БАКАЛАВРСЬКА РОБОТА

БР.КІ-31.00.00.000 ПЗ

Група КІ-21-2

Балита Ігор

2025

Міністерство освіти і науки України

Івано-Франківський національний технічний університет нафти і газу
Факультет інформаційних технологій

Кафедра комп'ютерних систем і мереж

Балита Ігор Миколайович

УДК 004.738.5

БАКАЛАВРСЬКА РОБОТА

Розробка комп'ютерної системи відеоспостереження для Калуського ліцею ім.Д.Бахматюка з безпечним збереженням даних

Комп'ютерна інженерія
(назва освітньої програми)

123 – Комп'ютерна інженерія
(шифр і назва спеціальності)

Робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Здобувач освітнього ступеня _____ *Балита І.М.*
(підпис, ініціали та прізвище здобувача)

Науковий керівник _____ *Кропивницька В.Б., доцент*
(підпис, прізвище, ім'я, по батькові, науковий ступінь, вчене звання керівника)

Допущено до захисту
Завідувач кафедри
д.т.н., професор _____ /С. І. Мельничук/
(посада) (підпис) (дата) (ініціали та прізвище)

Івано-Франківськ – 2025 рік

Івано-Франківський національний технічний університет нафти і газу

Факультет *Інформаційних технологій*

Кафедра *Комп'ютерних систем і мереж*

Освітньо-кваліфікаційний рівень *бакалавр*

Спеціальність *123 – Комп'ютерна інженерія*

ЗАТВЕРДЖУЮ:

Зав. кафедрою КСМ

д.т.н. С.І. Мельничук

« 05» травня 2025 року

З А В Д А Н Н Я

НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Балиті Ігорю Миколайовичу

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) *Розробка комп'ютерної системи відеоспостереження для Калуського ліцею ім. Д. Бахматюка з безпечним збереженням даних .*

керівник проекту (роботи) *Кропивницька Віталія Богданівна, доцент*

затверджені наказом вищого навчального закладу від *05.05.2025 № 275/7*

2. Строк подання студентом проекту (роботи) *12 червня 2025р.*

3. Вихідні дані до роботи *Методичні вказівки, технічна література*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) *1. Аналітичний огляд сучасних систем відеоспостереження в закладах освіти._ 2. Проєктування структури системи відеоспостереження для Калуського ліцею. Вибір обладнання та програмного забезпечення*

3. Реалізація логічної моделі системи. Вибір методів зберігання даних

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

_

6. Консультанти розділів роботи

7. Дата видачі завдання *29 січня 2025 р.* .

№ з/п	Назва етапів дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	*Збір інформації, вивчення літератури та пошук додаткової інформації*	*Лютий 2025р*	
2	*Аналітичний огляд сучасних систем відеоспостереження в закладах освіти*	*Березень 2025р*	
3	*Проєктування структури системи відеоспостереження для Калуського ліцею. Вибір обладнання та програмного забезпечення*	*Квітень 2025р*	
4	*Реалізація логічної моделі системи. Вибір методів зберігання даних і забезпечення їх захисту*	*Травень 2025р*	
5	*Оформлення додатків, дипломної роботи*	*Червень 2025р*	

Студент _____ *Балита І.М.*

Керівник роботи _____ *Кропивницька В.Б.*

АНОТАЦІЯ

Бакалаврська робота присвячена проектуванню комп’ютерної системи відеоспостереження для Калуського ліцею ім. Д. Бахматюка з безпечним збереженням даних.

Метою роботи є створення ефективної, масштабованої та безпечної системи відеоспостереження, яка підвищує рівень контролю за внутрішнім середовищем ліцею, сприяє запобіганню правопорушенням та забезпечує захист даних відповідно до сучасних вимог інформаційної безпеки.

У роботі представлено повний цикл розробки системи – від аналітичного огляду предметної області до реалізації логічної структури системи, вибору обладнання, програмного забезпечення та методів забезпечення безпеки відеоданих.

У вступі обґрунтовано актуальність теми, мету та завдання дослідження, визначено об’єкт і предмет роботи.

