Міністерство освіти і науки України
Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та охоронних систем
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА
ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

ПРОЕКТУВАННЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ СКЛАДСЬКОГО КОМПЛЕКСУ НОВОЇ ПОШТИ ВІДДІЛЕННЯ №1 М. ЛУЦЬКА

DESIGN OF A VIDEO SURVEILLANCE SYSTEM FOR THE WAREHOUSE COMPLEX OF NOVA POSHTA BRANCH NO. 1 IN LUTSK

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

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

Виконав: здобувач вищої освіти
групи ІСТО-41
Романюк Дмитро Степанович

_____
(підпис)

Керівник:
к.т.н., доцент
Терлецький Тарас Володимирович

_____
(підпис)

Кваліфікаційну роботу
допущено до захисту
«_____» червня 2026 р.
Гарант освітньої програми:
к.т.н., доцент
Терлецький Тарас Володимирович

_____
(підпис)

Луцьк – 2026 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Т. Терлецький
«_____» _____ 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Романюка Дмитра Степановича
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Проектування системи відеоспостереження складського комплексу Нової пошти відділення №1 м. Луцька*

Керівник роботи *к.т.н., доцент Терлецький Тарас Володимирович*

затверджені наказом закладу вищої освіти від «16» грудня 2025 року № 529/01-02

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 20.05.2026р.

3. Вихідні дані до роботи: *джерелом розробки є геопідкладка плану комплексу Нової пошти відділення №1 м. Луцька, науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області, різні інтернет-ресурси технічного спрямування, глибина архіву 30 днів.*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
вступ, технічна характеристика та службове призначення об'єкту розроблення, аналіз існуючих аналогів, обґрунтування теми кваліфікаційної роботи бакалавра та постановка задачі на проектування, розробка структурної схеми системи, проектування апаратної складової системи, практична реалізація системи, висновки.

5. Перелік графічного (ілюстративного) матеріалу:
набір слайдів презентації кваліфікаційної роботи

6. Консультанти розділів роботи

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

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

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Обґрунтування теми*	до 10.02.2026 р.	
2.	*Огляд літератури із досліджуваної проблеми*	до 10.03.2026 р.	
3.	*Розділ 1 Аналітичний огляд стану предметної області*	до 25.04.2026 р.	
4.	*Розділ 2 Обґрунтування вибору засобів та методів реалізації*	до 28.04.2026 р.	
5.	*Розділ 3 Практична реалізація*	до 30.04.2026 р.	
6.	*Оформлення пояснювальної записки*	до 05.05.2026 р.	
7.	*Представлення остаточного варіанту кваліфікаційної роботи керівникові*	до 10.05.2026 р.	
8.	*Нормоконтроль*	до 21.05.2026 р.	
9.	*Інструментальна перевірка на академічний плагіат*	до 22.05.2026 р.	
10.	*Здача кваліфікаційної роботи та всіх супровідних документів на кафедру*	до 02.06.2026 р.	

Здобувач вищої освіти _____ Романюк Д. С.
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Терлецький Т. В.
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Романюк Д. С. Проектування системи відеоспостереження складського комплексу Нової пошти відділення №1 м. Луцька. Рукопис.

Кваліфікаційна робота бакалавра ОП «Інформаційні системи та технології охорони і безпеки» спеціальності 126 Інформаційні системи та технології. Луцький національний технічний університет. Луцьк, 2026.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел.

У даній роботі в першому розділі охарактеризовано об’єкт захисту та визначені завдання на проектування системи відеоспостереження. Також проведено аналіз існуючих нормативних вимог до вирішення оперативних завдань відеоспостереження, які висувають до цифрових систем. Здійснено порівняльний аналіз існуючих технологій побудови систем відеоспостереження. Проведено обґрунтування теми кваліфікаційної роботи бакалавра та визначено завдання на проектування.

У другому розділі розроблено концепцію системи відеоспостереження на основі особливостей характерних зон комплексу. Обґрунтовано вибір технології побудови системи та спеціалізованого програмного забезпечення для моделювання системи, визначено базовий перелік обладнання.

Третій розділ присвячений питанням практичної реалізації системи. Створено 3D-модель об’єкту захисту із застосуванням IP Video System Design Tool, на основі якої змодельовано відеонагляд за кожною характерною зоною згідно розробленої концепції та визначено остаточний перелік обладнання. Пояснено підключення та налаштування мережевого обладнання системи.

Ключові слова: система відеоспостереження, оперативна задача, відеокамера, комутатор, відеореєстратор, кабельний журнал, піксель, матриця.

ANNOTATION

Romanyuk D. Design of a video surveillance system for the warehouse complex of Nova Poshta branch No. 1 in Lutsk. Manuscript.

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

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

In this work, the first section describes the object of protection and defines the tasks for designing a video surveillance system. An analysis of existing regulatory requirements for solving operational video surveillance tasks that are put forward to digital systems was also conducted. A comparative analysis of existing technologies for building video surveillance systems was carried out. The topic of the bachelor's qualification work was substantiated and design tasks were defined.

In the second section, the concept of a video surveillance system was developed based on the features of the characteristic zones of the complex. The choice of system construction technology and specialized software for system modeling is justified, and the basic list of equipment is determined.

The third section is devoted to the issues of practical implementation of the system. A 3D model of the protected object is created using the IP Video System Design Tool, based on which video surveillance of each characteristic zone is modeled according to the developed concept and the final list of equipment is determined. The connection and configuration of the system's network equipment is explained.

Keywords: video surveillance system, operational task, video camera, switch, video recorder, cable log, pixel, matrix.

ЗМІСТ

ВСТУП

Сучасна логістична інфраструктура України функціонує в умовах безпрецедентної інтенсивності операцій, жорстких вимог до збереження вантажів та системних безпекових викликів воєнного стану. Для лідера національного ринку експрес-доставки, компанії «Нова пошта», ефективність функціонування складських комплексів та інноваційних сортувальних терміналів безпосередньо залежить від швидкості обробки посилок та рівня захисту активів. Впровадження систем відеоспостереження є необхідністю, що інтегрує функції фізичної безпеки, контролю технологічних процесів, управління претензіями клієнтів та цивільного захисту персоналу.

Впровадження сучасної системи відеоконтролю безпосередньо впливає на фінансові показники компанії через оптимізацію претензійної діяльності. У сучасній практиці великих торговельних та логістичних компаній, таких як Jysk або SAT, врегулювання претензій щодо пошкодження чи втрати майна вимагає надання беззаперечних медіадоказів. Наявність страхового покриття вантажів від пошкоджень, втрат чи затримок мінімізує фінансові ризики, проте потребує детального розслідування кожного випадку для уникнення страхового шахрайства.

Об’єкт дослідження – IP-система відеоспостереження складського комплексу «Нової пошти» відділення №1 м. Луцька.

Предмет дослідження – концепція системи IP-відеоспостереження та топологічні аспекти вирішення оперативних завдань на основі розробленої 3D моделі об’єкту захисту, обладнання й кабельна інфраструктура, підключення та налаштування мережевого обладнання.

Мета кваліфікаційної роботи – проєктування IP-системи відеоспостереження складського комплексу «Нової пошти» відділення №1 м. Луцька для забезпечення повного візуального контролю зон обробки вантажу.

РОЗДІЛ 1
АНАЛІТИЧНИЙ ОГЛЯД СТАНУ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Характеристика об’єкту захисту та встановлення завдань на проектування системи відеоспостереження

Об’єктом проектування є система відеоспостереження, яка повинна забезпечувати візуальний контроль всіх необхідних зон складського комплексу «Нової пошти» відділення №1 м. Луцька. Така інформаційна система повинна стати комплексним інструментом безпеки та аналітики і забезпечувати виконання низки технічних та функціональних завдань, що характерні для подібних об’єктів захисту.

Вантажне відділення №1 «Нової пошти» в Луцьку є ключовим логістичним вузлом міста, що спеціалізується на обробці великовагових відправлень.

Супутниковий знімок території відділення №1 «Нової пошти» в Луцьку подано на рисунку 1.1.

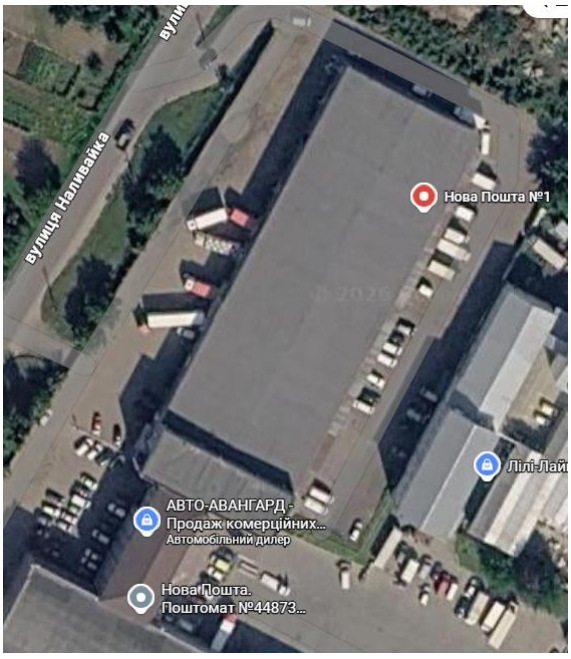

Рисунок 1.1 – Супутниковий знімок території відділення №1 «Нової пошти» в Луцьку

Території відділення №1 «Нової пошти» в Луцьку займає орієнтовну площу 7920м^2, яка утворене периметром 70 м на 112 м (визначено за картами Google Maps). Розмір складського приміщення становить 38 м на 96 м. Висота цього складського приміщення становить 7 м. У свою чергу, офісні приміщення, зони відпочинку персоналу та клієнтська зона займають 10 % від загальної площі цієї будівлі.

Як великий складський комплекс, це відділення має відповідну інфраструктуру: зону завантаження/розвантаження, зону приймання та видачі вантажів, зону зберігання поштових відправлень, зону паркування автотранспорту.

В'їзд на територію комплексу є один і розташований у північній його частині.

Зона завантаження/розвантаження обладнана рампами для фур та зручним під'їздом для великогабаритного транспорту.

Окрім стандартного приймання та видачі, тут доступні послуги пакування (флет-бокси, обрешетування), міжнародні відправлення та зона самообслуговування.

З огляду на специфіку об'єкта захисту, перш ніж проектувати систему відеоспостереження, потрібно вирішити низку питань: які зони логістичного центру потрібно контролювати і за якими критеріями, як і де встановити відеокамери та якими вони мать бути (тип, технічні характеристики), яку технологію для побудови системи використати [1]?

У подібного типу об'єкта захисту потрібно забезпечити повний візуальний контроль зон обробки вантажу.

В зонах завантаження/вивантаження (рампи) необхідна чітка фіксація номерних знаків автотранспорту, стану кузова та процесу переміщення палет, а в зонах зберігання – відсутність «сліпих зон» між стелажами та контроль доступу персоналу до комірок.

Роздільна здатність відеокамер має відповідати виконанню поставленої оперативної задачі стосовно характерної особливості зони спостереження відповідно до існуючих критеріїв світових стандартів [2-7].

Потрібно передбачити можливість використання спеціалізованих функцій покращення зображення для відеокамер, які будуть працювати в умовах різного освітлення (підтримка технологій WDR (Wide Dynamic Range) для компенсації засвітів від відчинених воріт складів у сонячний день та якісна ІЧ-підсвітка для роботи вночі, або BLC (Backlight Compensation) та HLC (Highlight Compensation) тощо).

Щоб забезпечити глибину архіву у 30 днів, необхідно спочатку встановити загальний бітрейт від усіх відеокамер, після чого визначити тип носіїв інформації та необхідну їх кількість.

1.2 Аналіз існуючих вимог до вирішення оперативних завдань відеоспостереження

Ступінь деталізації зображення є одним із вирішальних параметрів при виборі камери CCTV (Closed Circuit Television – телебачення замкнутого контуру). Цей показник, який відображає чіткість об’єкта, безпосередньо залежить від оперативних завдань, які має вирішувати система. Саме потреба формалізувати ці завдання призвела до появи понять «оперативна задача» та «оперативні стандарти». Дана концепція, сформульована у Великій Британії наприкінкінці 80-х років минулого століття, лягла в основу одного з перших світових стандартів безпеки – BS 8418:1987. Ці стандарти носять рекомендаційний характер.

Завдяки покращенню роздільної здатності аналогового CCTV, стандарт BS 8418:1987 було замінено на BS 8418:2009. Нова редакція стандарту значно розширила перелік оперативних завдань, включивши моніторинг, детектування, огляд, розпізнання, ідентифікацію та інспектування.

Завдання моніторингу в цій класифікації є базовим і передбачає лише оцінку загальної ситуації на об’єкті (наприклад, ситуація біля входу чи у вестибюлі). Він дозволяє виявити загальні зміни (наприклад, скупчення людей), але не надає деталізації, необхідної для розрізнення обличь та номерів автомобілів.

Завдання детектування передбачає гарантоване виявлення суб’єктів чи об’єктів спостереження в контрольованій зоні. Спостереження полягає у визначенні грубих характерних особливостей об’єкта чи суб’єкта спостереження з подальшим спостереженням за їх переміщенням з метою виявлення несанкціонованих або потенційно небезпечних дій.

Мета завдання розпізнавання – визначення приналежності суб’єкта або об’єкта спостереження чи їх елементів до певної групи об’єктів спостереження.

Вирішення завдання ідентифікації потребує можливість розрізняти досить дрібні, характерні деталі, наприклад особи людини, що входить на об’єкт, або номерний знак автотранспорту. Таким чином, ідентифікація – це процес впізнання суб’єкта або об’єкта по властивому йому або наданим йому ідентифікаційним ознакам.

До недана реалізацію поставлених оперативних завдань перед CCTV описували відповідні світові стандарти (табл. 1.1).

Таблиця 1.1 – Критерії вирішення оперативних завдань CCTV світових стандартів

№	Вид активності	Мінімально необхідна щільність пікселів (Пікс/м) відповідно AS 4806	Мінімально необхідна щільність пікселів (Пікс/м) відповідно EN IEC 62676	Мінімально необхідна щільність пікселів (Пікс/м) відповідно EN 50132
1	Моніторинг	17	15	12
2	Детектування	35	30	25
3	Спостереження	70	60	62
4	Розпізнавання	175	125	125
5	Ідентифікація	350	250	250
6	Інспектування	1000	1000	1000

Щільність пікселів (часто виражається в пікселях на метр) є фундаментальною – вона визначає, скільки деталей можна розрізнити, а отже, що оператори можуть надійно робити із зображеннями (виявляти, спостерігати, перевіряти, ідентифікувати, ретельно досліджувати).

Сучасний стан технологій CCTV характеризується переходом від пасивного спостереження до активного аналітичного моніторингу, що вимагає переосмислення методологічних підходів до визначення технічних вимог. Протягом останніх десятиліть базовим орієнтиром для галузі слугував європейський стандарт EN 50132-7, який було трансформовано у міжнародний стандарт IEC 62676-5 та впроваджено в Україні як ДСТУ EN IEC 62676-5: 2019 [3]. У 2014 році цей документ закріпив класичну модель DORI (Detection – виявлення, Observation – спостереження, Recognition – розпізнавання, Identification – ідентифікація), яка базувалася на візуальному сприйнятті оператором об’єктів на моніторах застарілих аналогових стандартів. Однак стрімкий розвиток цифрових сенсорів, алгоритмів стиснення відео та штучного інтелекту зробив попередні критерії недостатніми для вирішення сучасних оперативних завдань.

