Міністерство освіти і науки України

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

КВАЛІФІКАЦІЙНА РОБОТА
ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

ПРОЕКТУВАННЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ МАР'ЯНІВСЬКОГО ЛІЦЕЮ №2 ВОЛИНСЬКОЇ ОБЛАСТІ

DESIGN OF A VIDEO SURVEILLANCE SYSTEM FOR MARYANIV LYCEUM NO. 2, VOLYN REGION

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
Філярчук Володимир Ігорович
_____
(підпис)

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

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

Луцьк – 2026 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри КІБ
к.т.н., доцент Терлецький Т. В.
_____
«___» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Філярчуку Володимиру Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: *Проектування системи відеоспостереження Мар'янівського ліцею №2 Волинської області*

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

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

3. Вихідні дані до роботи: *Планувальне рішення будівлі школи та прилеглої території. Нормативні документи: ДСТУ EN 62676, ДСТУ EN 62676-1-1, ДСТУ EN 62676-4:2014, ДСТУ EN 50136-1, ДСТУ IEC60529, ДБН В.2.2-3:2018*

4. Зміст розрахунково-пояснювальної записки (перелік питань, що потрібно розробити): Розділ 1. Аналітичний огляд стану предметної області (техніко-економічна характеристика об'єкта; аналіз загроз та визначення зон підвищеного контролю; порівняльний аналіз архітектурних рішень систем відеоспостереження; огляд нормативно-правової бази та державних стандартів України); Розділ 2. Обґрунтування вибору засобів та методів реалізації (розробка концептуальної схеми та топології системи; розрахунок зон огляду, роздільної здатності та місць встановлення камер; обґрунтування та вибір апаратного забезпечення; розрахунок ємності сховища даних та пропускної здатності мережі); Розділ 3. Практична реалізація (схема підключення та інтеграції компонентів системи відеоспостереження в локальну мережу школи; забезпечення надійності та інформаційної безпеки). Список використаних джерел. Додатки.

5. Перелік графічного (ілюстративного) матеріалу: *Презентація на 12 слайдах*

6. Консультанти розділів роботи

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

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

КАЛЕНДАРНИЙ ПЛАН

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

Здобувач вищої освіти _____ (Філярчук В.І)
(підпис)

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

АНОТАЦІЯ

Філярчук В. І. Проектування системи відеоспостереження Мар’янівського ліцею №2 Волинської області. Рукопис.

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

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

У кваліфікаційній роботі досліджено особливості проектування та впровадження комплексної системи відеоспостереження для Мар’янівського ліцею №2 Волинської області з метою підвищення рівня безпеки навчального закладу. Проаналізовано техніко-економічні характеристики об’єкта, потенційні загрози та зони підвищеного контролю, а також проведено порівняльний аналіз сучасних архітектурних рішень і чинної нормативно-правової бази України щодо освітніх установ. Розроблено концептуальну схему та топологію системи, здійснено розрахунок зон огляду, роздільної здатності, місць встановлення відеокамер, необхідної пропускної здатності локальної мережі та ємності системи збереження даних. Обґрунтовано вибір сучасного апаратного та програмного забезпечення, представлено схему інтеграції компонентів у локальну мережу школи, а також визначено заходи щодо забезпечення надійності та інформаційної безпеки системи.

Ключові слова: система відеоспостереження, проектування безпекових систем, освітній заклад, топологія мережі, камери відеоспостереження, збереження даних, інформаційна безпека.

ANNOTATION

Filiarchuk V. Design of a video surveillance system for Maryaniv Lyceum No. 2, Volyn region. Manuscript.

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

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

The qualification paper investigates the features of designing and implementing an integrated video surveillance system for Marianivka Lyceum No. 2 of the Volyn Region to enhance the security level of the educational institution. The study analyzes the technical and economic characteristics of the facility, potential threats, and high-control zones, and provides a comparative analysis of modern architectural solutions and the current regulatory framework of Ukraine regarding educational institutions. A conceptual diagram and system topology have been developed; calculations for viewing zones, resolution, camera placement, required local network bandwidth, and data storage capacity have been performed. The choice of modern hardware and software is justified, a diagram for integrating components into the school's local area network is presented, and measures to ensure system reliability and information security are defined.

Keywords: video surveillance system, security system design, educational institution, network topology, CCTV cameras, data storage, information security.

ЗМІСТ

ВСТУП

Забезпечення безпечного середовища в закладах загальної середньої освіти є одним із пріоритетних завдань державної політики України в галузі освіти та національної безпеки. Сучасні заклади освіти стикаються з комплексом внутрішніх і зовнішніх загроз – від антропогенних чинників до ризиків техногенного й інформаційного характеру. Традиційні методи охорони та застарілі аналогові системи спостереження вже не здатні забезпечити оперативне реагування на інциденти, оскільки мають обмежену роздільну здатність, незахищені кабельні траси та позбавлені інструментів автоматизованого аналізу подій.

Ефективним розв’язанням цієї проблеми є впровадження та модернізація систем відеоспостереження на базі цифрових IP-технологій. Сучасні IP-архітектури, які функціонують у межах локальних обчислювальних мереж із використанням технології PoE, дозволяють отримувати високодеталізоване зображення, масштабувати систему без перебудови базової інфраструктури та інтегрувати інтелектуальну відеоаналітику. Це дає змогу мінімізувати вплив людського чинника та створити проактивне середовище безпеки.

Об’єкт дослідження – комплексна система безпеки та інженерно-технічна інфраструктура закладу загальної середньої освіти (на прикладі будівлі Мар’янівської ЗОШ І-ІІІ ступенів).

Предмет дослідження – архітектурні рішення, методи проектування, алгоритми функціонування та налаштування цифрових IP-систем відеоспостереження, а також інтеграція засобів відеоаналітики та інформаційної безпеки в локальну мережу навчального закладу.

Метою кваліфікаційної роботи є обґрунтування технічних рішень та розробка проєкту модернізації системи відеоспостереження освітнього закладу шляхом переходу на цифрову IP-архітектуру для підвищення загального рівня безпеки, забезпечення прецизійного моніторингу зон підвищеного ризику та захисту інформаційних ресурсів установи.

РОЗДІЛ 1
АНАЛІТИЧНИЙ ОГЛЯД СТАНУ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Техніко-економічна характеристика об’єкта

Успішне проєктування та впровадження сучасної цифрової системи відеоспостереження (СВН) вимагає детального аналізу архітектурно-планувальних рішень, специфіки функціонування, режиму роботи та наявної інженерної інфраструктури об’єкта захисту [1-3]. У даному дипломному проєкті об’єктом модернізації є Мар’янівська загальноосвітня школа І-ІІІ ступенів – типовий закладу загальної середньої освіти, що характеризується високою концентрацією людей у визначені проміжки часу та наявністю кількох зон із підвищеними вимогами до безпеки.

1.1.1 Архітектурно-планувальні та конструктивні особливості будівлі

Об’єкт являє собою капітальну багатоповерхову будівлю (основні поверхи (рис. 1.1-1.3), підвальні приміщення (рис. 1.4) та технічний горищний поверх), зведену за типовим проєктом із залізобетонних панелей та цегли. Загальна внутрішня площа об’єкта та конфігурація приміщень вимагають зонування системи відеонагляду на внутрішній (локальний) та зовнішній (периметральний) контури.

Головними архітектурними елементами об’єкта, що безпосередньо впливають на топологію мережі та розстановку камер, є:

– вхідна група та вестибюль: головний вхід, обладнаний тамбуром, є основною точкою розмежування доступу, де фіксується найбільший потік учнів, персоналу та відвідувачів у ранкові та вечірні години;

– коридори та розгалуження (1-й та 2-й поверхи): мають лінійну протяжну структуру з виходами на сходові клітки та евакуаційні шляхи. Довжина коридорів зумовлює необхідність використання довгофокусних камер або зустрічного розташування оптичних пристроїв для уникнення «сліпих зон»;

– харчоблок та їдальня: зона підвищеного матеріально-технічного контролю та санітарно-епідеміологічного нагляду. Специфіка приміщень

харчоблоку – підвищена вологість та коливання температур, що вимагає від обладнання високого класу захисту від вологи та пилу (не нижче IP66/IP67);

– спортивний зал: окремий масштабний блок у структурі будівлі площею 477 м² з високою стелею. Особливістю цієї локації є підвищений ризик травматизму, висока динаміка руху та загроза механічного пошкодження обладнання, що вимагає встановлення відеокамер у спеціальних антивандальних захисних кожухах (клас захисту IK10);

– підвальні приміщення: використовуються як інженерні вузли (введення комунікацій, водомірні та теплові вузли), а також частково адаптовані під найпростіші укриття для цивільного захисту, що робить їх об’єктами критичного контролю у сучасному безпековому контексті;

– прилегла територія та периметр: включає внутрішній двір, під’їзні шляхи для автотранспорту, спортивний майданчик та зони відпочинку. Периметр обмежений парканом, проте має кілька точок потенційного несанкціонованого проникнення.