У першому розділі виконано аналіз сучасних систем відеоспостереження, розглянуто практичні приклади впровадження в освітніх закладах, виконано порівняльний аналіз, визначено інформативні ознаки обраної системи та особливості її адаптації до умов навчального середовища.

У другому розділі спроєктовано архітектуру системи відеоспостереження для Калуського ліцею, розроблено структурну схему, обґрунтовано вибір обладнання та програмного забезпечення, описано логіку функціонування системи та принципи безпечного зберігання даних.

У третьому розділі розглянуто питання встановлення та налаштування системи, а також описано інструменти обслуговування й виявлення типових несправностей.

У четвертому розділі проведено оцінку ефективності впровадження системи, розраховано витрати на обладнання, монтаж, експлуатацію, а також запропоновано шляхи масштабування системи в майбутньому.

Ключові слова**:** відеоспостереження, безпека, навчальний заклад, архітектура системи, Partizan CMS, захист даних, IP-камери, масштабованість.

ANNOTATION

This bachelor's thesis is dedicated to the design of a computer-based video surveillance system for the Kalush Lyceum named after D. Bakhmatiuk, with a focus on secure data storage.

The goal of the work is to create an efficient, scalable, and secure video surveillance system that enhances control over the internal environment of the educational institution, helps prevent incidents, and ensures data protection in accordance with modern information security standards.

The thesis presents the full cycle of system development — from analytical review of the subject area to the implementation of the logical structure, selection of hardware and software, and the development of methods for secure video data storage.

The introduction substantiates the relevance of the topic, defines the purpose and objectives of the research, as well as the object and subject of the study.

The first chapter analyzes modern video surveillance systems, examines practical implementations in educational institutions, presents a comparative analysis, and identifies the key informative features of the proposed system and its adaptation to the school environment.

The second chapter is focused on the design of the video surveillance system architecture for the lyceum. It includes the development of the structural scheme, justification for the choice of equipment, the selection of software, and the description of system operation logic and data security principles.

The third chapter addresses system installation, configuration, and the use of tools for maintenance and troubleshooting.

The fourth chapter evaluates the effectiveness of the proposed solution, estimates the costs of equipment, installation, and operation, and outlines proposals for future system scaling.

Keywords: video surveillance, security, educational institution, system architecture, Partizan CMS, data protection, IP cameras, scalability.

ЗМІСТ

ВСТУП

Актуальність теми. В умовах сьогодення, питання безпеки навчальних закладів набуває особливої актуальності. Зростання рівня злочинності та хуліганства, а також загроза терористичних актів, роблять необхідним впровадження сучасних систем захисту, що забезпечують надійний контроль за територією та приміщеннями навчального закладу. Відеоспостереження є одним з найбільш ефективних інструментів для забезпечення безпеки, дозволяючи здійснювати моніторинг ситуації в режимі реального часу, запобігати правопорушенням та оперативно реагувати на надзвичайні події.

Калуський ліцей ім. Д. Бахматюка, як і будь-який інший навчальний заклад, потребує надійного захисту від зовнішніх та внутрішніх загроз. Впровадження сучасної комп'ютерної системи відеоспостереження з безпечним збереженням даних дозволить значно підвищити рівень безпеки учнів та співробітників, забезпечити збереження майна та створити сприятливі умови для навчання та виховання.

Об'єктом дослідження є процес забезпечення безпеки навчального закладу за допомогою комп'ютерної системи відеоспостереження.

Предметом дослідження є методи та засоби побудови комп'ютерної системи відеоспостереження з безпечним збереженням даних для Калуського ліцею ім. Д. Бахматюка.

Метою роботи є розробка комп'ютерної системи відеоспостереження для Калуського ліцею ім. Д. Бахматюка з безпечним збереженням даних, що забезпечить підвищення рівня безпеки та захисту навчального закладу.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

1. Проаналізувати існуючі системи відеоспостереження та визначити їхні переваги та недоліки.
2. Визначити вимоги до комп'ютерної системи відеоспостереження для Калуського ліцею ім. Д. Бахматюка.

3. Розробити архітектуру комп'ютерної системи відеоспостереження з урахуванням вимог безпеки та надійності.

