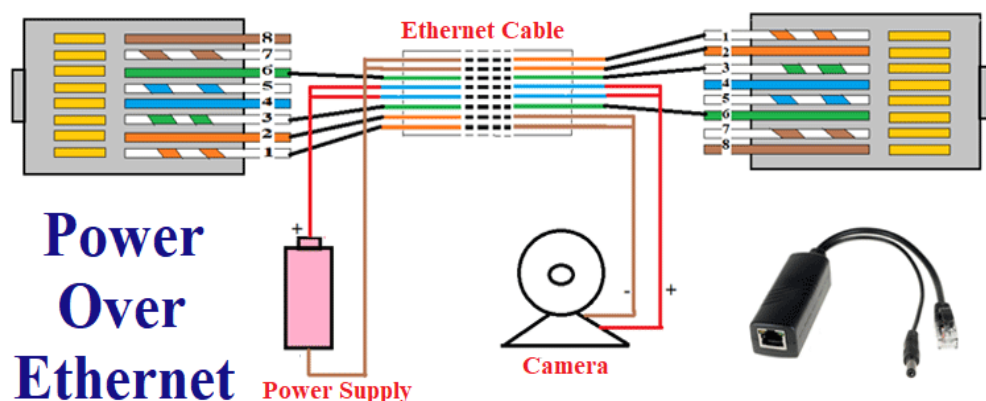


Рисунок 1.3 - Схема роботи PoE

Перед подачею живлення комутатор або інжектор виконує процедуру виявлення PoE-сумісного пристрою, вимірюючи опір навантаження та визначаючи, чи може підключений пристрій приймати живлення. Такий механізм гарантує, що PoE-обладнання не подає напругу на невідповідні пристрої та не створює ситуацій, які могли б призвести до пошкодження мережевих карт або кінцевих пристроїв. Після визначення класу навантаження комутатор автоматично виділяє необхідний бюджет потужності відповідно до стандарту IEEE.

Основними стандартами PoE є IEEE 802.3af (до 15,4 Вт), IEEE 802.3at або PoE+ (до 30 Вт) та IEEE 802.3bt (PoE++) [11], який дозволяє передавати від 60 до 90 Вт на порт. У системах відеоспостереження стандарт 802.3af – зазвичай використовується для стандартних фіксованих камер без IR-підсвітки, тоді як 802.3at застосовується для камер із потужною IR-підсвіткою, моторизованими

об'єктивами або невеликими PTZ-камерами. Стандарт 802.3bt використовується для великих PTZ, тепловізійних модулів або багатосенсорних камер, що вимагають значного енергоспоживання. Правильний підбір PoE-класа є критично важливим, оскільки недостатній бюджет призводить до перезапусків камер, некоректної роботи IR-підсвітки або втрати потоків.

Реальна робота PoE-системи тісно залежить від якості та довжини кабелю. При великих дистанціях зростає падіння напруги, тому для трас понад 80–90 метрів рекомендується використовувати кабель категорії не нижче Cat 6 або застосовувати PoE-екстендери. У логістичних об'єктах з великими складами, високими стелями та протяжними комунікаціями коректний розрахунок PoE-ліній має особливе значення. При перевантаженні PoE-комутатора або неправильному розподілі навантаження система може частково втратити працездатність, саме тому під час проєктування враховується загальний бюджет PoE, кількість портів та максимальна віддача на кожен сегмент.

PoE дозволяє централізовано керувати живленням камер через мережеве обладнання: здійснювати перезапуск порту, контролювати навантаження, моніторити енергоспоживання та будувати резервування. У системах корпоративного рівня застосовується резервоване живлення PoE-комутаторів через UPS або подвійне живлення, що забезпечує безперервність роботи відеоспостереження навіть при короткочасних збоях у мережі електроживлення. Для критично важливих зон (проходи, рампи, серверні приміщення) рекомендується застосовувати комутатори із захищеною архітектурою та підтримкою LACP або STP для підвищення відмовостійкості [11].

Саме PoE став ключовим елементом у стандартизації мережевих CCTV систем, оскільки забезпечує мінімальні вимоги до інфраструктури, високу надійність та знижує складність монтажу у великих проєктах логістичного спрямування.

1.3 Відеокодеки

Відеокодек – це механізм, який дозволяє перетворити «сире» відео з камери на потік даних, придатний для передачі мережею та для довготривалого зберігання. У сирому вигляді відео займає колосальні обсяги, і зберігати чи передавати його практично неможливо, тому кожна IP-камера обов'язково використовує кодек для стиснення. Робота кодека побудована на тому, що в більшості кадрів відео присутня велика кількість надлишкової інформації, це здебільшого фон, який не змінюється, або дрібні деталі, що не впливають на загальну картинку. Кодек аналізує ці кадри, відокремлює те, що справді змінюється, і передає лише різницю між кадрами, а не кожен кадр повністю. У системах відеоспостереження це критично важливо, адже від роботи кодека залежить, який бітрейт буде формувати камера, яким буде навантаження на мережу та скільки дискового простору знадобиться для архіву. У CCTV часто використовуються також так звані смарт-кодеки – це не окремі стандарти, а додаткові алгоритми оптимізації. Камера аналізує сцену: якщо в кадрі немає руху, вона знижує бітрейт; якщо з'являється рух або змінюється освітлення, вона динамічно підвищує якість. У деяких випадках такі алгоритми дають економію 50–80% місця в архіві, особливо на статичних сценах типу коридорів або відкритих територій вночі. Водночас сервер отримує нормальний потік, просто більш ефективно стиснутий [12].

Ще одна важлива річ у кодеках – структура кадрів. Камера не кодує всі кадри як повні. Повний кадр, так званий І-кадр, йде періодично й служить опорою. Між ними передаються Р- або В-кадри, які містять лише зміни. Чим менша частота І-кадрів і чим краще працює алгоритм прогнозування змін, тим нижчий бітрейт. Але занадто рідкі І-кадри можуть ускладнити роботу з архівом під час пошуку потрібного моменту.

Загалом, правильний вибір кодека в системі відеоспостереження – це баланс між якістю зображення, навантаженням на мережу та можливістю

забезпечити потрібний термін зберігання. Від того, який кодек використовується, залежить не лише архів, але й стабільність роботи усієї системи. Камери, сервери ВМС, мережеве обладнання – усе має працювати в одному режимі та бути розрахованим на ту кількість трафіку і те навантаження, яке формує саме кодек. Тому в професійних проєктах вибір кодека та його налаштувань – це не формальність, а один із ключових технічних етапів.

1.3.1 Кодек H.264

Кодек H.264 (AVC – Advanced Video Coding) – це стандарт стиснення відео, який широко використовується в системах IP-відеоспостереження завдяки оптимальному співвідношенню якості зображення і обсягу даних. Основна ідея H.264 полягає в тому, щоб максимально використовувати тимчасову та просторову кореляцію між кадрами. При кодуванні H.264 відео розбивається на макроблоки (найчастіше 16×16 пікселів), які аналізуються для передбачення руху – це називається motion estimation (Рис. 1.4). При цьому використовуються міжкадрові (inter-) передбачення: один кадр (I-кадр) кодується повністю, а наступні кадри (P-кадри або B-кадри) зберігають лише інформацію про відмінності від попередніх кадрів. Таке передбачення значно знижує обсяг даних, які потрібно зберігати або передавати, оскільки повторювані ділянки кодуються більш ефективно.

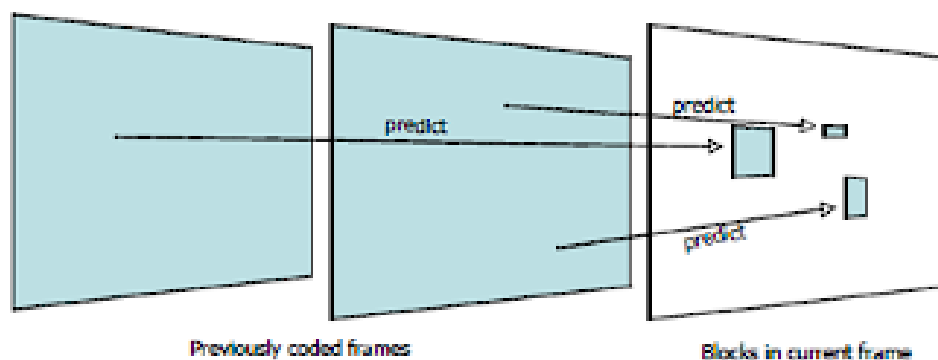


Рисунок 1.4 - Аналітика і передбачення руху під час роботи H.264 кодеку

Кодувальник H.264 використовує блокову структуру з можливістю поділу макроблоків на менші підблоки, що дає гнучкість: він може краще моделювати деталі й рух, покращуючи точність передбачення. Профіль H.264, який часто застосовується в IP-камерах, – це Baseline Profile, який підтримує лише I-кадри й P-кадри (без B-кадрів) [13].

Ще один важливий аспект – режим бітрейту. H.264 реалізує як VBR (Variable Bit Rate), так і CBR (Constant Bit Rate). У VBR бітрейт змінюється залежно від активності сцени: коли в кадрі мало руху – бітрейт знижується, коли багато – збільшується. Це корисно для систем відеоспостереження, щоб оптимізувати використання пропускної здатності мережі.

H.264-кодування має затримки при енкодингу/декодуванні, бо для створення P-кадрів потрібно використовувати дані з I-кадрів і проводити розрахунки векторів руху, а декодеру – буферизувати хоча б частину кадрів для відтворення. У випадку IP-відеоспостереження, H.264 балансує між ефективністю стиснення і апаратними вимогами, тому залишається дуже популярним на «камерах + сервер + VMS», оскільки забезпечує хорошу якість зображення при розумному навантаженні на мережу та накопичувальне сховище.

1.3.2 Кодек H.265

Кодек H.265, або HEVC (High Efficiency Video Coding), був розроблений для забезпечення значно вищої ефективності компресії відео, ніж H.264/AVC. Головна ідея HEVC – зменшити обсяг даних при збереженні подібного або навіть кращого рівня якості зображення, особливо для високої роздільної здатності (4K і вище) або камер з низькою динамікою руху. У H.265 використовуються великі блоки кодування, які називаються CTU (Coding Tree Units), що дозволяє краще адаптувати компресію до структури кадру: великі блоки використовуються там, де зміни мінімальні, а менші – там, де потрібна

велика деталізація чи рух. Для покращення передбачення руху H.265 застосовує складніші алгоритми motion estimation, які дозволяють моделювати рух із більшою точністю. Крім того, HEVC має вдосконалені методи ентропійного кодування, що забезпечує кращу компресію без значної втрати якості. Завдяки цьому бітрейт може бути значно знижений, а при збереженні прийняттого рівня візуальних артефактів система зберігає більше відео в архіві або використовує меншу пропускну здатність мережі [13].

У системах відеоспостереження переваги H.265 стають особливо відчутні, коли йдеться про великі об'єкти з багатьма камерами високої роздільної здатності: зменшення трафіку й швидка передача потоків забезпечують економію ресурсів мережі, а зниження об'єму архіву – менші витрати на дискові масиви. Проте використання HEVC накладає підвищені вимоги на обчислювальні ресурси серверів або клієнтів, які декодують відео: для розкодування H.265 часто потрібні процесори з більшою потужністю або апаратне прискорення (наприклад, GPU або спеціалізовані прискорювачі). Також слід враховувати, що старіші платформи VMS або клієнтські пристрої можуть не повністю підтримувати HEVC або потребувати оновлень. Важливо перевіряти сумісність з усіма компонентами системи – камерами, серверами, віддаленими клієнтами. У деяких інсталяціях може бути прийнятним гібридний підхід: частина камер використовує H.265 для запису, інша – H.264 для моніторингу або сумісності [14].

1.3.3 Кодек MJPEG – технічний опис

Кодек MJPEG (Motion JPEG) – це формат, при якому кожен кадр відеопотоку кодується окремо як JPEG-зображення. На відміну від H.264 чи H.265, тут не використовується міжкадрове стиснення: кожен кадр зберігається як незалежний JPEG, що забезпечує максимальну якість окремого кадру, але значно збільшує обсяг даних та трафік у мережі.

Основна перевага MJPEG у системах відеоспостереження – це точність відтворення деталей, особливо у тих випадках, коли важлива кожна деталь кадру. Наприклад, при розпізнаванні номерних знаків (LPR), контролі зони або OCR-аналізі MJPEG дозволяє уникнути артефактів, які виникають через міжкадрове кодування H.264/H.265. Також цей формат зменшує затримку при декодуванні, бо немає необхідності аналізувати попередні кадри, що робить його зручним для систем реального часу з високою швидкістю кадрів.

Недоліки MJPEG очевидні: через відсутність міжкадрової компресії бітрейт і обсяг архіву сильно зростають. Для прикладу, камера, яка передає 1080p при 30 fps, може генерувати потік у десятки разів більший, ніж при H.264, що накладає великі вимоги на мережеву інфраструктуру та сховище. У практичних інсталяціях MJPEG рідко використовується для багатокамерних систем і зазвичай обмежується однією камерою або вузькими задачами високої точності.

У більшості сучасних IP-камер є можливість комбінованого потоку: основний потік для архіву й перегляду використовує H.264/H.265 для економії ресурсів, а другий потік – MJPEG, наприклад, для LPR-аналітики або передачі через спеціалізовані робочі станції, де важлива деталізація кадру [15].

1.4 Протоколи передачі даних у CCTV

У системах IP-відеоспостереження основні функції передачі відео, керування камерами та взаємодії з VMS забезпечуються набором стандартних мережевих протоколів. Вони визначають, яким чином камера «спілкується» з сервером або клієнтським програмним забезпеченням, як відбувається доступ до потоків, як передаються події та як синхронізуються режими роботи.

RTSP використовується для організації доступу до відеопотоків: через нього VMS отримує live-відео та може керувати тим, який саме потік запитувати. RTP/RTCP застосовуються для транспортування медіаданих та

контролю стабільності передачі, що дозволяє отримувати відео без розривів і затримок [16].

Стандарт ONVIF відіграє ключову роль у сумісності обладнання різних виробників. Завдяки йому VMS може автоматично виявляти камери, отримувати їх характеристики та виконувати базові функції на кшталт керування PTZ, доступу до подій або налаштування профілів відео. Це значно спрощує інтеграцію змішаних систем [17]

HTTP/HTTPS використовуються для доступу до веб-інтерфейсу камери, обміну службовими даними та роботи з API. Захищений варіант (HTTPS) забезпечує захист конфігурацій та облікових даних при підключенні [18].

Для синхронізації часу застосовується NTP, завдяки чому всі камери та сервери мають однакові часові мітки. Це важливо для коректної роботи архіву, журналів подій і аналітики.

У випадках, коли потрібно передавати один відеопотік одразу кільком клієнтам, використовуються multicast-механізми на основі IGMP. Це дозволяє оптимізувати навантаження на мережу.

Окрім цього, камери та VMS працюють на стандартних мережевих протоколах рівня TCP/IP (DHCP, DNS, ARP, ICMP), які забезпечують базову мережеву взаємодію: отримання адрес, маршрутизацію та доступність пристроїв [19].

Загалом ці протоколи формують фундамент роботи будь-якої системи відеоспостереження: вони забезпечують передачу відео, інтеграцію обладнання, безпеку, стабільність зв'язку та коректну взаємодію між усіма елементами інфраструктури.

1.4.1 RTSP

Це протокол керування відеопотоком. Він сам нічого не кодує і не стискає, за це відповідають кодеки на кшталт H.264 чи H.265. Завдання RTSP –

дати можливість клієнту (VMS, плеєру, робочій станції) запросити відеопотік у камери, запустити його, поставити на паузу, зупинити або переключити. Тобто це «мова», якою камера та клієнт домовляються, як саме передавати відео.

У реальній роботі систем відеоспостереження RTSP майже завжди йде в парі з RTP/RTCP. RTP відповідає за сам трафік – тобто за передачу кадрів відео й аудіо. RTCP – це додатковий контроль: він синхронізує потоки, стежить за затримками, втратами пакетів, тобто за якістю трансляції. Це важливо для живого відео, особливо коли мова про PTZ-камери або аналітику, яка потребує стабільної та прогнозованої затримки.

RTSP підтримує різні варіанти підключення: стандартний прямий перегляд, доступ до запису, multicast для економії трафіку або unicast – коли кожному клієнту віддається окремий потік. На практиці це той механізм, завдяки якому будь-яка IP-камера може інтегруватися з VMS незалежно від виробника, якщо вона підтримує стандартний RTSP-URL.

Переваги RTSP у системах відеоспостереження полягають у забезпеченні гнучкого керування потоками, підтримці декількох користувачів, сумісності з різними кодеками і платформами, а також у можливості інтеграції в VMS різних виробників через стандартні команди. Протокол дозволяє працювати як у локальній мережі, так і через VPN для віддаленого доступу. Недоліки RTSP пов'язані з тим, що сам протокол не шифрує дані, тому при передачі через відкриті мережі потрібні додаткові шари безпеки, такі як TLS/HTTPS або VPN, а також протокол чутливий до втрат пакетів у мережі, що може впливати на якість відеопотоку при нестабільному з'єднанні [17].

У сучасних IP-камерах RTSP є стандартним протоколом для інтеграції з VMS і забезпечує універсальний доступ до потоків відео незалежно від виробника. Використання RTSP дозволяє будувати централізовані системи відеоспостереження, де окремі камери і сервери працюють як єдина мережа з можливістю керування, моніторингу та аналітики відео.

1.4.2 HTTP та HTTPS у системах IP–відеоспостереження

HTTP (HyperText Transfer Protocol) є одним із базових транспортних механізмів, які використовуються IP–камерами для передачі службових даних, конфігурацій, метаданих та окремих типів відеопотоків. У контексті систем відеоспостереження цей протокол виконує роль каналу керування і запитів між клієнтом (VMS, адміністратор, веб–браузер) та камерою. Через HTTP здійснюється доступ до веб–інтерфейсу камер, запуск або зупинка аналітичних подій, передача метаданих, інтеграція з API виробника та ONVIF, а також отримання управлінських команд, наприклад PTZ. На відміну від RTSP, який використовується для потокової передачі відео в реальному часі, HTTP застосовується ширше – як універсальний протокол взаємодії між різними елементами архітектури системи.

HTTPS є захищеною версією HTTP і використовується всюди, де необхідно забезпечити захист даних від перехоплення або модифікації під час передачі. У сучасних IP–камер та професійних VMS перехід на HTTPS став обов’язковим у корпоративних мережах, оскільки протокол забезпечує шифрування TLS, автентифікацію серверів та захист налаштувань камер, логінів, API–запитів та всіх критичних операцій. Для інтегрованих систем відеоспостереження використання HTTPS особливо важливе при роботі у великих логістичних комплексах, де доступ до камер часто здійснюється через L3–сегментацію, VPN–тунелі або зовнішні канали. Відсутність шифрування створює ризики перехоплення паролів, підміни конфігурації або доступу до внутрішніх мереж через скомпрометовані камери [18].

У VMS типу Milestone XProtect, Hanwha Wave або Luxriot HTTPS використовується для підключення до камер, які підтримують сертифікати, а також для безпечного обміну аналітичними даними. Сучасні камери Axis і Hanwha підтримують вбудоване керування сертифікатами, завантажувати сертифікати від корпоративних СА, що робить HTTPS стандартом безпечного

розгортання у великих системах. Крім того, саме через HTTPS працюють REST API, через які відбувається інтеграція відеосистем з VMS, системами контролю доступу, аналітичними платформами та хмарними сервісами.

HTTP також активно використовується для передачі MJPEG–потоків, які не потребують складних механізмів синхронізації, а також для отримання snapshot–кадрів, що часто застосовуються у LPR–системах, розпізнаванні подій, верифікації тривог та при інтеграції із зовнішніми модулями. Однак класичний HTTP не забезпечує реального часу та не гарантує доставки, тому для відеопотоків високої якості в полі використовуються інші протоколи, тоді як HTTP/HTTPS залишаються основою для керування, метаданих та доступу до сервісних функцій.