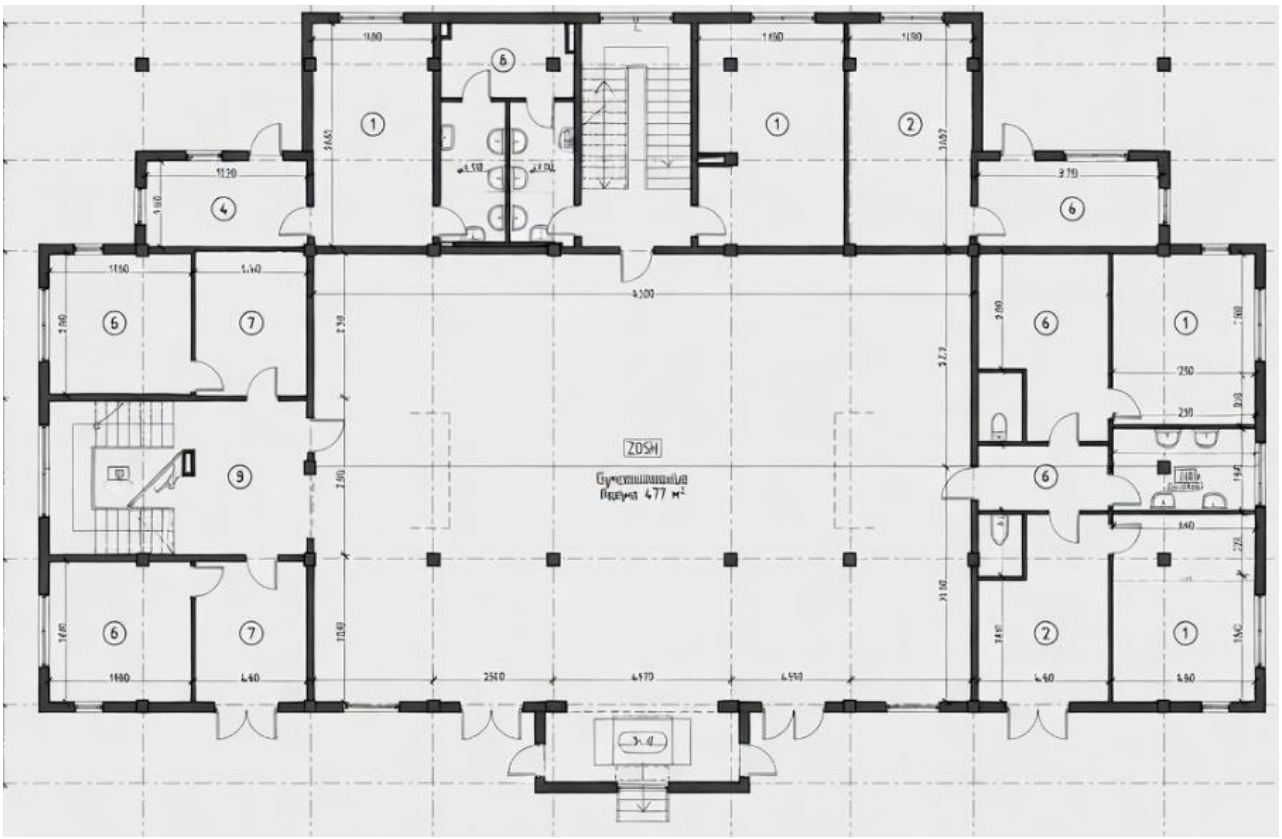

Рисунок 1.1 – Плану 1-го поверху

Рисунок 1.2 – План 2-го поверху

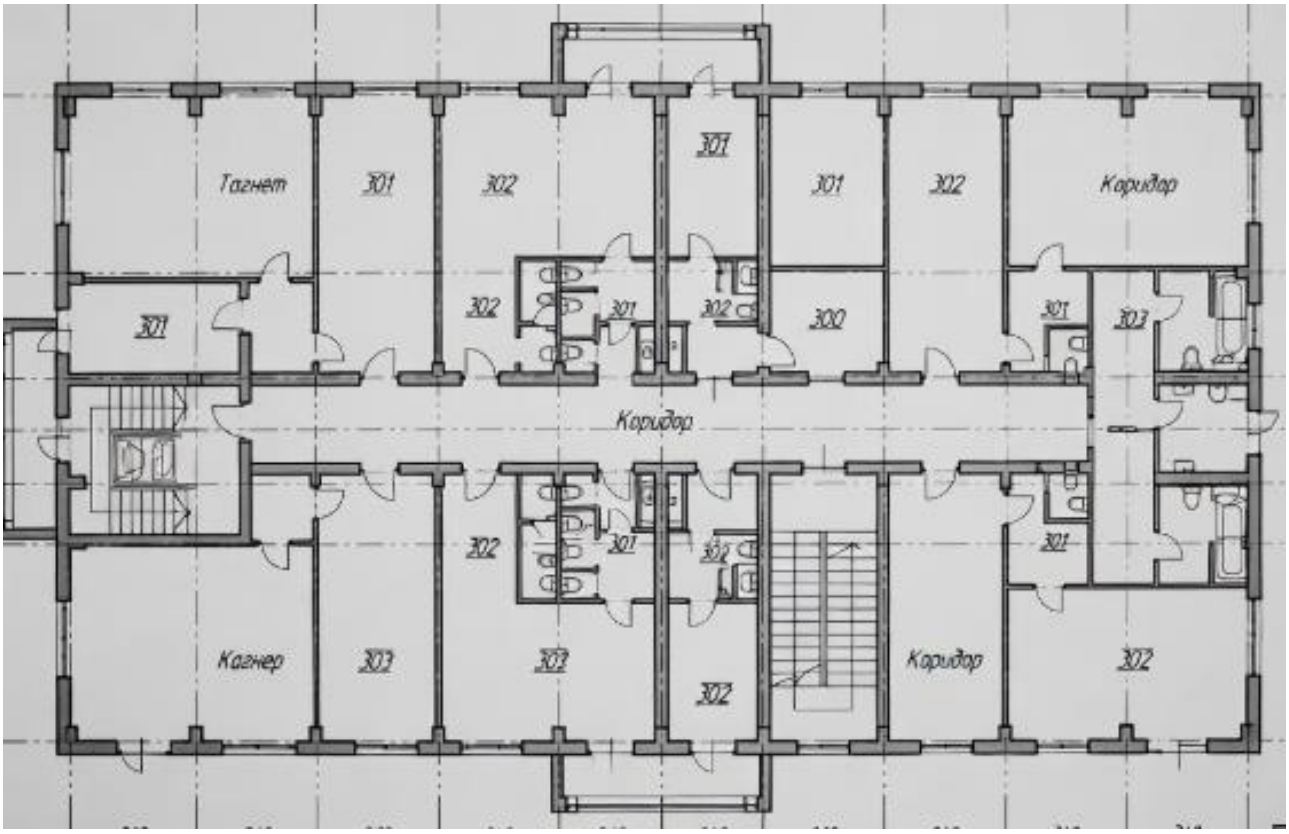

Рисунок 1.3 – План 3-го поверху

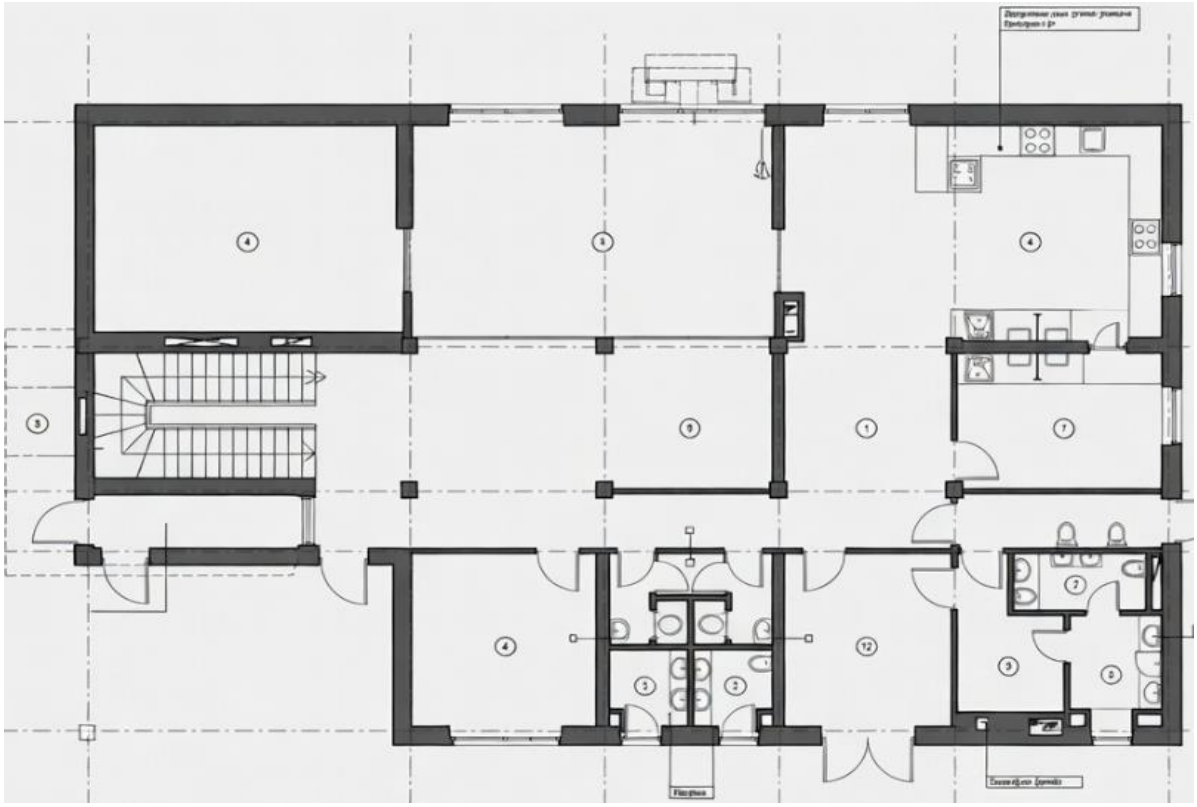

Рисунок 1.4 – План підвалу

1.1.2 Функціонально-організаційні характеристики об’єкта

Режим роботи об’єкта проекьування є циклічним та поділяється на кілька фаз:

– активна фаза (07:30-18:00): максимальне навантаження на інфраструктуру, масове перебування дітей (від 6 до 17 років), вчителів та технічного персоналу. У цей період СВН виконує функцію оперативного моніторингу громадського порядку, запобігання конфліктним ситуаціям, контролю за сторонніми особами та превенції правопорушень;

– пасивна фаза (18:00-07:30) та вихідні/святкові дні: будівля перебуває під охороною чергового персоналу. У цей час СВН переходить у режим детекції руху (відеоаналітика) для фіксації спроб проникнення на територію чи всередину будівлі, крадіжок або виникнення аварійних ситуацій (задимлення, затоплення).

1.1.3 Наявна інженерно-технічна інфраструктура

На момент аналізу в закладі функціонує морально та фізично застаріла аналогова система відеоспостереження, яка має низку суттєвих недоліків:

– низька роздільна здатність (не дозволяє ідентифікувати обличчя людей на відстані понад 3-5 метрів);

– аналогові коаксіальні кабелі мають високий рівень загасання сигналу та чутливі до електромагнітних завад від силових ліній 220/380 В;

– відсутність централізованого архівування з глибоким резервуванням та засобів інтелектуального пошуку в архіві;

– вразливість кабельних трас до навмисного пошкодження.

Електропостачання будівлі здійснюється від промислової мережі за III категорією надійності, що для цифрової системи безпеки є недопустимим. Нова IP-система повинна проєктуватися із застосуванням джерел безперебійного живлення (ДБН В.2.5-56:2014) для забезпечення автономної роботи камер та серверного обладнання протягом мінімум 0,5-2 годин у разі знеструмлення об’єкта.

1.1.4 Економічне обґрунтування модернізації

З економічного погляду, повна заміна застарілої системи на сучасну IP-архітектуру є доцільнішою, ніж постійні витрати на ремонт аналогового обладнання. Впровадження технології PoE (Power over Ethernet) дозволяє передавати інформаційний сигнал і живлення камери по одному кабелю «вита пара» (UTP Cat 5e/6), що вдвічі знижує витрати на кабельну продукцію та монтажні роботи.

Використання сучасних кодеків стиснення (H.265/H.265+) мінімізує витрати на купівлю жорстких дисків (HDD) для сервера, оскільки обсяг трафіку знижується на 40-50% без втрати якості зображення [4, 5]. Окрім того, автоматизація процесу охорони за допомогою відеоаналітики зменшує навантаження на персонал охорони та знижує ризик фінансових збитків від актів вандалізму чи крадіжок майна громади.

Таким чином, Мар’янівська ЗОШ І-ІІІ ступенів є складним об’єктом для проєктування СВН, що вимагає комплексного підходу: від врахування агресивного середовища харчоблоку та специфіки спортзалу (477 м²) до побудови захищеної від завад і збоїв локальної обчислювальної мережі.

1.2 Аналіз потенційних загроз безпеці навчального закладу та визначення зон підвищеного контролю

На основі аналізу планувальних рішень будівлі загальноосвітньої школи (літера А-3) та її інженерної інфраструктури виділено основні категорії загроз і визначено зони, які потребують підвищеної уваги при проектуванні систем безпеки та моніторингу.

Для закладу освіти найбільш значущими є три основні групи загроз, які впливають на безпеку учнів, персоналу та стабільність роботи установи.

Антропогенні загрози пов’язані з умисними або необережними діями людей, що порушують нормальне функціонування навчального закладу. Найчастіше це несанкціоноване проникнення сторонніх осіб на територію або всередину будівлі. Такі випадки можуть бути як випадковими, коли відсутній належний контроль доступу, так і навмисними – з метою порушення порядку або отримання доступу до приміщень чи матеріальних цінностей [6, 7].

До цієї групи також належать акти вандалізму, які проявляються у свідомому пошкодженні майна: меблів, технічного обладнання, елементів будівлі або систем безпеки. Це призводить не лише до фінансових втрат, а й до перебоїв у навчальному процесі та загального зниження рівня безпеки.

Окремо слід виділити крадіжки, зокрема комп’ютерної техніки, мультимедійного обладнання та іншого цінного майна. Найбільш уразливими є комп’ютерні класи, лабораторії та спортивні приміщення, де зосереджене дороге або мобільне обладнання. Причинами таких інцидентів зазвичай є слабкий контроль доступу, відсутність відеоспостереження або недостатній фізичний захист приміщень.

До найбільш критичних антропогенних загроз належать потенційні терористичні дії, які можуть створювати небезпеку для життя та здоров’я людей і призводити до дестабілізації роботи закладу. Хоча ймовірність таких випадків невисока, їх наслідки є надзвичайно серйозними, тому потрібні системи контролю доступу, відеоспостереження та швидкого реагування.

У цілому ці загрози формують основу для побудови багаторівневої системи безпеки, що поєднує технічні засоби, організаційні заходи та чітко регламентовані правила доступу.

Техногенні загрози пов’язані з відмовами інженерних систем або аваріями, що виникають під час експлуатації обладнання [8-10]. Однією з найнебезпечніших є пожежа, яка може виникнути через перевантаження електромережі, коротке замикання або несправність електроприладів. Найбільш ризиковими зонами є харчоблок, електрощитова та котельня, де розміщене нагрівальне обладнання. Також суттєву небезпеку становлять аварії систем водопостачання та опалення. Прорив труб або вихід з ладу обладнання може спричинити затоплення приміщень і пошкодження техніки. Відмова системи опалення, у свою чергу, призводить до зниження температури в будівлі, що ускладнює навчальний процес або навіть може його призупинити.

Таким чином, техногенні загрози мають високий потенціал матеріальних втрат і впливають на безперервність роботи закладу, тому потребують системраннього виявлення – пожежної сигналізації, датчиків протікання та моніторингу інженерних мереж.

Класифікація функціональних зон об’єкта та заходи контролю безпеки подана в таблиці 1.1.

Таблиця 1.1 – Матриця функціональних зон об’єкта та їх контролю

Категорія зони	Приміщення (згідно з планом)	Необхідні заходи контролю
Периметр та входи	Тамбури (16, 29, 56), центральний та запасні входи	Відеоспостереження, система контролю доступу (СКД)
Життєзабезпечення	Котельня (Б-1), електрощитова (10), підвал	Датчики диму, затоплення, датчики відкриття дверей
Адміністративно-фінансова	Кабінет директора (23), вчительська (24)	Охоронна сигналізація, обмеження доступу
Зони масового скупчення	Спортзал (53), їдальня (3), коридори (2, 21, 35, 52, 58)	Панорамне відеоспостереження, системи оповіщення
Технологічна	Кабінет інформатики (51), книгосховище (32)	Моніторинг мережевої активності, пожежна сигналізація

Інформаційні загрози стосуються порушення конфіденційності, цілісності та доступності даних, що обробляються в інформаційних системах школи.