4. Вибрати оптимальні технічні засоби (відеокамери, обладнання для обробки та зберігання даних, програмне забезпечення) для реалізації системи.

5. Забезпечити безпечне зберігання відеоданих з урахуванням вимог конфіденційності та захисту інформації.

6. Оцінити ефективність розробленої системи відеоспостереження.

У процесі виконання бакалаврської роботи використано наступні методи дослідження:

- аналіз літературних джерел: для вивчення існуючих систем відеоспостереження та методів забезпечення безпеки;

- системний аналіз: для визначення вимог до комп'ютерної системи відеоспостереження;

- метод порівняльного аналізу: для зіставлення різних підходів до організації систем відеоспостереження та вибору найбільш оптимальних рішень для конкретного навчального закладу;

- метод експертних оцінок: для оцінки ефективності запропонованих рішень та їхньої відповідності вимогам безпеки.

Практичне значення полягає у можливості впровадження розробленої комп'ютерної системи відеоспостереження в Калуському ліцеї ім. Д. Бахматюка. Результати роботи можуть бути використані для підвищення рівня безпеки та захисту навчального закладу, а також для розробки аналогічних систем в інших освітніх установах.

Крім того, розроблені алгоритми обробки відеоданих та методи забезпечення безпечного зберігання інформації можуть бути використані в інших сферах, де потрібен надійний захист відеоінформації.

1 АНАЛІЗ СУЧАСНОГО СТАНУ ПРОБЛЕМИ

1.1 Аналіз нормативно-правової та технічної документації

Розробка комп'ютерної системи відеоспостереження у закладах освіти вимагає обов'язкового врахування чинної законодавчої бази, технічних норм та правил безпечної експлуатації. Нижче подано основні положення, які регулюють проєктування та впровадження подібних систем, зокрема в Калуському ліцеї ім. Д. Бахматюка:

1. Закон України «Про захист персональних даних» [1] встановлює, що зображення особи, отримане через відеокамеру, належить до категорії персональних даних. Відповідно, обробка таких даних повинна здійснюватися на законних підставах, наприклад — для забезпечення безпеки. Обов'язковими є інформування всіх осіб про ведення спостереження, дотримання конфіденційності, а також обмеження доступу до архівів.

2. Закон України «Про освіту» [2] (стаття 25) вимагає від освітніх закладів забезпечення безпечного середовища для учнів та працівників. Це створює правову підставу для впровадження відеоспостереження як засобу профілактики порушень та правопорушень.

3. Закон України «Про інформацію» [3] встановлює вимоги до захисту приватного життя, обмеження доступу до інформації про особу, а також принципи законного збору та обробки даних.

4. Закон України «Про основні засади забезпечення кібербезпеки» [4] визначає напрями захисту інформаційних систем, серед яких — запобігання несанкціонованому доступу, шифрування переданих даних, аудит подій.

З метою дотримання вищезазначених норм, у межах дипломної роботи сформовано проєкт політики безпеки системи відеоспостереження:

1. Мета. Забезпечення безпечного, прозорого та законного функціонування системи відеоспостереження з метою охорони майна, а також захисту учнів, персоналу та відвідувачів.

2. Зона покриття. Відеокамери встановлюються виключно у загальнодоступних приміщеннях: входи/виходи, коридори, подвір'я. Камери не встановлюються в класах, туалетах, роздягальнях — відповідно до принципів непорушності приватного простору.

3. Доступ до відео. Доступ мають лише уповноважені особи (директор, заступник з безпеки, черговий адміністратор). Ідентифікація здійснюється через індивідуальні облікові записи та паролі.

4. Зберігання даних. Відео зберігається на локальному сервері до 30 днів з подальшим автоматичним видаленням. У випадках розслідувань термін може бути подовжено на запит поліції чи адміністрації.

5. Логування подій. Усі дії користувачів (вхід у систему, перегляд, експорт відео) фіксуються у журналі подій, який зберігається 90 днів.

6. Захист даних. Сервер розташовується в окремому приміщенні з обмеженим фізичним доступом. Передача відео здійснюється у зашифрованому вигляді (TLS/HTTPS). Передбачено щоденне резервне копіювання.