Із розвитком кібербезпеки HTTPS фактично став стандартом для професійних систем відеоспостереження. Виробники камери переходять на обов'язкове шифрування, забороняють старі протоколи (TLS 1.0/1.1), впроваджують HSTS і забезпечують контроль сертифікатів. Це дозволяє інтегрувати камери в IT–інфраструктуру підприємств без створення додаткових ризиків для мережі.

1.4.3 ONVIF

ONVIF (Open Network Video Interface Forum) є міжнародним галузевим стандартом, розробленим для забезпечення сумісності між IP–камерами, відеореєстраторами, VMS та іншими пристроями фізичної безпеки різних виробників. Його ключова мета полягає у створенні єдиного механізму взаємодії, незалежного від конкретної марки обладнання. Завдяки цьому ONVIF став основою інтеграції у сучасних системах відеоспостереження, де одночасно використовуються камери, VMS і мережеві пристрої різного походження.

Стандарт базується на використанні веб-сервісів та XML-опису функцій пристрою, що дозволяє системам керування отримувати інформацію про підтримувані профілі, параметри потоку, конфігурацію кодування, перелік подій, PTZ-можливості, мережеві налаштування та інші сервіси. ONVIF не визначає апаратну реалізацію, а лише встановлює спільний формат взаємодії, що дає можливість масштабувати системи без прив'язки до конкретних платформ.

У професійних системах відеоспостереження ONVIF використовується насамперед для автоматичного виявлення камер у мережі, їх додавання до VMS, налаштування потоків (primary/secondary), синхронізації часу, активації подій та отримання метаданих. Саме цей стандарт дозволяє VMS типу Milestone XProtect, Hanwha WAVE, Luxriot EVO або інших платформ коректно інтегрувати до системи обладнання сторонніх виробників. Підтримка ONVIF стала критичною умовою для великих логістичних об'єктів, де розгортання системи може виконуватись поетапно й включати комбіноване обладнання.

У стандарті передбачені різні профілі, які відповідають за певний функціонал. Найбільш поширеним став профіль S, орієнтований на потокове відео, події та PTZ-керування. Для аналітики та метаданих використовується профіль M, який забезпечує передачу даних від вбудованих AI-модулів: траєкторії об'єктів, LPR-даних, класифікації подій. Профіль T орієнтований на H.265, передавання метаданих та сучасні формати відео. Наявність різних профілів дозволяє підбирати обладнання відповідно до вимог конкретного проєкту [19]

ONVIF також визначає модель подій, що є важливою складовою систем технічної безпеки. Через неї передаються сигнали про детекцію руху, тривоги відеоаналітики, порушення тамперингу, втрату мережі, зміну конфігурації та інші стани. Завдяки уніфікованій структурі подій VMS може використовувати аналітику від камер різних брендів без додаткових модулів інтеграції.

Важливою частиною стандарту є вимоги до безпеки: використання HTTPS, сертифікатів, TLS–шифрування для передавання конфігурацій та подій. У останніх специфікаціях ONVIF вводить обов’язкові механізми захищеного доступу, що дозволяє використовувати камери у корпоративних мережах із підвищеними вимогами до кіберзахисту.

ONVIF фактично став галузевим стандартом для професійних систем відеоспостереження. Завдяки його застосуванню проєктування систем на логістичних об’єктах спрощується, зменшується залежність від конкретного виробника, а масштабування та модернізація не потребують повної заміни всієї інфраструктури.

1.5 Принцип роботи систем керування відео (VMS) на прикладі Milestone XProtect

Системи керування відео (Video Management Systems, VMS) являють собою програмно–апаратні комплекси, призначені для централізованого приймання, обробки, зберігання та надання доступу до відеоданих з мережевих камер. У сучасних IP–системах відеоспостереження VMS виконує роль базового керуючого шару, який забезпечує узгоджену взаємодію між камерами, серверами зберігання та клієнтськими додатками.

Було розглянуто принципи функціонування однієї з найбільш розповсюджених VMS–платформ. XProtect реалізує класичну клієнт–серверну архітектуру, у якій сервери відповідають за обробку та запис відео, а клієнти – за конфігурацію системи й оперативний доступ до відеопотоків. Такий підхід дозволяє розгортати систему в масштабах від невеликих локальних об’єктів до великих розподілених структур з тисячами камер.

Загалом архітектура XProtect забезпечує можливість централізованого керування всіма елементами системи, стабільний запис відео та масштабованість від одного сервера до багатосерверних інсталяцій із десятками

віддалених майданчиків. Завдяки чіткій розподіленій структурі та поділу ролей між серверними компонентами система зберігає працездатність навіть у разі відмови окремих її частин, що відповідає вимогам сучасних логістичних об'єктів до безперервності та надійності відеоконтролю.

1.5.1 Склад серверних компонентів Milestone Xprotect

Система Milestone XProtect побудована за модульним принципом, де різні функціональні завдання покладені на окремі серверні компоненти (Рис. 1.5).

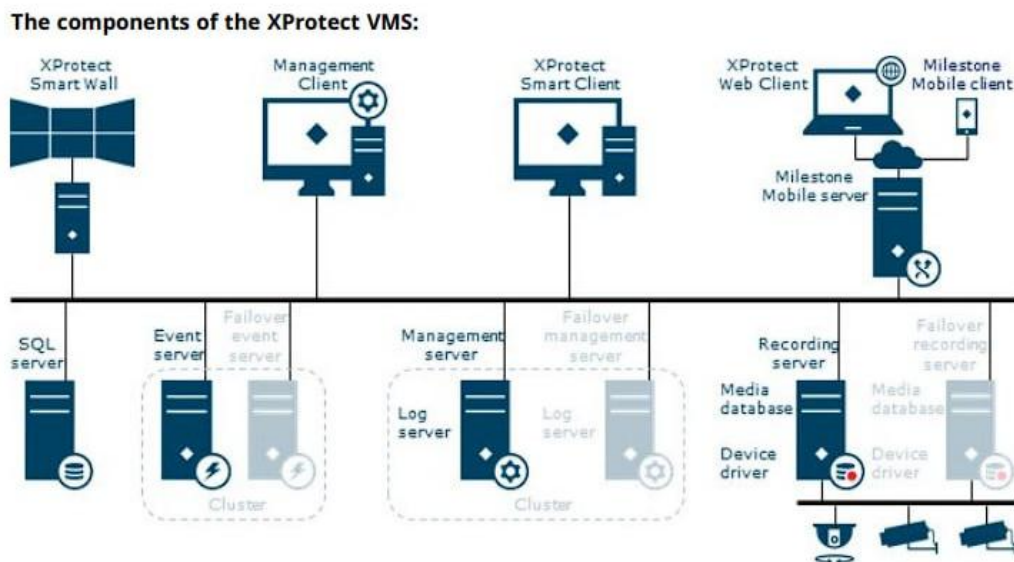


Рисунок 1.5 - Схема компонентів системи Milestone Xprotect

Такий поділ дозволяє масштабувати систему, оптимізувати навантаження, підвищити відмовостійкість і гнучкість [20]. Нижче описані ключові серверні компоненти, їх призначення та функції:

Management Server – центральний компонент VMS, який відповідає за конфігурацію всієї системи, управління користувачами, правами доступу, правилами роботи, розподіл налаштувань між іншими серверами. У базі даних (Microsoft SQL Server) зберігається вся інформація про систему: камери, їх налаштування, політики запису, користувачів, події та права. Дана архітектура дозволяє при потребі реалізувати режим кластера (Failover Management Server),

щоб у разі збою одного вузла інший миттєво взяв на себе функції управління, що важливо для високонавантажених або відповідальних об'єктів.

Recording Server – компонент, який відповідає за зв'язок з пристроями (IP–камери, відео/аудіо енкодери, I/O–модулі, джерела метаданих), прийом відео/аудіо/метаданих, їх запис та зберігання у медійну базу даних, а також надання доступу клієнтам до живих або записаних потоків. Recording Server відповідає за функціонал core VMS: запис, зберігання, видачу відео, статус пристроїв, тригери подій у разі збоїв або тривоги, генерацію метаданих для пошуку (наприклад, за рухом) та можливість взаємодії з іншими продуктами (при використанні технології Milestone Interconnect [21]).

Media Database – власне сховище, оптимізоване для зберігання аудіо/відео контенту та метаданих. Цей компонент забезпечує механізми багаторівневого архівування, «догляду» відео (video grooming), шифрування, цифрового підпису записів. Така база дозволяє організовувати складну політику зберігання (короткостроковий архів, довготривале зберігання, резервування тощо), що є критичним для логістичних об'єктів із високим потоком даних.

Event Server – компонент, який відповідає за обробку подій, тривоги, карту об'єкта, інтеграцію з сторонніми системами і модулями через API (MIP SDK). Всі системні події, тривоги, інтеграційні сигнали (наприклад, з контролю доступу, аналітики, сигналізації) консолідуються тут. Event Server веде базу тривоги і подій, керує логікою реагування, підтримує функції карт (Maps / Smart Maps), та дозволяє підключення зовнішніх плагінів або аналітичних модулів. Це створює єдине вікно для інтеграції VMS з іншими системами безпеки та контролю.

У разі великих систем передбачене резервування Event Server через кластер (Failover).

Log Server – служба для збору системних логів, аудиту користувацьких дій, записів подій і тригерів. Використовує окрему або спільну SQL–базу з Management Server і забезпечує ведення трьох типів логів: системних (помилки,

попередження, інформаційні), аудиторських (дії користувачів), а також логи, створені на основі правил (rule log) – наприклад, при спрацюванні тривоги або події. Це дає змогу вести повний облік подій, забезпечувати аудит та розслідування інцидентів.

SQL Server – реляційна база даних, яка зберігає конфігурацію системи, записи подій, тривог, логів. Залежно від розміру системи, SQL Server може бути встановлений на Management Server або на окремому виділеному сервері. Для великих інсталяцій рекомендується використовувати корпоративну версію SQL Server (Standard чи Enterprise), встановлену на виділений диск для мінімізації навантаження й забезпечення стабільності роботи.

Mobile Server / Web Gateway (Mobile/Web Server) – компонент, що надає доступ до відеопотоків і архівів через веб-браузер або мобільні пристрої (Smartphone, Tablet). Mobile Server приймає потоки з Recording Server та, за потреби, виконує транскодування відео – це використовується для потоків, кодек яких, не підтримується на мобільних пристроях. У великих розгортаннях такі сервіси рекомендується встановлювати на окремі виділені сервери задля розвантаження основних Recording Server.

API Gateway / MIP VMS API – компонент, який забезпечує RESTful API та WebSocket-інтерфейси для інтеграції VMS з іншими системами (контроль доступу, ERP, WMS, аналітика, хмарні сервіси тощо). Він може бути встановлений на тому ж сервері, що Management Server, або на окремому хості; при цьому підтримується мультисерверна схема. Через API Gateway здійснюється конфігурація, керування подіями, запити метаданих і взаємодія з зовнішніми додатками.

Такий модульний підхід дає змогу побудувати систему гнучко: для невеликих проєктів достатньо одного фізичного сервера з усіма компонентами, а для великих логістичних майданчиків – виділити кожен компонент на окремий сервер, забезпечити резервування, балансування навантаження та підвищену надійність. Згідно з рекомендаціями Milestone – при системах із

більш ніж ~100 камерами доцільно використовувати окремі виділені сервери для основних компонентів [22]

1.5.2 Логіка потоків даних, запису і зберігання відео

У системі Milestone XProtect передавання, обробка та зберігання відеоданих побудовані за принципом розподіленої архітектури, де кожен компонент виконує чітко визначену роль. Джерелом відео є IP–камери, які передають потоки на Recording Server за стандартними протоколами, включно з RTSP/RTP для відео, HTTP/HTTPS для службових запитів та ONVIF для конфігурації й подій. Між камерою і сервером формується постійний керуючий канал, через який сервер задає параметри потоку, перемикає профілі кодування або ініціює повторне підключення. Потік фактично надходить лише тоді, коли сервер цього потребує: наприклад, для запису, для аналітики або для відображення у клієнта. Такий підхід дозволяє оптимізувати навантаження на мережу й камери і тим самим масштабувати систему без надмірних ресурсних витрат [23].

Після отримання даних Recording Server пропускає їх через внутрішній pipeline, де пакети впорядковуються, перевіряються на цілісність, синхронізуються за таймкодами та проходять через модуль, що визначає, чи потрібно їх фіксувати за поточною політикою запису. Сам запис здійснюється у власну файлову структуру Milestone – Media Database. Її формат орієнтований на високу швидкість обробки, тому відео зберігається у вигляді блоків, а окремі індексні файли дозволяють фактично миттєво знаходити потрібні часові діапазони при відтворенні. Запис може вестися в кілька рівнів зберігання: «гаряча» база для короткострокового доступу розташовується на SSD тоді як довготривалий архів переміщується на повільніші сховища, включаючи NAS, SAN або дискові масиви великої місткості. Переміщення між рівнями здійснюється автоматично відповідно до розкладу або політики retention [24].

Для клієнтів логіка доступу до відео побудована так, щоб Management Server не був задіяний у передачі відеопотоків. Smart Client, Web Client або мобільний клієнт отримують від нього лише конфігурацію, правила доступу та інформацію про те, який Recording Server відповідає за конкретну камеру. Подальше з'єднання встановлюється безпосередньо між клієнтом і Recording Server, що забезпечує мінімальні затримки і знімає навантаження з центральних сервісів. Під час перегляду архіву сервер знаходить потрібні блоки за часовими індексами, витягує їх із медіабази та відправляє клієнту у вихідному кодеку або у транскодованому вигляді, якщо цього потребує клієнтський режим роботи.

У системі також існує окрема логіка роботи з подіями та аналітикою. Метадані, отримані з камер або сторонніх модулів, потрапляють через Recording Server до Event Server, який виконує обробку правил, тригерів, тривог і взаємодію з підсистемами доступу, LPR чи аналітичними модулями. Клієнти отримують ці дані синхронізовано разом із відео [25].

Завдяки такій архітектурі XProtect дає змогу будувати системи з тисячами камер, без перевантаження центральних компонентів і без необхідності в складній маршрутизації потоків. Управління, запис, доступ до відео та обробка подій чітко розділені, що підвищує відмовостійкість і спрощує адміністрування.

1.5.3 Масштабованість, відмовостійкість, резервування і розподілені системи

У сучасних системах відеоспостереження для логістичних об'єктів ключовим аспектом ефективності є здатність VMS інфраструктури масштабуватися, залишатися доступною при збої окремих компонентів та забезпечувати безперервний доступ до відеоданих у режимі 24/7. Під час аналізу архітектури Milestone XProtect було розглянуто підходи, які платформа застосовує для досягнення високого рівня продуктивності, відмовостійкості й керованості в розподілених середовищах.

На рівні масштабованості система XProtect побудована як модульна, де кожен основний компонент (Management Server, Recording Servers, Event Server, Log Server, Mobile Server) може розгортатися окремо і незалежно один від одного. Завдяки цьому кількість серверних вузлів може збільшуватися відповідно до зростання кількості камер, трафіку, географічних майданчиків або вимог до аналітики. Гнучкість масштабування забезпечується тим, що Recording Server не має жорстких обмежень щодо кількості камер і може бути доданий у систему будь-коли, не порушуючи роботи існуючої інфраструктури. Такий підхід дозволяє логістичним об'єктам розширювати систему поступово – від кількох зон до недоступності. Для Recording Server платформа пропонує повноцінну модель Recording Server Failover, коли резервний сервер перебуває у «гарячому» або «теплому» режимі очікування, отримуючи конфігурацію основного й автоматично активуючись при збоях. Така схема забезпечує безперервний запис відеопотоків навіть у випадку фізичного виходу з ладу обладнання, що є критично важливим для зон відвантаження, рамп, складів тимчасового зберігання, пунктів пропуску транспорту та територій з підвищеним ризиком інцидентів [26].

Суттєву роль відіграє також можливість побудови розподілених систем. У логістичних компаніях часто існує потреба об'єднати декілька складів або хабів у різних містах у єдину централізовану систему. XProtect підтримує сценарії Federated Architecture, де кожен майданчик має власний повноцінний Management Server, а центральний офіс виконує функцію «вузла федерації». Такий підхід дозволяє керувати всіма об'єктами, залишаючи їх автономними, що значно підвищує стабільність та спрощує адміністрування. Федерація застосовується для компаній, що мають десятки об'єктів, і дозволяє реалізувати єдині політики доступу, централізовані журнали подій, узгоджене управління аналітичними модулями та контроль стану обладнання на всіх локаціях [27].

Резервування систем зберігання також займає центральне місце в інфраструктурі відеоспостереження. XProtect підтримує використання NAS,

SAN і кластеризованих файлових систем, дозволяючи будувати сховища з високою доступністю. Можливе застосування RAID–масивів, резервних пулів дисків, віддаленого архівування та перенесення записів між дисковими групами без переривання роботи серверів. За потреби система може зберігати дублікати відео одночасно на двох різних Recording Server або в окремому Safe Storage, що мінімізує ризик втрати критичних даних.

Загалом під час аналізу архітектури Milestone було встановлено, що платформа реалізує підхід, орієнтований на безперервність роботи, що дозволяє логістичним об'єктам підтримувати високий рівень операційної безпеки. Висока масштабованість, можливості резервування та підтримка розподілених систем роблять XProtect одним із найбільш придатних рішень для складських і транспортно–логістичних комплексів, де критично важливими є як надійність системи, так і можливість швидкого її розширення відповідно до бізнес–потреб [28].

Сотень камер та десятків площадок, зберігаючи керованість із єдиного центру.

Важливим аспектом є забезпечення відмовостійкості, оскільки логістичні комплекси працюють у режимі безперервних циклів і не допускають втрати відеодоказів чи припинення моніторингу. Архітектура Milestone XProtect підтримує кілька механізмів резервування. Для Management Server застосовується кластеризація або його дублювання через Failover Management Server, який автоматично перебирає функції основного у разі його падіння.

1.6 Загальні принципи роботи відеоаналітики та AI

Відеоаналітика в сучасних IP–системах відеоспостереження базується на методах комп'ютерного зору та алгоритмах штучного інтелекту, які перетворюють відеопотоки з камер на структуровані цифрові дані. Основною метою є автоматичне виявлення об'єктів, аналіз їх поведінки та генерація

метаданих, які використовуються для пошуку, індексації, створення подій або автоматизації сценаріїв у системах керування відео. Робочий процес включає поетапну обробку: первинне захоплення відео, нормалізацію зображення, детекцію об'єктів на основі моделей глибокого навчання, класифікацію типів об'єктів, відстеження їх руху та подальше формування інформаційних структур для запису у систему.

Однією з ключових тенденцій розвитку є поява edge-аналітики, яка виконується безпосередньо на камері. У камерах, оснащених спеціалізованими процесорами, реалізуються моделі детекції транспортних засобів, людей, номерних знаків, визначення напрямку руху або оцінки щільності трафіку. Обробка даних на рівні пристрою знижує навантаження на мережу, оскільки передаються не «важкі» відеопотоки, а компактні метадані, а також підвищує відмовостійкість системи у випадку втрати зв'язку з сервером. Такі камери можуть автономно виконувати підрахунок об'єктів, контроль зон, виявлення вторгнень чи інших сценаріїв.

Серверна аналітика використовується у системах, де потрібна висока точність, складні алгоритми або аналіз великої кількості камер одночасно. На потужних серверних вузлах, часто оснащених графічними прискорювачами, здійснюється глибоке розпізнавання подій, обробка архівного відео, пошук за атрибутами, побудова поведінкових моделей або мультиоб'єктний трекінг. У цьому випадку аналітика може виконуватися паралельно для десятків тисяч кадрів за секунду, що дозволяє використовувати її у масштабних логістичних комплексах, транспортних вузлах або промислових підприємствах [29].