Основною проблемою є несанкціонований доступ до локальної мережі, серверів або робочих станцій. Це може відбуватися як через зовнішні атаки, так і через внутрішні порушення при недостатньому розмежуванні прав доступу.

Особливо чутливими є бази даних учнів, які містять персональну інформацію, а також адміністративні та фінансові дані. Їх витік або пошкодження може призвести до юридичних наслідків, порушення законодавства про захист персональних даних і втрати довіри до закладу.

Найбільш вразливими є кабінет інформатики та адміністративні підрозділи, де зосереджені комп'ютерні системи та мережеве обладнання. Основні ризики пов'язані з використанням шкідливого програмного забезпечення, підбором паролів, експлуатацією вразливостей або методами соціальної інженерії.

Для зниження цих ризиків необхідно впроваджувати комплексний підхід: розмежування доступу, використання фаєрволів та систем виявлення вторгнень, регулярне резервне копіювання та постійний моніторинг активності в мережі.

Відповідно до експлікації приміщень, будівля закладу освіти поділяється на функціональні зони з різним рівнем критичності, який визначається їх призначенням, кількістю відвідувачів, наявністю матеріальних цінностей та можливими наслідками реалізації загроз.

Відповідно до аналізу планувальних рішень будівлі, найбільш критичними зонами з точки зору безпеки є підвальні приміщення, перший поверх, а також другий і третій поверхи.

Підвальні приміщення характеризуються підвищеним ризиком підтоплення та виникнення пожеж у зв'язку з розташуванням у них кухні та декількох складських приміщень. У цій зоні доцільно передбачити встановлення інтелектуальних аналізаторів середовища для раннього виявлення аварійних ситуацій.

Перший поверх є найбільш вразливим до несанкціонованого проникнення через велику кількість вхідних груп і вікон. Особливу увагу слід приділити спортивному залу площею 477 м², де рекомендується застосування системи

відеоспостереження з високою роздільною здатністю для повного виключення сліпих зон.

На другому та третьому поверхах, де зосереджена основна маса навчальних класів, головним пріоритетом є забезпечення швидкої та безпечної евакуації в разі надзвичайних ситуацій. Критичним елементом тут є постійний контроль стану сходових кліток з метою недопущення їх захаращення та підтримання прохідності.

1.3 Порівняльний аналіз архітектурних рішень сучасних систем відеоспостереження

Вибір архітектури системи відеоспостереження (CCTV) є одним із визначальних етапів проєктування комплексної системи безпеки, оскільки саме архітектурне рішення впливає на ефективність функціонування системи, можливість її подальшого розширення, рівень надійності та витрати на технічне обслуговування. Від правильно обраної структури залежить якість передачі відеоданих, стабільність роботи обладнання, швидкість доступу до архівів та інтеграція із суміжними системами безпеки.

На сучасному етапі розвитку систем відеоспостереження найбільш поширеними є три основні архітектурні підходи: аналогові системи, цифрові IP-системи та гібридні рішення. Кожен із цих варіантів має власні технічні особливості, переваги та обмеження, що визначають доцільність їх застосування залежно від масштабів об’єкта, вимог до якості відеозображення та бюджету проєкту.

Аналогові системи відеоспостереження є традиційним рішенням, у якому передача відеосигналу здійснюється коаксіальними кабелями до відеореєстратора. Основною перевагою таких систем є відносно низька вартість обладнання та простота монтажу. Водночас вони мають обмеження щодо роздільної здатності, масштабованості та можливостей інтеграції із сучасними цифровими сервісами.

IP-системи відеоспостереження базуються на використанні цифрових мереж передачі даних та IP-камер, які передають відеопотік через локальну мережу або мережу Інтернет. Такі системи забезпечують високу якість зображення, підтримують інтелектуальну аналітику, віддалений доступ, гнучке масштабування та інтеграцію з іншими компонентами системи безпеки. Саме IP-архітектура нині вважається найбільш перспективною для закладів освіти завдяки можливості централізованого керування та високому рівню функціональності [11-14].

Гібридні системи поєднують елементи аналогових та IP-рішень і використовуються переважно під час модернізації існуючих систем безпеки. Вони дозволяють поступово переходити до цифрової інфраструктури без повної заміни наявного обладнання, що дає змогу оптимізувати фінансові витрати та забезпечити сумісність різних поколінь технічних засобів.

Модернізовані аналогові системи відеоспостереження є розвитком класичних CCTV-рішень та передбачають передачу відеосигналу високої роздільної здатності через коаксіальні кабельні лінії. Сучасні технології, такі як AHD, HD-TVI та HD-CVI, дозволяють забезпечувати якість зображення до формату 4K без необхідності повного переходу на IP-інфраструктуру. Це робить подібні системи актуальними для модернізації вже існуючих аналогових мереж відеоспостереження.

Модернізовані аналогові системи відеоспостереження залишаються досить поширеним рішенням, насамперед через свою відносно невисоку вартість як обладнання, так і монтажу. Особливо це помітно у випадках, коли на об’єкті вже прокладена коаксіальна кабельна інфраструктура – тоді витрати на впровадження системи суттєво зменшуються. Такі системи також приваблюють простотою налаштування та експлуатації, оскільки не потребують складного мережевого адміністрування і працюють за більш традиційним принципом передачі відеосигналу.

Разом із тим вони мають і суттєві обмеження. Найбільш очевидне – це необхідність прокладання окремого кабелю до кожної камери, що створює

труднощі при монтажі у великих або багатоповерхових будівлях і збільшує загальну складність системи. У результаті розширення такої мережі стає менш зручним і більш затратним. Крім того, модернізовані аналогові системи досить слабо інтегруються із сучасними інструментами відеоаналітики. У більшості випадків їх функціонал обмежується базовим записом і переглядом відео, тоді як більш складні функції, такі як розпізнавання облич або автоматичне виявлення інцидентів, реалізуються або частково, або взагалі відсутні.

IP-системи відеоспостереження, навпаки, є більш сучасним і функціонально розвиненим рішенням. Вони працюють на основі локальних мереж передачі даних, де кожна камера є окремим мережевим пристроєм із власною IP-адресою. Така архітектура дозволяє отримувати відео високої якості та забезпечує значно кращу деталізацію зображення, що особливо важливо для контролю входів, коридорів та прилеглих територій навчальних закладів.

Однією з ключових переваг IP-систем є використання технології PoE (Power over Ethernet), яка дозволяє передавати живлення та дані одним кабелем. Це значно спрощує монтаж, зменшує кількість проводки та загалом робить систему більш акуратною та економічною в обслуговуванні. Також такі системи легко масштабуються – додавання нових камер або серверів не потребує кардинальної перебудови всієї інфраструктури. Окремо варто відзначити можливість інтеграції з іншими системами безпеки, такими як контроль доступу, пожежна сигналізація або системи оповіщення.

Іншою важливою перевагою є підтримка інтелектуальної відеоаналітики. Сучасні IP-системи можуть виконувати детекцію руху, розпізнавання облич, контроль периметра та навіть аналіз поведінки, що значно підвищує рівень безпеки та зменшує навантаження на операторів. Водночас до недоліків таких систем можна віднести вищу вартість обладнання та підвищені вимоги до мережевої інфраструктури, оскільки передача великої кількості відеопотоків високої роздільної здатності створює значне навантаження на мережу.

Хмарні (cloud) системи відеоспостереження є ще більш сучасним підходом, де зберігання та обробка відеоданих здійснюється на віддалених

серверах [15, 16]. У цьому випадку відео передається через інтернет до дата-центрів, де відбувається його зберігання та обробка. Часто використовується і гібридний варіант, коли основні дані зберігаються локально, а резервні копії дублюються у хмарі.

Головною перевагою таких систем є можливість віддаленого доступу – користувач може переглядати відео та керувати системою з будь-якого місця через інтернет без складних налаштувань. Крім того, хмарні рішення забезпечують високу відмовостійкість: навіть у разі пошкодження або втрати локального обладнання відеоархів залишається збереженим. Також такі системи добре масштабуються, дозволяючи швидко додавати камери або збільшувати обсяг зберігання без серйозної модернізації інфраструктури.

Результати порівняльного аналізу архітектурних рішень [11-16] подано в таблиці 1.2.

Таблиця 1.2 – Порівняльна таблиця архітектурних рішень

Параметр порівняння	Аналогова (AHD)	Цифрова (IP)	Хмарна (VSaaS)
Якість зображення	Середня/Висока	Дуже висока	Висока (залежить від каналу)
Складність монтажу	Висока (окремий кабель до кожної камери)	Середня (використання комутаторів)	Низька
Можливості аналітики	Базові (на рівні реєстратора)	Просунуті (на борту камери)	Високі (серверні алгоритми)
Масштабованість	Обмежена кількістю портів реєстратора	Майже необмежена	Висока
Рекомендація для школи	Не рекомендується	Оптимально для локального моніторингу	Як додатковий бекап

Водночас є і певні недоліки. Основний з них – залежність від стабільного інтернет-з’єднання, оскільки перебої можуть впливати на доступ до відео або швидкість передачі даних. Крім того, використання хмарних сервісів зазвичай передбачає регулярні абонентські витрати, що в довгостроковій перспективі може збільшувати загальну вартість системи.

Разом із тим використання хмарних технологій має і певні недоліки. Основним обмеженням є залежність від стабільності та пропускної здатності

інтернет-каналу. У разі перебоїв зв’язку можуть виникати затримки передачі відеоданих або тимчасова недоступність віддаленого архіву. Особливо критичним це є для систем із великою кількістю камер високої роздільної здатності, які генерують значний мережевий трафік.

Додатковим фактором є наявність регулярної абонентської плати за використання хмарних сервісів, яка залежить від обсягу збережених даних, кількості камер та доступних функцій аналітики. У довгостроковій перспективі це може збільшувати експлуатаційні витрати порівняно з локальними системами зберігання.

Для загальноосвітньої школи І-ІІІ ступенів у смт Мар’янівка найбільш доцільним рішенням є впровадження цифрової IP-архітектури системи відеоспостереження. Такий вибір обумовлений кількома ключовими перевагами. По-перше, IP-система дозволяє ефективно використовувати існуючу або проектовану локальну обчислювальну мережу закладу, що суттєво знижує витрати на монтаж додаткових комунікацій. По-друге, вона забезпечує високу роздільну здатність зображення, необхідну для надійної ідентифікації облич учнів і відвідувачів. По-третє, сучасні IP-камери підтримують розвинені функції інтелектуальної відеоаналітики, зокрема детекцію залишених предметів, контроль перетину віртуальних ліній у зонах підвищеного ризику та інші аналітичні модулі.

1.4 Огляд нормативно-правової бази та державних стандартів щодо встановлення систем відеоспостереження в освітніх установах України

Проектування та експлуатація систем відеоспостереження у закладах загальної середньої освіти регулюється комплексом законодавчих актів, що визначають технічні вимоги, правила збереження даних та захист конституційних прав громадян.

Законодавчі акти загальної дії:

– Конституція України (ст. 32): гарантує невтручання в особисте життя. Відеозйомка в школі можлива лише з метою гарантування публічної безпеки;

– цивільний кодекс України (ст. 307): регламентує захист інтересів фізичної особи при проведенні фото-, кіно-, теле- та відеозйомок. Згідно з кодексом, зйомка у громадських місцях (яким є школа) є допустимою, проте потребує відкритості (наявність попереджувальних табличок);

– закон України «Про захист персональних даних»: визначає відеозображення особи як персональні дані. Це накладає зобов'язання щодо суворого обмеження доступу до архівів та визначення відповідальних осіб.

Основна нормативно-правова база [17-20] та технічні стандарти у сфері проектування систем відеоспостереження зведені до таблиці 1.3.

Таблиця 1.3 – Нормативно-правові та технічні документи, що регулюють проєктування систем відеоспостереження

Документ	Сфера регулювання	Примітка для проекту
ЗУ «Про освіту»	Забезпечення безпечного середовища	Фундамент для встановлення СВН
ДСТУ EN 62676-4	Настанови щодо вибору пристроїв	Вибір роздільної здатності камер
Лист МОН № 1/9-40	Безпека в освітніх закладах	Рекомендації щодо комплексного захисту

При розробці технічної частини проекту необхідно керуватися наступними стандартами:

– ДСТУ EN 62676 «Системи відеоспостереження охоронного призначення»: основний стандарт, що визначає технічні вимоги до систем відеоспостереження для використання у сфері безпеки.

– ДБН В.2.2-3:2018 «Будинки і споруди. Заклади освіти»: містить вимоги до інженерного обладнання шкіл, зокрема в контексті антитерористичних заходів та безпеки середовища.