7. Відповідальність. Порушення політики використання карається дисциплінарно. Заборонено несанкціоноване використання відео.

8. Правова база. Уся система функціонує відповідно до законів України, з обов'язковим інформуванням працівників та учнів про наявність відеоспостереження.

Для забезпечення сумісності, надійності та безпеки системи відеоспостереження враховано наступні стандарти:

1. ONVIF [6] (Open Network Video Interface Forum)

Міжнародний стандарт сумісності для IP-обладнання. Використання ONVIF-сумісних камер дозволяє інтегрувати різні пристрої в єдину систему без обмеження вибором виробника.

2. ISO/IEC 27001 [5] — Система управління інформаційною безпекою

Описує методи управління ризиками, політики доступу, заходи щодо захисту даних, ведення журналів подій, резервного копіювання, політику збереження.

3. ДСТУ EN 62676 / IEC 62676 [8]

Стандарти для відеоспостереження в сфері безпеки. Регламентують технічні параметри: роздільна здатність, якість запису, частота кадрів, зони виявлення руху.

4. ДСТУ ISO/IEC 29100 [7]

Модель захисту приватності в IT-системах. Визначає базові принципи, як-от мінімізація збирання даних, контроль доступу, прозорість процесів.

Аналіз нормативно-правової бази та технічних вимог свідчить про те, що система відеоспостереження повинна функціонувати в межах чітко визначеного правового поля, з дотриманням принципів законності, конфіденційності та безпеки. У дипломному проєкті ці вимоги реалізовані через політику безпеки, обмеження доступу, шифрування даних, журналювання дій та відповідний вибір обладнання.

1.2 Інформаційні ознаки системи

У межах цієї бакалаврської роботи розглядається система відеоспостереження як інформаційна система, що забезпечує автоматизоване збирання, зберігання, обробку та представлення відеоінформації для підвищення рівня безпеки в навчальному закладі. Така система має всі характеристики повноцінної інформаційної системи — вона забезпечує обробку даних у вигляді відеопотоків, архівування інформації, взаємодію з користувачем через графічний інтерфейс та реалізує функції контролю доступу до даних.

Інформаційний процес, що реалізується в системі, охоплює:

- отримання відеоданих з ір-камер, які передають потік у цифровому вигляді;
- обробку інформації — наприклад, детекцію руху, визначення подій;
- зберігання архівів відеозаписів для подальшого аналізу;
- виведення інформації користувачеві у вигляді потокового перегляду або запису через клієнтський застосунок (локально або віддалено).

У рамках цієї роботи досліджується інформаційна система відеоспостереження на базі програмного забезпечення Partizan CMS, яка реалізує усі згадані етапи інформаційного процесу.

Інформативні ознаки системи (ключові параметри):

- масштабованість системи — можливість гнучко розширювати систему до 30+ камер без додаткових ліцензій або значного ускладнення інфраструктури. У нашому випадку вже передбачено використання 27 камер з поділом на дві логічні підсистеми (1-й поверх і 2-й + 3-й поверхи);
- безпечне зберігання відеоінформації — впроваджена концепція локального архіву відео із циклічним перезаписом на спеціалізованих HDD (WD Purple), що дозволяє гарантувати збереження даних протягом 14 днів і захищає відео від несанкціонованого доступу через механізми авторизації та ізоляцію мережі;
- інтерфейс взаємодії з користувачем — простий клієнт Partizan CMS дозволяє забезпечити повноцінний моніторинг у режимі реального часу, архівний перегляд, управління камерами, налаштування сповіщень про рух без необхідності високої кваліфікації персоналу;
- сегментування системи по поверхах — з огляду на технічні обмеження та особливості будівлі, система реалізована як розподілена: окремі сервери/ПК для 1-го поверху та для 2-го і 3-го, що зменшує навантаження і підвищує надійність.

Інформаційна система спостереження, розроблена в рамках цієї роботи, не лише повторює типові функції аналогічних рішень, але й адаптується до умов саме освітнього закладу: з урахуванням кількості учасників освітнього процесу, особливостей будівлі, нормативних обмежень та потреб адміністрації ліцею. Таким чином, проєктована система має персоналізований характер та орієнтована на забезпечення конкретних інформаційних потреб закладу.