Поєднання edge- та серверної аналітики забезпечує гібридну архітектуру, у якій камера виконує базову фільтрацію та виявлення подій, тоді як сервер – глибоку обробку, агрегацію метаданих та інтелектуальний пошук. Такий підхід забезпечує оптимальний баланс між навантаженням на мережу, точністю алгоритмів і масштабованістю системи [30].

1.6.1 Типи відеоаналітичних задач у логістиці та транспортній інфраструктурі

У логістичних об'єктах відеоаналітика застосовується для автоматизації контролю, підвищення безпеки та оптимізації операційних процесів. Основні категорії аналітичних задач включають детекцію об'єктів, класифікацію та трекінг рухомих об'єктів, контроль зон доступу, підрахунок кількості транспортних засобів і людей, а також розпізнавання номерних знаків і поведінкових сценаріїв. Детекція та класифікація об'єктів дозволяє автоматично визначати наявність транспортних засобів, пішоходів, вантажів або спеціальної техніки. У логістичних центрах це застосовується для контролю руху автомобілів на рампах, зон завантаження та вивантаження, а також на внутрішніх територіях складів. Аналітика здатна визначати тип транспортного засобу, його розмір, напрямок руху та швидкість. Завдяки трекінгу система може відстежувати траєкторію руху об'єктів, визначати зони заторів та оптимізувати маршрути переміщення техніки всередині об'єкта. Підрахунок об'єктів є однією з ключових аналітик для управління логістичними потоками. За допомогою edge або серверної аналітики фіксується кількість автомобілів або людей у певних зонах у заданий проміжок часу. Це дозволяє автоматизувати облік відвідувачів, визначати завантаженість рамп, оцінювати продуктивність вантажно-розвантажувальних операцій та планувати ресурси для оптимального обслуговування. Такі функції реалізовані як на бортовій аналітиці камер Axis або Hanwha, так і на серверній платформі Вежа Інкорсофт, що зображено на рисунку 1.6, де дані збираються, агрегуються та обробляються у реальному часі [31].

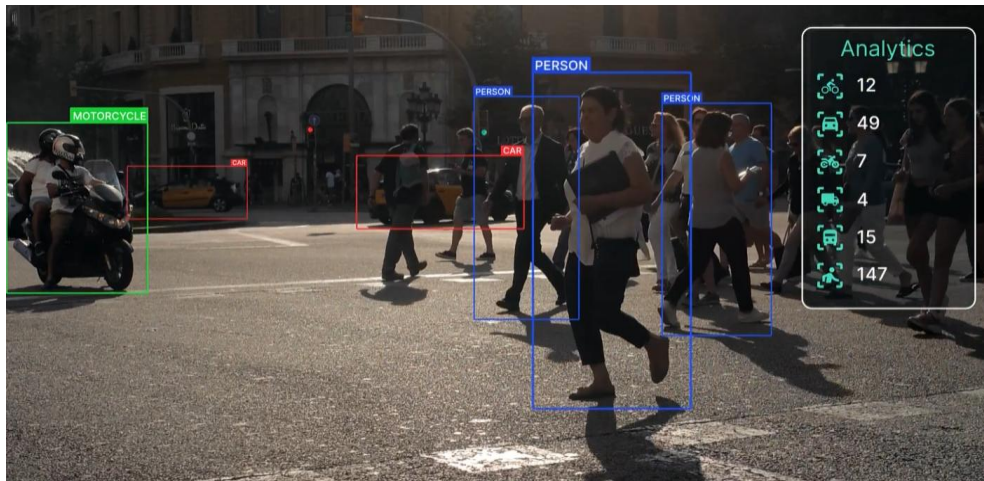


Рисунок 1.6 - Розпізнавання людей і транспорту завдяки аналітиці

Контроль зон, зображений на рисунку 1.7, є критичною функцією безпеки та управління доступом. За допомогою віртуальних зон і ліній, які визначаються в системі, можна виявляти вторгнення, перебування об'єктів у заборонених зонах, порушення маршруту або незаконне припаркування. У логістичних хабах це дозволяє забезпечити контроль рамп, складів з обмеженим доступом, зон відвантаження та стоянок спецтехніки. Інтеграція аналітики з VMS дозволяє налаштовувати тригери, формувати події та повідомлення у разі порушень, що значно підвищує оперативну реакцію охорони.

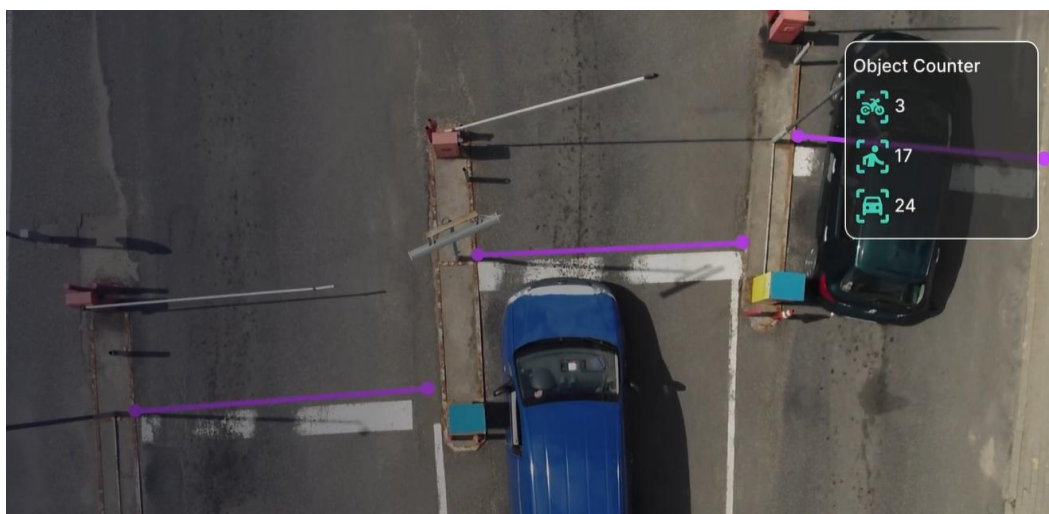


Рисунок 1.7 - Контроль віртуальних зон

Розпізнавання номерних знаків (LPR/ANPR) (Рис. 1.8) є ще однією важливою задачею, особливо у транспортній логістиці. Ця аналітика дозволяє автоматизувати пропуск транспортних засобів, вести облік в'їздів та виїздів, контролювати дотримання правил та відстежувати переміщення автотранспорту по території. Камери з вбудованою AI-аналітикою здатні виконувати попередню детекцію номерних знаків на рівні edge, а серверні модулі Вежа або Milestone XProtect забезпечують точне розпізнавання та інтеграцію з базами даних [32].

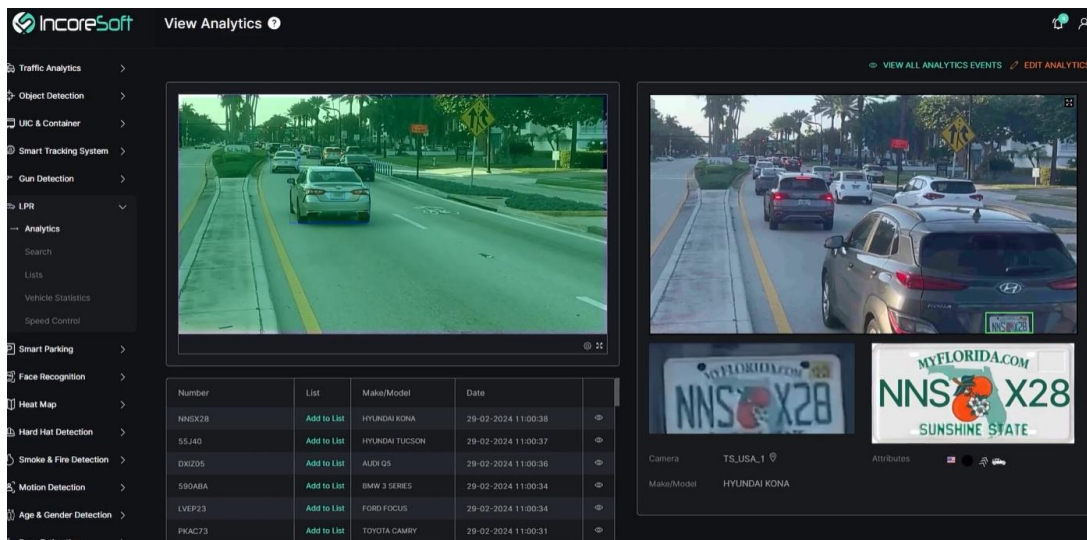


Рисунок 1.8 - Розпізнавання номерних знаків

Загалом, типи аналітичних задач у логістиці та транспорті поєднують детекцію, класифікацію, трекінг, підрахунок, контроль зон та розпізнавання подій (рис. 1.8). Використання edge-аналітики в камерах зменшує навантаження на мережу та сервери, а серверна аналітика забезпечує більш точну обробку, об'єднання даних з декількох камер та інтеграцію у VMS. Такий підхід дозволяє ефективно контролювати рух і безпеку об'єкта, оптимізувати логістичні процеси та швидко реагувати на інциденти [32].

1.7 Висновки з розділу 1

У першому розділі було сформовано теоретичну основу, необхідну для розроблення ефективної системи відеоспостереження на логістичних об'єктах. Розгляд ключових технологічних компонентів, принципів їх взаємодії та вимог до побудови СВС дав змогу визначити, які саме характеристики системи є критично важливими для умов логістичної інфраструктури. Логістичні майданчики та склади мають складну організацію просторів, високу інтенсивність руху транспорту, велике різноманіття виробничих зон та підвищені ризики втручання чи помилок персоналу, що обумовлює жорсткі вимоги до точності, стійкості та швидкості роботи відеосистем.

У межах розділу було узагальнено принципи функціонування IP-камер, мережових технологій, серверних рішень та систем зберігання, а також сучасних методів відеоаналітики. Показано, що побудова СВС у логістиці вже давно виходить за рамки суто охоронної функції: система виконує роль інструмента контролю операційних процесів, оптимізації логістичних потоків, підвищення безпеки та прозорості виробничих операцій. Саме тому теоретичні підходи до вибору камер, проєктування мережевої інфраструктури та застосування аналітичних алгоритмів мають враховувати не лише загальні технічні критерії, а й специфіку логістичного середовища.

Теоретичний аналіз також показав, що сучасні тенденції у відеоспостереженні спрямовані на інтелектуалізацію за рахунок аналітики на рівні камери, інтеграцію з корпоративними інформаційними системами, кіберзахист та оптимізацію мережевого навантаження. Це створює нові підходи до побудови архітектури систем — від централізованих рішень до гібридних моделей, що поєднують серверну та edge-аналітику.

Таким чином, перший розділ сформував фундаментальні знання про принципи роботи та вимоги до сучасних систем відеоспостереження, окреслено

базові критерії вибору обладнання та технологій, а також підготував ґрунт для подальшого практичного проектування та аналітичного порівняння в наступних розділах дипломної роботи.

2 АНАЛІЗ ОБ'ЄКТА ТА ВИЗНАЧЕННЯ ВИМОГ ДО СИСТЕМИ

Розглянутий об'єкт являє собою типовий складський комплекс у межах міста, призначений для зберігання товарно–матеріальних цінностей та забезпечення операцій із приймання, розміщення і відвантаження вантажів. Основна частина будівлі представлена єдиним великим приміщенням зоною зберігання, що містить стелажне обладнання та внутрішні транспортні маршрути, які використовуються персоналом і складською технікою (візками, роками тощо). Допоміжну структуру складають кілька невеликих приміщень технічного призначення, зокрема кімната персоналу, адміністративний кабінет, підсобне або інженерне приміщення та зона для короткочасного пакування або сортування (рис. 2.1). Оскільки об'єкт належить до категорії логістичних, він характеризується підвищеним рівнем ризиків, пов'язаних із зберіганням матеріальних цінностей, обмеженим доступом у внутрішні приміщення та необхідністю контролювати пересування персоналу й рух товарів.



Рисунок 2.1 – Мапа логістичного складу

У зовнішній частині території наявні ключові ділянки, що потребують постійного відеоконтролю: периметр будівлі, в'їзна зона для транспорту та потенційні під'їзні шляхи, якими можуть наближатись сторонні особи або транспортні засоби. Зовнішнє спостереження необхідне для раннього виявлення небажаної активності, фіксації руху в темний час доби, контролю відвантажувальних процесів та документування інцидентів, пов'язаних із проникненнями на територію.

Проведений аналіз функціонального призначення об'єкта дозволив визначити ключові вимоги до системи відеоспостереження. У зоні зберігання головним завданням є фіксація діяльності персоналу, контроль за дотриманням регламентів роботи, запобігання внутрішнім крадіжкам і наближенню сторонніх осіб до товарів. У зв'язку з наявністю стелажів та можливих мертвих зон система повинна забезпечувати достатнє перекриття видимості, коректну роботу в умовах змішаного освітлення та можливість чіткого розпізнавання подій на всій площі приміщення. У внутрішніх кімнатах, що використовуються для адміністративних або допоміжних задач, відеофіксація має забезпечувати контроль доступу та документування операцій із документацією або цінностями.

Для зовнішнього периметру ключовими є вимоги до роботи в умовах низької освітленості, стійкості до погодних факторів, здатності виявляти рух, фіксувати події на відстані та забезпечувати правильне відтворення кольорів і форм об'єктів навіть у сутінках або під вуличним освітленням. Окрему увагу приділено можливості інтеграції зовнішніх камер з аналітичними алгоритмами, зокрема для виявлення проникнення або перебування осіб у заборонених зонах. Аналіз дозволив визначити оптимальне первинне розміщення камер – 8 внутрішніх камер у критичних точках зони зберігання та суміжних приміщень, а також 5 зовнішніх камер по периметру будівлі та на основних під'їзних шляхах. Така конфігурація забезпечує повне покриття ключових ділянок, мінімізує сліпі зони і створює базову інфраструктуру для впровадження як

класичного моніторингу, так і відеоаналітики. На основі вимог об'єкта сформовано технічні критерії вибору камер, мережевого обладнання та VMS, що стають основою для подальших етапів проектування.

На об'єкті вже існує система відеоспостереження, рисунок 2.2, яка працює на локальній VMS-платформі, встановленій на сервері замовника. У поточній конфігурації змонтовано шість внутрішніх камер, одна з яких потребує заміни через несправність або невідповідність технічним вимогам. Частина кабельної інфраструктури, що була прокладена раніше, не забезпечує покриття нових зон спостереження, тому потребує перепроєктування й часткового перенесення трас.

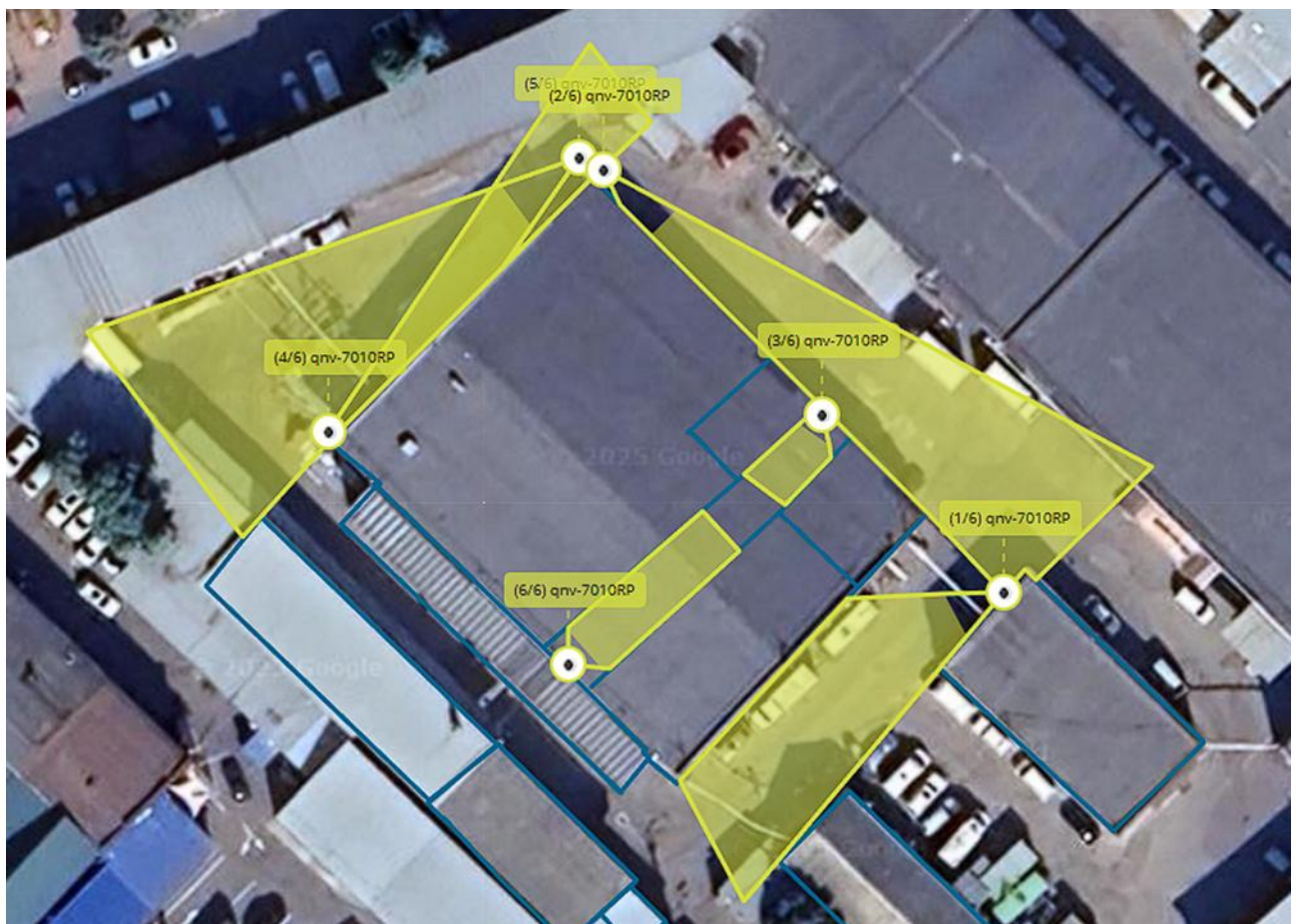


Рисунок 2.2 - Зображення нинішньої системи відеонагляду

Замовник поставив завдання модернізувати систему, розширивши її таким чином, щоб відеоспостереження повністю охоплювало всі внутрішні приміщення складу та зовнішній периметр. Зокрема, необхідно додати камери у зонах зберігання, у приміщеннях із персоналом, у коридорах та в місцях, де відбувається рух техніки. Також потрібно забезпечити контроль периметра та в'їзної групи для фіксації транспортних засобів, їхніх номерних знаків та часу перебування на території.

Окрім фізичного розширення системи, необхідно перевірити, чи відповідає наявний сервер ресурсним вимогам – чи здатен він обробляти збільшену кількість відеопотоків, забезпечувати достатній обсяг архіву та стабільну роботу VMS. Додатково слід врахувати можливість майбутнього впровадження відеоаналітики, зокрема контролю доступу по зонах, відстеження переміщення транспорту та базових функцій підрахунку персоналу.

2.1 Розроблення структурної та функціональної схеми системи

Для проектування системи відеоспостереження на логістичному складі було використано спеціалізований інструмент Axis Site Designer [33], який дозволяє моделювати реальні умови об'єкта, підбирати моделі камер, розраховувати зони покриття та оптимізувати їх розміщення відповідно до технічних вимог. Ця веб-утиліта дає можливість створити структурну схему системи, враховуючи висоту монтажу, геометрію приміщень, інтенсивність освітлення, наявність перешкод та необхідний рівень деталізації зображення. Також Axis Site Designer дозволяє оцінити навантаження на мережеве обладнання, орієнтовний бітрейт потоків та прогнозований обсяг архіву, що важливо для подальшого розрахунку серверної частини Milestone XProtect.