– ДБН В.2.5-56:2014 «Системи протипожежного захисту»: регулює інтеграцію відеоспостереження з системами автоматичного пожежогасіння та оповіщення.

Окрім загальнодержавних нормативно-правових актів і технічних стандартів, важливу роль у процесі впровадження та експлуатації систем відеоспостереження в закладах загальної середньої освіти відіграє локальне регулювання. Саме внутрішні організаційні документи визначають порядок практичного використання системи відеоспостереження, регламентують права та обов'язки відповідальних осіб, а також забезпечують дотримання етичних норм і прав учасників освітнього процесу.

На рівні закладу освіти зазвичай формуються положення про систему відеоспостереження, інструкції для персоналу та регламенти доступу до відеоматеріалів. У цих документах чітко визначається, хто має право перегляду записів, за яких умов вони можуть використовуватися, а також порядок їх зберігання і видалення. Окрему увагу приділяють обмеженню доступу до архівів з метою запобігання несанкціонованому використанню персональних даних учнів та працівників.

Важливим аспектом локального регулювання є також визначення зон відеоспостереження. Як правило, камери встановлюються у місцях загального користування (коридори, входи/виходи, подвір'я), тоді як простори, пов'язані з приватністю (роздягальні, санітарні кімнати), не підлягають відеофіксації. Такі обмеження закріплюються внутрішніми наказами адміністрації та узгоджуються з вимогами чинного законодавства щодо захисту персональних даних.

Окремо регламентується питання інформування учасників освітнього процесу про наявність системи відеоспостереження. Це може реалізовуватися через інформаційні таблички, стенди або внутрішні повідомлення, що забезпечує принцип відкритості та прозорості використання таких систем. Крім того, у локальних документах часто передбачаються процедури реагування на інциденти, виявлені за допомогою відеоспостереження, включно з порядком передачі інформації адміністрації або відповідним службам.

Ключовим документом локального рівня є наказ директора закладу освіти про впровадження системи відеоспостереження. У такому наказі визначається правова підстава встановлення системи, основна мета її використання, перелік

зон моніторингу та відповідальні особи, які мають право доступу до відеоархівів. Для закладів освіти головною метою впровадження СВН є забезпечення безпеки учнів, педагогічного персоналу та матеріальних цінностей, а також запобігання надзвичайним ситуаціям і правопорушенням.

У наказі також повинні бути чітко визначені місця встановлення камер відеоспостереження. Як правило, камери розміщуються на входах до будівлі, у коридорах, на сходових клітках, у місцях масового перебування людей, біля евакуаційних виходів, на території подвір'я та в інших критично важливих зонах об'єкта. При цьому обов'язково враховується принцип пропорційності між рівнем безпеки та правом людини на приватність.

Окремо регламентуються терміни зберігання відеозаписів, які є одним із ключових параметрів організації роботи системи відеоспостереження. У більшості випадків для закладів освіти рекомендований період зберігання становить від 14 до 30 діб, що вважається достатнім для виявлення та аналізу можливих інцидентів, після чого дані автоматично видаляються або перезаписуються в процесі циклічного оновлення архіву.

Тривалість архівації визначається комплексно та залежить від кількох факторів, зокрема технічних можливостей системи зберігання, обсягу доступного дискового простору, налаштувань якості відеозапису (роздільна здатність, частота кадрів, ступінь компресії), а також внутрішніх вимог безпеки конкретного закладу освіти. У деяких випадках, за наявності підвищених вимог до безпеки, термін зберігання може бути збільшений, однак це повинно бути належним чином обґрунтовано та закріплено у внутрішніх регламентуючих документах.

Доступ до архівів відеозаписів повинен бути чітко регламентований і максимально обмежений з метою забезпечення конфіденційності та захисту персональних даних. Як правило, такий доступ надається виключно уповноваженим особам, до яких належать керівник закладу освіти, системний адміністратор або відповідальний за технічне обслуговування системи, а також, у разі потреби, представники служби безпеки. Усі операції перегляду, копіювання

або експорту відеоматеріалів мають фіксуватися в журналі подій для забезпечення контролю та запобігання несанкціонованому використанню даних.

Важливим елементом локального регулювання є положення про відеоспостереження – внутрішній нормативний документ, що розробляється безпосередньо для конкретного закладу освіти. У випадку Мар'янівської ЗОШ такий документ визначає порядок функціонування системи відеоспостереження, правила обробки та зберігання відеоінформації, процедури доступу до записів, а також механізми захисту персональних даних учасників освітнього процесу.

Крім того, положення встановлює відповідальних осіб за технічне супроводження системи, регламентує їхні повноваження та зони відповідальності, а також описує порядок реагування на нештатні ситуації або виявлені інциденти безпеки. Окремо можуть визначатися процедури ведення журналу доступу до архівних матеріалів і контролю за використанням відеоданих, що дозволяє забезпечити прозорість та підзвітність усіх операцій із системою.

Положення про відеоспостереження обов'язково узгоджується з адміністрацією закладу, трудовим колективом та представниками батьківського комітету, що сприяє врахуванню інтересів усіх учасників освітнього процесу. Такий підхід забезпечує баланс між вимогами безпеки, правом на приватність і принципами відкритості, а також підвищує рівень довіри до впровадженої системи відеонагляду в межах закладу освіти.

Особлива увага при впровадженні СВН приділяється дотриманню етичних норм та прав людини. Відеоспостереження не повинно створювати умов для надмірного контролю або психологічного дискомфорту учнів і працівників. Саме тому законодавством та внутрішніми документами визначено перелік зон, у яких встановлення камер категорично заборонене. До таких зон належать туалетні кімнати, роздягальні, душові приміщення, медичні кабінети та інші приміщення, де людина має право на приватність і конфіденційність.

Не менш важливою вимогою є обов'язкове інформування про здійснення відеоспостереження, яке розглядається як один із базових принципів прозорого

та законного функціонування систем безпеки. На всіх входах до будівлі, по периметру території закладу, а також у зонах безпосереднього розміщення камер повинні бути встановлені інформаційні таблички або попереджувальні знаки з чітким повідомленням «Ведеться відеоспостереження».

Такі позначення виконують не лише інформативну, але й превентивну функцію, оскільки завчасно повідомляють відвідувачів, працівників і здобувачів освіти про факт здійснення відеоконтролю. Це сприяє підвищенню дисципліни, зменшенню ризику порушень громадського порядку та формуванню усвідомленого ставлення до правил поведінки на території закладу.

Крім того, належне інформування є важливою складовою дотримання вимог законодавства у сфері захисту персональних даних, оскільки забезпечує принцип відкритості та прозорості обробки інформації. У комплексі з іншими організаційними та технічними заходами це дозволяє сформувати правомірну та соціально прийнятну модель використання систем відеоспостереження в освітньому середовищі.

Додатково локальні нормативні документи визначають порядок реагування на інциденти, правила передачі відеоматеріалів правоохоронним органам, вимоги до резервного копіювання даних та відповідальність осіб за неправомірне використання інформації. Це дозволяє забезпечити не лише технічну ефективність системи, а й правомірність її експлуатації в освітньому середовищі.

Отож, нормативне забезпечення СВН у закладах освіти формує комплексну систему вимог, яка поєднує правові, технічні та організаційні аспекти та спрямована на забезпечення безпеки учасників освітнього процесу при одночасному дотриманні їхніх конституційних прав.

Комплексний підхід до організації відеоспостереження дозволяє підвищити рівень безпеки учнів, педагогічного персоналу та матеріальних цінностей закладу, забезпечити оперативне реагування на надзвичайні ситуації, а також мінімізувати ризики несанкціонованого доступу, правопорушень і техногенних інцидентів. Водночас важливим принципом залишається дотримання конституційних прав людини, зокрема права на приватність, захист

персональних даних та недопущення надмірного контролю в освітньому середовищі.

1.5 Постановка завдань на кваліфікаційну роботу бакалавра

Проектування та модернізація систем відеоспостереження на базі цифрових IP-технологій вимагає суворого дотримання балансу між підвищенням рівня захищеності об’єкта та збереженням конституційних прав громадян на приватність, що регламентується чинним законодавством України (Конституція України, Закон України «Про захист персональних даних», стандарти серії ДСТУ EN 62676 та будівельні норми ДБН В.2.2-3:2018). Все це зумовлює високу теоретичну та практичну актуальність обраного напряму дослідження.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– дослідити техніко-економічні характеристики навчального закладу, визначити зони підвищеного контролю та проаналізувати потенційні загрози його безпеці з урахуванням чинного законодавства й нормативно-правової бази України;

– здійснити порівняльний аналіз сучасних архітектурних рішень та технологій побудови систем відеоспостереження для визначення оптимального підходу до побудови проектованої системи;

– спроектувати концептуальну схему та топологію системи відеоспостереження об’єкта, визначити оптимальні місця встановлення відеокамер із розрахунком їхніх зон огляду та роздільної здатності;

– вибрати необхідне апаратне забезпечення, виконати інженерні розрахунки ємності системи збереження даних (архіву) та необхідної пропускної здатності локальної мережі для забезпечення стабільної роботи системи;

– розробити схему підключення та інтеграції компонентів системи в локальну мережу школи, описати процес налаштування програмного забезпечення для моніторингу та адміністрування, а також запропонувати заходи щодо забезпечення надійності та інформаційної безпеки системи.

РОЗДІЛ 2
ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ ТА МЕТОДІВ РЕАЛІЗАЦІЇ

2.1 Розробка концептуальної схеми та топології системи відеоспостереження об’єкта

Концепція побудови системи відеоспостереження для закладу загальної середньої освіти базується на використанні сучасної IP-архітектури, що забезпечує високу ефективність передачі відеоданих, централізоване керування обладнанням та можливість інтеграції із суміжними системами безпеки. Основою такої концепції є застосування цифрових мережевих технологій, у яких кожна камера функціонує як окремий мережевий пристрій, що передає відеопотік через локальну обчислювальну мережу до центрального вузла обробки та зберігання даних.

При проєктуванні системи враховано особливості об’єкта (рис. 2.1-2.3), зокрема значну площу будівлі школи, наявність великої кількості функціональних приміщень та триповерхову структуру споруди. Такі характеристики об’єкта потребують побудови масштабованої та структурованої мережі, здатної забезпечити стабільну роботу значної кількості IP-камер без перевантаження каналів передачі даних та втрати якості відеосигналу.