1.3 Аналіз існуючих рішень у сфері освіти

Аналіз існуючих рішень у сфері освіти вимагає комплексного підходу, оскільки системи відеоспостереження все частіше інтегруються в освітні заклади для забезпечення безпеки та покращення навчального середовища. Важливо розуміти, що СВС в школах та університетах - це не просто камери, а складні системи, які можуть включати в себе елементи контролю доступу, системи оповіщення та інтелектуальні функції аналізу відео.

Одним з основних напрямків застосування СВС є забезпечення фізичної безпеки. Відеокамери встановлюються на вході до будівель [9], в коридорах, на спортивних майданчиках та інших публічних місцях для запобігання несанкціонованому доступу та виявлення потенційних загроз [10]. Особливо актуальним є використання СВС для попередження булінгу, вандалізму та інших антисоціальних проявів [11]. В разі виникнення надзвичайних ситуацій, таких як пожежа або напад, СВС можуть бути інтегровані з системами оповіщення для оперативного інформування учнів та персоналу [9].

Окрім безпеки, СВС можуть використовуватися для контролю відвідування та обліку учнів. Системи розпізнавання облич дозволяють автоматично реєструвати присутність учнів на заняттях [10], що значно спрощує роботу викладачів та адміністрації. З іншого боку, такий підхід викликає питання приватності та захисту персональних даних, що потребує ретельного правового регулювання та етичного обґрунтування.

Сучасні СВС все частіше використовують інтелектуальні функції аналізу відео [13]. Це дозволяє не лише фіксувати події, але й автоматично виявляти підозрілу поведінку, розпізнавати об'єкти та визначати потенційні загрози. Наприклад, система може автоматично сповістити охорону про виявлення сторонньої особи на території школи або про скупчення людей у незвичному місці.

Важливо враховувати, що впровадження СВС в освітніх закладах має супроводжуватися чіткими правилами та процедурами використання [12].

Необхідно забезпечити прозорість та відкритість для учнів, батьків та персоналу щодо цілей та методів відеоспостереження. Також слід приділяти увагу захисту даних та запобіганню зловживанням системою.

Окрім вже згаданих чинників, варто додати, що системи відеоспостереження в освітніх закладах можуть виконувати й інші важливі функції. Наприклад, вони можуть бути використані для моніторингу поведінки учнів під час перерв та після уроків [13], що дозволяє виявляти випадки булінгу або інших негативних явищ. Також, відеозаписи можуть бути корисними для аналізу ефективності навчального процесу та виявлення проблемних зон у навчанні.

Важливим аспектом є забезпечення захисту від кібератак на системи відеоспостереження [14]. Зловмисники можуть отримати доступ до відеокамер та використовувати їх для шпигунства, саботажу або розповсюдження шкідливого контенту. Тому необхідно вживати заходів для захисту СВС від несанкціонованого доступу та кібератак, таких як використання надійних паролів, оновлення програмного забезпечення та встановлення брандмауерів.

Необхідно також враховувати питання енергоефективності СВС [15]. Відеокамери та сервери можуть споживати значну кількість електроенергії, що призводить до збільшення витрат на утримання системи. Тому слід вибирати енергоефективні моделі камер та використовувати технології стиснення відео для зменшення обсягу даних, що передаються та зберігаються.

Одним з прикладів впровадження систем відеоспостереження у школах різних країн є система Hikvision у загальноосвітніх школах Польщі (м. Краків).

У місті Краків понад 120 державних шкіл було обладнано системами відеоспостереження на базі рішень від Hikvision. Камери були встановлені в коридорах, біля входів, у їдальнях, спортивних залах та на подвір’ях. Система побудована на основі IP-камер з PoE-живленням і централізованим сервером з програмним забезпеченням HikCentral Professional.

Особливості:

- запис ведеться безперервно (24/7) зберігається 30 днів;

- виявлення порушень (групова бійка, залишені предмети);
- доступ мають лише адміністратори шкіл через захищений інтерфейс.

Результати: згідно з міським звітом, на 37% зменшилась кількість актів вандалізму та на 20% - конфліктних ситуацій між учнями в школах з відеоспостереженням.