Рис. 2.3 – Розбиття будівель на умовні цифри

Об'єкт складається з шести внутрішніх приміщень (рис. 2.3). Для кожного приміщення було визначено свою функціональність, рівень ризику та вимоги до деталізації, на основі чого обрано відповідні моделі камер. Таке зонування дозволило сформувати логічну функціональну схему системи: внутрішні камери забезпечують контроль персоналу, технічних зон та зони зберігання, а зовнішні – контроль транспортних потоків, периметру та логістичних операцій на вулиці.

Перша будівля логістичного комплексу складається з двох поверхів, однак система відеоспостереження впроваджується лише в тій частині, яка фактично належить замовнику та не передана в оренду іншим компаніям. Таким чином, реальна зона відповідальності охоплює приблизно третину площі споруди, включаючи робочі приміщення, допоміжні зони та міжповерхові переходи. Основним елементом цієї частини є коридор першого поверху, який

використовується як транзитний шлях між складськими приміщеннями та службовими кімнатами.

У коридорі вже була встановлена застаріла камера (рис. 2.4), яка не забезпечувала достатнього рівня деталізації, мала обмежений динамічний діапазон і нестабільно працювала за умов змішаного освітлення. Саме тому в процесі модернізації передбачена її заміна на модель Hanwha Canon VB–M614VE. Ця камера була обрана з огляду на її технічні можливості, сумісність із існуючою VMS Milestone XProtect та відповідність вимогам до коридорних приміщень. На мапі (рис. 2.5), можемо оглянути її кут огляду.



Рисунок 2.4 - Камера в 1 будівлі під заміну

Hanwha Canon VB–M614VE має моторизований варіооб'єктив із фокусною відстанню 2.8–8.8 мм, що дозволяє оптимально налаштувати кут огляду коридору, усуваючи «сліпі зони». Завдяки 1/3" CMOS–матриці та підтримці широкого динамічного діапазону камера забезпечує стабільний

рівень деталізації навіть у ситуаціях, коли коридор частково освітлений природним світлом з бокових кімнат, а частково – штучним освітленням. Коридори логістичних об'єктів часто мають змінний рівень освітлення, і саме WDR дозволяє уникати пересвітів та провалів у тінях.

Додатковою перевагою цієї моделі є підтримка стандартів ONVIF та профільної інтеграції з Milestone, що дає змогу напряму працювати з відеопотоками, керувати параметрами та повністю використовувати серверні можливості VMS, включно з записом за подією, аналітикою руху та централізованим керуванням. Камера також має антивандальний захист IK10, що є критично важливим у коридорах, де спостерігається висока інтенсивність переміщення персоналу, обладнання та візків. Високий рівень захисту від механічних пошкоджень мінімізує ризик умисного чи випадкового виведення камери з ладу.

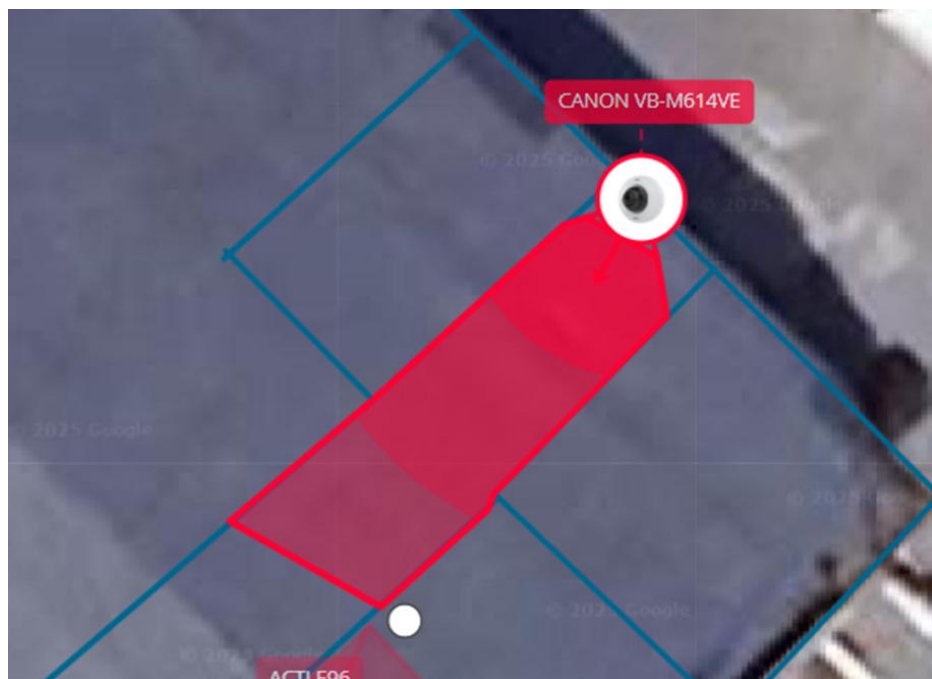


Рисунок 2.5 - Позначення Canon VB–M614VE на мапі

Окремо слід зазначити, що камера обладнана ІЧ-підсвічуванням та здатна забезпечувати повноцінний огляд навіть при вимкненому освітленні на нічний

час. Для логістичного об'єкта це важливо через нічні зміни та необхідність контролю пересування персоналу та вантажів у позаробочий період. Крім того, камера підтримує змінну частоту кадрів і кодеки H.264/H.265, що дозволяє оптимізувати навантаження на існуючий сервер та архів. Сам коридор має лінійну конфігурацію, тому камера встановлюється у торцевій частині на висоті приблизно 2,6–2,8 метра, що забезпечує максимальну довжину огляду та мінімізує спотворення перспективи. Така позиція дозволяє охопити всю робочу зону, дверні прорізи та точки можливого доступу до службових приміщень. Після встановлення камера інтегрується в існуючу мережеву інфраструктуру, підключається до PoE-комутатора та конфігурується на сервері XProtect із заданими параметрами бітрейту, FPS та профілем зберігання.

Другий ярус першої будівлі (рис. 2.6) обладнується окремою камерою для контролю продукції, розміщеної на стелажах.



Рисунок 2.6 - Приміщення і умовне позначення камери

У цій зоні встановлюється AXIS ACTI E96 - панорамна камера з круговим оглядом, яка дозволяє повністю накрити простір без потреби в додаткових точках відеофіксації. Завдяки fish-eye об'єктиву, ця камера забезпечує одночасний моніторинг усіх полиць і проходів, включно з верхніми ярусами, де звичайні камери формують суттєві мертві зони. На мапі (рис. 2.7), можемо оглянути її кут огляду.

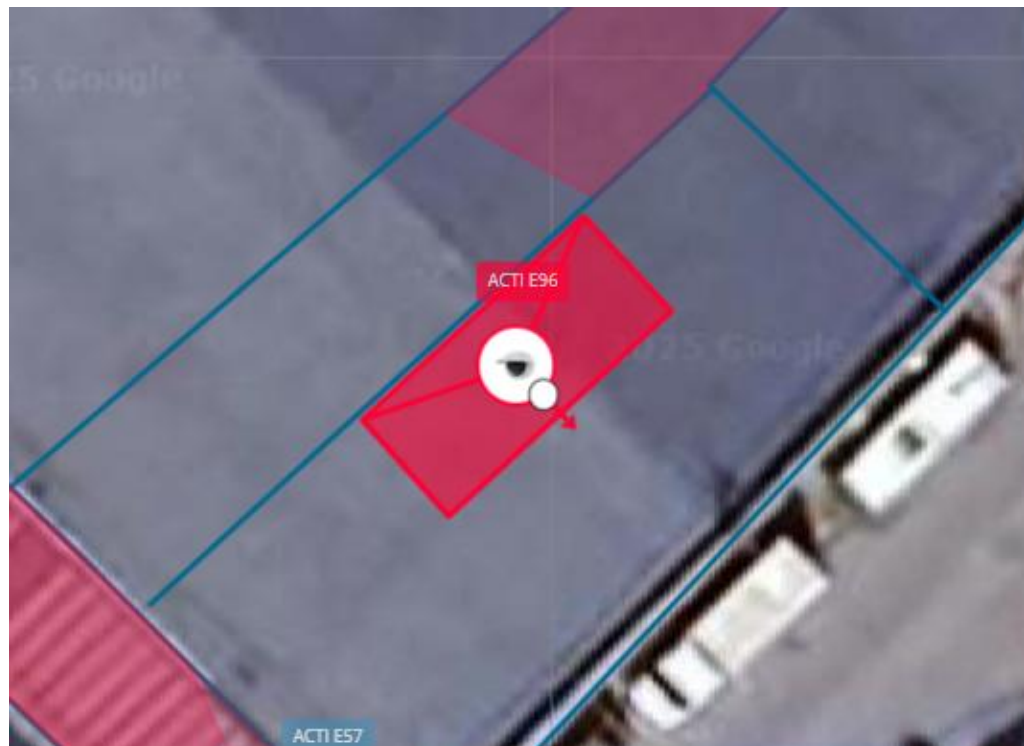


Рисунок 2.7 - Позначення АСТІ Е96 на мапі

Панорамний формат дає можливість переглядати сцену як у сферичному режимі, так і у розгорнутих проєкціях, що спрощує аналіз подій та прискорює пошук конкретних маніпуляцій із товаром. Встановлення на верхній точці другого ярусу дозволяє покрити всю площу робочої зони, контролювати завантаження, переміщення та зберігання продукції без втрати оглядовості. Камера інтегрується з Milestone XProtect, підтримує декілька одночасних потоків та оптимально підходить для задачі загального моніторингу великої кількості стелажів. Як результат, панорамна камера на другому ярусі забезпечує

повний контроль складської зони, дає можливість зафіксувати будь-які дії персоналу та мінімізує потребу у додаткових пристроях для верхнього рівня першої будівлі.

Опис другої будівлі та обґрунтування вибору камер: друга будівля логістичного комплексу являє собою велике одноповерхове приміщення відкритого типу, яке використовується як основна зона зберігання та внутрішньої логістики (рис. 2.8). Приміщення має значну площу, відсутні внутрішні перегородки та присутні високі стелажі, через що формуються численні потенційні мертві зони, які необхідно враховувати під час проектування системи відеоспостереження. Загальна структура зони передбачає постійне переміщення персоналу, техніки та вантажних візків, тому забезпечення оглядовості та деталізації тут є критично важливе.



Рисунок 2.8 - Друге приміщення і умовне позначення камери

Для цього об'єкта було прийнято рішення встановити камеру Hanwha QNV-7010, яка оптимально підходить для великих внутрішніх просторів завдяки поєднанню високої роздільної здатності, широкого кута огляду та стабільної роботи при складному освітленні. Модель обладнана 4-мегапіксельним сенсором із прогресивною розгорткою та фіксованим об'єктивом 2.8 мм, що дозволяє покривати значну частину приміщення одним пристроєм без дефіциту деталізації. Широкий горизонтальний кут огляду забезпечує візуальний контроль проходів між стелажми, зони під'їзду навантажувачів та загальний огляд простору. На мапі (рис. 2.9), можемо оглянути її кут огляду.

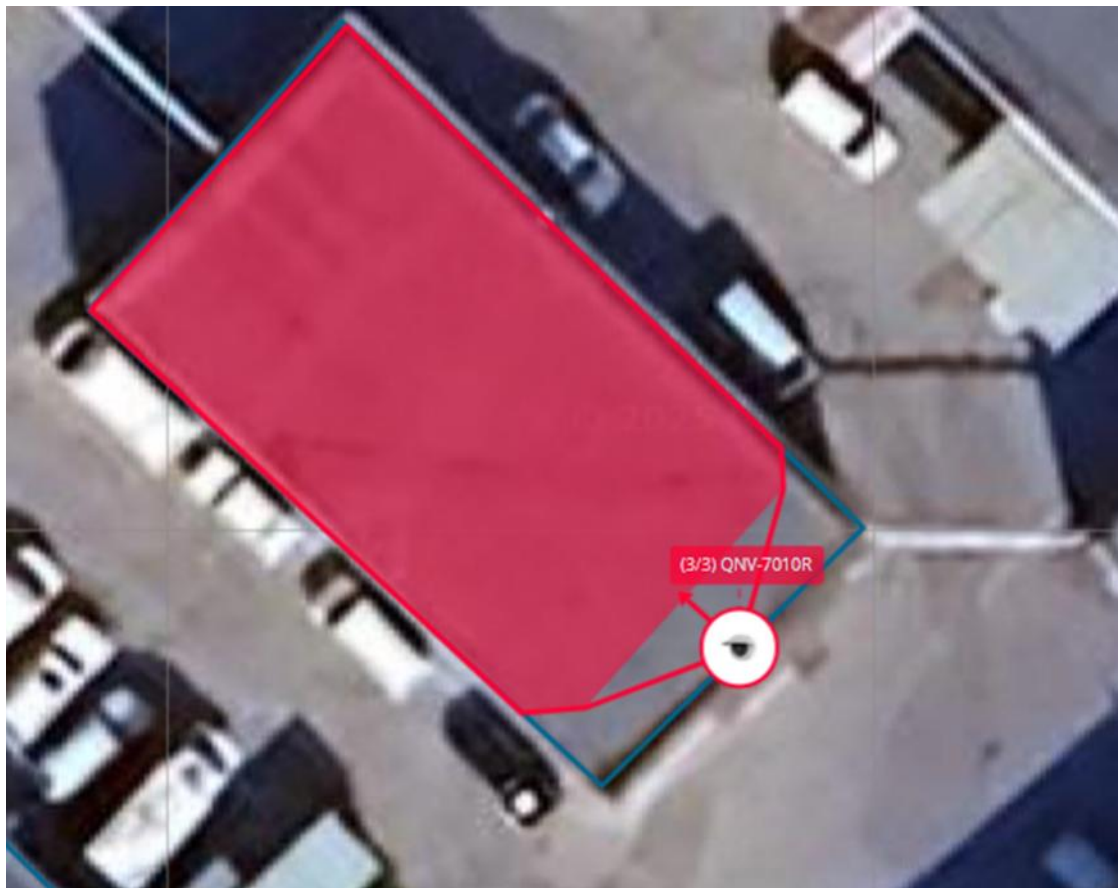


Рисунок 2.9 - Зображення камери на мапі другої будівлі

Камера підтримує технологію широкого динамічного діапазону (WDR до 120 дБ), що є важливим для приміщень зі змінним або нерівномірним

освітленню. У великих складських будівлях часто зустрічається ситуація, коли одна частина зали добре освітлена лампами або LED-світильниками, а інша потрапляє в тінь через високі стелажі. Завдяки WDR камера забезпечує збалансоване зображення, зберігаючи деталізацію об'єктів як у яскравих, так і затемнених зонах. Підтримка ІЧ-підсвічування дозволяє отримувати повноцінне зображення навіть у разі відсутності освітлення у вечірній або нічний час.

Антивандальний корпус класу IK10 забезпечує захист камери від випадкових ударів та механічних пошкоджень, що є актуальним у великих складських приміщеннях, де під час руху техніка може зачіпати обладнання. Камера також має ступінь захисту IP66, що дозволяє встановлювати її в умовах підвищеної запиленості, яка властива складським площам.

Інтеграція Hanwha QNV-7010 з платформою Milestone XProtect виконується через rtsp, onvif або власні протоколи саме для цих моделей камер, що забезпечує стабільний прийом відеопотоку, налаштування бітрейту, FPS та відповідності профілю запису. Під час конфігурації камери виконується оптимізація бітрейту з урахуванням об'єму архіву та пропускної здатності мережі. Модель підтримує кодеки H.264 та H.265, що дозволяє ефективно зменшити навантаження на сервер та мінімізувати використання накопичувача, зберігаючи при цьому необхідну якість зображення.

Камера встановлюється під стелею у центральній частині приміщення, що дозволяє охопити максимальну площу без провалів у видимості. Така позиція забезпечує огляд загального потоку переміщень персоналу, контроль зони доступу до стелажів та виявлення потенційно небезпечних ситуацій. Завдяки достатній висоті монтажу мінімізується ризик пошкодження камери, а огляд залишається стабільним незалежно від розташування вантажів та техніки. На мапі (рис. 2.11), можемо оглянути її кут огляду.

Опис зовнішньої камери для контролю в'їзду до другої будівлі: на фасаді другої будівлі (рис. 2.10), безпосередньо над основним вхідним порталом,

встановлюється камера Uniview IPC3232ER–DV. Її розміщення під козирком дозволяє забезпечити стабільний огляд під'їзної зони вантажівок та всієї діяльності, пов'язаної з розвантаженням та переміщенням вантажів. Дана ділянка є критично важливою для безпеки логістичного процесу, оскільки саме тут здійснюється прибуття транспортних засобів, фіксація осіб, котрі займаються розвантажуванням, а також контроль за дотриманням внутрішніх процедур.



Рисунок 2.10 - Друге приміщення і умовне позначення камери

Камера Uniview IPC3232ER–DV використовує 4–мегапіксельний сенсор із фіксованим об'єктивом, що дозволяє отримувати деталізоване зображення облич водіїв, державних номерних знаків та руху вантажів у межах в'їзної площадки. Широкий кут огляду забезпечує охоплення всієї робочої зони без суттєвих провалів у видимості, що особливо важливо у випадках одночасного перебування кількох працівників або декількох одиниць техніки.

Підтримка широкого динамічного діапазону дозволяє камері працювати при різкому переході між яскравим зовнішнім освітленням та затемненими зонами під навісом. Такий контраст є типовим для зовнішніх входів складських приміщень, тому здатність стабілізувати експозицію забезпечує чітку ідентифікацію об'єктів навіть за умов прямого сонячного світла або контрового освітлення. Крім того, вбудоване інфрачервоне підсвічування забезпечує безперервний контроль в нічний час, коли фіксується значна частина логістичних операцій.

Антивандальний корпус класу IK10 та ступінь захисту IP67 дозволяють використовувати камеру в умовах вуличної експлуатації, захищаючи її від фізичних впливів, дощу, пилу та перепадів температур. Це важливо з огляду на інтенсивний рух транспорту та можливі випадкові механічні контакти під час маневрування вантажівок.

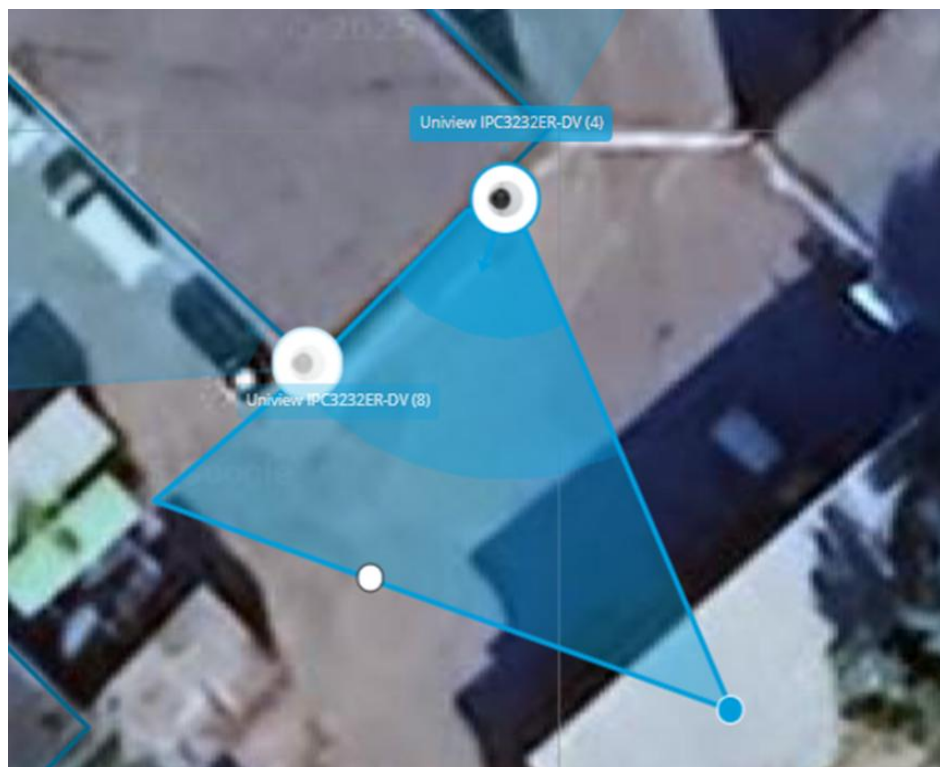


Рисунок 2.11 - Зображення камери Uniview IPC3223ER–DV на мапі

Камера інтегрується з платформою Milestone XProtect через ONVIF, що забезпечує стабільний прийом відеопотоку, можливість налаштування параметрів компресії та оптимізацію бітрейту відповідно до вимог архівації. У конфігурації камери передбачено використання кодеків H.264/H.265 для зниження навантаження на мережу та сервер без втрати необхідної деталізації.