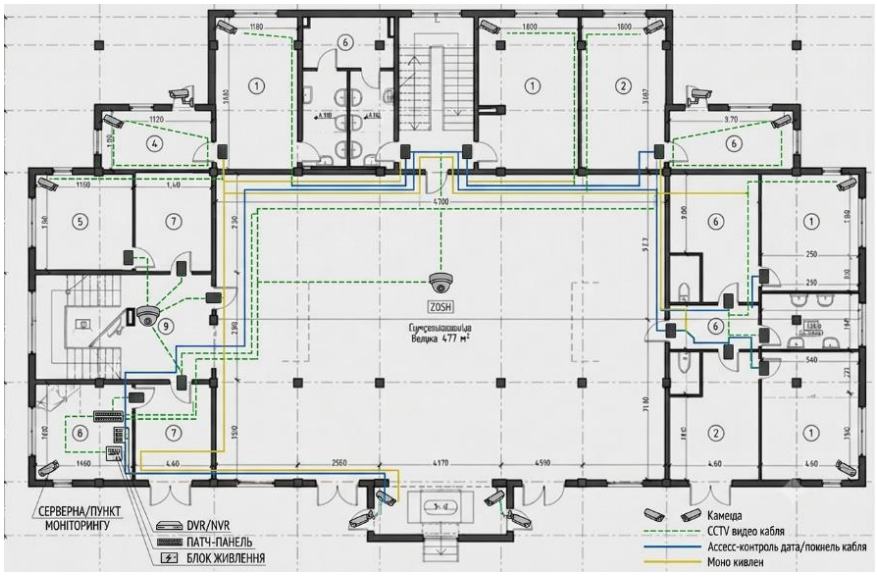

Рисунок 2.1 – Схема розміщення кабелів та камер на першому поверсі

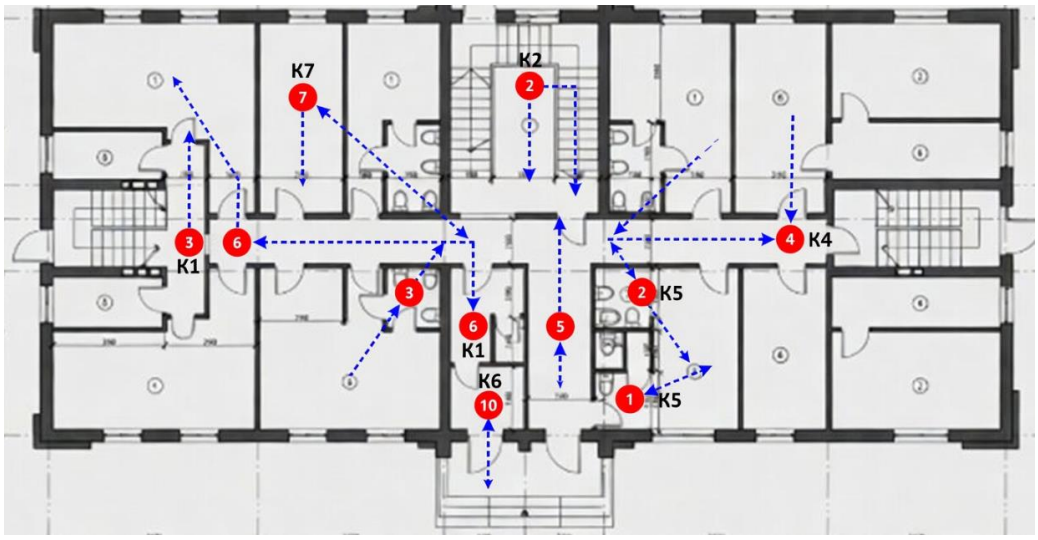

Рисунок 2.2 – Схема розміщення камер на другому поверсі

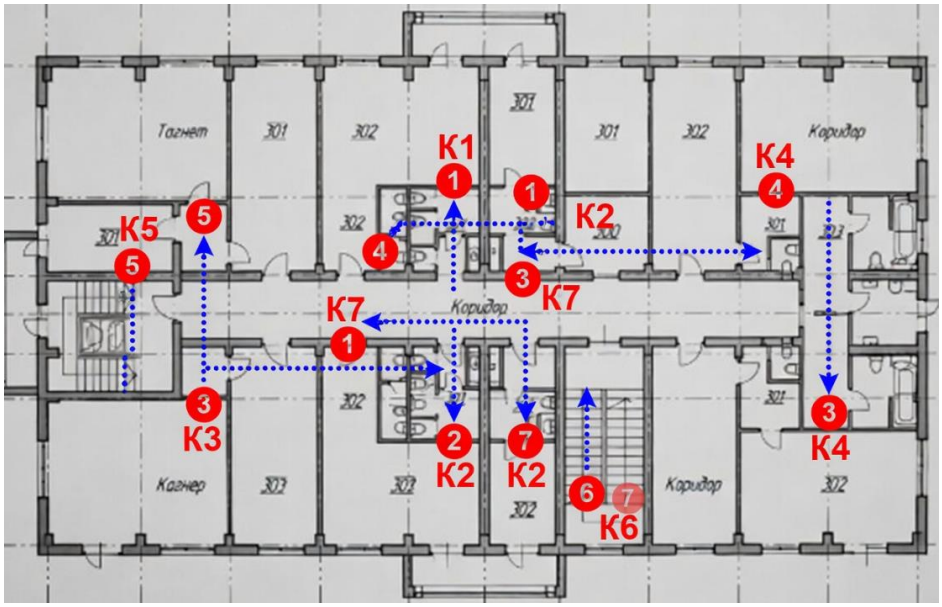

Рисунок 2.3 – Схема розміщення камер на третьому поверсі

Для реалізації системи обрано топологію типу «ієрархічна зірка», яка є одним із найбільш ефективних рішень для багаторівневих мережевих систем відеоспостереження [2, 12, 18]. У межах цієї архітектури мережа поділяється на декілька рівнів: периферійний рівень із підключенням IP-камер, проміжний рівень комутації та центральний вузол керування. Камери підключаються до локальних PoE-комутаторів, розміщених на кожному поверсі або в окремих функціональних секторах будівлі, після чого мережевий трафік передається до центрального комутаційного вузла та мережевого відеореєстратора (NVR).

Використання децентралізованого розподілу живлення на базі технології PoE (Power over Ethernet) дозволяє суттєво спростити кабельну інфраструктуру системи [21]. Передача живлення та даних одним Ethernet-кабелем зменшує кількість комунікацій, спрощує монтажні роботи та забезпечує гнучкість розміщення обладнання. Крім того, локалізація PoE-комутаторів на окремих поверхах дає змогу знизити довжину кабельних ліній і підвищити загальну надійність системи.

Однією з ключових переваг топології «ієрархічна зірка» є високий рівень відмовостійкості. У разі пошкодження окремої лінії зв’язку або виходу з ладу периферійного комутатора відмова впливає лише на окремий сегмент мережі, тоді як інші елементи системи продовжують працювати у штатному режимі. Це особливо важливо для закладів освіти, де безперервність функціонування системи безпеки має критичне значення.

Додатковою перевагою обраної архітектури є зручність адміністрування та технічного обслуговування. Централізоване керування дозволяє здійснювати моніторинг стану камер, перегляд відеоархівів, оновлення програмного забезпечення та зміну конфігурації системи з єдиного робочого місця адміністратора. Такий підхід значно спрощує експлуатацію системи та скорочує час реагування на можливі несправності.

Важливою особливістю архітектури є також можливість поетапного масштабування системи. За необхідності до існуючої мережі можна додавати нові IP-камери, комутатори або серверні ресурси без суттєвого впливу на працездатність уже розгорнутої інфраструктури. Це забезпечує гнучкість розвитку системи відповідно до майбутніх потреб закладу освіти.

Мережева інфраструктура системи відеоспостереження побудована за трирівневою ієрархічною моделлю (рис. 2.4), що відповідає топології «ієрархічна зірка» та забезпечує ефективну передачу відеоданих у межах будівлі закладу освіти. Така структура дозволяє раціонально розподілити мережеві ресурси, підвищити відмовостійкість системи, а також спростити її адміністрування та подальше масштабування.

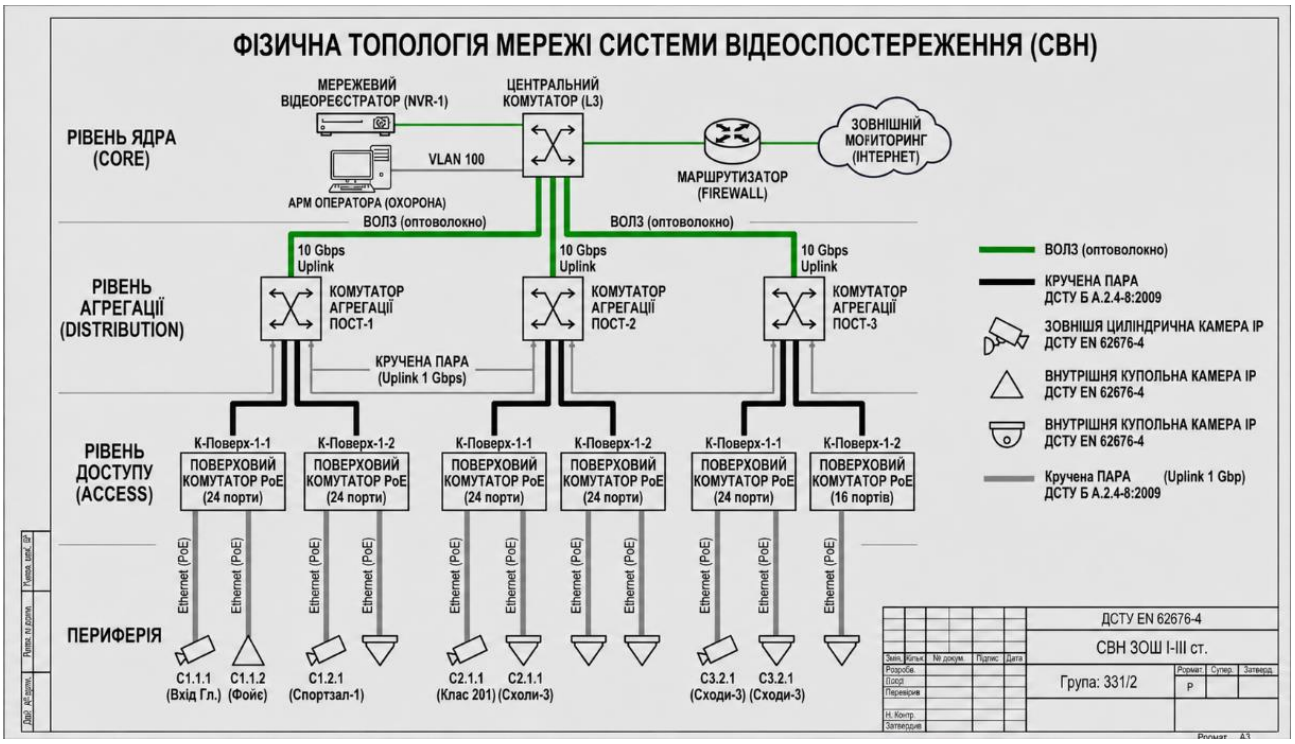

Рисунок 2.4 – Фізична топологія мережі

Модель включає три рівні: доступу, розподілу та ядро мережі, кожен з яких виконує власні функції в процесі передачі та обробки даних. Такий підхід є типовим для сучасних мережевих систем безпеки, оскільки забезпечує логічне розмежування навантаження та стабільну роботу всієї інфраструктури.

Рівень доступу (Access Layer) є нижнім рівнем і забезпечує безпосереднє підключення IP-камер до мережі. Для цього використовуються PoE-комутатори, розміщені на кожному поверсі будівлі. Камери підключаються до найближчих комутаторів через кабель Cat5e або Cat6, по якому одночасно передаються дані та живлення. Це дозволяє мінімізувати кількість окремих кабельних ліній і спрощує монтаж].

Рівень агрегації (Distribution Layer) виконує функцію об’єднання трафіку від комутаторів доступу та передачі його до ядра системи. Він забезпечує концентрацію мережевих потоків, маршрутизацію, сегментацію та контроль навантаження, що підвищує загальну продуктивність і стабільність системи відеоспостереження.

Ядро системи (Core Layer) є верхнім рівнем ієрархічної архітектури та забезпечує централізоване керування всією системою відеоспостереження. На цьому рівні здійснюється обробка, запис і зберігання відеоданих, а також доступ до архівів і потокового відео в реальному часі.У проєктованій системі ядро мережі реалізовано на базі центрального керованого комутатора, який виконує роль основного вузла передачі даних між рівнем агрегації та кінцевими серверними ресурсами. До цього комутатора підключається мережевий відеореєстратор (NVR), що забезпечує запис, архівацію та управління відеопотоками з усіх IP-камер системи. Саме NVR виступає основним елементом зберігання відеоінформації, формуючи централізований архів подій за визначений період часу.

Додатково до ядра системи підключається робоча станція оператора, яка розміщується на посту охорони першого поверху. Через цю станцію здійснюється моніторинг відеопотоків у реальному часі, перегляд архівних записів, керування камерами (зокрема PTZ-функціями за наявності) та взаємодія з програмним забезпеченням системи відеоспостереження. Таким чином, робоча станція виконує функцію інтерфейсу між оператором і всією системою безпеки об’єкта.

Ядро системи відповідає за реалізацію основних функцій управління відеоспостереженням, зокрема централізовану обробку даних, координацію потоків інформації, контроль доступу до архівів та забезпечення взаємодії між різними компонентами мережі. На цьому рівні також можуть реалізовуватися механізми резервного копіювання, синхронізації даних та інтеграції з іншими системами безпеки закладу, такими як система контролю доступу або пожежна сигналізація.

Важливою характеристикою Core Layer є висока продуктивність і надійність обладнання, оскільки саме цей рівень обробляє весь обсяг відеотрафіку, що надходить від усіх підключених камер. Тому до центрального комутатора та серверного обладнання висуваються підвищені вимоги щодо пропускної здатності, стабільності роботи та можливості масштабування.

Логічна структура системи відеоспостереження включає взаємодію кількох основних функціональних вузлів подана на рисунку 2.5.

Периферійні пристрої представлені двома типами камер: внутрішніми купольними камерами для моніторингу коридорів і навчальних класів та вуличними циліндричними камерами з інфрачервоним підсвічуванням для спостереження за периметром будівлі та спортивним майданчиком.