Також хорошим прикладом є використання системи Partizan CMS у школах України (Житомирська область).

У 2022–2023 рр. в межах програми «Безпечна школа» частину шкіл Житомирської області було оснащено камерами Partizan IPO-2SP SE, які об'єднуються в локальну мережу з PoE-комутаторами і підключаються до безкоштовного ПЗ Partizan CMS. Це рішення обрано через простоту, низьку ціну та відсутність ліцензійних платежів.

Особливості:

- ПЗ встановлено на комп'ютері охоронця;
- зберігання записів - 7–14 днів;
- немає аналітики, але є підтримка сповіщення про рух;
- доступ до архівів - за запитом адміністрації.

Результати: зменшилась кількість крадіжок особистих речей у школах; зафіксовані випадки виявлення сторонніх осіб на території школи після уроків.

Ще одним прикладом використання таких систем є система Ajax + камери Dahua у приватному ліцеї (м. Львів).

Приватний ліцей у Львові реалізував гібридну систему відеонагляду на базі IP-камер Dahua із вбудованим відеоаналітичним модулем та інтеграцією з системою Ajax. Ключова відмінність - інтелектуальна аналітика, розпізнавання облич та поведінки.

Особливості:

- кожен вхід до класу обладнаний камерою з розпізнаванням облич;
- дані зберігаються на NAS-сервері протягом 60 днів;
- виявлення залишених предметів, підозрілої поведінки;
- доступ керівництва через додаток Ajax PRO.

Результати: покращена безпека, запобігання булінгу, фіксація порушень санітарних норм (маски, дистанція під час карантину).

В таблиці 1.1 порівнюються описані в цьому підрозділі системи відеоспостереження з урахуванням функціональних можливостей, складності впровадження, вартості та доцільності для використання в закладах середньої освіти.

Таблиця 1.1 - Порівняння систем відеоспостереження в освітніх закладах

Критерій	**Hikvision (Польща)**	**Partizan CMS (Житомир)**	**Dahua + Ajax (Львів)**
Тип камер	IP-камери Hikvision	IP-камери Partizan IPO-2SP SE	IP-камери Dahua
Кількість камер (середньо на школу)	16–24	6–12	20+
Програмне забезпечення	HikCentral Professional	Partizan CMS	Ajax PRO + Dahua SmartPSS
Живлення	PoE	PoE	PoE
Наявність відеоаналітики	Так (рух, групи, забуті речі)	Ні (тільки базова детекція)	Так (аналітика, обличчя, поведінка)
Зберігання архіву	До 30 днів	7–14 днів	До 60 днів (NAS)
Тип доступу до камер	Локальний + віддалений (VPN)	Локальний через ПК	Віддалений, мобільний додаток
Можливість масштабування	Висока	Обмежена	Висока
Інтерфейс користувача	Професійний, складний	Простий	Інтуїтивний, зручний
Орієнтовна вартість (на школу)	$4 000–7 000	$600–1 200	$5 000–8 000
Потреби в IT-персоналі	Так	Ні	Частково
Підходить для муніципальних шкіл	Частково (дорого)	Так	Частково (приватний сегмент)

Як видно з аналізу реальних впроваджень, системи відеоспостереження можуть значно відрізнятись за функціональністю, складністю обслуговування та вартістю. Найдоступнішим і найпростішим рішенням для державних закладів

освіти в Україні залишається поєднання Partizan IPO-2SP SE + Partizan CMS, що дозволяє мінімізувати витрати і водночас забезпечити базовий рівень безпеки.

Більш просунуті системи, як-от Dahua + Ajax або Hikvision, дають розширені можливості (аналітика, інтеграція, розпізнавання), але потребують вищого бюджету, наявності серверного обладнання і підготовленого IT-персоналу. Вони можуть бути доцільними для великих ліцеїв, приватних шкіл або в рамках муніципальних проєктів «Безпечне місто».

Враховуючи специфіку Калуського ліцею, доцільно орієнтуватися на бюджетні IP-рішення з відкритим ПЗ, які дають змогу масштабування та забезпечують базову функціональність без надмірних витрат.