Опублікування у жовтні 2025 року оновленого стандарту IEC 62676-4: 2025 [5] ознаменувало нову еру у стандартизації – перехід від суб’єктивного оцінювання «якості сцени» до об’єктивного моделювання візуальної продуктивності системи. Нова модель, відома під абревіатурою OODPCVS (Overview – огляд, Outline – структурування, Discern – розрізнення, Perceive – сприйняття, Characterize – характеризування, Validate – перевірка, Scrutinize – ретельне дослідження), розширює кількість рівнів деталізації з чотирьох до семи, що дозволяє більш гнучко підходити до проектування систем у залежності від конкретних ризиків та завдань. Ця еволюція відображає розуміння того, що сучасні системи відеоспостереження працюють не лише для людського ока, а й для машинного зору, де точність алгоритмів прямо залежить від щільності пікселів та рівня цифрового шуму.

Перехід до стандарту 2025 року зумовлений також необхідністю врахування артефактів цифрової компресії та впливу низького освітлення на сучасні IP-камери. Якщо раніше ідентифікація вважалася можливою при 250 пікселях на метр [4, 7], то реальна практика показала, що в умовах недостатнього світла або при використанні кодеків H.265 з високим ступенем стиснення такої щільності недостатньо для позитивної ідентифікації. Таким чином, оновлений стандарт підвищує планку вимог, роблячи системи більш надійними для аналізу та автоматизованого розпізнавання обличь.

Розуміння різниці між моделями 2014 та 2025 років є важливим для проектувальників та замовників. Стара модель DORI була занадто дискретною, що призводило до переплати за надлишкову якість або, навпаки, до неможливості виконати завдання через недостатню деталізацію. Нова модель OODPCVS пропонує більш детальний градієнт, що дозволяє оптимізувати витрати на інфраструктуру [8, 9].

Порівняльна характеристика критеріїв 2014 та 2025 років подано в таблиці 1.2.

Таблиця 1.2 – Порівняльна характеристика критеріїв вирішення оперативних задач CCTV за стандартами 2014 та 2025 років

Рівень деталізації (2014)	Рівень деталізації (2025)	Щільність пікселів (px/m)	Оперативне призначення та можливості
Detection	Overview	20	Виявлення наявності об’єкта та руху на великих відстанях
-	Outline	40	Визначення контурів та напрямку руху об’єкта
Observation	Discern	80	Розрізнення цілей, ідентифікація рухів людей, тварин або авто
Recognition	Perceive	125	Сприйняття об’єктів без детальних ознак статі чи одягу
Identification	Characterize	250	Визначення типу особи, ходи, поведінки та категорій авто
-	Validate	500	Верифікація відомих осіб, розпізнавання номерних знаків
Inspection	Scrutinize	1500	Максимальна деталізація для встановлення особи (рівень фото на паспорт), розпізнати транспортні засоби за моделлю та роком випуску, а також прочитати реєстраційний номер транспортного засобу.

Застосування рівнів Validate та Scrutinize замість колишньої «Ідентифікації» дозволяє розділити завдання на ручну перевірку оператором (Validate) та безумовне форензичне підтвердження особи (Scrutinize). Рівень Scrutinize базується на стандартах якості для біометричних фотографій (ISO/IEC 19794-5), що забезпечує юридичну вагомість отриманих доказів у кримінальних провадженнях.

Після внесення змін до стандарту проектувальники мають свободу адаптувати свої проектні рішення до IEC 62676-4: 2025, коли це можливо, або підтримувати проект технічного обслуговування в актуальному стані відповідно до IEC 62676-4: 2014.

1.3 Аналіз технологій побудови систем відеоспостереження

Технологічна основа будь-якої системи відеоспостереження базується на можливостях оптико-електронного перетворення. У 2025 році спостерігається остаточне завершення епохи CCD-сенсорів. Незважаючи на те, що історично CCD переважали CMOS за світлочутливістю та рівнем шуму, сучасні досягнення в напівпровідниковій індустрії змінили баланс сил. Компанія Sony оголосила про повне припинення виробництва лінійок CCD до 2025 року, що знаменує перехід до CMOS як безальтернативного стандарту [10].

Сучасна архітектура CCTV зазнала фундаментальних трансформацій, перетворившись із простих засобів фіксації зображення на складні інформаційні системи. Вибір архітектури побудови системи відеоспостереження визначає не лише її поточну функціональність, але й довгострокову життєздатність, масштабованість та рівень захищеності активів. В основі будь-якого архітектурного порівняння лежить протистояння двох рішень: аналогової передачі сигналу в замкнутому циклі та цифрової мережевої передачі на основі інтернет-протоколів – IP-системи CCTV.

Фундаментальна відмінність між архітектурами полягає у фізичному способі формування та транспортування відеоданих. Традиційна архітектура

CCTV базується на аналоговому сигналі, який передається від камери до цифрового відеореєстратора (DVR) за допомогою коаксіального кабелю (рис. 1.2). У цій моделі камера виконує функцію пасивного датчика, який захоплює світловий потік і перетворює його на електричний сигнал, тоді як вся інтелектуальна обробка, включаючи оцифрування, стиснення та запис, відбувається централізовано на DVR.

Рисунок 1.2 – Архітектура аналогової CCTV

На противагу цьому, IP-архітектура базується на концепції камери як автономного комп’ютера, здатного самостійно оцифровувати зображення, застосовувати алгоритми стиснення та передавати дані у вигляді пакетів через мережу Ethernet або Wi-Fi. Це дозволяє будувати децентралізовані системи, де потоки даних можуть бути спрямовані на мережеві відеореєстратори (NVR), хмарні сховища або локальні накопичувачі без необхідності прямого фізичного з’єднання кожної камери з центральним пристроєм.

Розуміння цих відмінностей дозволяє глибше проаналізувати якість зображення. В аналогових системах зображення формується як прямокутник з пікселів, де при збільшенні масштабу втрачається деталізація через растрову природу сигналу та втрати при передачі по кабелю. IP-камери забезпечують набагато вищу щільність пікселів і використовують прогресивну розгортку, що важливо для ідентифікації обличь та державних номерних знаків транспортних засобів. Наприклад, перехід від 2 Мп до 5 Мп камери забезпечує приріст деталізації на 35-40%, що суттєво розширює операційні можливості системи.

Рисунок 1.3 – Архітектура цифрової CCTV

Порівняльна характеристика цих двох архітектур подано в таблиці 1.3.

Таблиця 1.3 – Порівняльна характеристика аналогової та цифрової CCTV

Критерій	Аналогова архітектура	Цифрова архітектура
Природа сигналу	Аналоговий електричний сигнал	Цифрові пакети даних (TCP/IP)
Фізичне середовище	Коаксіальний кабель (RG59/RG6)	Вита пара (Cat5e/6), Оптика, Wi-Fi
Максимальна роздільна здатність	Обмежена (зазвичай до 5-8 Мп в TVI/CVI)	Практично необмежена (4K, 8K, 12Мп+)
Інтелектуальна обробка	Централізована (на боці DVR)	Децентралізована (на боці камери/Edge)
Дистанційне керування	Обмежене або через окремий кабель	Пряме керування через мережевий інтерфейс

Існують також і гібридні CCTV, які виступають технологічним мостом між перевіреною надійністю аналогових стандартів та потенціалом цифрових мережевих рішень. Архітектура таких систем базується на здатності об’єднувати різнорідні методи передачі даних у єдину керовану структуру, що дозволяє організаціям максимізувати ефективність існуючої інфраструктури, одночасно впроваджуючи передові алгоритми аналізу та високу роздільну здатність зображення.

Гібридна архітектура відеоспостереження визначається як система, що інтегрує аналогові камери (CVBS, AHD, HD-TVI, HD-CVI) та IP-камери в межах єдиної мережі управління. Центральним елементом такої системи є гібридний відеореєстратор (HVR – Hybrid Video Recorder), який виконує роль

«двомовного транслятора», здатного одночасно обробляти сирі електричні сигнали з коаксіальних ліній та інкапсульовані цифрові пакети з мережі Ethernet.

Рисунок 1.4 – Архітектура гібридної CCTV

На відміну від систем попереднього покоління, де вибір стояв між замкнутими аналоговими контурами (DVR) та відкритими мережевими системами (NVR), гібридна модель пропонує адаптивність. Основна відмінність між NVR та DVR полягає в локалізації обробки відеоданих: системи DVR обробляють відео безпосередньо на реєстраторі, тоді як системи NVR отримують уже закодовані та оброблені дані від IP-камер. Гібридний реєстратор HVR поєднує обидва підходи, що вимагає специфічної внутрішньої архітектури, здатної динамічно розподіляти обчислювальні ресурси між апаратними енкодерами для аналогових входів та програмними стеками для обробки мережевих потоків.

Економічна доцільність такої гібридної архітектури підтверджується тим, що вона дозволяє уникнути повної заміни кабельної інфраструктури під час модернізації. Аналіз впровадження показує, що для типової 16-канальної системи перехід на повністю IP-рішення може коштувати значно дорожче через необхідність прокладання нових ліній зв’язку та закупівлю складного мережевого обладнання, тоді як гібридний підхід дозволяє зберегти до 60-70% існуючих капіталовкладень [11].

Архітектура побудови CCTV безпосередньо корелює з фізичною топологією об’єкта. Аналогові системи використовують топологію «зірка» або «home-run», де кожен пристрій має власну кабельну лінію до центру керування. Це створює громіздку інфраструктуру, особливо у великих будівлях, де сотні кабелів повинні сходитися в одній серверній кімнаті. Крім того, аналогові камери вимагають окремих ліній живлення або використання комбінованого кабелю, що додає складності монтажу.

IP-системи пропонують гнучку мережеву топологію. Завдяки використанню мережевих комутаторів, камери можуть бути об’єднані в локальні кластери, які потім підключаються до центрального вузла одним магістральним каналом. Ключовою перевагою тут є технологія Power over Ethernet (PoE), яка дозволяє передавати дані та живлення по одному кабелю Cat5e/6. Це знижує витрати на кабельну продукцію та спрощує інтеграцію з існуючою IT-інфраструктурою підприємства.

Сучасна мережева архітектура часто передбачає використання оптоволоконних ліній для з’єднання віддалених сегментів системи, оскільки вита пара обмежена відстанню у 100 метрів без додаткового посилення. Вибір між дротовим та бездротовим підключенням також є частиною архітектурного рішення: дротові системи на базі PoE вважаються найнадійнішими для великих об’єктів, тоді як бездротові Wi-Fi рішення підходять для малих просторів або тимчасових інсталяцій, де прокладання кабелю є неможливим.

У свою чергу, архітектура гібридних систем часто базується на поєднанні коаксіальних ліній та витої пари. Коаксіальний кабель забезпечує надійну передачу аналогових сигналів завдяки екрануванню, що захищає від перехресних завад. Проте для передачі IP-даних через існуючий коаксіал існують спеціалізовані конвертери, які використовують технологію ePoE, дозволяючи передавати цифровий сигнал та живлення на відстань до 1 км.

Архітектурний підхід до управління доступом та даними визначає стійкість системи до відмов та зручність її адміністрування. Централізована модель консолідує всю логіку прийняття рішень та зберігання даних в одній

системі. Це спрощує моніторинг, аудит та глобальне впровадження політик безпеки. Однак така архітектура має суттєвий недолік – наявність єдиної точки відмови. Якщо центральний сервер або база даних виходять з ладу, вся система стає непрацездатною.

Децентралізована архітектура розподіляє політики та процеси прийняття рішень між окремими сутностями системи (наприклад, інтелектуальними камерами або прикордонними шлюзами). Це усуває вузькі місця в мережі та забезпечує безперервність роботи навіть у разі часткового виходу інфраструктури з ладу. Децентралізовані моделі демонструють кращу масштабованість, оскільки додавання нових пристроїв автоматично збільшує загальну обчислювальну потужність системи.

В контексті зберігання відеоданих існує три основні архітектурні схеми: централізоване, Edge-зберігання та гібридне

При централізованому зберіганні відео з усіх камер передається на центральні сервери запису або великі дискові масиви. Це забезпечує зручність пошуку в єдиному архіві та можливість використання RAID-масивів для захисту від збоїв дисків.

Edge-зберігання передбачає запис безпосередньо на вбудовані накопичувачі камер (SD-карти). Це дозволяє системі функціонувати навіть під час повного розриву мережевого з’єднання з центром.

У свою чергу, гібридне зберігання комбінує обидва підходи, де Edge-запис виступає як резервний механізм, який автоматично синхронізується з центром після відновлення зв’язку.

Вибір між локальною та хмарною архітектурою залежить від можливостей та бажання замовника. Локальна архітектура передбачає повне володіння та управління апаратним забезпеченням, серверами та архівом на боці замовника. Це забезпечує максимальний контроль над даними, низьку затримку при перегляді та відсутність залежності від стабільності інтернет-каналу для виконання основних функцій запису.

Хмарна архітектура переносить функцію зберігання та управління на віддалені сервери провайдера. Це усуває потребу у придбанні та обслуговуванні власних серверів, забезпечує безшовний віддалений доступ та автоматичне оновлення програмного забезпечення. Однак даний підхід накладає суворі вимоги до смуги пропускання інтернету, оскільки передача відео високої роздільної здатності в режимі 24/7 споживає значні ресурси мережі.

Гібридна архітектура в цьому контексті стає «золотою серединою», дозволяючи зберігати критично важливі та чутливі дані локально (для дотримання вимог регуляторів), одночасно використовуючи хмару для масштабування архіву, аналітики або зручного доступу для віддалених користувачів.

У свою чергу, ефективність передачі та зберігання відеоданих кожної з наведених архітектури побудови CCTV залежить від використовуваних методів стиснення. Нестиснене відео стандарту 1080p при 30 кадрах на секунду потребує каналу близько 1.49 Гбіт/с, що є недоступним для більшості комерційних мереж. Архітектура CCTV повинна враховувати баланс між якістю зображення та пропускною здатністю.

Стандарт стиснення H.264 довгий час залишався домінуючим, забезпечуючи прийнятну якість при помірному бітрейті. Проте перехід до роздільної здатності 4K та 8K вимагав більш ефективних рішень, якими став стандарт стиснення H.265. Кодек H.265 використовує складніші алгоритми прогнозування руху та більші блоки дерева кодування, що дозволяє знизити вимоги до смуги пропускання на 40-50% порівняно з H.264 при збереженні аналогічної якості.

Пропрієтарні розширення, такі як H.265+ (від Hikvision) або Smart H.265+ (від Dahua), ще більше оптимізують цей процес шляхом аналізу сцени. Ці алгоритми ідентифікують статичний фон та рухомі об’єкти, виділяючи більше бітів для кодування руху та мінімізуючи витрати на незмінні ділянки кадру. У

сценаріях з низькою активністю (наприклад, порожні коридори вночі) H.265+ може забезпечити економію до 80% бітрейту.

Таким чином, використання ефективних кодеків безпосередньо впливає на архітектуру сховища: зменшення бітрейту вдвічі дозволяє або вдвічі збільшити глибину архіву на тих самих дисках, або вдвічі скоротити кількість необхідних накопичувачів, що суттєво знижує вартість володіння.

1.4 Обґрунтування теми кваліфікаційної роботи бакалавра та постановка задачі на проектування

Розробка системи відеоспостереження для складського комплексу «Нової пошти» відділення №1 м. Луцька дозволить отримати необхідну проекту документацію на потенційне впровадження цієї системи до наявної IT-інфраструктури об’єкта та стане комплексним інструментом безпеки та аналітики і забезпечить виконання низки технічних та функціональних завдань:

– візуальний контроль за технологічними процесами згідно програми графіку запису;

– запобігання та мінімізація ризиків пошкодження вантажів та їх крадіжки;

– отримання документальних доказів у разі розслідування інцидентів;

– підвищення рівня безпеки об’єкта;

– своєчасне інформування операторів та охорони про виникнення позаштатних ситуацій.