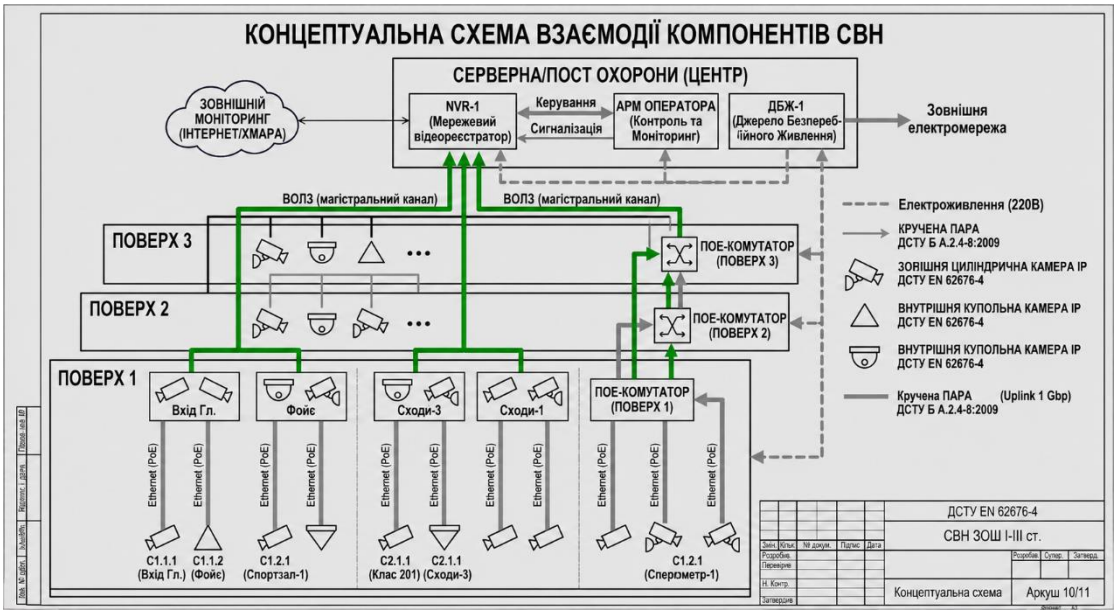

Рисунок.2.2 – Концептуальна схема взаємодії компонентів

Серверна частина системи відеоспостереження реалізована на базі мережевого відеореєстратора (NVR), який виконує функції централізованого приймання, обробки та зберігання відеопотоків від усіх підключених камер. Для забезпечення достатнього обсягу архівування використовується дискова підсистема великої ємності, що дозволяє організувати довготривале зберігання записів у циклічному режимі без втрати критично важливих даних.

З метою оптимізації використання дискового простору застосовується сучасний алгоритм стиснення відео H.265+, який забезпечує ефективну компресію відеопотоку при збереженні високої деталізації зображення. Завдяки цьому досягається істотне зменшення обсягу архіву, що безпосередньо підвищує

ефективність роботи сховища та знижує вимоги до апаратних ресурсів системи зберігання.

Підсистема електроживлення побудована на основі джерел безперебійного живлення (ДБЖ), які забезпечують стабільну роботу ключових компонентів системи, включаючи відеокамери, мережеві комутатори та відеореєстратор. У разі відключення основного електропостачання 220 В ДБЖ підтримують автономне живлення протягом визначеного часу, що дозволяє уникнути втрати даних, некоректного завершення роботи обладнання та перерв у відеомоніторингу.

Для підвищення рівня інформаційної безпеки, сегментації мережі та оптимізації передавання відеоданих система відеоспостереження логічно ізольована в окрему віртуальну локальну мережу VLAN 100 (Surveillance). Такий підхід дозволяє відокремити відеотрафік від основної навчальної мережі закладу, зменшити ризики несанкціонованого доступу до камер та підвищити загальну керованість мережевою інфраструктурою.

У межах виділеної VLAN використовується статична схема IP-адресації в діапазоні 192.168.100.0/24. Застосування статичних IP-адрес забезпечує однозначну ідентифікацію кожного мережевого пристрою (камер, NVR, комутаторів), виключає можливість конфліктів адрес та спрощує адміністрування системи, зокрема при діагностиці та масштабуванні інфраструктури.

Додатково на мережевому обладнанні налаштовано механізм пріоритезації трафіку QoS (Quality of Service), який забезпечує підвищений пріоритет для відеопотоків у порівнянні з іншими типами мережевого трафіку закладу. Це дозволяє мінімізувати затримки, уникати втрати кадрів та гарантувати стабільну пропускну здатність саме для критично важливих відеоданих.

У комплексі така конфігурація мережі забезпечує не лише стабільність та передбачуваність роботи системи відеоспостереження, але й підвищує її відмовостійкість в умовах пікових навантажень або одночасної роботи великої кількості мережевих сервісів у межах навчального закладу.

Розподіл мережевих вузлів за рівнями будівлі виглядає наступним чином:

– вузол 1 (підвал): комутатор на 8 портів, який обслуговує їдальню та входи до підвальних приміщень;

– вузол 2 (перший поверх): основний комутатор на 24 порти з підключеним NVR (пост охорони), що охоплює фойє, спортивний зал та периметр будівлі;

– вузол 3 (другий поверх): комутатор на 16 портів для обслуговування навчальних коридорів;

– вузол 4 (третій поверх): комутатор на 16 портів для навчальних коридорів.

2.2 Розрахунок зон огляду, роздільної здатності та місць встановлення відеокамер

Вибір місць встановлення камер та їх технічних параметрів здійснюється з метою забезпечення суцільного відеомоніторингу критичних зон будівлі та прилеглої території, а також можливості надійної ідентифікації осіб.

2.2.1 Критерії роздільної здатності (щільність пікселів)

Відповідно до вимог стандарту ДСТУ EN 62676-4, для різних функціональних зон встановлюються такі мінімальні значення щільності пікселів на метр (px/m):

– моніторинг (12,5 px/m) – для загального спостереження за рухом людей на прилеглій території школи;

– детектування (25 px/m) – для надійного виявлення присутності людини в коридорах та загальних приміщеннях;

– розпізнавання (125 px/m) – для визначення знайомих осіб (учнів, працівників) у навчальних класах та кабінетах;

– ідентифікація (250 px/m) – для однозначної ідентифікації незнайомих осіб у найбільш критичних зонах (вхідні групи, фойє, касова зона їдальні).

2.2.2 Геометричний розрахунок зони огляду

Для визначення необхідної фокусної відстані об’єктива (f) та горизонтального розміру зони огляду (W) застосовується формула (2.1):

$$f = h \times (L/H) \quad (2.1)$$

де: h – розмір матриці камери (мм);

L – відстань до об’єкта (м);

H – висота зони огляду на відстані L (м).

Для більшості внутрішніх приміщень школи (коридори та навчальні класи) обрано камери з фокусною відстанню 2,8 мм, що забезпечує широкий кут огляду (близько 100°). Таке рішення дозволяє охопити максимальну площу при мінімальній кількості камер, підтримуючи при цьому необхідний рівень деталізації.

Для організації відеоспостереження за периметром будівлі та спортивним залом передбачено застосування камер з фіксованою фокусною відстанню 4 мм, а також пристроїв, оснащених варіофокальними об’єктивами. Такий підхід забезпечує більш гнучку адаптацію системи до різних умов експлуатації та специфіки контрольованих зон.

Використання камер із фокусною відстанню 4 мм є доцільним для ділянок, де необхідно забезпечити збалансоване поєднання ширини огляду та деталізації зображення, зокрема при контролі відкритих просторів і відносно рівномірно освітлених територій. У свою чергу, варіофокальні об’єктиви дозволяють змінювати фокусну відстань у заданому діапазоні, що забезпечує можливість точного налаштування кута огляду та рівня збільшення зображення відповідно до конкретних вимог об’єкта.

Завдяки такій конфігурації стає можливим оптимізувати щільність пікселів у контрольованих зонах, що безпосередньо впливає на інформативність відеозапису та якість ідентифікації об’єктів. Це особливо важливо для ділянок із підвищеними вимогами до деталізації, таких як входи, проходи або спортивні майданчики, де необхідно забезпечити як широкий огляд сцени, так і можливість детального аналізу подій.

Важливим аспектом проектування є повне виключення «сліпих зон». У довгих шкільних коридорах (наприклад, приміщення №2 та №35) застосовується метод зустрічного спостереження. Камери встановлюються на протилежних кінцях коридору та спрямовуються одна на одну. Таке рішення дозволяє повністю перекрити всю довжину приміщення (табл. 2.1), усунути мертву зону безпосередньо під камерою, а також забезпечити дублювання зображення у разі спроби вандалізму або навмисного закриття об’єктива однієї з камер.

Таблиця 2.1 – Визначення місць встановлення (згідно з експлікацією плану)

Місце встановлення	Кількість камер	Тип камери	Цільове завдання
Центральний вхід (тамбур 1)	2	Купольна (4Мп)	Ідентифікація всіх відвідувачів
Коридори (1, 2, 3 поверхи)	12	Купольна (2Мп)	Детектування руху, контроль за порядком
Сходові клітки (17, 28, 55)	6	Купольна 2Мп)	Контроль шляхів евакуації
Спортзал (53)	4	Ширококутна (4Мп)	Охоплення великої площі, запобігання травматизму
Їдальня (3) та харчоблок	3	Купольна (2Мп)	Контроль за зберіганням продуктів та касовою зоною
Периметр (подвір’я)	8	Циліндрична (4Мп)	Контроль огорожі та прилеглої території

Висота встановлення камер підібрана з урахуванням ергономіки та захисту від втручання: внутрішні камери монтуються на висоті 2,5-2,7 м, а зовнішні – на висоті 3,5-4,0 м. Такий підхід робить обладнання практично недосяжним без спеціальних засобів, зберігаючи при цьому оптимальний ракурс спостереження.

2.3 Обґрунтування та вибір апаратного забезпечення

Вибір апаратного забезпечення системи відеоспостереження базується на необхідності забезпечення безперервного цілодобового моніторингу, високої деталізації відеозображення та підвищеної відмовостійкості всієї системи в умовах тривалої експлуатації [22-24]. Окрему увагу приділено здатності

обладнання стабільно працювати при різних навантаженнях, а також зберігати якість відеопотоку навіть у складних умовах освітлення або погодних факторів.

Для об’єкта обрано професійне мережеве обладнання, яке підтримує сучасний алгоритм компресії відео H.265+, що є вдосконаленою версією стандарту стиснення даних. Використання даного кодека дозволяє суттєво зменшити обсяг відеоданих, що зберігаються, забезпечуючи економію дискового простору до 70% у порівнянні з попередніми стандартами, без помітної втрати якості зображення.

Завдяки цьому підходу підвищується ефективність використання сховищ даних, зменшуються витрати на інфраструктуру зберігання, а також оптимізується робота мережевих ресурсів системи відеоспостереження. Це особливо важливо для об’єктів освітньої сфери, де необхідно забезпечити тривале архівування відеоінформації при обмежених технічних і фінансових ресурсах.

Для внутрішніх приміщень (коридори, навчальні класи, фойє та інші зони загального користування) застосовуються 4-мегапіксельні купольні IP-камери з фіксованим об’єктивом 2,8 мм (рис. 2.3). Такий тип обладнання є доцільним для інтер’єрного відеоспостереження, оскільки поєднує компактні розміри, антивандальне виконання та достатній рівень деталізації зображення для ідентифікації подій у межах приміщення.

Рисунок 2.3 – Камера відеоспостереження Hikvision DS-2CE56H0T-IRMMF

Завдяки широкому куту огляду в діапазоні приблизно 100-110° ці камери забезпечують ефективне покриття значної площі без необхідності встановлення великої кількості окремих пристроїв, що оптимізує як вартість впровадження, так і подальше обслуговування системи. Це особливо важливо для довгих коридорів та відкритих зон, де необхідно мінімізувати «сліпі» зони спостереження.

Додатково камери оснащені вбудованим інфрачервоним (ІЧ) підсвічуванням з дальністю дії до 30 м, що дозволяє забезпечувати якісну відеозйомку в умовах повної або часткової відсутності освітлення. Перехід у нічний режим здійснюється автоматично, що гарантує безперервність моніторингу незалежно від часу доби та рівня освітленості в приміщенні.

Для зовнішнього відеоспостереження периметра будівлі та спортивного майданчика застосовуються 4-мегапіксельні вуличні циліндричні IP-камери (рис. 2.4), виконані в антивандальному корпусі. Таке конструктивне виконання забезпечує підвищену стійкість до механічних пошкоджень, атмосферних впливів та несанкціонованого втручання, що є критично важливим для умов експлуатації на відкритій території.

Рисунок.2.4 – IP відеокамера IMOU Bullet 2E

Камери відповідають класу захисту IP67, що гарантує повну пилонепроникність і захист від тимчасового занурення у воду, а також мають

рівень механічної міцності IK10, який передбачає стійкість до ударних навантажень. Це дозволяє забезпечити стабільну роботу обладнання в умовах дощу, снігу, перепадів температур і можливих фізичних впливів з боку сторонніх осіб.

Окремою перевагою є наявність функції широкого динамічного діапазону WDR (120 дБ), яка забезпечує коректну передачу зображення в умовах складного освітлення. Завдяки цьому система ефективно компенсує різницю між яскравими та затемненими ділянками кадру, що особливо важливо при спостереженні за периметром у випадках прямого сонячного світла або контрового освітлення. У результаті формується збалансоване та інформативне відеозображення, придатне для подальшого аналізу подій.

Для обробки відеопотоків від 35-40 камер обрано професійний мережевий відеореєстратор (рис. 2.5), здатний працювати з 64 каналами та підтримувати вхідний потік не менше 320 Мбіт/с. Реєстратор комплектується дисковим масивом, який забезпечує зберігання архіву протягом 14-21 дня. Об’єм необхідного сховища розраховується за формулою (2.2):

Рисунок.2.5 – Відеореєстратор IMOU NVR-N110-8A0E

$$V = \frac{n \times B \times T \times 3600}{8 \times 10^6}, \quad (2.2)$$

де n – кількість камер;

B – середній бітрейт однієї камери (Мбіт/с);

T – кількість годин запису на добу.