Монтаж під козирком дозволяє одночасно захистити камеру від прямих опадів та отримати оптимальну перспективу, у якій фіксуються транспортні засоби на під'їзді, дії персоналу під час розвантаження та загальний стан вхідної зони будівлі. Це забезпечує повноцінний відеоконтроль усіх логістичних операцій, що відбуваються біля входу до другого складського приміщення.

Опис бічних камер на другій будівлі для контролю паркування та руху транспорту: для забезпечення повного контролю транспортної активності навколо другої будівлі додатково встановлюються дві камери Uniview IPC3232ER–DV (рис. 2.12) (рис. 2.14), розміщені з обох боків споруди. Ці ділянки використовуються для тимчасового паркування вантажних автомобілів, розвороту техніки та виконання допоміжних логістичних операцій, тому їх постійний відеоконтроль є необхідним для забезпечення безпеки та прозорості процесів. На мапі (рис. 2.13) (рис. 2.15), можемо оглянути їх кут огляду.



Рисунок 2.12 - Друге приміщення і умовне позначення камери Uniview IPC3223ER–DV на мапі

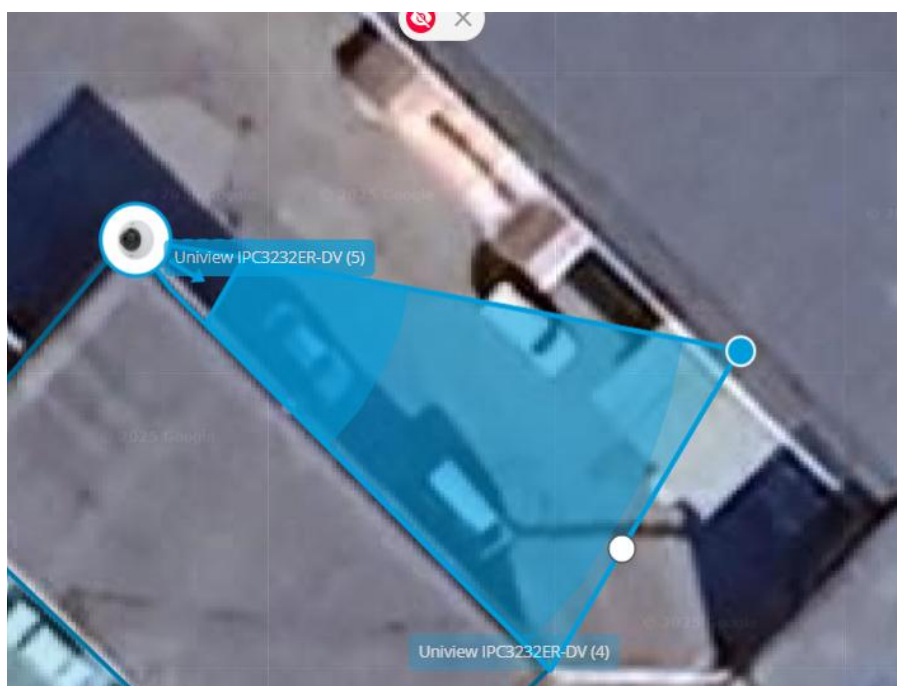


Рисунок 2.13 - Зображення камери Uniview IPC3223ER–DV на мапі



Рисунок 2.14 - Друге приміщення і умовне позначення камери Uniview IPC3223ER–DV на мапі



Рисунок 2.15 - Зображення камери Uniview IPC3223ER–DV на мапі

Камери розташовуються таким чином, щоб охоплювати бокові парковочні зони та прилеглі проїзди, фіксуючи переміщення транспорту, можливі порушення парковки та дії персоналу під час виконання технічних операцій. Uniview IPC3232ER–DV завдяки 4 Мп сенсору та широкому куту огляду дозволяє отримувати достатню деталізацію для розпізнавання моделей автомобілів, відстеження їхнього руху та фіксації взаємодії працівників з вантажем.

Оскільки бокові зони часто мають змішане освітлення – пряме сонячне світло вдень та часткові тіні від стін будівлі – важливою характеристикою є підтримка широкого динамічного діапазону. WDR забезпечує коректну передачу зображення без пересвітів та втрати деталей, що дозволяє ідентифікувати транспортні засоби в будь-який час доби. Вбудоване інфрачервоне підсвічування гарантує контроль за територією у вечірні години, коли на склад часто прибуває або від'їжджає техніка.

Антивандальний корпус та ступінь захисту IP67 дозволяють встановлювати ці камери в умовах зовнішньої експлуатації, де вони зазнають впливу дощу, пилу, вологи та механічних ризиків, пов'язаних із маневруванням великогабаритного транспорту.

Обидві камери інтегруються в систему Milestone XProtect на загальних принципах ONVIF. При конфігурації визначається оптимальна зона огляду та параметри відеопотоку для довготривалої архівації. Для зменшення навантаження на мережеву інфраструктуру застосовується стиснення H.265 із заданим обмеженням бітрейту.

Розміщення парних камер по боках будівлі забезпечує безперервний контроль за в'їздами та маневровими ділянками, дозволяє фіксувати перебіг логістичних операцій та своєчасно виявляти порушення, пов'язані з паркуванням транспортних засобів, блокуванням проходів або неправильним виконанням робіт персоналом. Це формує комплексний периметральний огляд території будівлі та підвищує загальний рівень безпеки логістичного об'єкта.

Третє приміщення є протяжним складським коридором значної довжини, який використовується для зберігання та переміщення товарів уздовж стелажних ліній. Геометрія приміщення формує характерну проблему для відеоспостереження: при встановленні камери на торцевій стіні або лише з одного боку утворюються мертві зони, а деталізація в дальній частині проходу суттєво знижується. Для таких типів приміщень рекомендованим є зональний підхід - розміщення камер уздовж осі коридору з перехресним напрямком огляду (рис. 2.16).



Рисунок 2.16 - Третє приміщення і умовне позначення двох Techwin QNO-8080R

Для цієї будівлі було обрано IP-камеру Hanwha Techwin QNO-8080R, яку встановлено під стелею на бокових стінах так, щоб дві камери дивилися одна на одну. Така схема дозволяє усунути ключову проблему - кожна камера компенсує власну мертву зону безпосередньо під собою, а загальний простір проходу покривається рівномірно з мінімальною втратою деталізації на дальніх ділянках. На мапі (рис. 2.17), можемо оглянути її кут огляду.

Модель QNO-8080R оснащена 5-мегапіксельним сенсором та моторизованим варіофокальним об'єктивом (приблизно 3.6-9.4 мм), що дозволяє точно налаштувати кут огляду відповідно до ширини проходу та вимог до деталізації. Така оптика особливо корисна для довгих складів, де необхідно знайти баланс між шириною зони охоплення та здатністю впевнено фіксувати дії персоналу, серійні номери палет чи можливі інциденти.

Технологія WDR (до 120 дБ) забезпечує коректну роботу камери в умовах змінного освітлення - зокрема у випадках, коли одна частина коридору освітлена природним світлом, а інша знаходиться в тіні. Вбудоване ІЧ-підсвічування великої дальності дозволяє отримувати повноцінну картинку навіть у нічний час, коли освітлення в складських коридорах часто перемикається в економний режим. Антивандальне виконання корпусу та ступінь захисту IP66 дозволяють встановлювати камеру в умовах підвищеної запиленості та ризику механічного контакту зі складаною технікою або персоналом. Обидві камери інтегруються в Milestone XProtect, де для них створені оптимізовані профілі запису з використанням кодека H.265 та контрольованим бітрейтом для зменшення навантаження на мережу. Завдяки тому, що камери працюють у перехресній конфігурації, відеоаналітика (контроль руху, підрахунок активності, виявлення небезпечних ситуацій) отримує стабільний набір даних без провалів у покритті.

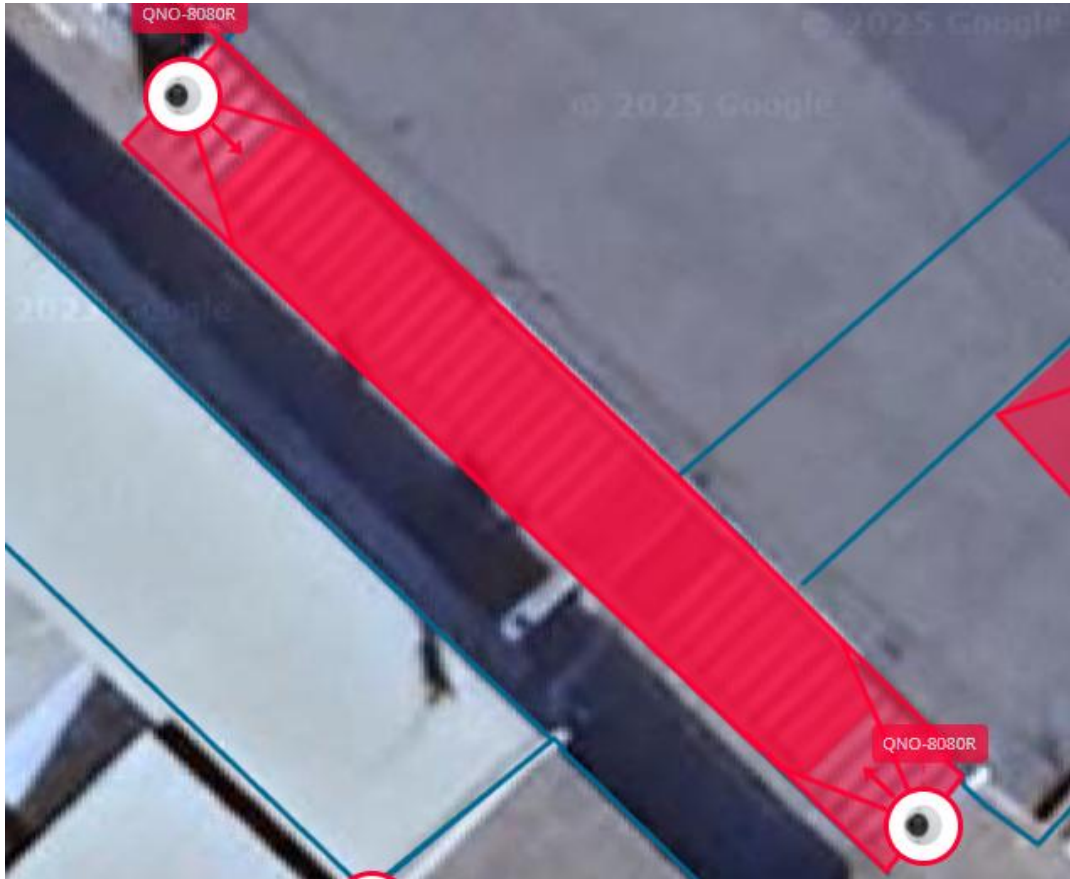


Рисунок 2.17 - Зображення двох камер QNO–8080R на мапі

Така схема розташування дозволяє досягти повного огляду складського проходу, усунути мертві зони та забезпечити високоякісний відеоконтроль у зоні, що має підвищену логістичну активність. Також третя будівля має два незалежних входи, розташованими на протилежних сторонах. Обидва входи активно використовуються для приймання та видачі товару, проходу персоналу, а також для переміщення дрібної техніки. Саме тому контроль цих точок є критично важливим - вони визначають основні потоки переміщення та потенційні ризики несанкціонованого доступу.

Для кожного з двох входів встановлено окрему камеру Uniview IPC3232ER–DV (рис. 2.18). Розміщення камер симетричне: одна фіксує перший вхід, друга - другий, що забезпечує повне покриття обох напрямків переміщення людей і вантажу. Логіка застосування цих камер повторює підхід, використаний у другій будівлі - фіксація транспортних засобів, які

під'їжджають до входу, документування процесів розвантаження, а також ідентифікація працівників або підрядників, що здійснюють переміщення товару. На мапі (рис. 2.19), можемо оглянути її кут огляду.

Модель IPC3232ER-DV є оптимальним рішенням для входів завдяки поєднанню широкого кута огляду, стабільної роботи при змінному освітленні та наявності ІЧ-підсвічування. Камера забезпечує достатню деталізацію для розпізнавання осіб та контролю дій у безпосередній зоні доступу до будівлі. Технологія WDR дозволяє компенсувати контраст між зовнішнім денним світлом і внутрішнім освітленням складського приміщення, що особливо актуально для точок проходу.



Рисунок 2.18 - Третє приміщення і умовне позначення двох Univeiw IPC3223ER-DV на мапі

Антивандальний корпус купольного типу забезпечує стійкість до випадкових ударів, пересувної техніки та впливу навколишнього середовища. Завдяки класу захисту IP66 камера може експлуатуватися навіть у напівзовнішніх складських умовах, де підвищена запиленість та перепади температур є нормою.

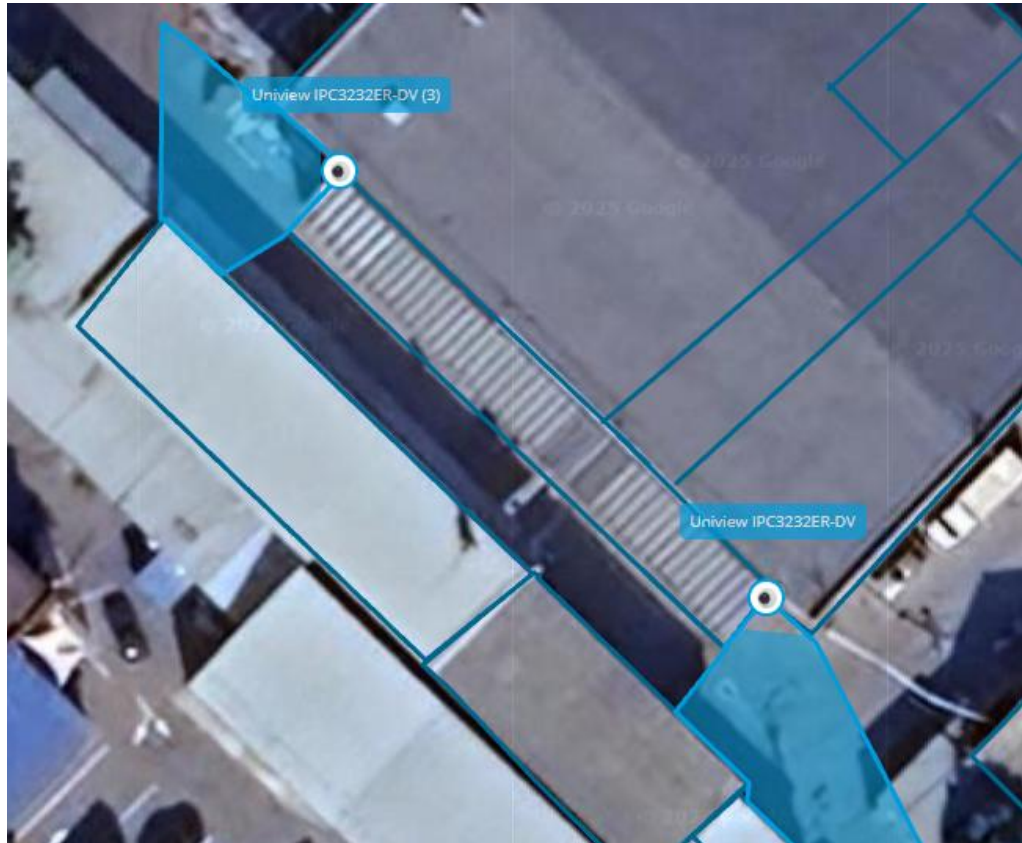


Рисунок 2.19 - Зображення двох камер Uniview IPC3223ER–DV на мапі

Інтеграція камер Uniview з Milestone XProtect здійснюється через ONVIF, що забезпечує стабільний обмін відеопотоками, налаштування бітрейту, FPS і профілів запису. Камери підтримують кодування у форматах H.264 та H.265, що сприяє оптимізації навантаження на серверну інфраструктуру.

Встановлення камер саме на входах дозволяє вирішити ключові задачі: контроль доступу, фіксацію всіх операцій розвантаження, документування пересування товару та запобігання інцидентам, пов'язаним із проникненням сторонніх осіб. Дві камери забезпечують симетричне покриття всього

периметру доступу до будівлі та формують повний запис усіх логістичних процесів у точках входу.

Опис четвертої будівлі та обґрунтування вибору камери: четверта будівля логістичного комплексу за своїми функціональними характеристиками та планувальною структурою є аналогічною до другої - це відкрите складське приміщення середнього розміру без внутрішніх перегородок (рис. 2.20). Основна особливість полягає у формі приміщення - будівля має компактнішу площу, а зона входу розташована на одному з кутів, що визначає необхідність контролю як внутрішнього простору, так і напрямку руху персоналу та техніки від входу в бік складальної зони. На мапі (рис. 2.21), можемо оглянути її кут огляду.



Рисунок 2.20 - Четверте приміщення і умовне позначення камери XND–A8085RV

Для забезпечення повного огляду вибрано купольну IP-камеру Hanwha XND-A8085RV, яку встановлено в протилежному від входу куті під стелею.

Таке розташування дозволяє максимально ефективно використати оглядовий потенціал купольної камери – модель має широкий кут огляду та можливість точного позиціонування завдяки варифокальному моторизованому об'єктиву (приблизно 3.9–9.4 мм). Установка в кутовій точці дає змогу охопити майже всю площу приміщення без необхідності додаткових точок відеоспостереження.