Проектована система повинна відповідати наступним вимогам:

– вирішувати поставлені оперативні задачі стосовно визначених характерних зон;

– бути енергоефективною та стійкою до зникнення напруги в загальній електромережі;

– фіксувати відеодані протягом 30 календарних днів.

Для вирішення поставлених завдань необхідно:

– розробити концепцію системи відеоспостереження;

– визначити технологію реалізації системи та встановити перелік необхідного обладнання;

– створити 3D-модель об’єкту захисту у спеціалізованому програмному забезпеченні;

– обрати необхідне обладнання та змоделювати роботу системи відеоспостереження;

– здійснити аналіз сформованих моделей на відповідність поставленим оперативним задачам;

– розрахувати загальний бітрейт з камер і забезпечити 30 денну глибину архіву;

– скласти кабельний журнал і встановити потреби в кабелі.

РОЗДІЛ 2
ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ ТА МЕТОДІВ РЕАЛІЗАЦІЇ

2.1 Розробка концепції системи відеоспостереження

Процес цифрової трансформації логістичного сектору в Україні вимагає переходу від традиційних методів забезпечення безпеки до створення багатофункціональних екосистем, де відеодані стають ключовим активом для прийняття управлінських рішень. Вантажне відділення №1 міста Луцьк, що розташоване за адресою вулиця Карбишева, 1 (див. рис. 1.1), є стратегічно важливим вузлом, здатним обробляти відправлення вагою до 1100 кг та палетовані вантажі. Географічне розміщення об’єкта захисту в межах потужного промислово-ділового кластеру, поруч із бізнес-центром «МЕДІА» та культурно-розважальним центром «Адреналін-Сіті», накладає особливі вимоги до зовнішнього моніторингу та управління транспортними потоками на під’їзних шляхах. Створення сучасної системи відеоспостереження для такого об’єкта передбачає не просто фіксацію подій, а глибоку інтеграцію з внутрішніми інформаційними системами компанії для забезпечення тотальної прозорості кожного етапу руху вантажу.

Логістичний термінал такого типу, як відділення №1 у Луцьку, виконує комплекс функцій: від вивантаження та приймання великовагових відправлень до сортування, групування та подальшої відправки за міжобласними напрямками. Враховуючи, що термінали за своєю природою є високотехнологічними вузлами з інтенсивним рухом персоналу та техніки, система відеоспостереження повинна вирішувати питання не лише фізичної безпеки, а й оптимізації операційних витрат.

Специфіка вантажного відділення №1 полягає в обслуговуванні як роздрібних клієнтів, так і великих бізнес-партнерів, що вимагає розмежування зон доступу та специфічного контролю за обробкою палет.

Беручи до уваги технічні та функціональні завдання системи CCTV, які висвітлено в п. 1.4 даної роботи, необхідно окреслити типи оперативних задач,

що відповідають конкретному процесу, та відповідні критерії їх виконання у відповідності до ДСТУ EN IEC 62676-5: 2019 [3] (див. табл. 1.1).

Перший рубіж, який має контролювати система CCTV, – периметр складського комплексу, який утворено глухим парканом з бетонних плит висотою 2500 мм з одним в'їздом у північній його частині. Згідно [3] для спостереження за периметром має виконуватися оперативне завдання «Детектування» – гарантоване виявлення суб'єктів чи об'єктів спостереження в контрольованій зоні. Для виконання такого оперативного завдання необхідно забезпечити щільність пікселів в районі 30 пікс/м. Встановлювати відеокамери доцільно уздовж огорожі для контролю прилеглої території та власної зони об'єкта за схемою «один за одним» (рис. 2.1). Кожна попередня камера буде контролювати «мертву зону» наступної, гарантуючи надійність всієї системи. Крок встановлення камер будемо обирати з міркувань розв'язання задачі виявлення вторгнення в область для конкретної ділянки периметра.

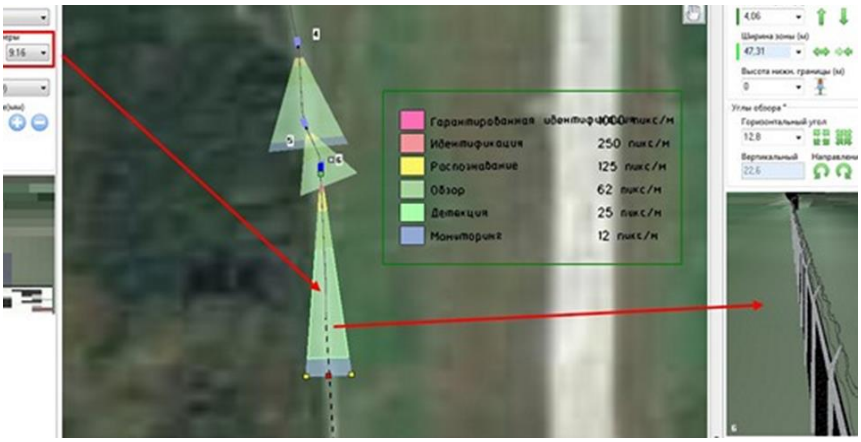

Рисунок 2.1 – Схема встановлення відеокамер «один за одним»

На прямолінійних ділянках рекомендовано обирати відеокамери з довгофокусними об'єктивами 12-16 мм, збільшуючи тим самим зону впевненого виявлення порушника [12]. Найбільш ефективний в плані збільшення кроку встановлення відеокамер при схемі «один за одним» є формат 9:16 (т. зв. «коридорний» формат) з роздільною здатністю до 2 Мп [1].

Для ефективного контролю та розслідування можливих інцидентів необхідно також контролювати номера всього автотранспорту, які в’їжджають на територію комплексу, та людей. У цьому випадку контроль в’їзду і входу на територію розподіляється на оперативні задачі «ідентифікацію/фіксацію» автомобільних номерів, та «ідентифікацію/верифікацію» людей, що входять на територію. Така оперативна задача, згідно відповідних вимог [3], виконується при 250 пікс/м в зоні сцени кадру.

Реалізація вище згаданого завдання, стосовно нашого випадку, можлива однією відеокамерою з довгофокусним об’єктивом і формфактором матриці 9:16, яка має бути встановлена не надто високо, але подалі від в’їзду [1]. Окрім щільності пікселів, що припадають на номер важливі ще два параметри – кут нахилу камери, який повинен бути не більше 30° у вертикальній площині, і не більше 20° в горизонтальній (рис. 2.2).

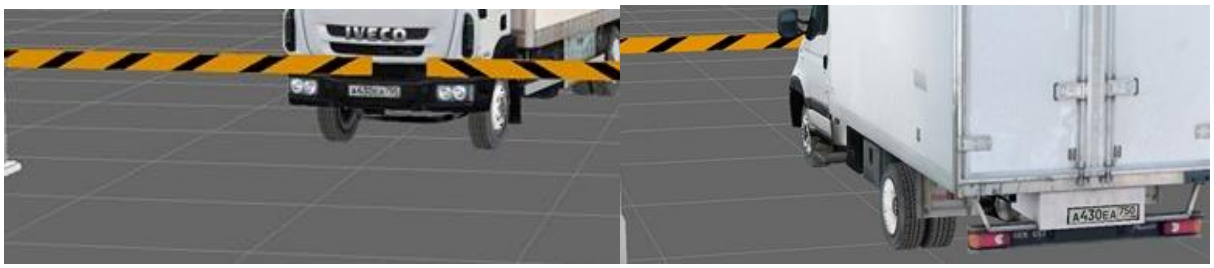

Рисунок 2.2 – Приклад картинки з відеокамери на в’їзді до території при кутах нахилу камери не більше 30° у вертикальній площині, і не більше 20° в горизонтальній

У свою чергу, спостереження за зоною паркування спрощується, оскільки не потрібно ідентифікувати номери автотранспорту і суб’єктів – ця задача вже виконана на в’їзді. Для паркування достатньо вирішити оперативне завдання розпізнавання. Це пояснюється тим, що за непрямими прикметами, часу появи в кадрі вже можна звірити об’єкт з тим, який був ідентифікований на в’їзді до території комплексу.

Відеоспостереження за автотранспортом в зоні паркування повинно забезпечувати 125 пікселів на метр [3] для виконання оперативного завдання

«розпізнавання» з рекомендованим формфактором матриці відеокамери приблизно 1/3" і короткофокусним фіксованим об’єктивом [1].

В зоні розвантаження вантажу на рампі «… потрібно фіксувати час подачі авто, дії співробітників, події при розвантаженні, а також відстежувати переміщення вантажів з машин на склад… [1]» (рис. 2.3).

Рисунок 2.3 – Приклад фіксації зони розвантаження на рампі

Для вирішення оперативного завдання «спостереження» в зоні розвантаження можна використати наступні типи камер: короткофокусні панорамні або FishEye камери, встановлені під стелею (рис. 2.4). Забезпечення даного завдання можливе при щільності пікселів 60 Пікс/м [3] в кадрі сцени.

Завданням CCTV на складі є «… контроль переміщення товарів і контроль дотримання персоналом регламентів компанії… [1]». Основна проблема при плануванні такої системи на складі – висотні стелажі, які утворюють багато рядів з проїздом поміж ними погружчиків. А у нашому випадку це висота до 7 метрів. Можливим рішенням даного завдання є застосування панорамних або FishEye камер на перетині стелажів. При цьому картинка достатня для оперативної задачі «спостереження» за переміщенням співробітників, техніки і вантажів. Таким чином, необхідне забезпечення картинки не нижче 60 Пікс/м в кадрі сцени.

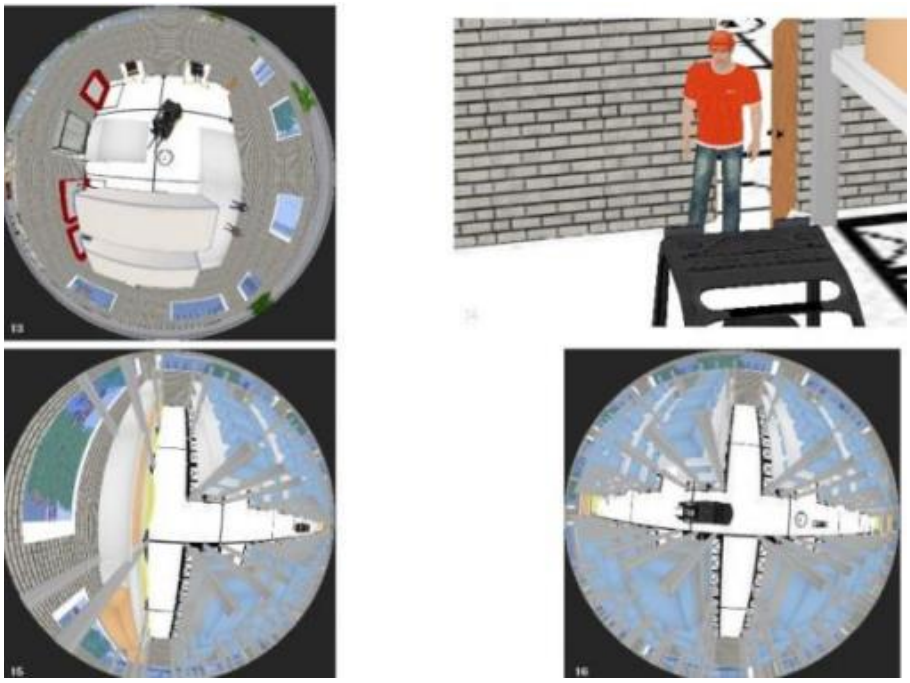

Рисунок 2.4 – Приклад зображення з FishEye камер в зоні переміщення вантажів та на перетині стелажів

В якості альтернативного варіанту можна застосувати в проміжках між рядами стелажів пару довгофокусних камер з «коридорним» форматом матриці 9:16, зони огляду яких перекривають «мертві зони» один одного.

Таким чином, для забезпечення безпеки та створення активу для прийняття управлінських рішень в зонах складського комплексу «Нової пошти» відділення №1 м. Луцька необхідно забезпечити виконання оперативних завдань, подано в таблиці 2.1.

Таблиця 2.1 – Оперативні завдання на проектування CCTV

Зона спостереження	Тип оперативної задачі	Критерії	Характеристики обладнання
Периметр	Детектування	30 пікс/м	Відеокамери з довгофокусними об’єктивами 12-16 мм, формат матриці 9:16
В’їзд на територію комплексу	Ідентифікація	250 пікс/м	Матриця 9:16, короткофокусний фіксований об’єктив
Паркування	Розпізнавання	125 пікс/м	Матриця приблизно 1/3", короткофокусний фіксований об’єктив
Розвантаження	Спостереження	60 пікс/м	Короткофокусні панорамні або FishEye камери
Стелажів	Спостереження	60 пікс/м	Короткофокусні панорамні або FishEye камери чи довгофокусні камери з форматом матриці 9:16

Встановлені оперативні задачі і критерії їх вирішення стосовно конкретних зон складського комплексу «Нової пошти» відділення №1 м. Луцька складають основу концепції на проектування системи CCTV.

2.2 Обґрунтування вибору технології побудови системи та основного обладнання

Аналіз існуючих технологій побудови CCTV, проведений у п. 1.3 даної роботи, вказав на доцільність вибору архітектури цифрової CCTV (IP-відеоспостереження), оскільки він дозволяє реалізувати бізнес-аналітику, автоматизувати контроль за технологічним процесом та забезпечити потрібну роздільну здатність для вирішення необхідних оперативних завдань.

Політика конфіденційності та безпеки «Нової пошти» [13] прямо вказує на використання сучасних технологій для захисту життя, здоровёя та життєво важливих інтересів, включаючи біометричну ідентифікацію обличь. Це вимагає впровадження обладнання з підтримкою алгоритмів глибокого навчання (Deep Learning), які здатні мінімізувати вплив людського фактора та забезпечити цілодобовий моніторинг без втрати концентрації. Впровадження цифрової системи дозволяє не лише фіксувати правопорушення, але й оптимізувати внутрішні процеси складу, такі як швидкість розвантаження, дотримання правил охорони праці та ефективність використання складських площ.

Цифрова архітектура відеоспостереження базується на передачі даних у вигляді пакетів через стандартні мережеві протоколи, що докорінно відрізняється від аналогової передачі електричного сигналу по коаксіальному кабелю. Основною перевагою IP-систем є можливість обробки сигналу безпосередньо в камері, що перетворює її на автономний інтелектуальний пристрій. Для логістичного центру в Луцьку це означає можливість розпізнавання номерів автомобілів, зчитування штрих-кодів з посилок та детекцію аномальної поведінки без необхідності постійної участі оператора.

Аналогові технології, навіть у сучасних форматах HD-TVI або AHD, мають обмежену масштабованість та чутливі до електромагнітних завад, яких багато на сучасному складі через роботу електротранспорту. IP-відеоспостереження використовує цифрові протоколи передачі, які забезпечують потрібну чіткість зображення незалежно від відстані передачі (при використанні оптичних ліній зв'язку або повторювачів). Гнучкість управління правами доступу та можливість віддаленого перегляду з будь-якої точки планети через захищені канали VPN роблять IP-системи стандартом для територіально розподілених компаній, таких як «Нова пошта».

Хоча вартість окремої IP-камери може бути вищою за аналогову, загальна вартість проекту часто виявляється нижчою для великих об'єктів. Це пояснюється використанням наявної IT-інфраструктури, економією на кабельних лініях завдяки PoE та меншою кількістю необхідних камер через ширші кути огляду та вищу роздільну здатність цифрових пристроїв. Крім того, IP-реєстратори (NVR) часто пропонують кращу щільність зберігання даних та гнучкіші механізми резервування, що життєво важливо для забезпечення 30-денного архіву, встановленого внутрішніми регламентами компанії.