1.4 Загальна структура системи відеоконтролю

Сьогодні більшість проєктів з безпеки базуються на сучасних багатофункціональних цифрових системах відеоконтролю, які відповідають актуальним вимогам безпеки об'єктів. Цифрові системи відеоконтролю мають такі важливі переваги [16, 17, 18]:

- висока якість зображення;
- простота управління відеореєстратором і камерою;
- можливість тривалого зберігання даних;
- дистанційне керування системою;
- синхронізація аудіо та відео;
- висока частота кадрів;
- використання стандартного ПК для обробки даних.

Схему цифрової системи відеоконтролю представлено на рисунку 1.1.

Рисунок 1.1 – Система цифрового відеоконтролю

Останніми роками ринок пропонує широкий вибір цифрових систем відеоконтролю, кожна з яких заявляє про свою універсальність та здатність вирішувати будь-які завдання. Це ускладнює вибір оптимальної системи для замовника. Складність вибору також пов'язана з тим, що багато фірм є маловідомими на ринку, а характеристики систем часто подаються у спотвореному вигляді, в першу чергу, в рекламних цілях, що вводить споживача в оману.

Це часто призводить до помилкового вибору цифрових систем відеоконтролю, які не відповідають вимогам технічних характеристик або мають надлишкові функції, що не використовуються в процесі експлуатації. В даний час спостерігається витіснення професійного аналогового обладнання з ринку більш технічно розвиненими та дешевими цифровими системами. Також можна помітити тенденцію до зменшення використання аналогового обладнання в сучасних охоронних комплексах, об'єкти стають інтегрованими розподіленими мережевими системами.

Цифрові системи відеоконтролю перевершують аналогові системи за якістю відео, зручністю використання відеоархіву та наявністю вбудованих багатоканальних детекторів руху. Нові системи значно підвищують рівень безпеки об'єкта. Сучасне цифрове обладнання відеоконтролю наближається за своїми характеристиками до інтелектуальних комп'ютерних систем, що дозволяє

гнучко забезпечувати безпеку об'єктів, використовуючи функції прийняття рішень, аналогічні людській логіці.

Цифрові системи відеоконтролю поділяються на два види [19]: інтегровані та неінтегровані системи.

Інтегровані системи безпеки є гнучкими, оскільки мають розширені функціональні можливості завдяки єдиній апаратно-програмній платформі. Основою інтегрованої системи відеоконтролю є автоматизована система управління із загальним центром управління на базі локальної комп'ютерної мережі. Система включає лінії комунікацій, контролери прийому інформації, які збирають та обробляють дані від датчиків (пожежної та охоронної сигналізації), а також керують засобами автоматизації (оповіщення, протипожежна автоматика та пожежогасіння, інженерні системи).

Неінтегровані системи, на відміну від інтегрованих, є автономними. Вони можуть мати декілька простих тривожних входів/виходів, подібно до аналогових систем відеоконтролю. Іноді, звичайні тривожні входи/виходи помилково представляються як інтеграція, що є некоректним з огляду на примітивну логіку обробки тривожних подій [20].

Серед систем цифрового відеоконтролю виділяють професійні системи, які характеризуються:

- високою якістю відеоряду;
- швидкою обробкою відеосигналів;
- збільшеною ємністю архіву;
- високою надійністю;
- наявністю просунутого детектора руху.

Розглядаючи цифрові системи відеоконтролю, можна виділити дві важливі характеристики [21]:

- можливість роботи в LAN/WAN мережах, що забезпечує віддалений доступ та адміністрування через інтернет;

- функціональність: системи поділяються на вузькоспеціалізовані та багатофункціональні.

Багатофункціональні системи забезпечують гнучку роботу з відеоархівами, багатоканальний цифровий відеозапис, синхронізований запис та читання, а також поєднують функції мультиплексування, відеозапису та відеокомутації. Вузькоспеціалізовані системи мають обмежений набір функцій і використовуються для конкретних завдань, наприклад, для розпізнавання номерних знаків автомобілів.

Для Калуського ліцею найбільш доцільним є використання цифрової системи з підтримкою онлайн-доступу та базової аналітики, яка забезпечує надійність, масштабованість і відповідність вимогам чинного законодавства.