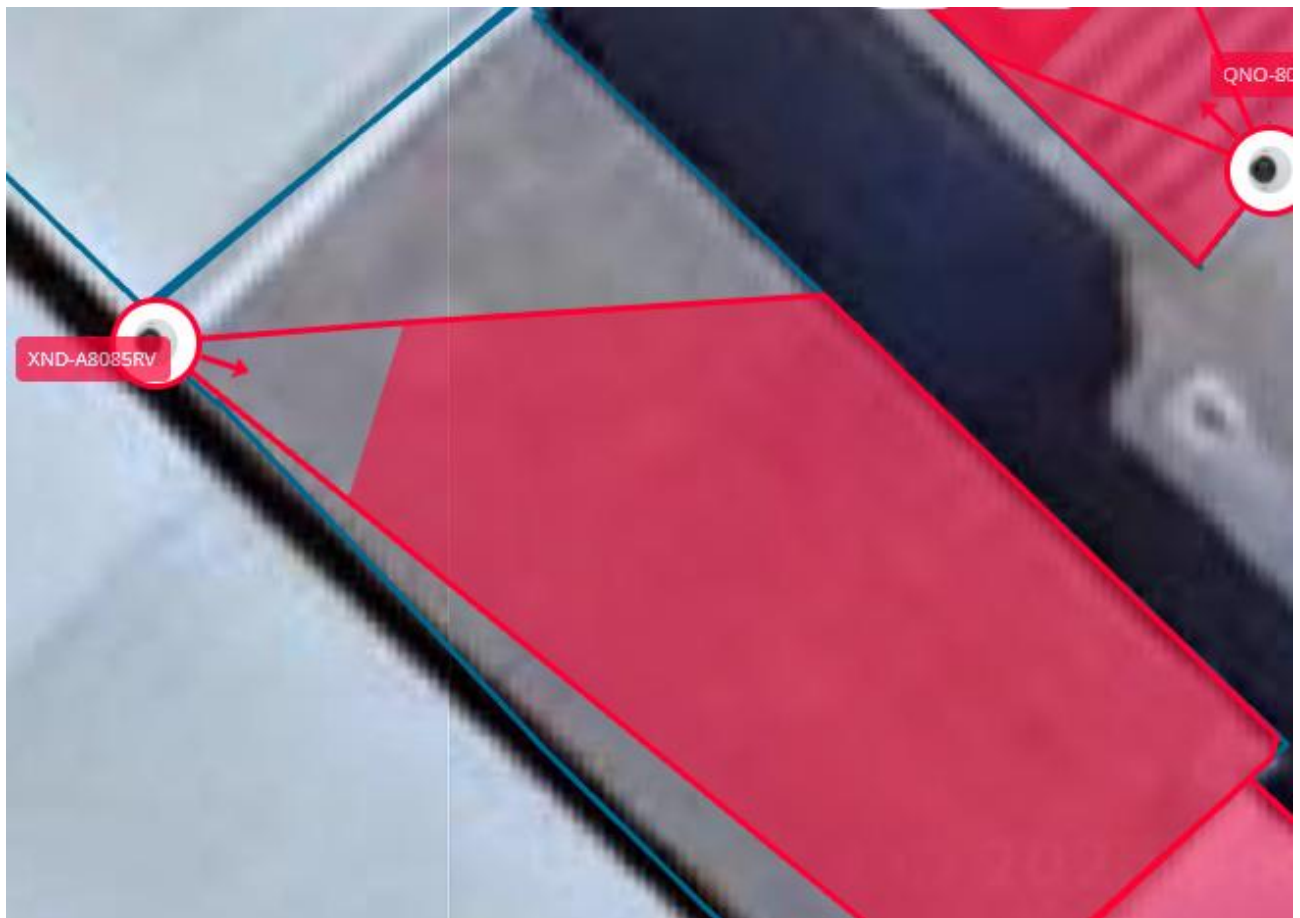


Рисунок 2.21 - Зображення камери XND-A8085RV на мапі

Перевага купольного виконання в цьому випадку полягає у широкому діапазоні кутів нахилу та панорамування, що дозволяє сформувати оптимальну зону контролю навіть у складних геометричних конфігураціях. Також купольні камери менш схильні до фізичного пошкодження та мають кращу стійкість до випадкових зачіпань підйомною технікою, що є поширеною проблемою на складах.

Модель XND-A8085RV належить до серії Wisenet X та оснащена 6-мегапіксельним сенсором з високою світлочутливістю, що забезпечує чітке зображення навіть у приміщеннях зі змішаним або слабким освітленням. Технологія WDR (до 150 дБ) дозволяє збалансувати кадр при різкій різниці яскравості – наприклад, у зонах поблизу воріт або входних дверей, де природне світло може суттєво контрастувати з внутрішнім освітленням.

Вбудоване ІЧ-підсвічування гарантує стабільний огляд у нічний час або в періоди економного освітлення, що часто практикується на складах. Камера також підтримує інтелектуальні алгоритми Wisenet AI (у тому числі класифікацію об'єктів, виявлення людей/транспортних засобів), що додатково підвищує якість моніторингу внутрішньої активності. Корпус камери відповідає класам захисту IK10 та IP66, що дозволяє використовувати її у запилених складських приміщеннях та забезпечує стійкість до механічних впливів. Інтеграція XND-A8085RV з платформою Milestone XProtect виконується через ONVIF, RTSP або фірмовий драйвер Wisenet, що забезпечує коректне передавання метаданих, зокрема даних AI-аналітики. Камера розрахована на роботу з кодеками H.264/H.265, що оптимізує навантаження на мережу та сервер.

Встановлення камери у протилежному від входу куті дозволяє повністю контролювати ключові зони: напрямок руху транспорту після заїзду, роботу персоналу в центральній частині складського простору, зону навантаження та загальний потік операцій. Завдяки широкому куту огляду та правильному позиціонуванню камера формує цілісне, безперервне покриття більшої частини будівлі.

П'яте та шосте приміщення розташовані в межах першої будівлі, однак фізично розділені стіною та виконують різні функції у внутрішній логістиці складу (рис. 2.22). Обидві зони мають невелику площу, просту конфігурацію та передбачувані траєкторії руху персоналу, що визначає специфіку їхнього відеоконтролю. Основним завданням системи у цих приміщеннях є фіксація

наявності продукції, контроль того, що саме розміщується на зберігання, а також моніторинг дій працівників складу у цих робочих точках.



Рисунок 2.22 - П'яте і шосте приміщення і умовне позначення камери QNV-7010R

Для цього було обрано камеру Hanwha QND-7010R, яка завдяки компактному виконанню та широкому куту огляду забезпечує необхідне покриття без мертвих зон. На мапі (рис. 2.23), можемо оглянути їх кут огляду. Модель оснащена 4-мегапіксельним сенсором з фіксованим об'єктивом 2.8 мм, що дозволяє повністю охопити невеликий простір навіть при монтажі в крайових точках. Наявність ІЧ-підсвічування забезпечує стабільну якість зображення при недостатньому освітленні - типова особливість технічних або внутрішніх складських кімнат. Підтримка базового WDR гарантує коректну передачу сцени за умов, коли в дверний проріз надходить денне світло або коли вмикається локальна лампа. Камера без проблем інтегрується з Milestone XProtect через ONVIF, RTSP або власний драйвер Wisenet, що дозволяє конфігурувати оптимальні параметри потоку та забезпечити стабільний запис.

У п'ятому приміщенні камера встановлюється над входом, на гіпсокартонній поверхні, забезпечуючи погляд зверху на дверний вузол та зону

розміщення продукції. Такий монтаж дозволяє фіксувати всі маніпуляції працівників від моменту входу до завершення роботи з матеріалами.

У шостому приміщенні камера розміщується у верхньому куті на гіпсокартонній стіні, що дає можливість охопити приміщення по ширині та висоті, включно з робочими полицями та точками, де персонал залишає або переміщує продукцію. Завдяки широкому куту огляду модель QND-7010R забезпечує повний контроль простору без потреби у додаткових камерах.



Рисунок 2.23 - Зображення камери QNV-7010R на мапі

У комплексі така конфігурація дозволяє забезпечити повноцінний моніторинг двох малих приміщень, зафіксувати дії персоналу та стан продукції.

Комплексне оновлення системи відеоспостереження забезпечує повне покриття як внутрішніх, так і зовнішніх зон логістичного об'єкта, формуючи цілісну інфраструктуру контролю без прогалин у видимості. Первинно на складі вже функціонувало шість камер: чотири з них були встановлені по периметру, а дві - у внутрішніх приміщеннях. Одна з внутрішніх камер

потребувала заміни через технічний стан і невідповідність сучасним вимогам до якості зображення.

Під час проєктування система була суттєво розширена відповідно до реальних сценаріїв роботи складу. Загалом додано вісім нових внутрішніх камер, які забезпечують повний контроль переміщення персоналу, моніторинг продукції у робочих зонах, фіксацію процесів укладки та контролювання складських операцій. Додатково встановлено панорамну камеру на другому ярусі першої будівлі, що дозволяє здійснювати огляд продукції на стелажах у верхній зоні без необхідності монтажу додаткових точкових камер. Окремо було внесено заміну старої камери у коридорі першого поверху, де встановлено нову модель із відповідною оптикою та кращим охопленням простору.

Зовнішня інфраструктура також була значно посилена: розгорнуто п'ять нових камер для контролю ситуації на під'їздах, точках заїзду та розвантаження, а також на бічних частинах будівель, де фіксується рух вантажівок і легкового транспорту. Це дозволяє безперервно відстежувати логістику прибуття, процеси вивантаження товару та дії персоналу, що працює із зовнішніми вантажами.

У підсумку сформована система забезпечує безперервну видимість усіх критичних напрямків - від моніторингу внутрішньої діяльності до контролю периметра, транспортних потоків та моніторингу товару (рис. 2.24). Встановлені камери утворюють логічно узгоджену структуру, у якій кожен пристрій займає своє функціональне місце, усуває мертві зони та доповнює інші точки спостереження. Система охоплює всі ключові процеси складу, підвищує рівень безпеки, сприяє оптимізації роботи персоналу та забезпечує надійний візуальний контроль у режимі реального часу.

Схема прокладання UTP-ліній побудована з урахуванням оптимальної довжини кожного сегмента, дотриманням стандарту Ethernet до 100-120 метрів та резервом для можливих змін конфігурації. У місцях, де кабелі проходять поблизу силових трас, забезпечено необхідне рознесення для уникнення електромагнітних перешкод. Для зовнішніх камер передбачені окремі лінії живлення та мережеві канали, додатково захищені гофрованими трубами або металевими коробами залежно від умов монтажу на фасаді.

Усі кабелі сходяться в центральну точку - серверну частину системи, де встановлено мережеве обладнання та відеореєстраційний сервер. Завдяки структурованому підходу вдалося створити зрозумілу, логічну та масштабовану інфраструктуру, у якій кожна лінія точно прив'язана до своєї камери й відповідає вимогам подальшого супроводу та обслуговування.

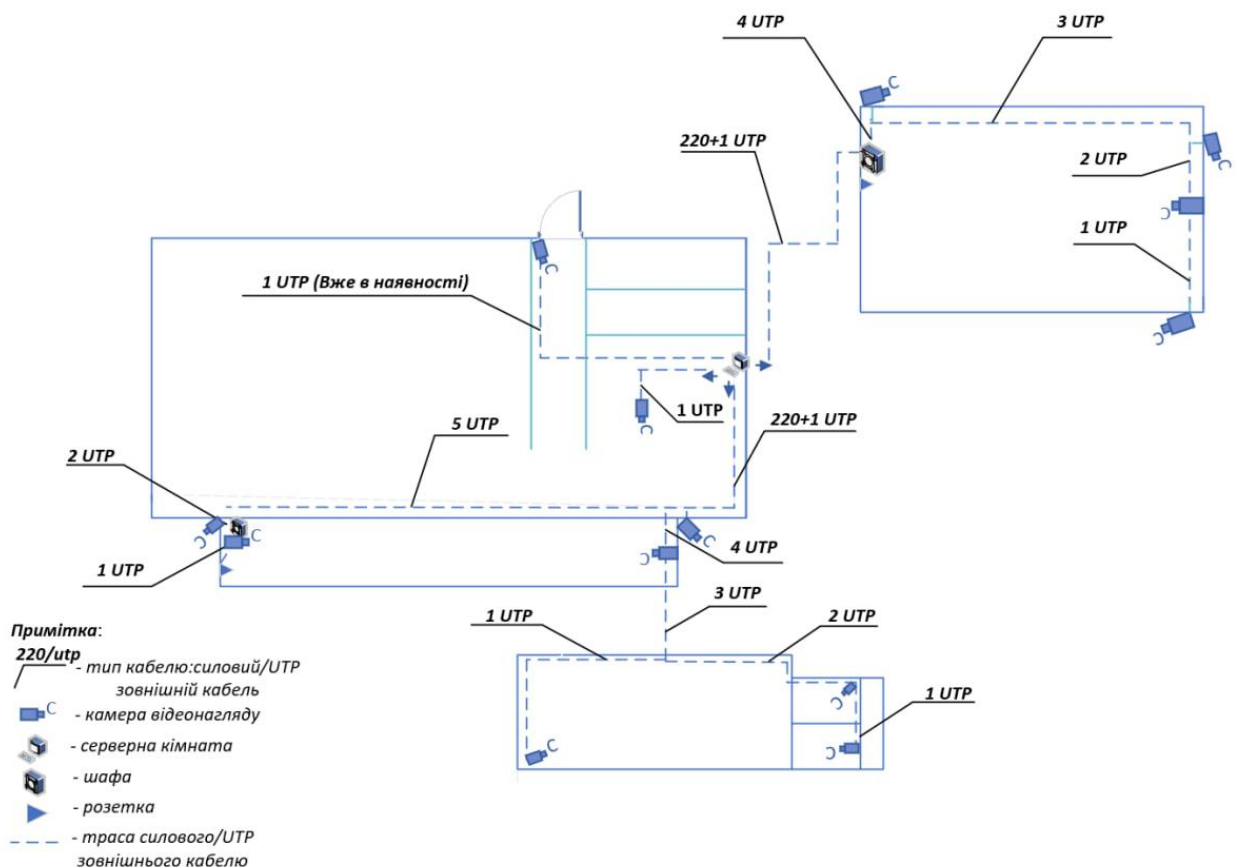


Рисунок 2.25 - Схема трас силових/UTP кабелів

Для побудови низьковольтної інфраструктури системи була використана кабельна лінія UTP категорії Cat6, що забезпечує достатню пропускну здатність для передачі відеопотоків у високій роздільній здатності та створює резерв для подальшого масштабування системи. Кабель відповідає вимогам до роботи з PoE-живленням, що дозволило відмовитися від окремих силових трас для більшості внутрішніх камер та спростити загальну топологію.

У другій будівлі було встановлено окремий телекомунікаційний шафа, у якій розміщено комутаційне обладнання - PoE-комутатор, що забезпечує живлення та передачу даних для локальних камер цього об'єкта. Такий підхід мінімізує довжину окремих сегментів мережі, зменшує навантаження на магістральні лінії та забезпечує стабільність роботи камер у віддалених частинах складу. Монтаж комутатора у локальній шафі також спрощує сервісне обслуговування й забезпечує ізоляцію зони комутації від основної серверної.

Усі кабельні лінії, прокладені від камер у всіх будівлях, сходяться до центральної серверної кімнати, де розміщено відеосервер та основний мережевий комутатор системи відеоспостереження. Така централізація гарантує узгодженість всієї архітектури, спрощує адміністрування та дозволяє здійснювати моніторинг стану мережі з однієї точки.

Прокладання кабелю виконано з дотриманням вимог щодо рознесення слабкострумів і силових ліній, мінімізації перехрещень та уникнення зон потенційних електромагнітних перешкод. У місцях вертикального та горизонтального проходження кабелі укладені в пластикові або металеві коробки залежно від умов експлуатації, а зовнішні ділянки додатково захищені гофрованою трубою. Така структура кабельної системи дозволяє забезпечити надійне з'єднання навіть при значній довжині ліній та гарантує стабільність роботи системи у довгостроковій перспективі.

2.3 Калькуляція сервера

Для забезпечення стабільної роботи системи відеоспостереження та коректного формування відеоархіву було виконано детальний розрахунок серверної частини, що включає оцінку навантаження на систему, параметрів потоків, сумарного бітрейту та необхідного обсягу зберігання даних. Цей розрахунок проводився як для потреб внутрішнього менеджменту, так і для формування технічних вимог до сервера запису, який буде інтегрований у загальну архітектуру Milestone XProtect.

Оцінка розпочиналася з аналізу кожної камери, її роздільної здатності, кадрової частоти, типу кодека та середнього бітрейту в реальних умовах роботи. Окремо враховувався вплив режимів WDR, нічного підсвічування та динамічних сцен, оскільки вони істотно збільшують навантаження на пропускну здатність та процесор сервера. На основі цих параметрів було зведено сумарний прогнозований бітрейт усіх внутрішніх та зовнішніх камер, включаючи як нові пристрої, так і наявні камери попередньої системи.

Далі проводився розрахунок обсягу архіву, необхідного для забезпечення заданого строку зберігання відеоданих (1 місяць). У процесі враховувалася структура запису – запис по руху, а також коефіцієнт компресії та можливі сезонні зміни навантаження. Після узгодження термінів зберігання з менеджментом був проведений підсумковий розрахунок обсягу дискової підсистеми з урахуванням резерву на майбутнє масштабування та потребу у RAID-захисті.

Окремо оцінювалася продуктивність CPU та необхідний обсяг оперативної пам'яті з урахуванням вимог Milestone XProtect щодо одночасної кількості потоків, роботи аналітики та навантаження від клієнтів перегляду. Оскільки сервер виступає як центральний елемент архітектури, було визначено вимоги до мережевих інтерфейсів, резервування каналів, швидкості комутації

та пропускної здатності між серверною та телекомунікаційними вузлами об'єкта.

Калькуляція відбувалась на веб-утиліті Milestone XProtect Calculator [34], у підсумку сформовано комплексну калькуляцію серверної конфігурації, що включає оцінку продуктивності, дискового набору, мережевої інфраструктури та можливостей масштабування. Цей звіт використовується менеджментом для прийняття рішень щодо закупівлі обладнання, а також слугує технічною основою для побудови сервера запису, який забезпечує надійну, безперебійну роботу всієї системи відеоспостереження.

Таблиця 2.1 - Розрахунок Менеджмент сервера

Специфікація менеджмент серверу		Зберігання живої бази даних	
Кількість серверів	1	Кількість для серверу	3
Тип процесору	Intel Xeon 3408u	Тип рейду	5
Операційна система	2*300 GB RAID 1	Розмір диску	960 GB
Тип диску	Enterprise SSD	Тип диску	Enterprise SSD
ОЗУ	16 GB	Необхідна ємність	42 GB

Таблиця 2.2 - Розрахунок специфікації і БД лайву для серверу запису

Специфікація сервера запису		Зберігання живої бази даних	
Кількість серверів	1	Кількість для серверу	3
Кількість камер на сервері	18	Тип диску	Enterprise SSD
Тип машини	Сервер	Тип рейду	5
Тип процесору	Intel Xeon 3408u	Розмір диску	960 GB
Операційна система	2*256 GB	Необхідна ємність	35 GB
ОЗУ	32 GB		

Таблиця 2.3 - Розрахунок архівної бази даних і мережевих інтерфейсів

Архівна база даних		Мережевий інтерфейс	
Кількість для сервера	3	Використання	Камера
Тип диску	Enterprise HDD	Швидкість	1 Gbps
Розмір диску	4 Gb	Необхідний бітрейт	47,8 Mbps
Тип рейду	5	Використання	Клієнт
Необхідна ємність	6,6 TB	Швидкість	1 Gbps
		Необхідний бітрейт	11,38 Mbps

2.4 Висновки з розділу 2

У процесі аналізу об'єкта та визначення вимог до системи було виконано комплексне дослідження умов експлуатації, технологічних процесів та ризиків, характерних для даного виробничого середовища. Дослідження показало, що об'єкт має низку особливостей — значну територію, наявність критичних зон, інтенсивний рух транспорту, роботу персоналу в умовах підвищеної небезпеки, а також вимоги до безперервності технологічного циклу. Це визначило необхідність застосування системи відеоспостереження з підвищеним рівнем надійності, стійкості та функціональної гнучкості.

Проведений аудит можливих загроз (техногенних, організаційних, інформаційних) дозволив сформулювати чіткі вимоги до розташування камер, їхніх технічних параметрів, стійкості до погодних умов, а також до здатності системи забезпечувати високу деталізацію зображення у ключових контрольних точках. Встановлено, що для забезпечення повного циклу моніторингу необхідні різні типи камер — оглядові, PTZ, камери з бортовою аналітикою та спеціалізовані моделі для зон з вибухонебезпечним середовищем.