При проектуванні системи для відділення №1 м. Луцьк необхідно враховувати стандарти TAPA FSR (Facility Security Requirements), які розроблені Асоціацією захисту вантажів, що перевозяться. Ці вимоги є світовим еталоном для логістичних центрів і забезпечують мінімізацію ризиків втрати вантажів. TAPA FSR передбачає три рівні сертифікації (Level 1, 2, 3) [14, 15], де кожен рівень визначає специфічні вимоги до покриття відеоспостереженням та освітлення.

Згідно зі стандартами TAPA, відеоспостереження повинно забезпечувати безперервний контроль над критичними зонами:

– периметр та точки в'їзду/виїзду: камери мають фіксувати номерні знаки автомобілів та обличчя водіїв у будь-який час доби;

– зони вантажних рамп: кожна рампа повинна перебувати під наглядом камер, що дозволяють фіксувати процес передачі вантажу та цілісність пломб.

– сортувальні та складські площі: необхідно виключити «сліпі зони» у місцях накопичення та обробки вантажів.

Проект для Луцького терміналу має бути орієнтований на відповідність Level 2 TAPA FSR, що передбачає обов’язкове використання цифрових систем з можливістю швидкого пошуку в архіві та інтеграцією з системами тривожної сигналізації. Це також узгоджується з дорожньою картою TAPA 2026, яка підвищує вимоги до кібербезпеки систем відеоспостереження та якості нічної зйомки.

На зовнішньому периметрі та в’їзді на територію, враховуючи розташування в промисловій зоні Луцька, камери повинні мати високий ступінь захисту від вологи та пилу (IP67) та бути вандалозахищеними (IK10).

На рампах відбувається інтенсивний процес розвантаження та завантаження фур. Тут необхідно фіксувати не лише факт прибуття машини, а й стан вантажу, маніпуляції персоналу та дотримання техніки безпеки. Застосування спеціалізованих док-камер з широким динамічним діапазоном (WDR 120-140 дБ) дозволить уникнути засвітів від неба на фоні темного кузова автомобіля, забезпечуючи чітке зображення процесу всередині вантажного відсіку.

У зоні обслуговування клієнтів фокус зміщується на фіксацію обличь та запис звуку для вирішення спірних ситуацій. Компактні купольні камери з вбудованими мікрофонами та можливістю двостороннього аудіозв’язку є оптимальним рішенням для робочих місць операторів.

Для забезпечення стабільної роботи системи на такому великому об’єкті, як Луцький термінал, необхідно виконати точні розрахунки мережевої пропускної здатності, об’єму зберігання даних та енергоспоживання.

Згідно з регламентом, дані повинні зберігатися 30 календарних днів. Для оптимізації витрат на жорсткі диски без втрати якості зображення планується використати інтелектуальний кодек H.265+, який зменшує об’єм даних на 75% порівняно з H.264.

Математична модель розрахунку необхідної ємності базується на формулі:

$$V = \frac{n \times R \times T}{8 \times 1024 \times 1024}, \tag{2.1}$$

де n – кількість камер; R – середній бітрейт однієї камери (біт/с); T – час зберігання в секундах.

Використання PoE технології дозволить передавати дані та живлення по одному кабелю UTP Cat 5e/6, що важливо для великих складів. Загальний бюджет потужності PoE-комутаторів повинен розраховуватися з урахуванням пікового споживання камер. Ці дані будуть встановлені на основі обраного обладнання в процесі проектування системи.

Для захисту від перебоїв в електропостачанні передбачено встановлення джерела безперебійного живлення (UPS). Розрахунок ємності акумуляторів базується на необхідності підтримки роботи системи протягом мінімум 30 хвилин для коректного завершення запису або переходу на резервний генератор.

Для реалізації проекту буде обрано професійне обладнання світових лідерів у галузі безпеки – Hikvision та/або Dahua Technology.

Базовими варіантами камер відеоспостереження пропонуються:

– Hikvision DS-2CD2043G2-LI2U: вулична циліндрична камера з технологією AcuSense. Призначена для контролю периметра та складських проїздів;

– Dahua DH-IPC-HFW2849S-S-IL: камера з технологією Smart Dual Light, що забезпечує кольорове зображення при детекції об’єктів вночі (рекомендується для зон вантажних рамп, де важлива правильна ідентифікація кольорів транспортних засобів та посилок);

– Hikvision iDS-2CD7A46G0/P-IZHSY: спеціалізована ANPR-камера для розпізнавання номерних знаків (встановлюється на в’їзді до терміналу).

Перелік обладнання, яке планується застосувати для побудови системи відеоспостереженні, подано в таблиці 2.2.

Таблиця 2.2 – Пропонований перелік необхідного обладнання для побудови системи

Найменування обладнання	Модель	Призначення
IP-камера ANPR	Hikvision DS-2CD7A46G0/P	В’їзд/виїзд, контроль номерних знаків
IP-камера периметра	Hikvision DS-2CD2043G2-LI2U	Зовнішній контур території складу
IP-камера рампи	Dahua DH-IPC-HFW2849S-S-IL	Висока деталізація зон навантаження
IP-камера Склад	Hikvision DS-2CD2143G2-I	Зони зберігання
Мережевий реєстратор (NVR)	Hikvision DS-9664NI-M8	Запис та обробка 64 каналів відео
Жорсткий диск	WD Purple 10TB (WD101PURP)	Спеціалізований архів
PoE Комутатор	Hikvision DS-3E1526P-SI	Живлення та об’єднання камер у мережу
Серверна шафа	19" 12U стінова	Монтаж центрального обладнання
Джерело БЖ (UPS)	APC Smart-UPS 2200VA	Безперебійне живлення системи
Кабель передачі даних	UTP Cat 5e Outdoor/Indoor	Магістралі зв'язку та живлення PoE

Впровадження цифрової архітектури відеоспостереження на базі IP-технологій для складського комплексу «Нова пошта» у м. Луцьку є стратегічним рішенням, яке відповідає вимогам часу та внутрішнім стандартам компанії. Використання обладнання Hikvision та Dahua дозволить створити багатофункціональну систему охорони.

Планується реалізація проекту з побудови гігабітної мережі з високим запасом бюджету PoE та встановлення центрального реєстратора M-серії, що забезпечить платформу для майбутнього впровадження нових AI-сервісів без заміни основного обладнання.

2.3 Обґрунтування вибору спеціалізованого програмного забезпечення для моделювання системи

Проектування сучасних комплексів відеоспостереження вимагає від інженерів та інтеграторів високої точності розрахунків, суворого дотримання галузевих стандартів та мінімізації проектних помилок ще на стадії концептуальної розробки. Просте двовимірне розміщення умовних графічних позначень камер на планах поверхів більше не відповідає вимогам замовників і специфікаціям складних інфраструктурних об’єктів, таких як логістичні центри, аеропорти чи університетські кампуси. Застосування універсальних графічних пакетів або простих калькуляторів часто призводить до виникнення сліпих зон, неправильного вибору фокусних відстаней об’єктивів та помилок у розрахунку пропускної здатності мереж, що виявляються вже під час монтажу або експлуатації системи [16].

Процес проектування безпекових рішень зазнав суттєвих змін під впливом цифровізації та посилення нормативних вимог до якості відеоданих, що використовуються в судово-медичних та юридичних цілях. Проектувальник має розв’язати комплексне тривимірне рівняння, де змінними виступають фізична геометрія приміщення, оптичні характеристики об’єктивів, роздільна здатність сенсорів камер, параметри стиснення відеопотоків, мережева топологія та вимоги до глибини архіву збереження інформації.

Аналіз впровадження систем на великих об’єктах показує, що більшість фінансових втрат інтеграторів пов’язані з необхідністю коригування проекту під час пусконалагоджувальних робіт, переносом неправильно розміщених камер або закупівлею додаткових серверних потужностей. Саме тому вибір спеціалізованого програмного інструменту має безпосередній вплив на зниження ризиків та успішну здачу проекту замовнику.

Серед доступних інструментів автоматизованого проектування особливе місце посідає програмний комплекс IP Video System Design Tool (розробка компанії JVSG). Цей продукт активно використовують понад 15 000 компаній у

всьому світі, включаючи лідерів ринку безпеки та консалтингу, таких як ADT, AXIS, Bosch, Dahua, G4S, Hanwha Wisenet, Hikvision, Honeywell, Sony, Verint, Mott MacDonald та WSP [17].

Головною перевагою IP Video System Design Tool є можливість створення точної тривимірної копії об’єкта проектування без необхідності тривалого вивчення складних інженерних інтерфейсів важких CAD-систем. Проектувальник завантажує підкладки планів у форматах JPEG, PNG, PDF або DWG і безпосередньо в середовищі програми зводить стіни, додає вікна, двері та об'єкти інтер’єру.

У версії програмного забезпечення 2026 року суттєво модернізовано алгоритми взаємодії об’єктів у тривимірному просторі. Перешкоди великих габаритів – такі як вантажівки, поїзди, автобуси, стелажі чи офісні шафи –тепер фізично коректно блокують промені огляду камер у симуляції. Це дозволяє уникнути помилок при проектуванні складських і транспортних вузлів, де перешкоди можуть створювати тривалі динамічні або постійні сліпі зони, що важливо для нашого проекту.

Окрім моделювання перешкод, програма дозволяє імпортувати користувацькі 3D-моделі у форматах OBJ та Collada (DAE) , а також містить велику вбудовану бібліотеку моделей, яка в останній версії поповнилася специфічними об'єктами, такими як палети, яхти, вітрильники та різноманітні конфігурації книжкових полиць і складських стеків. Симуляція оптичної системи враховує не лише геометричні параметри розміщення камери (висоту монтажу, кут нахилу, ротацію), а й складні фізичні параметри об’єктива, включно з математичним моделюванням дисторсії за моделлю Брауна-Конраді, що є важливим для точного проектування ширококутних об’єктивів із помітним викривленням простору.

Для об’єктивного обґрунтування вибору IP Video System Design Tool проведено комплексне зіставлення з ключовими альтернативами, присутніми на ринку. Ринок пропонує кілька категорій ПЗ: хмарні швидкі інструменти,

спеціалізоване математичне інженерне ПЗ та безкоштовний софт від виробників камер (табл. 2.3).

Таблиця 2.3 – Порівняльний аналіз спеціалізованих САПР CCTV

Критерій порівняння	JVSG IP Video System Design Too	CCTV Design Tool	VideoCAD/ CCTVCAD	IPVM Camera Calculator	Брендові утиліти виробників
Тип розгортання	Десктопний додаток	Хмарний веб-додаток	Локальний десктопний додаток	Хмарна веб-платформа	Веб-додаток або мобільна утиліта
Тривимірна візуалізація	Повноцінне 3D-моделювання сцени	Відсутня (виключно двовимірне 2D-планування)	Потужне математичне 3D-моделювання зон	Відсутня (тільки двовимірні зони на мапі)	Базове двовимірне накладання кутів без реального 3D
Вимоги до мережі інтернет	Не потрібен (повна автономність після інсталяції)	Потрібен постійний швидкісний доступ	Не потрібен	Потрібен постійний швидкісний доступ	Потрібен постійний швидкісний доступ
Сумісність із брендами	Мультивендорна база (понад 20 750 моделей камер)	Мультивендорна база (понад 23 000 моделей камер)	Мультивендорна база з ручним налаштуванням	Мультивендорна база (постійне оновлення)	Сувора прив'язка до обладнання одного виробника

Беручи до уваги дані таблиці 2.3 та досвід, отриманий під час навчання на спеціальності «Інформаційні системи та технології» у ЛНТУ, обрано для вирішення поставлених задач IP Video System Design Tool.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ

3.1 Створення 3D-моделі об’єкту захисту

Модель об’єкту захисту складського комплексу «Нової пошти» відділення №1 м. Луцька здійснено на основі завчасно підготовленого файлу підкладки, який отримано з супутникового знімку.

Дану підкладку завантажено до робочого середовища IP Video System Design Tool та змасштабовано по відношенню до ширини в’їзду до комплексу, яка складає 5 метрів.

Побудову 3D-модель складського комплексу (рис. 3.1) здійснено за принципом нашарування конструкції: асфальтована ділянка (шар рівня землі), фундамент будівлі і рампа (шар/поверх 1 висотою 0,8 м), зовнішня конструкція будівлі (шар/поверх 2 висотою 7 м), внутрішні офісні приміщення (шар/поверх 2 висотою 3 м).

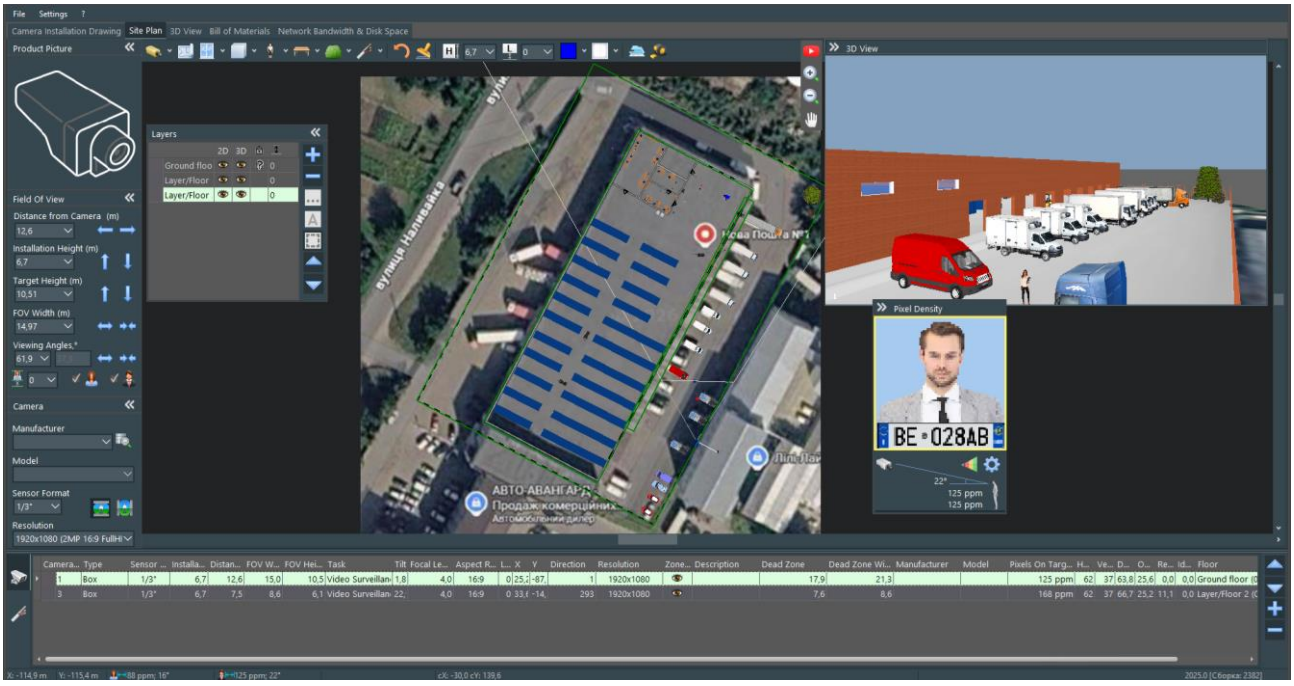

Рисунок 3.1 – 3D-модель складського комплексу «Нової пошти» відділення №1 м. Луцька

Біля рампи розставлено моделі вантажівок, а у середині складу здійснено імітацію складських рядів та обладнання офісних приміщень.