Для 35 камер при цілодобовому записі та середньому бітрейті 4 Мбіт/с (з урахуванням H.265+) для 14-денного архіву необхідно приблизно 24 ТБ. Це рішення реалізовано за допомогою трьох жорстких дисків спеціальної серії Surveillance об’ємом по 8 ТБ кожен.

Живлення камер і передача даних здійснюється через керовані PoE+ комутатори (стандарт IEEE 802.3at). На кожному поверсі встановлено 24-портовий комутатор з бюджетом потужності не менше 370 Вт, а в якості ядра мережі використовується гігабітний L3-комутатор з SFP-портами для підключення волоконно-оптичних магістралей.

Специфікація апаратного забезпечення проектованої системи відеоспостереження подана в таблиці 2.2.

Таблиця 2.2 – Перелік та технічні параметри апаратних засобів системи відеоспостереження

Найменування	Характеристики	Кількість
IP-камера внутрішня	4Мп, 2.8мм, PoE, H.265+	25 шт.
IP-камера вулична	4Мп, 4.0мм, IP67, WDR	10 шт.
Відеореєстратор NVR	64 канали, 8 HDD slots, 4K	1 шт.
Жорсткий диск (HDD)	8 ТБ, Surveillance series	3 шт.
PoE-комутатор	24 порти PoE+, 2 SFP Uplink	3 шт.
ДБЖ (UPS)	3000VA, Online типу	1 шт.

2.4 Розрахунок ємності системи збереження даних та необхідної пропускної здатності локальної мережі

Важливим етапом проектування системи відеоспостереження є забезпечення безперервного запису архіву та стабільної передачі даних без затримок і втрати пакетів [4, 25].

Для оцінки навантаження на локальну мережу розраховується сумарний вхідний бітрейт R_{total} від усіх камер за формулою(2.3):

$$R_{total} = \sum_{i=1}^{n} (B_i \times k), \quad (2.3)$$

де n – кількість камер (35 шт.);

B_i – середній бітрейт однієї камери (≈ 4 Мбіт/с для 4 Мп при H.265+);

k – коефіцієнт пікового навантаження (1,2).

Розрахунок показує, що сумарне навантаження відеотрафіку системи становить приблизно 168 Мбіт/с. Отримане значення є прийнятним для обраної архітектури мережі та не створює критичних навантажень на її ключові вузли.

На рівні доступу навантаження, яке припадає на один 24-портовий PoE-комутатор, не перевищує 60-72 Мбіт/с. Це значення суттєво нижче порогового рівня у 80% від номінальної пропускної здатності порту, що вважається граничною межею для стабільної роботи мережевого обладнання. Таким чином, забезпечується робота комутаторів у штатному режимі без ризику перевантаження та деградації якості передачі відеопотоку.

На рівні агрегації та ядра мережі використання гігабітних інтерфейсів (1 Гбіт/с) формує значний запас пропускної здатності відносно розрахункового навантаження. У даному випадку резерв становить приблизно шестикратне перевищення відносно пікового трафіку, що дозволяє компенсувати можливі коливання навантаження, службовий трафік, а також майбутнє її масштабування.

У результаті така мережева конфігурація забезпечує стабільну та безперебійну передачу відеоданих без втрат пакетів і затримок навіть у пікові періоди активності системи відеоспостереження.

Глибина зберігання архіву для закладів освіти має становити не менше 14 діб. Необхідний об’єм дискового простору V розраховується за формулою(2.4):

$$V = \frac{R_{total} \times T \times 3600 \times D}{\{8 \times 10^6\}}, \quad (2.4)$$

де T – 24 години запису на добу,

D – 14 діб.

За розрахунками для безперервного запису всіх 35 камер потрібно приблизно 25,4 ТБ. З урахуванням форматування та службової інформації реальна необхідна ємність становить близько 28 ТБ.

Для забезпечення надійності та відмовостійкості системи зберігання відеоданих обрано спеціалізовані жорсткі диски класу Surveillance (наприклад, WD Purple), які розроблені для роботи у режимі безперервного навантаження 24/7 та оптимізовані для обробки багатопотокових відеозаписів від декількох камер одночасно. Такі накопичувачі відрізняються підвищеною стійкістю до тривалих циклів запису, зменшеним рівнем зносу та стабільною продуктивністю в умовах постійної роботи.

У складі системи використовується чотири жорсткі диски ємністю по 8 ТБ кожен, що формує загальну сиру місткість сховища на рівні 32 ТБ. Запис відеоданих організовано у режимі циклічного перезапису, що дозволяє безперервно підтримувати архів без необхідності ручного втручання у процес очищення або розширення сховища.

Застосування інтелектуального кодека H.265+ додатково підвищує ефективність використання дискового простору за рахунок адаптивного зниження бітрейту у статичних або малозмінних сценах. Це дозволяє значно оптимізувати обсяг збережених даних без суттєвого погіршення якості відеозображення, що в свою чергу потенційно збільшує глибину архіву до 20–25 діб залежно від інтенсивності відеопотоку та умов спостереження.

Таким чином, спроектована мережева інфраструктура на базі гігабітного ядра та дискова підсистема загальним обсягом 32 ТБ повністю відповідають вимогам технічного завдання. Вони забезпечують стабільну та безперервну роботу системи відеоспостереження Мар’янівської ЗОШ із достатнім ресурсним резервом для подальшого масштабування та розширення кількості камер у разі необхідності.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ

3.1 Схема підключення та інтеграції компонентів системи відеоспостереження в локальну мережу школи

Розроблена схема (рис. 3.1) відображає архітектуру інтеграції підсистеми відеоспостереження у загальну інформаційно-телекомунікаційну інфраструктуру ЗОШ І-ІІІ ст. (смт Мар'янівка). Основним принципом побудови є створення конвергентного середовища, де відеодані передаються паралельно з іншими потоками безпеки, але логічно ізольовані для запобігання конфліктам.

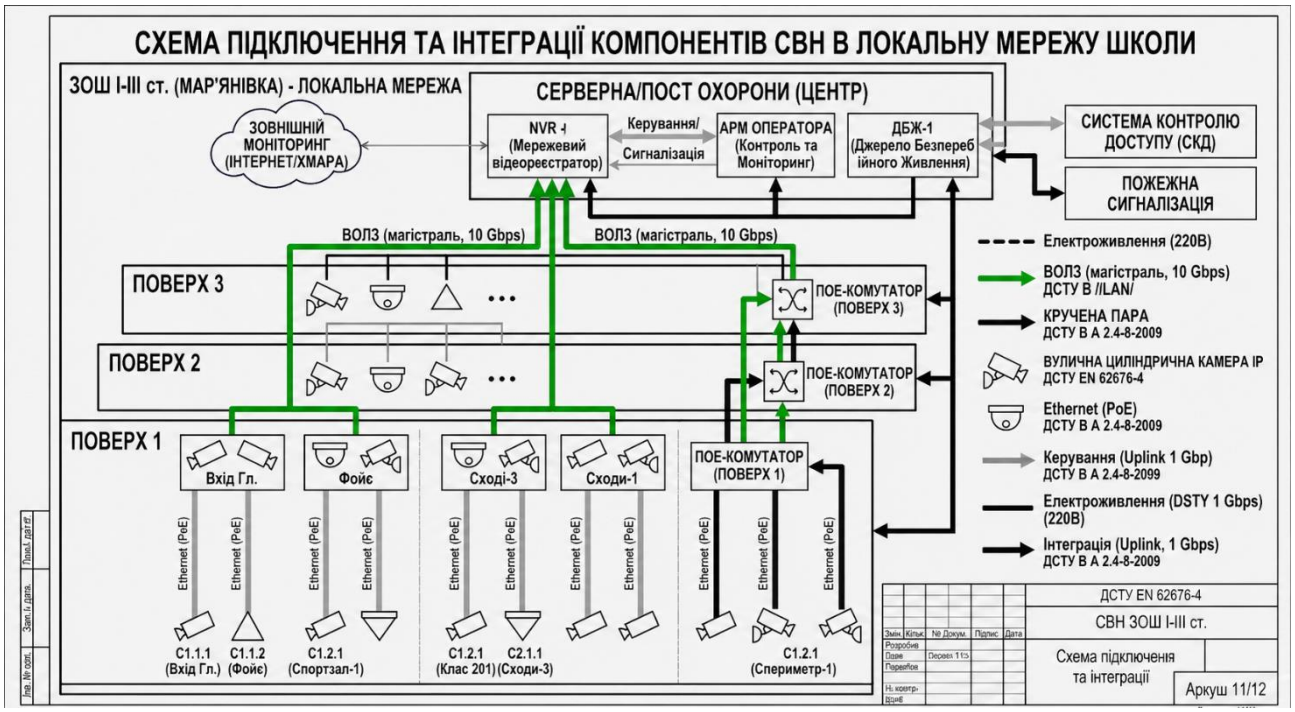

Рисунок 3.1 – Схема підключення та інтеграції компонентів

Для забезпечення стабільної роботи системи відеоспостереження та захисту від несанкціонованого доступу передбачено її інтеграцію в локальну мережу закладу на основі технології VLAN [12, 18. 21].

Весь трафік від IP-камер та мережевого відеореєстратора (NVR) виділено в окремий віртуальний сегмент – VLAN 100 (Surveillance). Таке рішення дозволяє повністю ізолювати систему відеоспостереження від загальної навчальної

мережі школи, включаючи кабінети інформатики та Wi-Fi для вчителів. Завдяки цьому значно знижується навантаження на основну мережу та забезпечується надійний захист архіву від несанкціонованого доступу з боку учнів та сторонніх осіб.

На транспортному рівні магістральні канали між поверхами реалізовані на базі волоконно-оптичних ліній зв'язку (ВОЛЗ) з пропускною здатністю 10 Гбіт/с. Використання оптики гарантує високу швидкість передачі даних і повну відсутність затримок («фрізів») навіть при одночасній трансляції потоків високої чіткості від 35 і більше камер.

Відповідно до концептуальної схеми (рис. 3.1), система відеоспостереження інтегрована з двома ключовими інженерними комплексами безпеки будівлі.

Інтеграція з системою контролю та управління доступом (СКД) забезпечує автоматичну реакцію на події доступу. При зчитуванні карти або спробі проходу через контрольовані точки (зокрема, центральний вхід) на моніторі оператора охорони автоматично виводиться зображення з відповідної камери, що дозволяє оперативно оцінити ситуацію в реальному часі.

Інтеграція з протипожежною автоматикою передбачає автоматичний перехід системи у підвищений режим роботи при надходженні сигналу «Тривога». У такому випадку СВН перемикається на максимальну частоту кадрів на відповідному поверсі та автоматично виводить на робоче місце оператора відеотрансляцію основних шляхів евакуації. Це суттєво підвищує ефективність реагування персоналу в надзвичайних ситуаціях.

Центральним елементом інтеграції системи відеоспостереження є Пост охорони, де зосереджено основні вузли керування та моніторингу.

На посту розміщено мережевий відеореєстратор (NVR), який виконує функцію шлюзу між ізольованою мережею камер та іншими компонентами системи. Робоче місце оператора (АРМ) підключене до центрального комутатора через гігабітний інтерфейс, що забезпечує високу швидкість відгуку, комфортну роботу з інтерфейсом та швидкий пошук у відеархіві.

Доступ до системи ззовні організовано через захищений VPN-канал. Це дозволяє адміністрації закладу та уповноваженим представникам правоохоронних органів здійснювати віддалений перегляд відеопотоків і архівних записів у режимі реального часу.

Для забезпечення безперервної роботи всіх критичних компонентів передбачено використання джерел безперебійного живлення (ДБЖ). Центральний вузол, що включає відеореєстратор та активне мережеве обладнання, захищений ДБЖ типу On-line. Таке рішення повністю усуває вплив перепадів напруги та забезпечує автономну роботу системи протягом 30–60 хвилин, чого достатньо для завершення евакуації або переходу на резервне живлення від котельні.

3.2 Налаштування програмного забезпечення для моніторингу та адміністрування

Ефективність системи відеоспостереження значною мірою залежить не тільки від апаратної частини, а й від правильного налаштування програмного забезпечення, яке забезпечує інтерфейс взаємодії користувача з системою.

Для адміністрування обрано спеціалізоване професійне ПЗ (HikCentral, iVMS-4200 або аналогічні VMS-платформи), яке встановлюється на робочому місці оператора. Програмне забезпечення забезпечує відображення живого відео в реальному часі (до 64 каналів одночасно), підтримку мультимоніторних конфігурацій, а також зручну роботу з архівом завдяки часовій шкалі (Timeline) з кольоровим маркуванням подій.