Крім того, аналіз існуючої інфраструктури показав необхідність модернізації мережевого сегмента — оптимального розміщення комутаційного обладнання, забезпечення гарантованої пропускну здатності, резервування

живлення та використання промислових стандартів грозозахисту. Це дозволило сформулювати вимоги до майбутньої топології системи, включаючи централізовані серверні вузли, PoE-комутатори, структуру каналів передачі та вимоги до безперебійної роботи системи.

На основі детального аналізу експлуатаційного циклу об'єкта були сформульовані вимоги до PaaS-рівня системи: зручність обслуговування, можливість швидкої заміни пристроїв, мінімізація простоїв при оновленні та відновленні роботи, відповідність політикам інформаційної безпеки та інтеграція з допоміжними системами (LPR, face recognition, контролем доступу). Особливу увагу приділено вимогам до масштабованості, що дозволяє адаптувати систему до майбутнього розширення без значних змін архітектури.

Таким чином, у результаті виконаного аналізу було сформовано технічно обґрунтований комплекс вимог, що визначає ключові параметри майбутньої системи відеоспостереження. Ці вимоги стали базою для проектування архітектури, вибору обладнання, розрахунку серверної інфраструктури та формування підходів до подальшої реалізації проєкту, що забезпечує відповідність системи умовам об'єкта та необхідному рівню безпеки.

З АНАЛІЗ СУЧАСНИХ ТЕНДЕНЦІЙ РОЗВИТКУ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Системи відеоспостереження за останні роки перестали бути просто інструментом фіксації подій. Індустрія змістилася у бік інтелектуальних платформ, де камера вже не виступає пасивним датчиком, а стає повноцінним вузлом обробки даних. Головна тенденція - перехід від простого запису до моделі, де відео використовується як джерело аналітики, що може автоматично підтримувати процеси безпеки та операційний контроль. Одним із основних драйверів розвитку стало поширення мережевих камер із вбудованими обчислювальними модулями. Edge-обчислення набули практичного сенсу: сучасна камера вже здатна виконувати задачі, які кілька років тому вимагали окремих серверів із GPU - від виявлення руху з урахуванням контексту до розпізнавання об'єктів і поведінкових сценаріїв. Це суттєво зменшує навантаження на мережу та дозволяє будувати розподілені системи без єдиного критичного вузла. Паралельно зростають вимоги до кібербезпеки. Камера стала повноцінним мережевим пристроєм, а отже - потенційною точкою атаки. Тому виробники впроваджують захищене завантаження, апаратне шифрування, сертифіковані прошивки та контроль цілісності системи. Особливо це стосується корпоративних та промислових проєктів, де ризики саботажу чи втручання значно вищі, ніж у побутових установках.

Ще одна тенденція - розвиток кодеків і оптимізацій відеопотоку. Якщо раніше H.264 був стандартом за замовчуванням, то зараз практично всі професійні системи працюють на H.265, а виробники додають власні Smart-алгоритми, які адаптивно знижують бітрейт залежно від динаміки сцени. Це дозволяє суттєво скоротити обсяги архіву без суттєвої втрати якості. З огляду на те, що у сучасних проєктах може бути десятки або сотні камер, оптимізація потоку стала окремим напрямом розвитку. Водночас індустрія рухається у бік мультисенсорних пристроїв. Камери з декількома сенсорами, панорамним

оглядом або комбінацією ширококутної та телеоптики дозволяють покривати великі зони без збільшення кількості точок монтажу. Це знижує вартість інфраструктури та спрощує обслуговування. Такі рішення особливо актуальні на великих промислових об'єктах, виробництвах і бурових майданчиках, де доступ до обладнання часто обмежений.

Також посилюється тенденція інтегрованості. Камери, VMS, мережеве обладнання, системи доступу та стороння аналітика дедалі частіше працюють як єдина екосистема. API, ONVIF, відкриті SDK і платформи на кшталт ACAP чи Hanwha Wise AI дозволяють розширювати функціональність без зміни апаратної частини. В результаті системи стають більш модульними та гнучкими [35].

Загалом сучасні системи відеоспостереження переходять від «заліза» до інтелектуальних, програмно-керованих рішень, де основною цінністю стає не сама камера, а ті дані й алгоритми, які вона здатна генерувати.

3.1 Порівняння брендів камер відеоспостереження: Axis, Hanwha проти китайських виробників

На сучасному ринку систем відеоспостереження бренди Hikvision, Dahua та інші китайські бренди займають значну частку інсталяцій завдяки нижчій вартості та широкій доступності. Проте попри їхню популярність у масових або побутових системах, саме на об'єктах критичної інфраструктури, банківського сектору, енергетики, медицини, промисловості й державних установах ці рішення практично не використовуються. Для таких сфер ключовими є надійність, кіберстійкість, підтримка та довготривала експлуатація, і саме Axis Communications традиційно залишається для них еталоном професійного відеоспостереження.

В незалежному порівняльному тестуванні камер 4K PoE від The Smart Home Hookup камери Axis і Hanwha показали найкращі результати за

критеріями розпізнавання та деталізації. Зокрема, при ідентифікації об'єктів на дистанції 50 футів Axis отримала максимальний бал 10.0, тоді як Hikvision - 8.0, а при зйомці рухомих об'єктів Axis досягла 9.7 проти 8.0 у конкурентів. Для побутових систем така різниця може здаватися незначною, проте на стратегічних або промислових майданчиках різниця між 8 та 10 у якості може стати критичною [36].

Перевага Axis підтверджується довірою з боку державних клієнтів у всьому світі. Наприклад, місто Вісенте Лопес (Аргентина) встановило понад 800 камер Axis для потреб громадської безпеки та моніторингу інфраструктури. У Делі, Індія, велике державне підприємство SCOPE Minar впровадило централізовану систему відеоспостереження Axis, що дозволило одночасно підвищити рівень безпеки та зменшити витрати на обслуговування. На фоні цього підходу китайські виробники стикаються з численними державними обмеженнями: у 2022-2024 роках обладнання Dahua та Hikvision було заборонено або обмежено у Великобританії, Канаді, Австралії, Індії, а також в урядових структурах США відповідно до Закону про національну оборону (NDAA). Рішення таких країн базуються на ризиках кібербезпеки та непрозорості виробників [37].

У сфері кіберзахисту Axis дотримується системної та відкритої стратегії: з 2013 року компанія регулярно публікує офіційні повідомлення про кіберзагрози, у 2014 створила власну команду кібербезпеки, а у 2016 увела цифровий підпис прошивок для гарантії справжності ПЗ. Надалі Axis впровадила TLS-шифрування, підтримку IEEE 802.1X, політику Security by Design, стандартизацію розробки IoT-пристроїв та сертифікацію за FIPS 140-2, що визнається урядом США [38]. Така прозорість та передбачуваність кардинально контрастує зі станом безпеки китайських камер, які роками страждають від критичних вразливостей, витоків даних та експлойтів. Відомими є випадки масових зломів хмарних сервісів, віддаленого виконання команд та багаторічних проблем з прошивками, через які в мережі з'являлися

інтерактивні мапи з доступом до зламаних камер Hikvision у США та Європі. Ці інциденти не лише підривають репутацію виробників, а й призводять до реальних оперативних ризиків: у 2024 році СБУ повідомила про використання сторонніх камер російськими спецслужбами для коригування ударів по Києву [39].

Ще одним ключовим аспектом є якість виготовлення та здатність камер працювати в екстремальних промислових умовах. Натомість китайські моделі, часто побудовані на дешевших матеріалах, швидше деградують: зустрічаються випадки запотівання, корозії та втрати зв'язку вже через 1–2 роки роботи, особливо у середовищах з екстремальними температурами. Форумні звіти користувачів прямо вказують на нестабільність деяких моделей Hikvision при температурах нижче -16°C , що неприпустимо для промислових об'єктів. Також існує ціла мапа на відкритих ресурсах взломаних камер Hikvision (рис. 3.1) [40].

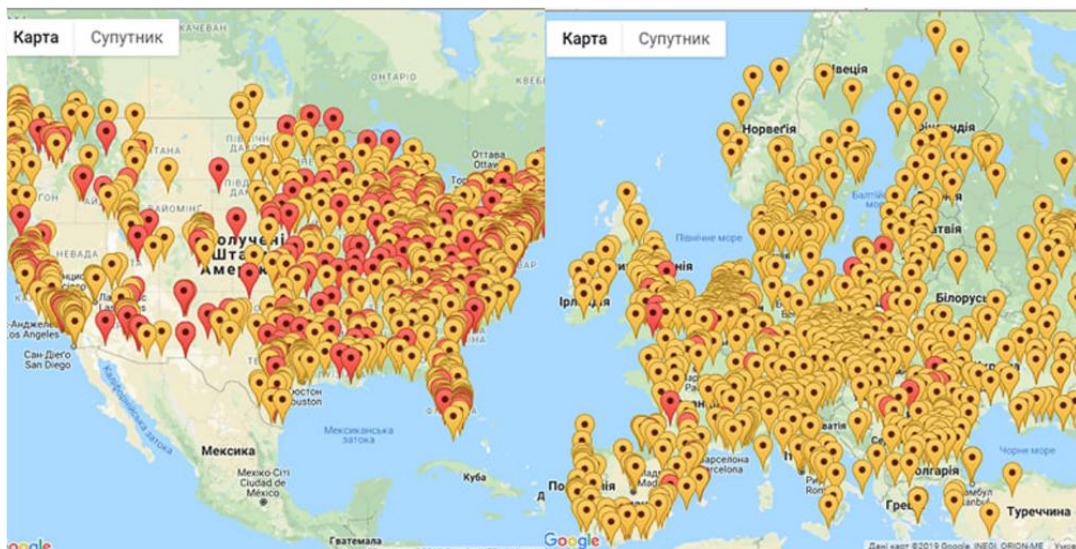


Рисунок 3.1 - Мапа взломаних камер Hikvision

Питання підтримки також є важливим. Axis надає п'ятирічну гарантію без доплат, забезпечує щонайменше сім років оновлень безпеки, детальну технічну документацію, інструменти для дизайнерів, а також прозору політику життєвого циклу продуктів з попередженням про зняття з виробництва.

Водночас підтримка Hikvision, Dahua та інші залежить від регіону, часто обмежується двома–трьома роками, а багато бюджетних та OEM–моделей взагалі не отримують оновлень. Наявність ребрендингу (HiLook, EZVIZ, Digoо тощо) ще більше ускладнює отримання офіційної підтримки та прошивок.

Таким чином, порівняння професійних систем відеоспостереження демонструє кардинальну різницю між підходами Axis, Hanwha і китайських виробників. Axis пропонує високу надійність, передбачуваний життєвий цикл, потужну кібербезпеку, довгострокову підтримку та пристрої, що реально розраховані на важкі умови експлуатації. У той час як китайські бренди орієнтовані переважно на масовий ринок, мають менш прозорий підхід до безпеки і часто не відповідають вимогам об'єктів підвищеної критичності, де ціна помилки може бути надзвичайно високою [41].

3.2 Порівняння серверної і бортової аналітики

При розгляді систем відеоспостереження дуже часто постає питання: де має виконуватись відеоаналітика - прямо в камері або на стороні сервера (VMS). Камери Hanwha Wisenet демонструють, що «вбудований» підхід має низку переваг: такі камери вже оснащені алгоритмами на базі ШІ, які здатні на місці – прямо в корпусі – виконувати класифікацію об'єктів у кадрі (люди, транспорт, номери, обличчя), детектувати перетин віртуальних ліній, виявляти рух, подавати метадані (атрибути: тип об'єкта, положення, час) разом із відеопотоком [42].

Такий підхід має сенс, коли потрібно миттєво отримати детект або тривожну подію – без затримки на передачу всього відео на сервер для обробки. Камера сама відфільтровує «невідповідні» кадри (наприклад, без руху або без цікавих об'єктів) і передає або записує вже чи то подію, чи потенційно важливі фрагменти – що значно зменшує обсяг трафіку та навантаження на серверну інфраструктуру.

З іншого боку, серверне рішення - як Vezha дає гнучкість, масштабованість і централізований контроль аналітики. Vezha пропонує модулі відеоаналітики, які можуть працювати з потоками з будь-яких камер: розпізнавання номерних знаків, облич, об'єктів, аналіз трафіку, події, пошук за архівом, формування статистики [43].

Цей підхід зручний, коли система велика, з багатьма камерами, коли потрібно узагальнити події, робити пошук за архівом, застосовувати єдині політики, або комбінувати дані з різного обладнання. Сервер може агрегувати дані, вести централізований журнал подій, створювати аналітику: скільки було проходів, хто, коли, можливо інтегрувати результати з іншими системами безпеки чи бізнес-аналітикою.

При цьому варто розуміти компроміси. Вбудована аналітика (як у Wisenet) означає, що навантаження на мережу і сервер мінімізоване - обробка відбувається на камері, отже потрібні камери достатньо дорогі, і їх «розумність» обмежена тими алгоритмами, які закладені виробником. Якщо ж потрібно виконувати складну аналітику - пошук, кореляцію подій між камерами, побудову статистики, підрахунок потоку, поведінковий аналіз або кастомні сценарії, - серверне рішення дає набагато більше контролю та можливостей.

Для великих об'єктів, промислових майданчиків або там, де потрібна централізована робота з архівом, масштабування, регулярний аналіз – комбінація обох підходів може бути оптимальною: розумні камери + VMS з аналітикою. Наприклад, можна використовувати AI-камери (Wisenet або Axis) для детекту, а Vezha (рис. 3.2) – для агрегації, архівації, побудови статистики, подій, звітів.

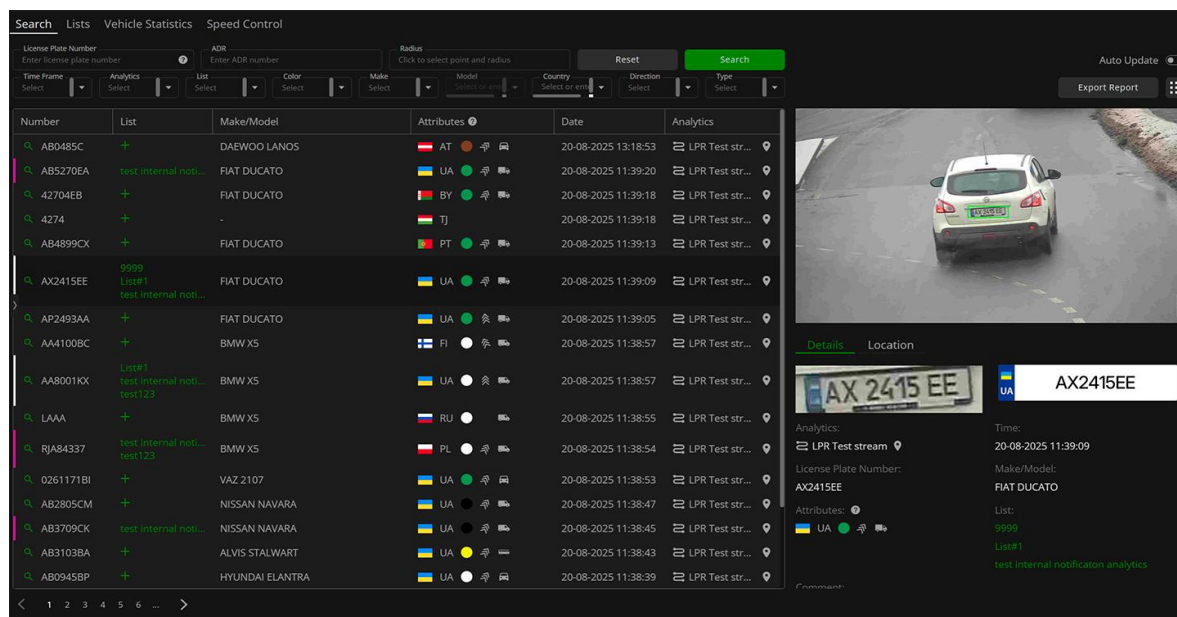


Рисунок 3.2 - Робота серверної аналітики LPR

Вбудована аналітика Hanwha Wisenet (рис. 3.3) - швидка, локальна, мінімізує навантаження, зручна для простих задач детекту; серверна аналітика Vezha VMS - централізована, масштабована, гнучка, придатна для складного, багатокамерного, корпоративного/промислового відеоспостереження.

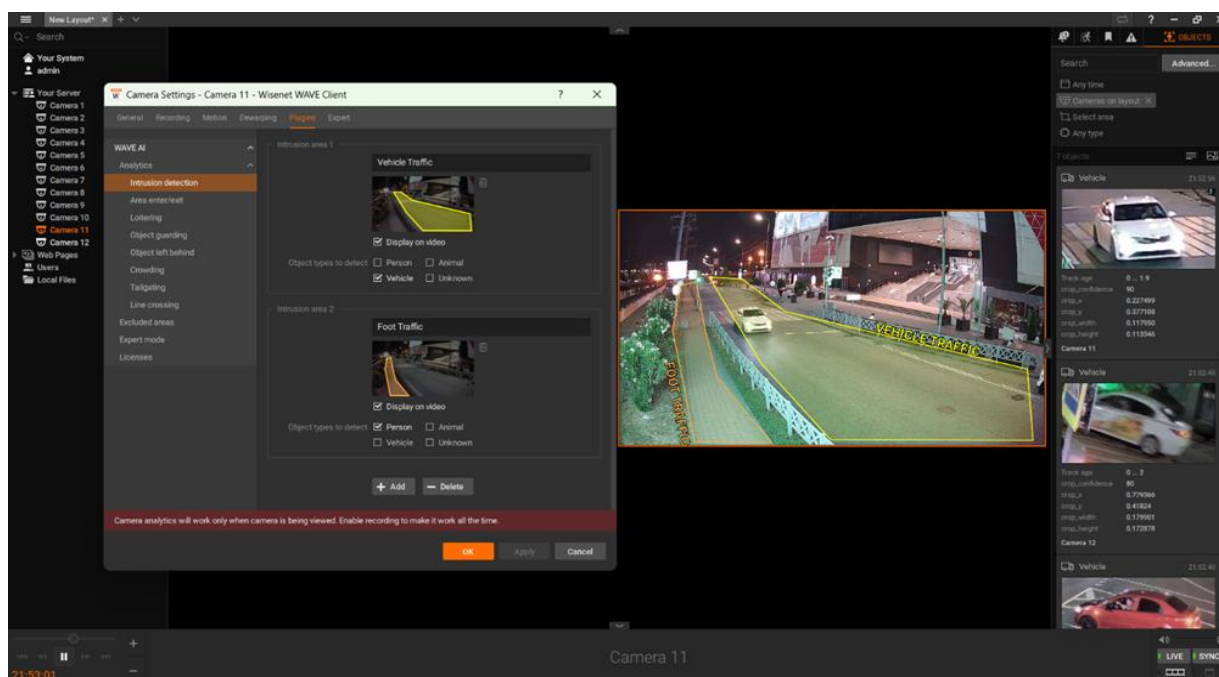


Рисунок 3.3 - Робота бортової аналітики LPR

Ще одна важлива відмінність між бортовою аналітикою камер та серверною аналітикою полягає в тому, як саме зберігаються та обробляються дані про обличчя, номерні знаки чи інші біометричні атрибути. Камери з вбудованим ШІ - як Hanwha Wisenet або деякі моделі Axis - виконують лише детект на місці. Тобто камера може визначити, що в кадрі є людина, обличчя або транспортний засіб, може додати метадані до відеопотоку, але сама по собі вона не зберігає повноцінну базу облич, шаблонів, історію пересувань чи архів співставлень. На борту камери немає довготривалої пам'яті для таких даних - і це зроблено свідомо, як з вимог кібербезпеки, так і через апаратні обмеження [44].