Зовнішній периметр території огороджено парканом.

3.2 Моделювання роботи системи відеоспостереження та аналіз сформованих моделей на виконання поставлених оперативних задач

Моделювання роботи системи відеоспостереження здійснено в ліцензійному програмному забезпеченні IP Video System Design Tool версії Base. Дана версія має обмеження за кількістю одночасно встановлених камер – 16 відеокамер, а попередній аналіз показав, що сумарна кількість камер перевищить 30 штук. З огляду на це даний проект розбито на підзадачі: захист периметра і в'їзду на територію; зони паркування та розвантаження; зона стелажів.

Моделювання системи відеоспостереження здійснено на основі розробленої концепції та обґрунтування вибору технології побудови даної системи та основного обладнання, що висвітлено в п. 2.1 і 2.2 даної роботи.

Аналіз сформованої моделі здійснено згідно критеріїв просторової роздільної здатності (рис. 3.2).

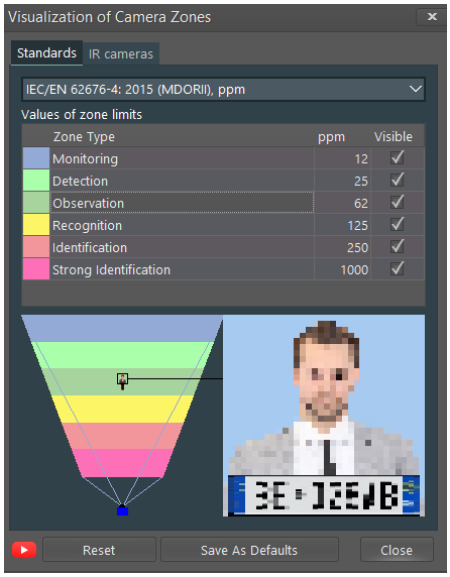

Рисунок 3.2 – Критерії просторової щільності пікселів за IEC/EN 62674-4: 2015

Для охорони периметра використано 4 циліндричні камери марки Hikvision DS-2CD2043G2-L12U з роздільною здатністю 4 Мп та фокусною відстанню 6 мм (рис. 3.3). Кожна з цих камер встановлена на висоті 3,5 м вище рівня землі вздовж паркана на спеціальних стійках.

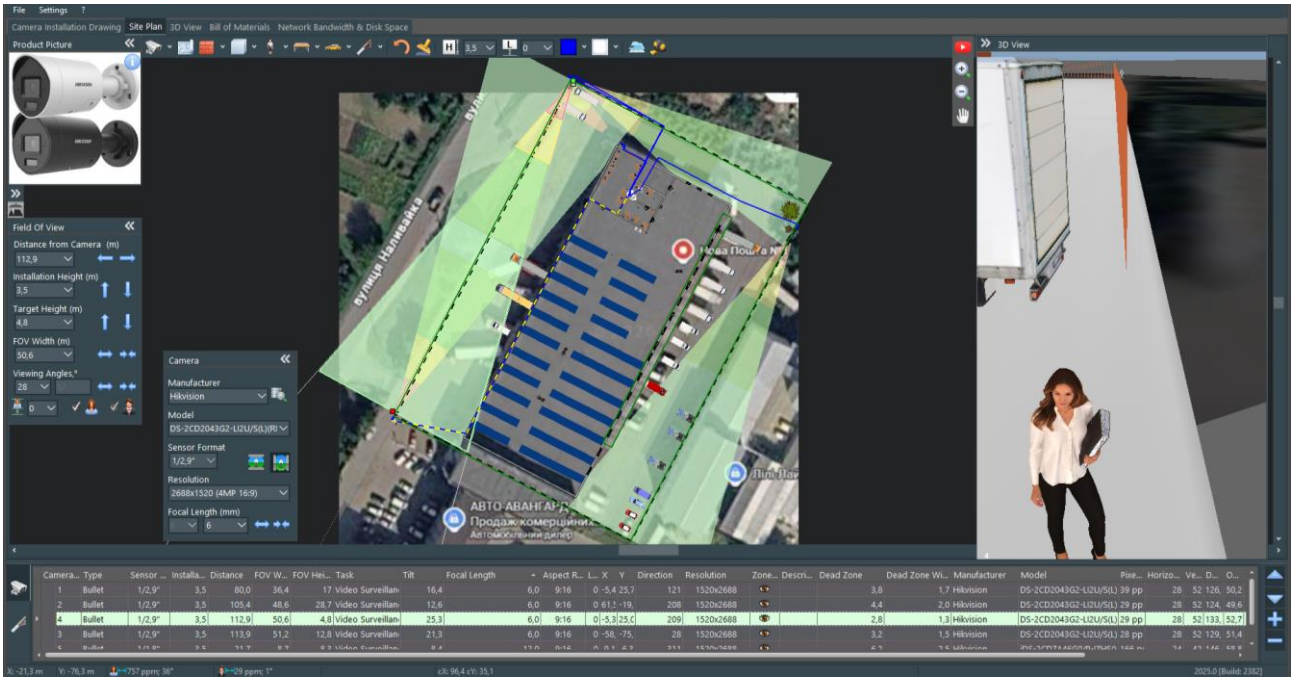

Рисунок 3.3 – Модель охорони периметра комплексу

Відеокамери Hikvision DS-2CD2043G2-L12U потребують живлення DC 12 В та підтримують стандарт живлення PoE 802.3af, що важливо для нашого запланованого варіанту архітектури побудови системи CCTV.

Шляхом порівняння рисунків 3.2 і 3.3 видно, що кожна відеокамера периметра виконує поставлену оперативну задачу – детектування.

Для контролю в’їзду на території складського комплексу використано циліндричну відеокамеру Hikvision iDS-2CD7A46G0/P з роздільною здатністю 4 Мп та фокусною відстанню 12 мм (рис. 3.4). Дану камеру встановлено на зовнішній стіні комплексу на висоті 3,5 м над рівнем землі. Кути нахилу камери відповідають вимогам до ідентифікації номерних занаків автотранспорту: менше 30° у вертикальній площині, і менше 20° в горизонтальній площині.

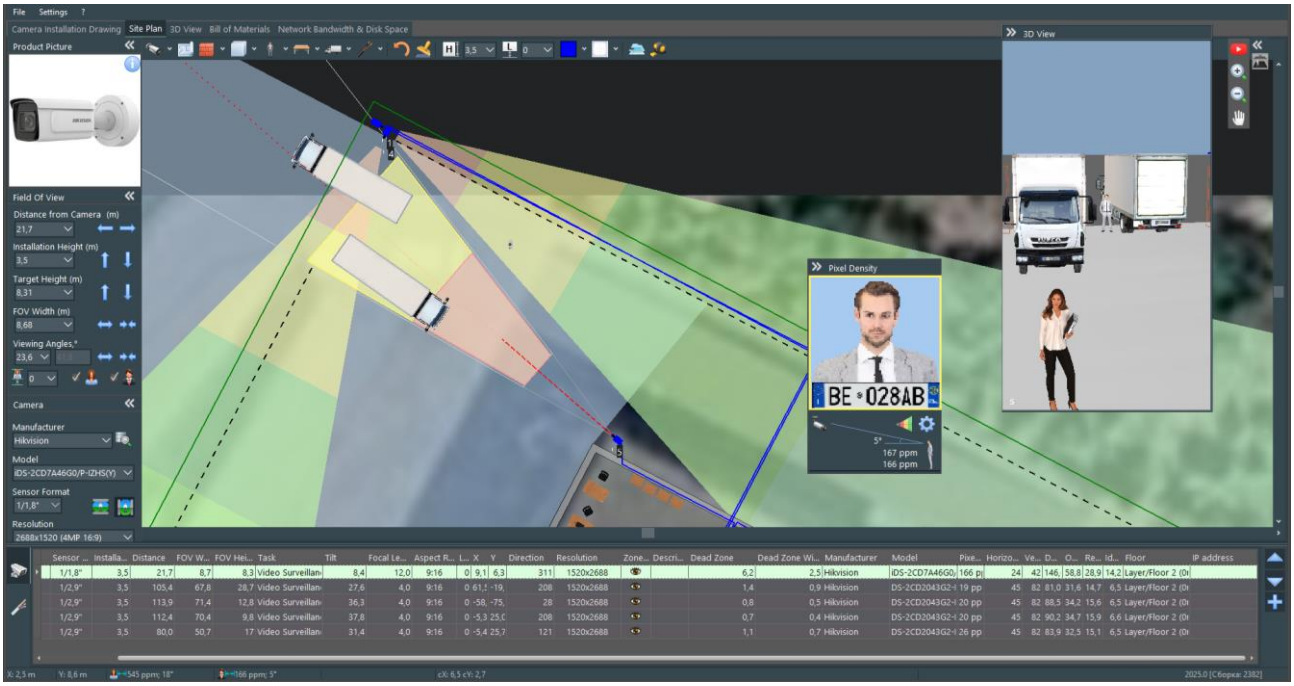

Рисунок 3.4 – Модель контролю в’їзду на територію комплексу

Відеокамери Hikvision iDS-2CD7A46G0/P потребує живлення DC 12 В та підтримує живлення PoE.

Шляхом порівняння рисунків 3.2 і 3.4 видно, що кожна відеокамера виконує поставлену оперативну задачу – ідентифікацію.

Наступним кроком в моделюванні першої підсистеми було встановлення необхідного комутаційного обладнання в кімнаті охорони: серверна стійка, блок живлення, мережевий відеореєстратор, PoE комутатор тощо.

Від кожної відеокамери до PoE комутатора, встановлено в кімнаті охорони, прокладали на моделі кабель витої пари. Кожен відрізок цього кабелю автоматично прораховувзя за довжиною та заносився програмою до кабельного журналу (рис. 3.5).

Як видно з кабельного журналу, добжина кожної кабельної траси перебуває в межах вимог відповідного стадарту (гарантований синал для IP системи – 100 м) і лише одна траса має довжину 116 м, що є не критично для якості сисгналу.

Для побудови даної частини системи відеоспостереження потрібно 307 м кабелю витої пари. Беручи до уваги практичні рекомендації з проектування

мереж відеоспостереження [18] збільшуємо отримане значення на 10% і отримуємо 338 м.

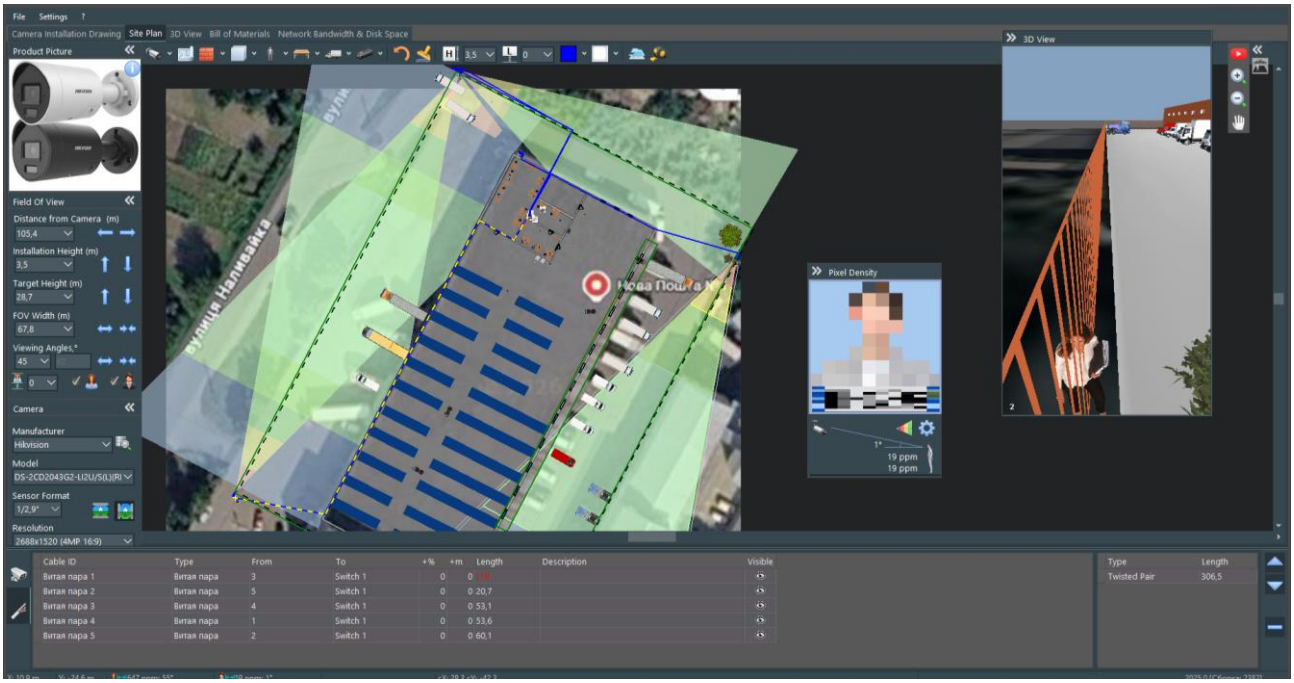

Рисунок 3.5 – Модель прокладання кабельних трас першої підсистеми

За сформованою моделю отримано специфікацію (рис. 3.6) на необхідне обладнання.

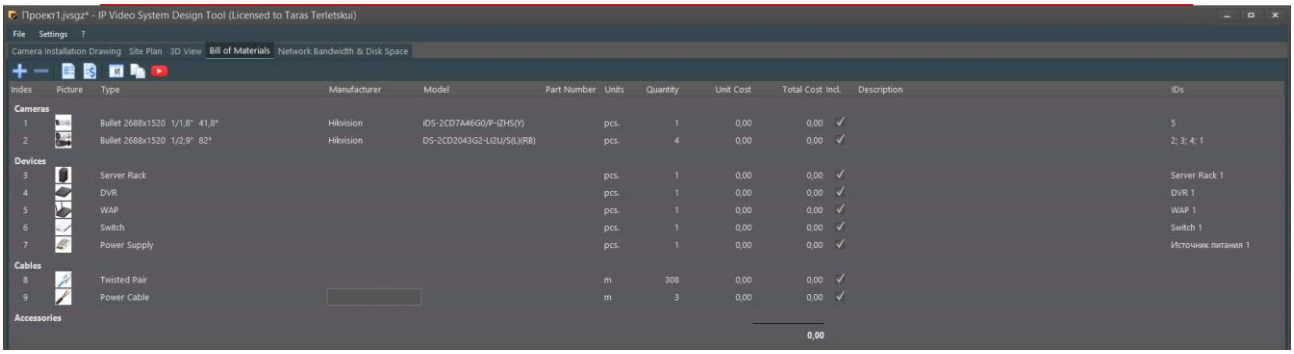

Рисунок 3.6 – Специфікація обладнання першої підсистеми

Наступним етапом стало розрахунок трафіка та необхідного дискового об’єму для збереження інформації.

В середовищі IP Video System Design Tool є вкладка «Трафік та об’єм диска» де для кожного типу відеокамери задавалися наступні параметри: тип

камери, тип кодека, тип стискання інформації, розмір кадра, FPS, глибина архіву, кількість камер, % запису. За цими даними програма розраховувала трафік, об’єм необхідного дискового простору – 4516 Gb і бітрейт (рис. 3.7).