На етапі налаштування виконується комплекс заходів щодо підвищення надійності та захисту системи. Усі камери та відеореєстратор синхронізуються з єдиним сервером часу (NTP), що забезпечує метрологічну точність відеозаписів при їх використанні як доказової інформації. Впроваджується рольова модель доступу (RBAC), відповідно до якої адміністратор має повні права, оператор

охорони може переглядати відео в реальному часі та архів за останні 24 години, а представники адміністрації закладу отримують доступ лише до визначених зон.

З метою кіберзахисту змінюються стандартні порти керування, активується шифрування трафіку (HTTPS/TLS) та встановлюються складні паролі. Система налаштовується на автоматичне реагування на події: детекцію руху з урахуванням зон ігнорування, перетин віртуальних ліній у критичних зонах (вхід до котельні), виявлення залишених предметів у фойє, а також автоматичне надсилання Email- та Push-сповіщень відповідальним особам у разі виникнення аварійних ситуацій.

Для оперативного реагування керівництва передбачено мобільний клієнтський додаток. Підключення здійснюється через захищений VPN-тунель або хмарний сервіс P2P. Для запобігання перевантаження мережного каналу мобільні пристрої за замовчуванням отримують суб-потік (зниженої якості), тоді як основний архів записується в максимальній якості (Main-stream).

Правильне налаштування програмного забезпечення перетворює систему відеоспостереження з пасивного засобу фіксації на активний інструмент забезпечення безпеки. Воно дозволяє оперативно інформувати персонал про загрози, забезпечує швидкий доступ до необхідної інформації та гарантує дотримання вимог законодавства України щодо захисту персональних даних.

3.3 Забезпечення надійності та інформаційної безпеки

Надійність та безпека системи відеоспостереження (СВН) Мар’янівської ЗОШ забезпечується комплексним підходом, що поєднує високу апаратну відмовостійкість та багаторівневий захист цифрової інформації.

Для гарантування безперервної роботи системи впроваджено кілька ключових рішень. Усі критичні компоненти (відеореєстратор та комутаційне обладнання) живляться від джерел безперебійного живлення типу On-line (з подвійним перетворенням), що захищає систему від перепадів напруги та

забезпечує автономну роботу протягом не менше 45 хвилин у разі відключення електропостачання.

Додатковим рівнем надійності є локальний запис на SD-карти ємністю 128 ГБ, встановлені в кожній IP-камері. У разі тимчасової втрати зв’язку з сервером (обрив кабелю чи збій комутатора) камери продовжують записувати відео на карту. Після відновлення з’єднання дані автоматично синхронізуються з центральним архівом завдяки функції ANR. Крім того, всі комутаційні вузли розміщені в телекомунікаційних шафах з організованою вентиляцією, що забезпечує оптимальний температурний режим роботи обладнання.

Зважаючи на інтеграцію СВН у локальну мережу школи, особлива увага приділяється захисту інформації. Трафік системи повністю ізольований у виділеному віртуальному сегменті VLAN, а доступ з навчальних комп’ютерів до IP-адрес камер заблокований на рівні списків контролю доступу (ACL). Передача відеопотоків здійснюється за протоколом RTSP поверх TLS/SSL, що унеможливлює перехоплення даних [8-10, 19, 20]. Додатково ПЗ реєстратора має захист від brute-force атак – автоматичне блокування IP-адреси після кількох невдалих спроб авторизації.

Відповідно до вимог Закону України «Про захист персональних даних» у системі реалізовані технічні заходи забезпечення цілісності та конфіденційності інформації. На кожен відеокадр накладається цифровий водяний знак (watermark) із зазначенням дати, часу та серійного номера камери, що дозволяє верифікувати автентичність запису при юридичному використанні. Уся діяльність користувачів фіксується в детальному журналі аудиту. Крім того, для камер, які частково захоплюють прилеглу приватну територію, налаштовано програмне маскування (privacy mask) – відповідні ділянки зображення не записуються в архів (табл. 3.1).

Запропонований комплекс організаційних і технічних заходів забезпечує високий рівень надійності системи відеоспостереження з коефіцієнтом готовності $K_g \geq 0{,}99$, що характеризується мінімальними простоями та стабільною роботою всіх компонентів навіть при окремих відмовах обладнання.

Досягнення такого рівня забезпечується резервуванням каналів зв’язку, використанням централізованого та розподіленого зберігання даних, відмовостійкою мережевою архітектурою, а також застосуванням обладнання з механізмами автоматичного відновлення з’єднань і балансування навантаження. Додатково підвищення надійності досягається за рахунок використання джерел безперебійного живлення (ДБЖ) та ієрархічної структури мережі, що зменшує вплив локальних відмов.

Таблиця 3.1 – Загрози функціонуванню системи відеоспостереження та методи їх нейтралізації

Загроза	Метод нейтралізації	Компонент
Вимкнення електрики	Автономне живлення	ДБЖ (UPS)
Крадіжка реєстратора	Резервне копіювання в хмару	FTP/Cloud Server
Злом пароля	Двофакторна автентифікація	ПЗ моніторингу
Фізичне пошкодження	Антивандальний корпус	Камери IK10

Впроваджені заходи також суттєво знижують ризики несанкціонованого доступу та витоку інформації завдяки сегментації мережі, обмеженню прав доступу, шифруванню даних і контролю автентифікації користувачів.

У результаті забезпечується не лише стабільна робота системи відеоспостереження, а й належний рівень інформаційної безпеки, необхідний для формування безпечного освітнього середовища.

ЗАГАЛЬНІ ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

У кваліфікаційній роботі бакалавра вирішено актуальну науково-практичну задачу з проектування та впровадження сучасної, надійної та безпечної системи відеоспостереження для Мар'янівського ліцею №2 Волинської області. За результатами проведеного дослідження та розробок зроблено такі висновки:

– на основі техніко-економічної характеристики Мар'янівського ліцею №2 визначено ключові зони підвищеного контролю (входи/виходи, периметр території, коридори, рекреаційні зони та подвір'я). Виявлено потенційні загрози безпеці навчального закладу, такі як несанкціоноване проникнення сторонніх осіб, правопорушення, вандалізм та виникнення аварійних ситуацій;

– здійснено детальний огляд чинного законодавства України та державних стандартів щодо встановлення систем відеоспостереження в закладах освіти. Проект реалізовано з чітким дотриманням прав учасників освітнього процесу на приватність, вимог Закону України «Про захист персональних даних» та правил техніки безпеки;

– за результатами порівняльного аналізу архітектурних рішень для ліцею було обрано сучасну цифрову IP-систему відеоспостереження. Розроблено концептуальну схему та зіркоподібну топологію мережі, що забезпечує високу масштабованість, гнучкість налаштування та простоту обслуговування;

– проведено точний розрахунок зон огляду, щільності пікселів (для ідентифікації, розпізнавання та детектування) та визначено оптимальні місця встановлення відеокамер з метою мінімізації «сліпих зон». Розраховано необхідну ємність системи збереження даних (HDD/мережевого сховища) для забезпечення глибини архіву відеозаписів терміном не менше 14-30 діб, а також обчислено пропускну здатність локальної мережі з урахуванням пікових навантажень від відеопотоків високої роздільної здатності;

– розроблено схему фізичного підключення та інтеграції IP-камер, комутаторів із підтримкою PoE (Power over Ethernet) та мережевого

відеореєстратора (NVR) в існуючу локальну комп'ютерну мережу школи. Налаштовано спеціалізоване програмне забезпечення для централізованого моніторингу, адміністрування та зручного віддаленого доступу адміністрації ліцею до відеопотоків;

– впроваджено комплекс заходів із кібербезпеки: розмежовано права доступу користувачів, налаштовано шифрування даних, змінено стандартні паролі пристроїв та захищено мережевий периметр від зовнішнього втручання. Для підвищення фізичної надійності передбачено використання джерел безперебійного живлення (ДБЖ), що гарантує автономну роботу системи у разі знеструмлення закладу.

Рекомендації щодо впровадження та експлуатації системи:

– перед фінальним запуском системи адміністрації Мар’янівського ліцею №2 рекомендується затвердити внутрішнє «Положення про відеоспостереження», ознайомити з ним під підпис співробітників, а також розмістити інформаційні таблички «Ведеться відеоспостереження» на всіх входах та в зонах огляду камер;

– проводити регулярне (не рідше одного разу на квартал) технічне обслуговування системи: очищення лінз відеокамер, перевірку температурного режиму роботи серверного обладнання, актуалізацію прошивок (firmware) пристроїв та тестування місткості акумуляторів у джерелах безперебійного живлення;

– за наявності додаткового фінансування, рекомендується інтегрувати систему відеоспостереження з елементами відеоаналітики (наприклад, розпізнавання облич на вході, детекція залишених предметів або інтеграція з системою контролю та керування доступом — СКУД / турнікетами), що дозволить автоматизувати процеси безпеки в ліцеї.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Stallings W. Network Security Essentials: Applications and Standards. URL: https://surl.li/hauxdk (access date: 12.01.2026).

2. CCNA 200-301. Official Cert Guide. Volume 1. URL: https://surl.li/owismn (access date: 14.01.2026).

3. CCNA 200-301 Official Cert Guide. Volume 2. URL: https://surl.li/zorgsj (access date: 14.01.2026).

4. The H.264 Advanced Video Compression Standard. URL: https://surl.li/avdmxt (access date: 18.01.2026).

5. G. J. Sullivan, J. Ohm, W. Han and T. Wiegand. Overview of the High Efficiency Video Coding (HEVC) Standard. *IEEE Transactions on Circuits and Systems for Video Technology*. Vol. 22, No. 12. Pp. 1649-1668.

6. Garcia M. L. The Design and Evaluation of Physical Protection Systems. URL: https://surl.li/aewtmv (access date: 18.01.2026).

7. Fischer R. J., Halibozek E. P., Walters D. C. Introduction to Security. URL: https://surl.li/aewtmv (access date: 18.01.2026).

8. Easttom C. Network Defense and Countermeasures. URL: https://www.scribd.com/document/888642194/Network-Defense-4th-Ed (access date: 18.01.2026).

9. Ciampa M. Security+ Guide to Network Security Fundamentals. 8th ed. Boston : Cengage Learning, 2024. 720 p.

10. Kim D., Solomon M. Fundamentals of Information Systems Security. 4th ed. Burlington : Jones & Bartlett Learning, 2022. 650 p.

11. Kalbo, Naor & Mirsky, Yisroel & Shabtai, Asaf & Elovici, Yuval. The Security of IP-Based Video Surveillance Systems. URL: https://surl.li/omlfyw (access date: 13.03.2026).

12. Cisco Enterprise Campus Infrastructure. Best Practices Guide. URL: https://www.cisco.com/c/dam/global/shared/assets/pdf/cisco_enterprise_campus_infrastructure_design_guide.pdf (access date: 04.04.2026).

13. The state of AI in video surveillance. URL: https://surl.li/wyfehn (access date: 04.04.2026).

14. Data Mining: Concepts and Techniques. URL: https://surl.li/bqfufy (access date: 10.04.2026).

15. Video Surveillance as a Service (VSaaS) Market Size, Share & Global Forecast 2026-2035 URL: https://surl.li/aewtmv (access date: 18.01.2026).

16, The Future of Emergency Response and Monitoring. URL: https://surl.li/flgioo (access date: 22.04.2026).

17. International Organization for Standardization. ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection Systems – Requirements. Geneva : ISO, 2022. 30 p

18. International Organization for Standardization. ISO/IEC 27002:2022 Information Security Controls. Geneva : ISO, 2022. 112 p.

19. The NIST Cybersecurity Framework (CSF) 2.0 Gaithersburg. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (access date: 25.04.2026).

20. NIST Special Publication 800-207: Zero Trust Architecture URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf (access date: 18.01.2026).

21. Telecommunications and exchange between information technology systems – Requirements for local and metropolitan area networks – Part 3: Standard for Ethernet AMENDMENT 14: Bidirectional 10 Gb/s, 25 Gb/s, and 50 Gb/s optical access PHYs New York. URL: https://surl.li/qstggl (access date: 28.04.2026). URL: https://surl.li/aewtmv (access date: 25.04.2026).

22. Safer Schools with K-12 Cloud Video Surveillance Solution Using Hikvision + Eagle Eye Networks. URL: https://surl.li/aewtmv (access date: 24.041.2026).ГКД:

23. DIGITAL TRANSFORMATION OF SECONDARY EDUCATION IN TIMES OF WAR: RELEVANCE FOR UKRAINE/ /URL: https://surl.li/aewtmv (access date: 18.01.2026).

24 Surveillance Storage Guide. URL: https://surl.li/aewtmv (access date: 18.01.2026).

25 Seagate Technology. Video Surveillance Storage Technology Guide. Fremont : Seagate Technology, 2024. 40 p. URL: https://surl.li/aewtmv (access date: 18.01.2026).

26. 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.