Натомість у серверних рішеннях, таких як Vezha, підхід інший: сервер не лише приймає потоки з камер, але й веде повноцінне збереження та обробку даних. Тут уже формується база усіх зафіксованих облич, номерних знаків, подій і проходів; до кожного запису додаються атрибути, час, камера, з якої отримано дані. Сервер може здійснювати пошук за архівом, порівнювати обличчя між різними камерами, робити вибірки, статистику, а також забезпечує масштабування самої бази. Це критично важливо для великих об'єктів, де потрібно відслідковувати переміщення людей по території, реєструвати всі спроби входу/виходу, будувати аналітику або інтегрувати дані з іншими системами безпеки [45].

Фактично різниця полягає в тому, що камера працює як сенсор із миттєвим розумінням того, що відбувається в кадрі, але без можливості формувати довготривалу історію. Сервер же - це вже повноцінний центр збереження та аналізу, де інформація не лише фіксується, але й накопичується, структурується та може використовуватися для комплексної аналітики. Тому в реальних системах дуже часто поєднують обидва підходи: камери забезпечують швидкий детект, а сервер - центральне сховище та інтелектуальну обробку.

3.3 Підходи до проектування топології інфраструктури відеоспостереження

Проектування топології інфраструктури відеоспостереження сьогодні базується на виборі між трьома ключовими архітектурами – централізованою, децентралізованою та гібридною. Кожен підхід має власні переваги й обмеження, та застосовується залежно від вимог до навантаження, масштабу, відмовостійкості й рівня інтелектуальних функцій, які очікуються від системи.

У класичній централізованій архітектурі всі основні процеси, включно з аналітикою, транскодуванням та записом відео, виконуються на центральному сервері або кластері серверів. Камери виступають переважно як пристрої збору зображення, передаючи потік через мережу до серверної частини. Такий підхід забезпечує високу керованість, простоту масштабування сховища та єдиний центр обробки даних, що полегшує адміністрування. Проте він створює значне навантаження на мережу та робить інфраструктуру залежною від серверних ресурсів: у разі відмови центрального вузла може відбутися втрата частини функціональності або зниження продуктивності. Централізована модель традиційно використовується у великих корпоративних системах із гарантованими каналами зв'язку та потребою в уніфікованих сценаріях аналітики.

Децентралізована архітектура базується на принципі рознесення інтелектуальних функцій на периферію - безпосередньо на IP-камери. Сучасні виробники, такі як Axis, Hanwha чи Mobotix, оснащують камери власними процесорами, які можуть виконувати аналітику на борту: розпізнавання об'єктів, детекцію транспортних засобів, виявлення вторгнень, облік людей тощо. Також підтримується edge-storage - локальний запис на SD-карту або внутрішній накопичувач із подальшою синхронізацією. Це дозволяє зменшити навантаження на сервери та мережу, підвищити відмовостійкість і забезпечити роботу навіть при втраті зв'язку із сервером. Водночас децентралізована модель

складніша в адмініструванні, потребує ретельного підбору продуктивних камер та має обмеження щодо масштабних кореляційних аналітик, де потрібна серверна обробка великих масивів даних.

Гібридний підхід поєднує сильні сторони обох моделей. Базова аналітика - детекція руху, базове розпізнавання, попередня фільтрація подій - виконується на камерах, що дозволяє оптимізувати мережеве навантаження та зменшити кількість непотрібних потоків. У той же час більш складні задачі, такі як міжкамерне відстеження об'єктів, глибинний аналіз, довгострокова аналітика, поведінкові моделі або розпізнавання високої точності, реалізуються на серверному рівні, де доступні більші обчислювальні ресурси. Такий підхід вважається оптимальним для сучасних систем відеоспостереження, оскільки дозволяє збалансувати продуктивність, стабільність та гнучкість розвитку.

Порівняння трьох моделей показує, що вибір архітектури визначається не лише бюджетом, а й особливостями об'єкта, вимогами до аналітики, умовами роботи мережі та рівнем відмовостійкості. Централізована модель забезпечує максимальну контрольованість, децентралізована - автономність і гнучкість, а гібридна - найбільш збалансовану інфраструктуру, здатну адаптуватися до реальних сценаріїв експлуатації та зростаючих потреб системи.

3.4 Аналіз життєвого циклу системи відеоспостереження та вплив довгострокових витрат на вибір архітектури

У сучасних проєктах систем відеоспостереження важливим є не лише первинний вибір обладнання чи архітектури, а й розуміння того, як система поводитиметься на довгій дистанції - протягом усього свого життєвого циклу. Навіть невеликі на перший погляд статті витрат у підсумку формують значну частину загального бюджету, і саме тому інженерне проєктування має враховувати їх ще на етапі планування. Діаграма (рис. 3.4), яка відображає розподіл витрат на обладнання, мережеву інфраструктуру, зберігання даних,

експлуатацію, обслуговування та можливі відмови системи, підкреслює: найбільший фінансові втрати - не на стартових інвестиціях, а на довгостроковому супроводі.

Це впливає на вибір підходу до проектування. Наприклад, дешевші камери можуть здатися вигідними на момент закупівлі, але їх використання суттєво збільшує частку витрат на обслуговування, відмови та перепроєктування, адже вони частіше виходять з ладу, складніше інтегруються з VMS та не забезпечують стабільну аналітику. Навпаки, бренди з надійною підтримкою та тривалим життєвим циклом зменшують ризики відмов і скорочують операційні витрати. Те саме стосується мережевої інфраструктури, сховищ і програмного забезпечення: системи, побудовані без запасу продуктивності, швидко створюють скриті витрати, які на діаграмі проявляються як статті експлуатації, обслуговування, підготовчих робіт і витрат на відновлення.



Рисунок 3.4 - Діаграма витрат на систему відеоспостереження

Таким чином, життєвий цикл системи відеоспостереження – це не лінійний процес, а сукупність взаємопов’язаних етапів, де якість рішень на старті визначає масштаб витрат у наступні роки. Саме тому грамотне проектування, вибір надійних компонентів і прогнозування експлуатаційних сценаріїв мають більшу вагу, ніж початковий бюджет обладнання. Система, побудована з урахуванням повного циклу витрат, працює стабільніше, рідше потребує втручання і забезпечує значно кращу економічну ефективність у довгостроковій перспективі.

3.5 Висновки з розділу 3

Висновки цього розділу формують цілісне розуміння того, як сучасні підходи до побудови систем відеоспостереження впливають на ефективність, масштабованість та економіку всього рішення. Проведений аналіз показав, що вибір камер, архітектури інфраструктури, концепції розрахунку серверних ресурсів і оцінка витрат по життєвому циклу системи є взаємопов’язаними елементами, які не можна розглядати ізольовано.

Порівняння брендів камер продемонструвало, що ринкові рішення суттєво різняться за якістю оптики, стійкістю аналітики, надійністю прошивань і загальною передбачуваністю роботи в довготривалій експлуатації. Це прямо впливає на обсяги сервісного обслуговування, частоту відмов і сумісність із професійними VMS, а отже - на загальну вартість володіння системою.

Аналіз різних підходів до проектування топології - централізованої, децентралізованої та гібридної - показав, що жодна з архітектур не є універсальною. Централізована модель забезпечує повний контроль і високу якість запису, але вимагає значних серверних ресурсів. Децентралізована орієнтована на розвантаження інфраструктури й покладає частину функцій на самі камери, але залежить від їхньої потужності та надійності. Гібридний підхід

поєднує обидві концепції та дозволяє адаптувати систему до різних сценаріїв, зберігаючи баланс між продуктивністю і вартістю.

Розгляд методів розрахунку серверів відеоспостереження показав, що коректний підбір процесора, накопичувачів, мережевих інтерфейсів і ресурсів RAM має критичне значення для стабільності роботи всієї системи. Сервер відеозапису виступає ключовим елементом VMS, і його недооцінка призводить до втрати кадрів, деградації продуктивності та необхідності дорогих модернізацій.

Окремий акцент на життєвому циклі системи дав змогу побачити, що найбільші витрати формуються не на етапі закупівель, а в процесі експлуатації. Саме тому вибір якісного обладнання, правильних архітектурних рішень і передбачення можливих навантажень відіграють ключову роль у довгостроковій ефективності системи.

Таким чином, третій розділ показав, що побудова системи відеоспостереження – це багатofакторний процес, у якому технічні, економічні та архітектурні рішення тісно переплітаються. Ефективність системи визначається не окремим компонентом, а узгодженістю всіх складових: від вибору камери до моделі зберігання відео й підходів до обслуговування. Саме комплексний підхід забезпечує надійну, масштабовану та економічно обґрунтовану систему відеоспостереження.

ВИСНОВКИ

У дипломній роботі було проведено повний комплекс досліджень, спрямованих на обґрунтування, проєктування та аналітичну оцінку сучасної системи відеоспостереження для складського об'єкта, з урахуванням технічних вимог, архітектурних рішень, особливостей інфраструктури та підходів до подальшої експлуатації. Отримані результати дозволили сформулювати цілісне бачення того, як має будуватися ефективна, масштабована і надійна система відеоконтролю.

У теоретичній частині роботи було детально розглянуто фундаментальні принципи функціонування систем відеоспостереження, включаючи особливості ІР-камер, мережевих протоколів, типів відеоаналітики, підходів до зберігання даних та ключових критеріїв, що визначають якість і стабільність роботи таких систем. Цей аналіз створив методологічну основу для коректного вибору технологій і дозволив забезпечити відповідність рішення сучасним стандартам галузі.

У прикладній частині проведено проєктування реальної системи відеоспостереження для комплексу будівель, де розміщені складські та виробничі приміщення. Було виконано зонування об'єктів, підбір камер з урахуванням умов експлуатації, геометрії приміщень, необхідної деталізації та задач: контроль доступу, моніторинг вантажних операцій, фіксація переміщення персоналу, нагляд за продукцією та зовнішньою територією. Розроблено схему кабельної інфраструктури, логіку підключення обладнання та концепцію серверної частини на базі Milestone XProtect із прорахунком ресурсів серверів для запису. У результаті сформовано збалансовану конфігурацію, яка забезпечує повне покриття всіх ризикових зон об'єкта.

Аналітичний розділ дозволив оцінити розроблене рішення у ширшому контексті – порівнюючи різні бренди камер, архітектури побудови системи (централізована, децентралізована, гібридна), принципи формування серверних

ресурсів і вплив рішень на повний життєвий цикл системи. Показано, що сучасні системи відеоспостереження вимагають не лише правильного підбору обладнання, але й розуміння економіки володіння, стабільності аналітики, надійності виробника та прогнозованості роботи в довгостроковій перспективі. Проведений системний аналіз підтвердив, що якість кінцевого рішення визначається не окремим компонентом, а узгодженістю всіх елементів – від камери до серверної архітектури та політики обслуговування.

Узагальнюючи, можна стверджувати, що поставлені у вступі мета та завдання дослідження виконані повністю. Розроблена система відеоспостереження відповідає функціональним потребам об'єкта, є технічно обґрунтованою, економічно доцільною та придатною до подальшого розширення. Проведений аналіз та створений проєкт можуть бути використані як цілісний методичний приклад для впровадження сучасних систем відеоконтролю на об'єктах подібного типу.

Робота демонструє, що комплексний підхід - поєднання теорії, практичного проєктування та аналітичної оцінки - дозволяє створити систему відеоспостереження, яка не лише закриває поточні задачі безпеки, але й забезпечує довгострокову стійкість, керованість і ефективність в умовах реальної експлуатації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. International Electrotechnical Commission IEC 62676–1
<https://webstore.iec.ch/en/publication/25038> (дата звернення: 10.06.2025).
2. International Electrotechnical Commission IEC 62676–2
<https://webstore.iec.ch/en/publication/21817> (дата звернення: 10.06.2025).
3. International Electrotechnical Commission IEC 62676–4
<https://webstore.iec.ch/en/publication/7238> (дата звернення: 10.06.2025).
4. International Electrotechnical Commission IEC 62676–2–2
https://online.budstandart.com/ru/catalog/doc-page.html?id_doc=83148
(дата звернення: 15.06.2025).
5. ISO/IEC 27001 – Wikipedia
https://en.wikipedia.org/wiki/ISO/IEC_27001 (дата звернення: 16.06.2025).
6. WDR Technology
<https://control.ua/blog/cho-takoe-wdr-blc-i-hlc-v-kamerah-videonablyudeniya.html> (дата звернення: 02.07.2025).
7. Shedding Light on Infrared Camera Technology
<https://www.securitymagazine.com/articles/88400-shedding-light-on-infrared-camera-technology> (дата звернення: 05.07.2025).
8. IR technology
https://www.lip-sunglasses.com/eye-protection-understanding-ultraviolet-and-visible-light/?srsltid=AfmBOoo79x_07VHRmxw-WvcY6dE544sQ6eF-zy03bWt7-Qc3APyhzz1A (дата звернення: 10.07.2025).
9. Optimized-IR – Axis
<https://www.axis.com/solutions/optimizedir> (дата звернення: 11.07.2025).
10. Power over Ethernet – LinkedIn
<https://www.linkedin.com/pulse/power-over-ethernet-poe-khaled-ibrahim>
(дата звернення: 14.07.2025).

11. Power over Ethernet – Wikipedia

https://en.wikipedia.org/wiki/Power_over_Ethernet (дата звернення: 21.07.2025).

12. Videocodec – Wikipedia

<https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%B4%D0%B5%D0%BE%D0%BA%D0%BE%D0%B4%D0%B5%D0%BA> (дата звернення: 28.07.2025).

13. H.264/H.265

<https://greenvision.ua/blog/formati-stisnennya-n-264-i-n-265-yak-cze-praczyuye-v-sistemah-videosposterezhennya?srsId=AfmBOooBErmkrYER-SJkDrjqS84dV5WIONdFRsitqaBmwwhJulgoxNCQ> (дата звернення: 01.09.2025).

14. H.265

https://vstarcam.ua/technology/h265/?srsId=AfmBOoqt5ZHR1YPGm_rAtd28yXEO53qt6D9TOk1ezZyp8INGJNNEiTsw (дата звернення: 10.09.2025).

15. MJPEG

<https://www.malbred.com/kodirovanie-video/kodek-mjpeg.html> (дата звернення: 11.09.2025).

16. Protocols in CCTV

<https://anela-tek.com/communication-protocols-in-cctv/> (дата звернення: 14.09.2025).

17. RTSP

<https://www.fs.com/blog/understanding-rtsp-and-rtsp-cameras-a-comprehensive-guide-7256.html> (дата звернення: 15.09.2025).

18. HTTP/HTTPS

<https://supportcommunity.milestonesys.com/s/question/0D53X00006QQAdUSAX/access-http-stream-for-a-specific-camera?language=ru> (дата звернення: 16.09.2025).

19. Onvif

<https://greenvision.ua/blog/chto-takoe-protokol-ONVIF?srsltid=AfmBOoo0Xe2D0Kz-XGYaf0meB3dXgmwEtFpMIuEyVKEFe0Luaqtde0RY>

(дата звернення: 18.09.2025).

20. Milestone XProtect VMS system architecture

https://doc.milestonesys.com/latest/en-US/wp_xpr_aws/appendix_a_milestone_xprotect.htm

(дата звернення:

20.09.2025).

21. XProtect Storage Architecture and Recommendations

https://doc.milestonesys.com/wp/pdf/en-US/XProtectStorageArchitectureAndRecommendations_2023-09.pdf

(дата звернення: 21.09.2025).

22. Milestone XProtect VMS on AWS

https://doc.milestonesys.com/latest/en-US/wp_xpr_aws/introduction.htm

(дата звернення: 22.09.2025).

23. Milestone Interconnect: White Paper

<https://ru.scribd.com/document/402569955/MS400860-CLI-MN-EN-v1-0-0>

(дата звернення: 24.09.2025).

24. VMS Design Guide

https://doc.milestonesys.com/latest/en-US/wp_sysarch/vms_design_guide.htm?tocpath=Whitepapers%7CSystem+Architecture+Guide+for+IT+Professionals%7C_wp_sysarch%7C_9&

(дата звернення: 27.09.2025).

25. Integration with standard IT technology

https://doc.milestonesys.com/latest/en-US/wp_sysarch/integration_with_standard.htm?tocpath=Whitepapers%7CSyst

[em%20Architecture%20Guide%20for%20IT%20Professionals%7C_wp_sysarch%7C_____10](#) (дата звернення: 27.09.2025).

26. Intelligent Network Video Understanding Modern Video Surveillance Systems

<https://www.routledge.com/Intelligent-Network-Video-Understanding-Modern-Video-Surveillance-Systems/Nilsson-Axis/p/book/9781032534718>

(дата звернення: 27.09.2025).

27. Video Analytics for Surveillance and Applications

<https://www.routledge.com/Intelligent-Network-Video-Understanding-Modern-Video-Surveillance-Systems/Nilsson-Axis/p/book/9781032534718>

(дата звернення: 29.09.2025).

28. A review of video surveillance systems

<https://www.sciencedirect.com/science/article/abs/pii/S1047320321000729>

(дата звернення: 29.09.2025).

29. Edge video analytics: A survey on Applications and Systems

<https://arxiv.org/abs/2211.15751> (дата звернення: 29.09.2025).

30. Analytics on the Edge vs. on the Server

<https://www.hanwhavision.com/en/news-center/1020419/>

(дата звернення: 01.10.2025).

31. Vezha Incoresoft Object Detection

https://docs.portal.incoresoft.com/partners_documents/UA%20Object%20Detection.pdf (дата звернення: 12.10.2025).

32. Vezha Incoresoft LPR

https://docs.portal.incoresoft.com/partners_documents/UA%20VEZHA%20LPR.pdf

(дата звернення: 13.10.2025).

33. Axis Site Designer

<https://sitedesigner.axis.com/> (дата звернення: 18.10.2025).

34. ACAP Axis

<https://www.axis.com/products/acap> (дата звернення: 18.10.2025).

35.Axis guide

https://www.anixter.com/content/dam/Suppliers/AxisCommunications/AxisDocuments/bc_techguide_33334_en_0811_lo.pdf (дата звернення: 18.10.2025).

36.BEST 4K PoE Security Camera: \$1100 vs \$110 Motorized Zoom Cameras

<https://www.thesmarthomehookup.com/2022-update-best-4k-poe-security-camera-1100-vs-110-motorized-zoom-cameras> (дата звернення: 18.10.2025).

37.Dahua Technology - Wikipedia

https://en.wikipedia.org/wiki/Dahua_Technology (дата звернення: 18.10.2025).

38.СБУ заблокувала вебкамери, які «засвітили» роботу ППО під час ракетної атаки РФ на Київ 2 січня (відео).

<https://ssu.gov.ua/novyny/sbu-zablokuvala-vebkamery-yaki-zasvityly-robotu-ppo-pid-chas-raketnoi-ataky-rf-na-kyiv-2-sichnia-video> (дата звернення: 18.10.2025).

39.The city of Vicente López has installed over 800 high technology cameras in government buildings, along public roads, in mass transit – as well as in patrol car

<https://www.axis.com/customer-story/public-safety-mobility-monitoring> (дата звернення: 20.10.2025).

40.Axis Support Lifecycle policy

<https://www.axis.com/support/warranty> (дата звернення: 21.10.2025).

<https://www.axis.com/support/product-lifecycle-policy> (дата звернення: 21.10.2025).

41.Мапа взломаних камер Hikvision

<https://ipvm.com/reports/hik-hack-map> (дата звернення: 21.10.2025).

<https://ipvm.com/reports/hik-hack-map> (дата звернення: 21.10.2025).

42.Incoresoft Videoanalytics

<https://incoresoft.com/products/> (дата звернення: 22.10.2025).

43. Hanwha Vision AI Solutions

<https://hanwhavision.eu/technology/ai-solutions/> (дата звернення: 23.10.2025).

44. Incoresoft VEZHA Documentation

<https://docs.incoresoft.com/iv/incoresoft-vezha-documentation-en-688129.html>
(дата звернення: 24.10.2025).

45. Vezha + Milestone block

<https://docs.incoresoft.com/ivms/latest/milestone-block-145818477.html>
(дата звернення: 25.10.2025).