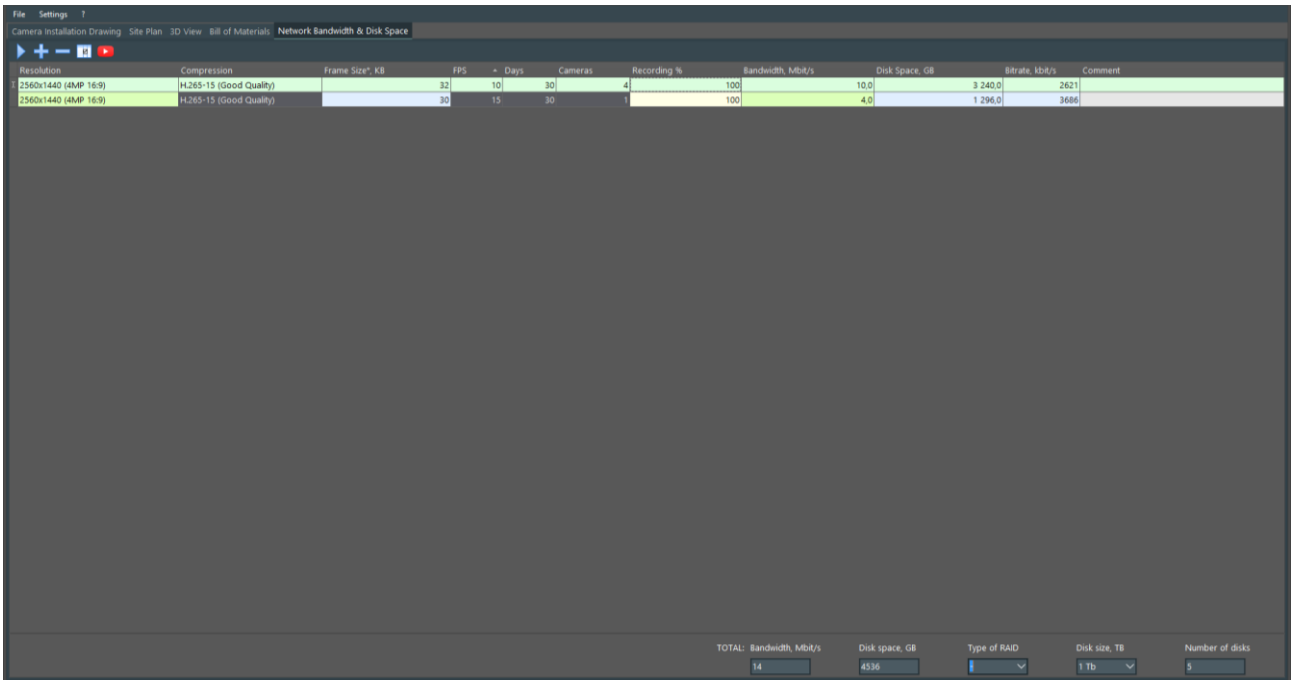

Рисунок 3.7 – Розрахунок дискового простору першої підсистеми

Обравши розмір дискового носія ми отримали необхідну кількість дисків, які дозволять зберігати дані протягом 30 днів – 5 дисків об’ємом 1 Тб кожен.

Моделювання другої підсистеми – зони розвантаження та паркування, проведено на основі розробленої концепції та обґрунтування вибору технології побудови даної системи та основного обладнання, що висвітлено в п. 2.1 і 2.2 даної роботи.

Для зони розвантаження використано короткофокусні відеокамери купольного типу виробництва Dahua DH-IPC-HDW3341F в загальній кількості 7 штук, які встановлено на висоті 2,6 м з боку кожної транспортної арки складу (рис. 3.8).

Ці камери є 2 Мп і мають формат кадра 16:9. Характерною особливістю їх є те, що вони оснащені технологією широкого динамічного діапазону (WDR), яка нормалізує яскраву картинку в найскладніших умовах контрасту освітлення [19] та функції Day/Night (ICR), 3DNR, AWB, AGC, BLC, які можна встановити

за потреби. Живлення камер здійснюється від 12V DC чи PoE (802.3af), а максимальна потужність споживання становить <7,3 Вт.

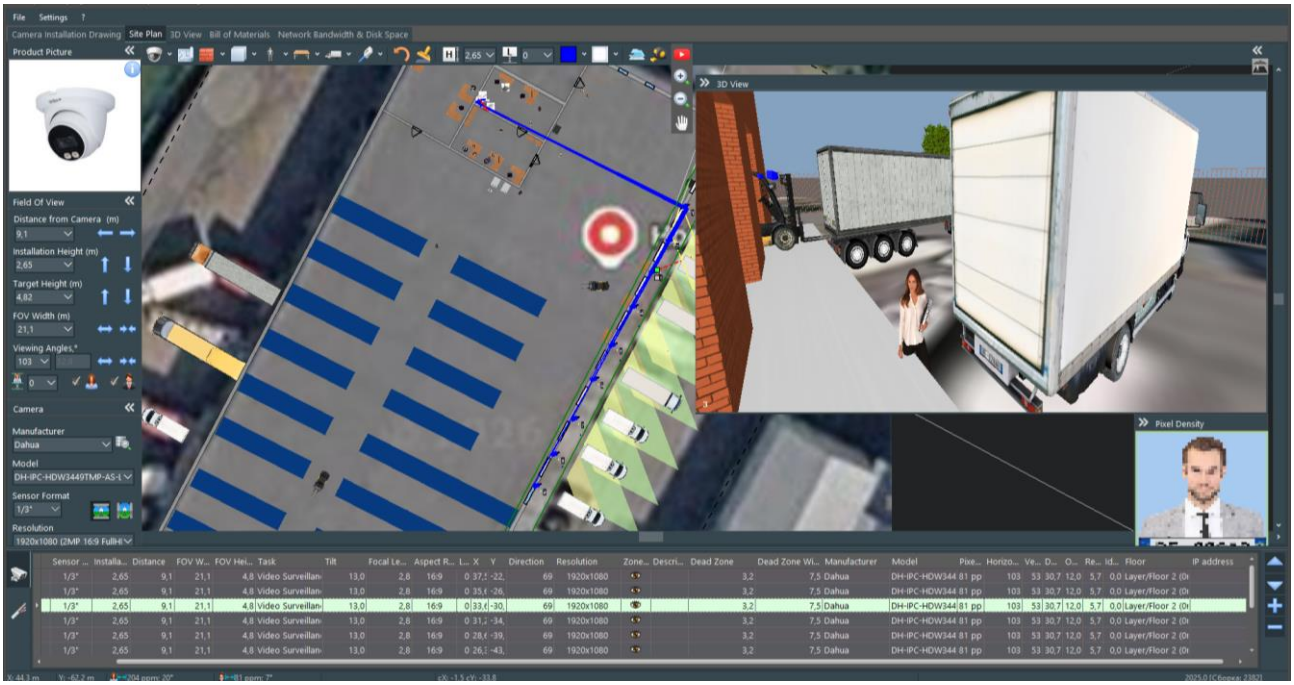

Рисунок 3.8 – Моделювання зони розвантаження

Шляхом порівняння рисунків 3.2 і 3.8 видно, що кожна відеокамери виконує поставлену оперативну задачу – спостереження.

У свою чергу, для спостереження за зоною паркування використано три циліндричні камери Dahua N42BD32: дві камери з форматом кадра 16:9 встановлено для спостереження за внутрішньою парковкою, а одну з форматом кадра 9:16 – зовнішньою (рис. 3.9). Перші дві камери встановлено на стіну складського комплексу на висоті 4 м, третю – стовп електроопори з права на в’їзді до території на висоті 5 м.

Таким чином, як видно з рисунка 3.9, для реалізації другої підсистеми достатньо використати 10 відеокамер.

Для побудови даної частини системи відеоспостереження потрібно 687 м кабелю витої пари. Беручи до уваги практичні рекомендації з проектування мереж відеоспостереження [18] збільшуємо отримане значення на 10% і отримуємо 755 м.

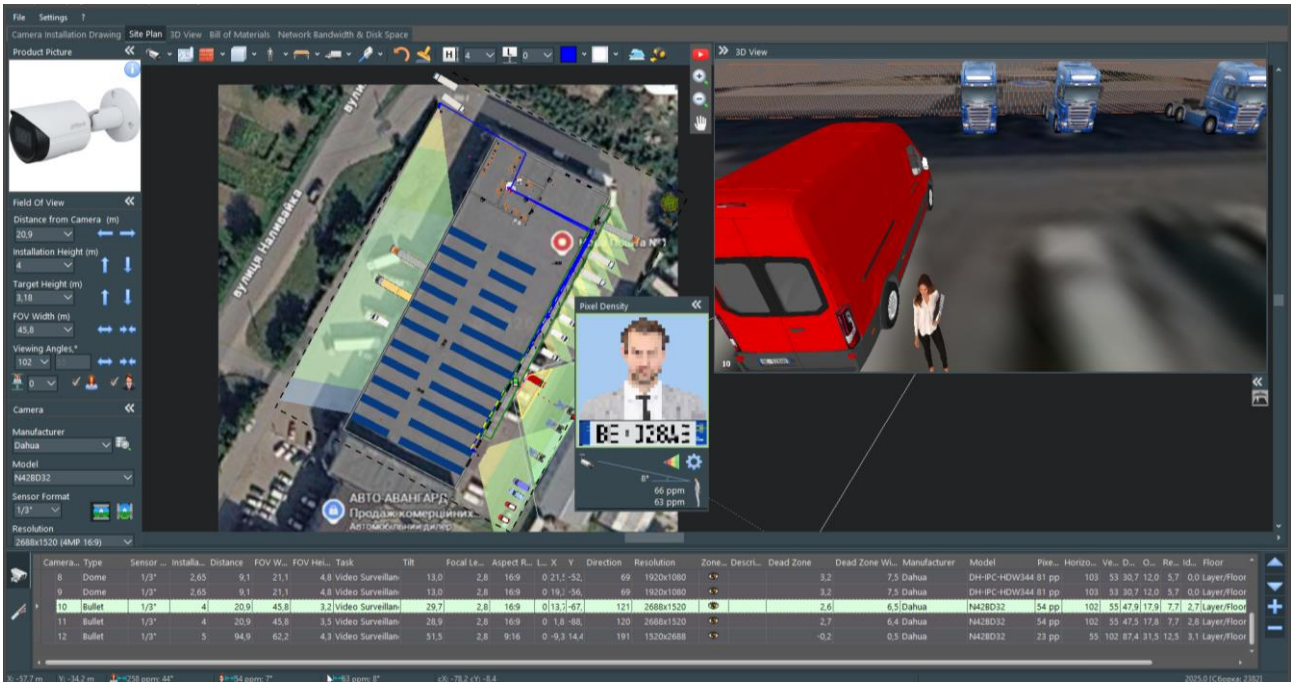

Рисунок 3.9 – Загальна модель другої підсистеми

Проведений розрахунок в середовищі IP Video System Design Tool показав, що обсяг інформації з цих камер протягом 30 календарних днів складе 10368 Gb (рис. 3.10).

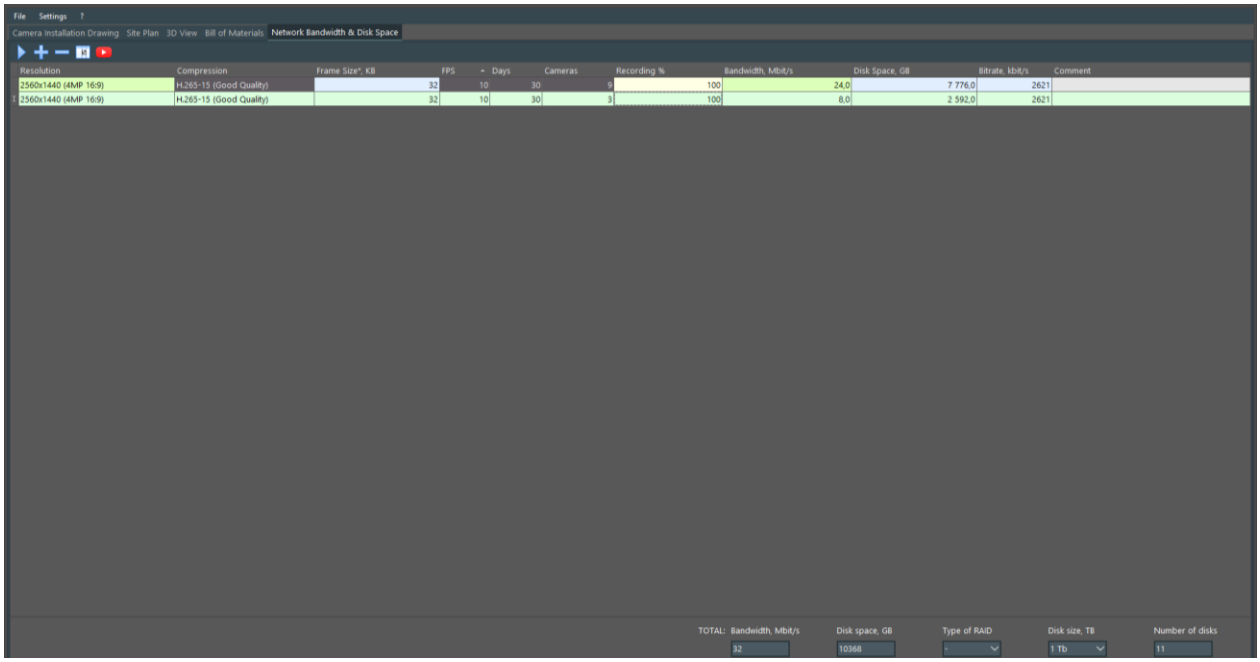

Рисунок 3. 10 – Розрахунок обсягу інформації з другої підсистеми

Моделювання третьої підсистеми – зони складу, проведено на основі розробленої концепції та обґрунтування вибору технології побудови даної системи та основного обладнання, що висвітлено в п. 2.1 і 2.2 даної роботи.

Для складської зони використано короткофокусні 4 Мп відеокамери купольного типу виробництва Hikvision DS-2CD2143G2-I з форматом кадра 9:16 в загальній кількості 12 штук, які встановлено на висоті 3,5 м між рядами стилажів (рис. 3.11). Даний формат кадра, як видно з риснка 3.11, дозволив звузити ширину зони спостереження та одно часно розтянути її за довжиною.

Шляхом порівняння рисунків 3.2 і 3.11 видно, що кожна відеокамери виконує поставлену оперативну задачу – спостереження.

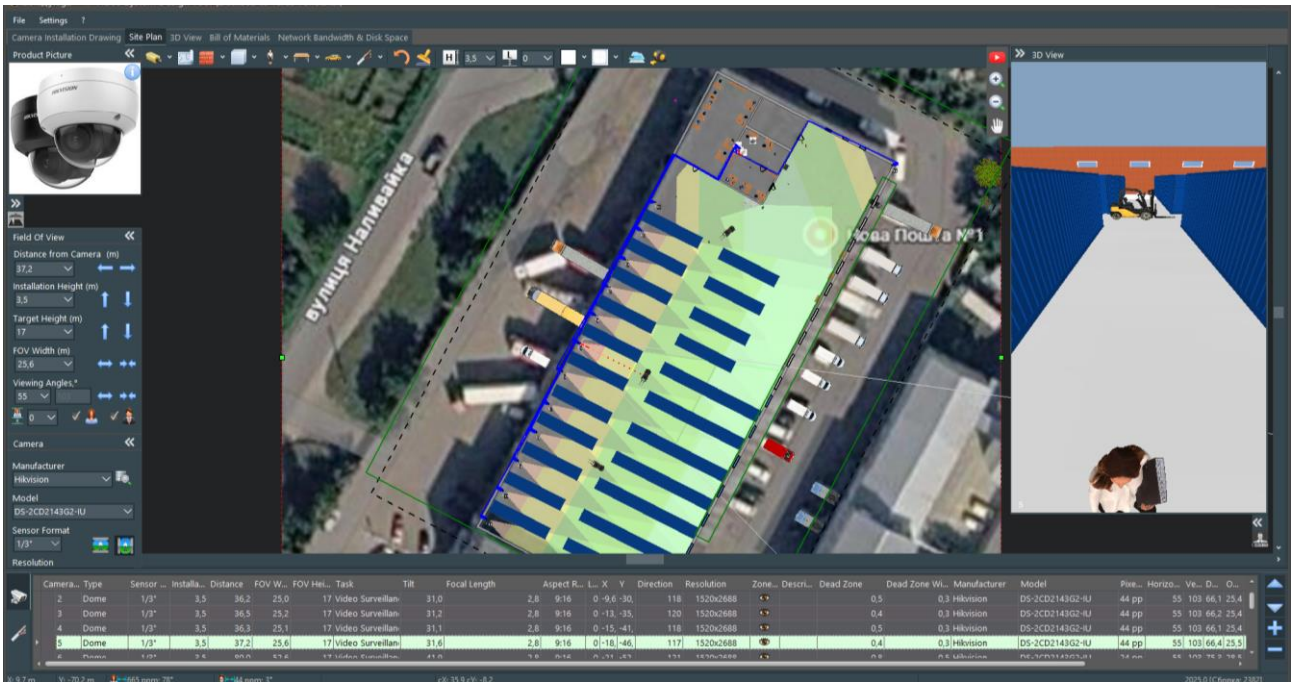

Рисунок 3.11 – Моделювання відеоспостереження складської зони

На початку складської зони розташований простір для маневрування автопогрузчиків та переміщення обслуговуючого персоналу і відвідувачів, які отримують/надсилають поштове відправлення. Для спостереження за даною зоною використано додатково тіж 4 Мп відеокамери купольного типу виробництва Hikvision DS-2CD2143G2-I, але з форматом кадра 16:9 в загальній кількості 2 штуки, які встановлено на висоті 2,5 м на стінах будівлі (рис. 3.12).

Даний формат кадра, як видно з риснка 3.11, дозволив звузити ширину зони спостереження та одно часно розтянути її за довжиною.

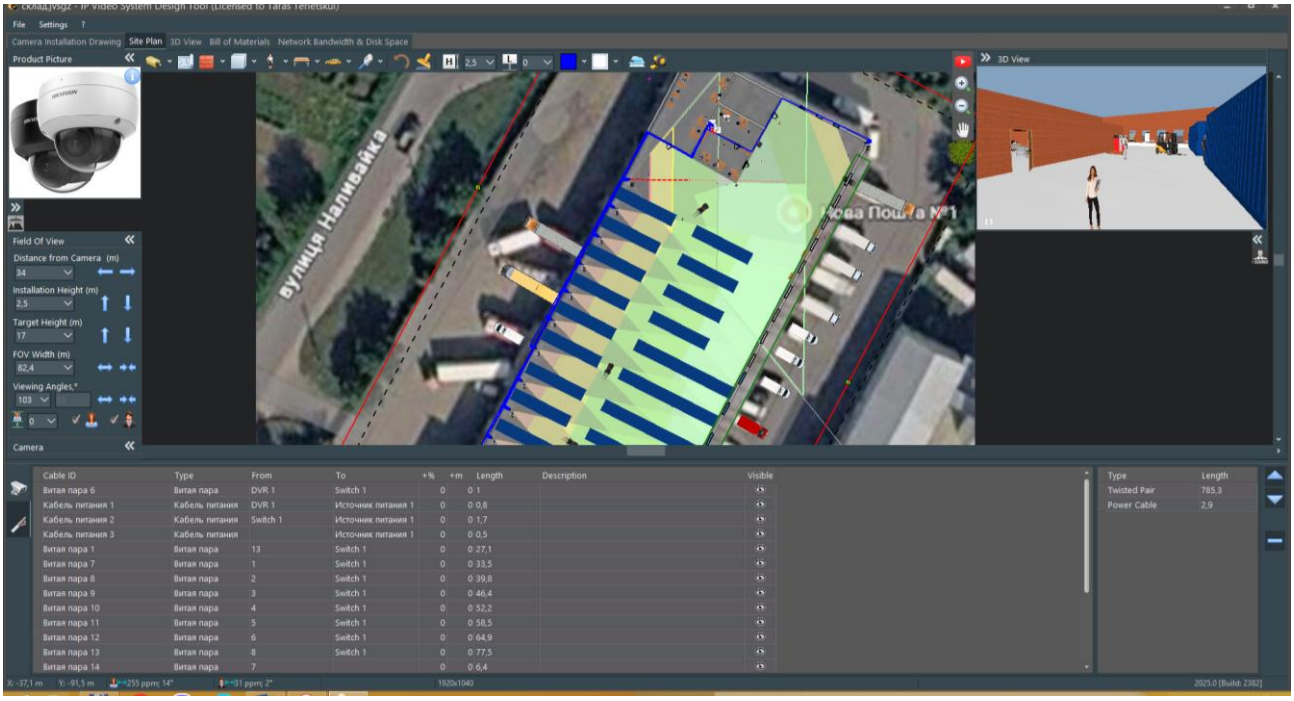

Рисунок 3.12 – Моделювання зони відвідувачів та сформований кабельний журнал третьої підсистеми

Для побудови даної частини системи відеоспостереження потрібно 786 м кабелю витої пари. Беручи до уваги практичні рекомендації з проектування мереж відеоспостереження [18] збільшуємо отримане значення на 10% і отримуємо 863 м.

Проведений розрахунок в середовищі IP Video System Design Tool показав, що обсяг інформації з цих камер протягом 30 календарних днів складе 12312 Gb.

Таким чином, взявши до уваги необхідний дисковий простір трьох підсистем встановлено загальний дисковий простір системи відеоспостереження для даного проекту глибиною в 30 календарних дні рівний 27196 Gb.

Для реалізації цього завдання потрібно три диски WD Purple 10 TB (WD101PURP) [20], що утворять цілком достатній загальний дисковий простір у 30 ТВ.

З вище поданого стає зрозуміло, що для виконання всіх поставлених оперативних задач потрібно мінімум 28 відеокамер, в ідеалі 39 відеокамер (це якщо ще 11 відеокамер встановити в складській зоні, спрямувавши їх на зустріч встановленим на протилежній стіні). Сумарна довжина кабелю витої пари для реалізації цього проекту потрібна 1956 м.

Беручи до уваги те, що на початку розробки проекту нами був закладений 64 канальний відеореєстратор, а розрахункова кількість відеокамер виявилася 28 штук, то потрібна заміна його на іншу модель із урахуванням можливостей подальшого масштабування системи. Для цього підійде 32 канальний Hikvision DS-7632NXI-K2 [21], у якого буде ще 4 порти на запас.

Для живлення та об’єднання камер у мережу пропонується використати замість 24 портового PoE комутатора Hikvision DS-3E1526P-SI два PoE комутатора Smart HIKVISION DS-3E1318P-EI(B), які підтримують потрібну нам технологію PoE 802.3af [22].

Сумарна потужність споживання системи відеоспостереження, встановлена на основі аналізу технічних характеристик кожної складової системи, становить 682 Вт. Застосування джерела безперебійного живлення APC Smart-UPS 2200VA дозволить, уразі знеструмлення загальної електромережі, повноцінно функціонувати системі понад 3 годин, що цілком достатньо для коректного завершення її функціонування чи переходу на резервний дизельний генератор.

3.3 Підключення та налаштування мережевого обладнання

Інтелектуальний керований комутатор другого рівня Hikvision DS-3E1318P-EI(B) розроблений спеціально для побудови надійних та масштабованих мереж IP-відеоспостереження. Фізичне виконання пристрою

базується на міцному металевому корпусі, який передбачає можливість монтажу в стандартну 19-дюймову стійку за допомогою комплектних монтажних кронштейнів (рис. 3.13).

Рисунок 3.13 – Комутатор Hikvision DS-3E1318P-EI(B) [23]

Комутаційна матриця пристрою забезпечує загальну продуктивність на рівні 9,2 Gbps, що гарантує безперешкодне проходження трафіку високої щільності від камер надвисокої роздільної здатності без ризику виникнення внутрішніх затримок. Портова конфігурація включає 16 портів Fast Ethernet (10/100 Mbps) з підтримкою технології PoE та 2 комбіновані гігабітні порти Gigabit Combo. Гігабітні комбо-інтерфейси мають комбіновану структуру: при підключенні мідного кабелю вони функціонують як порти RJ45, а при встановленні SFP-модуля і підключенні оптичного волокна автоматично переходять у режим оптичного порту. Якщо кабель RJ45 та оптичне волокно підключені одночасно, порт віддає пріоритет оптичному з’єднанню.

Для безпечного розгортання комутатора DS-3E1318P-EI(B) у робочому середовищі обов’язковою є процедура активації, оскільки за замовчуванням у пристрої відсутній встановлений пароль адміністратора. На етапі відвантаження з заводу комутатор налаштований на автоматичне отримання IP-адреси через DHCP. Якщо у мережевому сегменті відсутній DHCP-сервер, пристрій намагається призначити собі тимчасову IP-адресу з діапазону за замовчуванням – 192.168.1.64.

Унікальним архітектурним рішенням Hikvision є інтеграція статичної, незмінної адреси Super IP – 10.180.190.200. Ця адреса жорстко зафіксована на

рівні мікропрограми й не підлягає зміні. Вона призначена для екстреного доступу до веб-інтерфейсу керування, якщо основну динамічну або статичну адресу було втрачено. Для цього інженерному комп’ютеру достатньо призначити адресу з підмережі 10.180.190.x і підключитися патч-кордом до будь-якого вільного порту комутатора.

Первинна ініціалізація виконується за таким алгоритмом:

– клієнтський комп’ютер підключається до того самого фізичного сегмента мережі, де знаходиться комутатор і за допомогою фірмової утиліти SADP (Search Active Device Protocol) здійснюється сканування мережі на рівні L2-рівня для виявлення неактивного пристрою;

– запустивши веб-браузер (рекомендуються актуальні версії Microsoft Edge, Google Chrome або Mozilla Firefox), необхідно ввести виявлену IP-адресу комутатора або адресу 10.180.190.200 в рядок адреси;

– на сторінці активації створюється пароль для облікового запису адміністратора admin.

Після успішної активації адміністратор перенаправляється на сторінку мережевих налаштувань за шляхом System Management → Network Configuration → Network Configuration. Тут встановлюється статична IP-адреса, маска підмережі, шлюз за замовчуванням та DNS-сервери.

Для захисту від перехоплення трафіку під час віддаленого керування комутатор підтримує протокол SSH, який за замовчуванням вимкнений. При його активації через параметри безпеки доступ здійснюється під обліковим записом root, а паролем є встановлений під час активації пароль пристрою. Служба SADP також за замовчуванням увімкнена, що дозволяє виконувати мережеві зміни безпосередньо з утиліти.

Розділення мережі на віртуальні сегменти є важливим кроком для безпеки та стабільності систем відеоспостереження, оскільки це запобігає несанкціонованому доступу до камер з офісної мережі та мінімізує негативний вплив широкомовних штормів. DS-3E1318P-EI(B) підтримує стандарт 802.1Q VLAN з можливістю призначення ідентифікаторів у повному діапазоні від 1 до

4094. Максимальна кількість одночасно конфігурованих груп VLAN становить 128. VLAN з ідентифікатором 1 є системним за замовчуванням (Management VLAN) і використовується для керування; його видалення заблоковане на рівні системи.

Налаштування віртуальних мереж реалізується у розділі L2 Configuration → Port Attributes та 802.1Q VLAN. Порти комутатора можуть функціонувати у двох основних режимах:

– Access (абонентський порт) – використовується для підключення кінцевих пристроїв, які не підтримують тегування трафіку (наприклад, стандартних IP-камер або комп'ютерів). Вхідний нетегований кадр маркується встановленим на порту ідентифікатором PVID, а при виході з порту тег автоматично вилучається;

– Trunk (магістральний порт) – призначений для транзиту тегованого трафіку кількох віртуальних мереж між різними комутаторами або до маршрутизатора. Для налаштування такого порту обирається режим TRUNK, встановлюється транзитний PVID і вручну прописується список дозволених до передачі VLAN (VLAN Allowed).

Процедура налаштування виконується через меню L2 Configuration → Link Aggregation. Після створення логічної групи до неї додаються фізичні порти. На етапі проектування слід враховувати суворе обмеження: усі фізичні порти, що входять до однієї агрегаційної групи, повинні мати абсолютно ідентичні параметри роботи. Швидкість (Rate), режим дуплексу (Duplex), налаштування контролю потоку (Flow Control), приналежність до VLAN та режим великої дальності (Long-Range) мають повністю збігатися. Будь-яка невідповідність заблокує ініціалізацію віртуального інтерфейсу. Балансування навантаження здійснюється за алгоритмом аналізу MAC-адрес джерела та одержувача (Source and Destination MAC).

У системах відеоспостереження часто виникає потреба ізолювати камери одну від одної, щоб запобігти горизонтальному поширенню мережевих атак або шкідливого ПЗ між кінцевими пристроями, зберігши при цьому їхню

можливість зв’язку з центральним сервером чи відеореєстратором. Налаштування функції Port Isolation є простішою альтернативою створенню десятків окремих VLAN.

Конфігурування здійснюється в меню Security → Port Isolation (або Switch Configuration → Basic Configuration → Port Isolation у попередніх версіях):

– на графічній панелі комутатора обираються фізичні порти, які підлягають ізоляції;

– функція переводиться в стан Enable;

– після збереження налаштувань порти, що знаходяться в одній ізоляційній групі, повністю втрачають можливість обмінюватися будь-яким типом трафіку між собою. Водночас вони зберігають повний двонаправлений доступ до будь-яких інших портів комутатора, які не входять до цієї групи (наприклад, до гігабітних портів висхідного каналу, куди підключено мережевий реєстратор NVR).

Загальний енергетичний бюджет комутатора для живлення підключених споживачів становить 230 Вт. Порти з 1 по 16 підтримують стандарти живлення IEEE 802.3af (до 15,4 Вт на порт) та IEEE 802.3at (PoE+ до 30 Вт на порт).

Адміністратор може керувати живленням через веб-інтерфейс, клікнувши на іконку у верхньому правому кутку модуля PoE Power на головній сторінці або перейшовши у розділ PoE Management. Тут доступна активація чи деактивація PoE для кожного окремого порту та відображається реальна споживана потужність кожного підключеного пристрою.

Функція комутатора PoE Watchdog є інтелектуальним апаратним контролером, розробленим для автоматизації обслуговування системи відеоспостереження на портах з 1 по 16. Вона реалізує наступний механізм самовідновлення:

– комутатор постійно аналізує мережеву активність та обмін пакетами з кожним підключеним PoE-пристроєм;

– якщо IP-камера через програмний збій зависає та припиняє відповідати на запити, Watchdog фіксує відсутність активності на відповідному порті;

– вісля закінчення встановленого таймауту комутатор автоматично перезавантажує завислу камеру шляхом короткочасного повного знеструмлення відповідного PoE-порту з наступною повторною подачею живлення. Це виключає потребу у виїзді технічних фахівців для перезавантаження обладнання вручну.

Стандартне обмеження довжини мідного кабелю Ethernet становить 100 метрів. Для обходу цього ліміту в комутаторі реалізовано режим Long-Range на портах з 1 по 16. При активації цієї функції дальність стабільної передачі даних та живлення збільшується до 300 метрів, що актуально для нашого випадку, оскільки, одна лінія має довжину 116 метрів.

Для базового налаштування 32-канального мережевого відеореєстратора Hikvision DS-7632NXI-K2 (рис. 3.14) потрібно виконати кроки з первинної активації, конфігурації мережі, додавання камер та увімкнення аналітики AcuSense.

Рисунок 3.14 – Мережевий відеореєстратор Hikvision DS-7632NXI-K2 [24]

Процес розгортання починається з фізичного встановлення жорстких дисків у корпус відеореєстратора. Пристрій фіксується на стійці в чистому, добре вентильованому приміщенні. Після підключення кабелів живлення, монітора (через HDMI або VGA) та USB-миші система готова до першого запуску.

Усі сучасні пристрої Hikvision постачаються в неактивному стані з метою запобігання несанкціонованому доступу через стандартні фабричні паролі. Первинну активацію можна виконати за допомогою локального монітора, веб-інтерфейсу або утиліти SADP (Search Active Devices Protocol).

Утиліта SADP встановлюється на робочу станцію адміністратора, яка повинна перебувати в тому самому фізичному та логічному сегменті мережі (підмережі/VLAN), що й відеореєстратор. Процедура активації через SADP включає наступні кроки:

– запустити SADP (програма автоматично виявить неактивний пристрій);

– виділити відеореєстратор у списку та ввести новий пароль для адміністратора (admin) у відповідному полі;

– для спрощення відновлення пароля вказати відповіді на контрольні запитання або імпортувати файл GUID;

– змінити мережеві параметри: вимкнути DHCP для надання статичної адреси або увімкнути DHCP, якщо в мережі розгорнуто корпоративний сервер розподілу адрес. Натиснути кнопку підтвердження та ввести пароль адміністратора для збереження налаштувань.

За замовчуванням відеореєстратори Hikvision використовують статичну адресу 192.0.0.64, тоді як IP-камери мають заводську адресу 192.168.1.64. Якщо підключення здійснюється через веб-браузер, мережеву карту комп’ютера адміністратора необхідно попередньо перевести у відповідний діапазон (наприклад, встановивши IP-адресу 192.0.0.10 або 192.168.1.10 з маскою 255.255.255.0).

Існує дві основні технологічні моделі інтеграції камер у DS-7632NXI-K2: використання вбудованого PoE-комутатора (для моделей з індексом /16P) або підключення через загальну локальну мережу (LAN-mode).

Пристрої з вбудованим PoE-комутатором підтримують технологію Plug-and-Play. Підключення кабелю від неактивної камери безпосередньо до PoE-порту реєстратора ініціює автоматичну активацію камери із застосуванням пароля реєстратора та призначенням їй приватної адреси зі спеціального підмережевого пулу (зазвичай 192.168.254.xxx). Це ізолює трафік відеокамер від загальнокорпоративної мережі, значно знижуючи ризики кібератак та перевантаження комутаторів.

Для базової моделі без PoE-портів камери підключаються через зовнішній комутатор, що вимагає ручного додавання. Конфігурація здійснюється через веб-інтерфейс у розділі Configuration (Конфігурація) → System (Система) або Device Access (Доступ до пристроїв) → Camera (Камера).

Для інтеграції камер сторонніх виробників через протокол ONVIF необхідно попередньо зайти на веб-інтерфейс самої камери та увімкнути підтримку ONVIF у меню Network → Advanced Settings → Integration Protocol. Обов’язково створюється окремий ONVIF-користувач із правами адміністратора. Окремі прошивки також вимагають активації прапорця «Enable Hikvision-CGI» та встановлення методу автентифікації на рівні «Digest & ws-username token» або «digest/basic».

В оновленому інтерфейсі NVR 5.0 додана функція швидкого переходу (іконка монітора зі стрілкою у стовпчику «Operation»). Цей інструмент замінює класичний функціонал віртуального хоста, дозволяючи адміністратору в один клік відкривати веб-панель керування камери прямо через сесію реєстратора для налаштування фокусу, експозиції чи оновлення прошивки камери.

Застосування кодека H.265+ знижує споживання дискового простору та пропускної здатності мережі до 75% порівняно з базовим H.264. Проте, при експорті архіву на зовнішні USB-накопичувачі слід враховувати, що стандартні медіаплеєри на операційних системах Windows або macOS не завжди мають

інтегровані декодери для H.265+. У таких випадках разом із відеофайлами рекомендується експортувати фірмовий плеєр VSPlayer.

Для налаштування автоматичного видалення старих записів використовується параметр автоекспірації відеоархіву (Video Expiry Time) у додаткових налаштуваннях сховища. Якщо встановлено значення 0, відеореєстратор працює в стандартному режимі циклічного перезапису, автоматично стираючи найстаріші файли при заповненні дисків. Встановлення конкретного значення (наприклад, 30) обмежує глибину архіву рівно тридцятьма днями, навіть якщо на дисках залишається вільне місце.

Технологія штучного інтелекту AcuSense реалізує класифікацію об’єктів для мінімізації помилкових тривог. Найбільш поширеним та ефективним інструментом є детекція руху нового покоління – Motion Detection 2.0, яка аналізує сцену на наявність людей та транспортних засобів.

Конфігурація аналітики виконується за таким алгоритмом:

– перейти в розділ Configuration → Event Center → Event Configuration → Generic Event → Motion Detection;

– обрати канал камери та встановити прапорець Enable;

– якщо камера підтримує аналітику AcuSense, апаратна обробка залишається на стороні камери, а опція «Enable AI by NVR» вимикається. Якщо підключено звичайну камеру без AI, активується функція Enable AI by NVR. У цьому випадку реєстратор задіє власні ресурси для аналізу потоку (максимум до 2 каналів 4 Мп або 1 канал 8 Мп на весь пристрій);

– у списку Detection Target відмітити цільові об’єкти детекції: Human (людина) та/або Vehicle (транспортний засіб);

– для створення кастомної зони детекції слід видалити стандартну повноекранну маску кнопкою «Clear All». За допомогою інструмента «Draw Area» лівою кнопкою миші наноситься геометрична зона (до 4 зон, кожна може мати до 10 кутів для точного охоплення складного рельєфу ділянки). Права кнопка миші завершує малювання фігури;

– встановити розклад активності функції на вкладці Arming Schedule. За замовчуванням система пропонує цілодобовий моніторинг (24/7). За необхідності можна виключити робочі години з розкладу за допомогою інструмента стирання (Erase);

– визначити дії при детекції на вкладці Linkage Method:

a) Notify Surveillance Center – відправляє тривожне сповіщення з метаданими та фрагментом відео на мобільний застосунок Hik-Connect або клієнт iVMS-4200;

b) Alarm Pop-Up Window – розгортає зображення з тривожної камери на весь екран локального монітора реєстратора;

c) Buzzer – активує переривчастий звуковий сигнал на платі відеореєстратора;

d) Send Email – ініціює надсилання листа зі стоп-кадром події на налаштований SMTP-сервер;

e) Trigger Alarm Output – замикає фізичні контакти тривожного виходу для активації прожектора, сирени чи відкриття воріт.

Відеореєстратор DS-7632NXI-K2 здатний здійснювати детекцію, захоплення та порівняння обличь із базою даних у реальному часі. Процесор пристрою підтримує порівняння зображень по 4 каналах одночасно або повний цикл детекції та аналізу по 1 каналу (для звичайних некогнітивних камер).

Загалом, розгортання системи безпеки на базі мережевого відеореєстратора Hikvision DS-7632NXI-K2 вимагає від системного інженера розуміння апаратних обмежень процесора та мережевої топології.

ЗАГАЛЬНІ ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

У кваліфікаційній роботі бакалавра вирішено актуальну науково-технічну проблему проєктування та інтеграції сучасної IP-системи відеоспостереження складського комплексу «Нової пошти» відділення №1 м. Луцька. На основі опрацьованого матеріалу та 3D моделювання об’єкту захисту й функціонування IP-системи відеоспостереження отримано наступні висновки:

– згідно з розробленою концепцію системи відеоспостереження визначено характерні зони спостереження, визначено конкретні типи оперативних задач та необхідні критерії їх виконання;

– визначено, що реалізовувати систему відеоспостереження доцільно за IP-технологією, для якої було встановлено необхідний перелік базового обладнання;

– створена 3D-модель об’єкту захисту автоматизує проектні рішення та дає повну просторову уяву про нього;

– для вирішення поставлених оперативних завдань необхідно застосувати мінімум 28 відеокамер, а в ідеалі 39 відеокамер (якщо ще 11 відеокамер встановити в складській зоні, спрямувавши їх на зустріч встановленим на протилежній стіні), два PoE комутатора, мережевий 32 канальний відеореєстратор;

– за результатами аналізу сформованих моделей характерних зон спостереження складського комплексу підтверджено можливість реалізації поставлених оперативних задач обраними апаратними засобами IP-системи відеоспостереження;

– для забезпечити 30 денної глибини архіву потрібно три диски WD Purple 10 TB (WD101PURP), що утворять цілком достатній загальний дисковий простір у 30 TB;

– отриманий кабельний журнал дозволив встановити потреби в кабелі типу вита пара 1956 м.

Для підвищення ефективності, довговічності та відмовостійкості розробленої системи під час її практичної експлуатації рекомендується застосування джерела безперебійного живлення APC Smart-UPS 2200VA, яке дозволить, уразі знеструмлення загальної електромережі, повноцінно функціонувати системі понад 3 годин. Цього цілком достатньо для коректного завершення її функціонування чи переходу на резервний дизельний генератор.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Терлецький Т. В., Кайдик О. Л. САПР систем охорони і безпеки: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12/F Інформаційні технології спец. 126/F6 Інформаційні системи та технології денної та заоч. форм навч. Луцьк: ЛНТУ, 2025. 81 с. URL: https://surl.li/znbpah / (дата звернення: 11.04.26).

2. BS EN 62676-4:2015 Video surveillance systems for use in security applications. Application guidelines. URL: https://www.thenbs.com/PublicationIndex/documents/details?Pub=BSI&DocID=311425 (access date: 11.04.26).

3. ДСТУ EN IEC 62676-5: 2019 Системи відеоспостереження охоронного призначення. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=83148 (дата звернення: 11.04.26).

4. BS 7958:2015 Closed circuit television (CCTV) – management and operation – code of practice. URL: https://www.thenbs.com/PublicationIndex/documents/details?Pub=BSI&DocID=312704 (access date: 11.04.26).

5. Video surveillance systems for use in security applications – part 4: application guidelines, 2025. URL: https://webstore.iec.ch/en/publication/83425 (access date: 11.04.26).

6. Bahniuk, N., Terletskyi, N., Kaidyk, O., Kostiuchko, S., Kondius, S. Solving Operational Tasks in the Design of Video Surveillance Systems. 2025. CEUR Workshop Proceedings: Applied Information Technologies and Artificial Intelligence Systems (AIT&AIS 2025). Vol. 4160. Pp. 332-342. / URL: https://ceur-ws.org/Vol-4160/paper20.pdf (access date: 11.04.26).

7. Taras Terletskyi, Oleh Kaidyk, Larysa Pylypiuk, Inna Kondius, Nina Zdolbitska. Determining the Feasibility of Applying Existing Criteria for Solving Operational Problems in the Design of CCTV Information Systems. Security of

Infocommunication Systems and Internet of Things. 2023. Vol. 1, No. 1. / URL: https://doi.org/10.31861/sisiot2023.1.01009 (access date: 11.04.26).

8. IEC 62676-4:2025 Sets a New Benchmark for Video Surveillance Systems. URL: https://euro-security.de/en/iec-62676-42025-sets-a-new-benchmark-for-video-surveillance-systems/ (access date: 11.04.26).

9. Pixel density based on IEC 62676-4:2025. URL: https://whitepapers.axis.com/en-us/pixel-density-based-on-iec-62676-4-2025 (access date: 13.04.26).

10. CCD vs CMOS vs sCMOS. URL: https://www.ximea.com/support/wiki/allprod/CCD_CMOS_or_sCMOS (access date: 13.04.26).

11. How Can Hybrid DVRs Connect Your Analog and IP Cameras Together? URL: https://jer-tech.com/hybrid-dvrs-connecting-analog-ip-cameras/ (access date: 13.04.26).

12. Терлецький Т. В., Кайдик О. Л. Системи відеоспостереження: Конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12/F «Інформаційні технології» спеціальності 126/F6 «Інформаційні системи та технології» ОП «Інформаційні системи та технології охорони і безпеки» денної та заочної форм навчання Луцьк: ЛНТУ, 2026. 209 с. URL: https://repository.lntu.edu.ua/entities/methodologicalsupport/bd5cf896-890e-499b-bc70-4015a40626eb (дата звернення: 13.04.26).

13. Політика приватності Нової пошти. URL: https://novaposhta.ua/more/privacy-policy/ (дата звернення: 13.04.26).

14. TAPA FSR – Facility Security Requirements. URL: https://www.dnv.us/services/tapa-fsr-facility-security-requirements-4345/ (access date: 27.04.26).

15. What Makes a Warehouse TAPA-Certified and Why It Matters. URL: https://amworld.co.uk/what-makes-a-warehouse-tapa-certified-and-why-it-matters/ (access date: 27.04.26).

16. JVSG CCTV Video Surveillance Design & Planning Software 2026. URL: https://netviewcctv.co.uk/ipvsd-tool (access date: 27.04.26).

17. Designing Video Surveillance Systems Using JVSG Software. URL: https://www.scribd.com/document/1008373446/DESIGNING-VIDEO-SURVEILLANCE-SYSTEMS-USING-JVSG-SOFTWARE (access date: 27.04.26).

18. Системи відеоспостереження: Конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12/F «Інформаційні технології» спеціальності 126/F6 «Інформаційні системи та технології» ОП «Інформаційні системи та технології охорони і безпеки» денної та заочної форм навчання / укл. Терлецький Т. В., Кайдик О. Л. Луцьк: ЛНТУ, 2026. 209 с. URL: URL: https://repository.lntu.edu.ua/entities/methodologicalsupport (дата звернення: 30.04.26).

19. IP відеокамера Dahua DH-IPC-HDBW3441EP-AS (2.8 мм). URL: https://dahua-technology.com.ua/ua/dahua-dh-ipc-hdbw3441ep-28mm (дата звернення: 17.05.26).

20. Накопичувач HDD SATA 10.0TB WD Purple Pro 7200rpm 512MB (WD102PURP) URL: https://surl.li/retdeq (дата звернення: 19.05.26).

21. IP відеореєстратор Hikvision DS-7632NXI-K2 32-канальний. URL: https://hikvision.co.ua/hikvision-ds-7632nxi-k2/ (дата звернення: 19.05.26).

22. Комутатор Smart HIKVISION DS-3E1318P-EI(B). URL: https://hotline.ua/ua/computer-kommutatory/hikvision-ds-3e1318p-eib/ (дата звернення: 19.05.26).

23. DS-3E1318P-EI(B) 18-портовий Smart керований PoE комутатор Hikvision. URL: https://surl.li/hmnlsf (дата звернення: 19.05.26).

24. Відеореєстратор Hikvision DS-7632NXI-K2(D) 32-канальний AcuSense 4K 1U. URL: https://viatec.ua/ru/product/DS-7632NXI-K2d (дата звернення: 19.05.26).

25. Терлецький Т. В., Кайдик О. Л. Кваліфікаційна робота: методичні вказівки до виконання кваліфікаційної роботи бакалавра для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні

технології спеціальності 126 Інформаційні системи та технології денної та заочної форм навчання. Луцьк: ЛНТУ, 2025. 53 с.

26. ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання». URL: https://nv-oneu.com.ua/downloads/dstu-8302-2015.pdf (дата звернення: 20.05.26).

27. ДСТУ 3008:2015 «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення». URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=64463 (дата звернення: 20.05.26).