Висновок до розділу

У першому розділі було розглянуто сучасні системи відеоспостереження, їхнє призначення, класифікацію та особливості впровадження в навчальних закладах. Було проаналізовано приклади використання відеоспостереження в освітній сфері, зокрема в школах та університетах, що дозволило виявити типові задачі таких систем.

У межах розділу також сформульовано бачення системи відеоспостереження як інформаційної системи, що реалізує повноцінний інформаційний процес: збір, обробку, зберігання та передачу відеоданих. Визначено інформативні ознаки розроблюваної системи — масштабованість, сегментованість, надійне зберігання, віддалений доступ та адаптація до архітектури будівлі навчального закладу.

Крім того, проведено аналіз чинної нормативно-правової бази, яка регулює функціонування систем відеоспостереження в Україні. Було показано, що дотримання стандартів, таких як ISO/IEC 27001, ONVIF, ДСТУ EN 62676, є необхідною умовою для безпечного впровадження відеоспостереження в освітньому середовищі.

Отримані результати створили методологічну та нормативну основу для подальшого проєктування технічного рішення, що реалізується у наступному розділі.

2 ПРОЄКТУВАННЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ КАЛУСЬКОГО ЛІЦЕЮ

2.1 Схема системи відеоспостереження

Калуський ліцей імені Дмитра Бахматюка є одним з провідних освітніх закладів міста Калуш Івано-Франківської області. У ліцеї навчається 504 учня у 18 класах. Заклад функціонує як комунальна установа, забезпечуючи повну загальну середню освіту за кількома профілями (українська та іноземна філологія, математика).

У структурі закладу працює понад 70 осіб, із них 50 - педагогічні працівники, що забезпечують щоденну взаємодію з великою кількістю учнів.

Ліцей має досить велику будівлю, що включає:

- два крила з класними кімнатами;
- хол, гардеробну, кабінет охорони;
- їдальню, актовий зал;
- бібліотеку, спортивні зали;
- комп’ютерні класи й мультимедійні кабінети;
- подвір’я з футбольним і баскетбольним майданчиками.

Ця структура створює високу інтенсивність переміщення учасників освітнього процесу, особливо в коридорах, сходах, загальних приміщеннях (гардероб, їдальня тощо). Як наслідок, такі ділянки можуть вважатися ризиковими зонами з погляду безпеки.

У зв’язку з великою кількістю учнів, вчителів, технічного персоналу та відвідувачів, важливо забезпечити контроль за доступом, спостереження за переміщенням, а також реакцію на надзвичайні ситуації:

- контроль за входом/виходом сторонніх осіб;
- запобігання актам вандалізму, крадіжкам, булінгу;
- безпечна поведінка в місцях скупчення (їдальня, гардероб, актовий зал);

- надання доказової бази при виникненні конфліктних чи надзвичайних ситуацій;
- підвищення дисципліни та прозорості навчального процесу.

Ліцей має сучасну матеріально-технічну базу, що створює сприятливі умови для впровадження ІТ-рішень, зокрема:

- наявність кабінетів з інтернет-з’єднанням;
- навчальні класи з підведеним живленням і мультимедійним обладнанням;
- простір для монтажу PoE-мережі;
- приміщення охорони, придатне для розміщення серверного обладнання;
- закрита територія з визначеними точками доступу.

Таким чином, структура ліцею, чисельність учасників освітнього процесу, а також розгалуженість внутрішніх маршрутів переміщення обґрунтовують потребу в побудові системи відеоспостереження. Така система дозволить підвищити рівень безпеки, дисципліни та керованості внутрішнього середовища навчального закладу, а також відповідатиме вимогам сучасної інформаційної політики та захисту в освітній сфері.

Проєктована система відеоспостереження для Калуського ліцею охоплює три поверхи навчального корпусу й забезпечує централізований моніторинг за переміщенням людей, контролем доступу до основних приміщень, дотриманням безпеки та дисципліни. На рисунку 2.1-2.2 подано опис функціонального зонування ліцею, який є основою для розміщення елементів відеоспостереження.

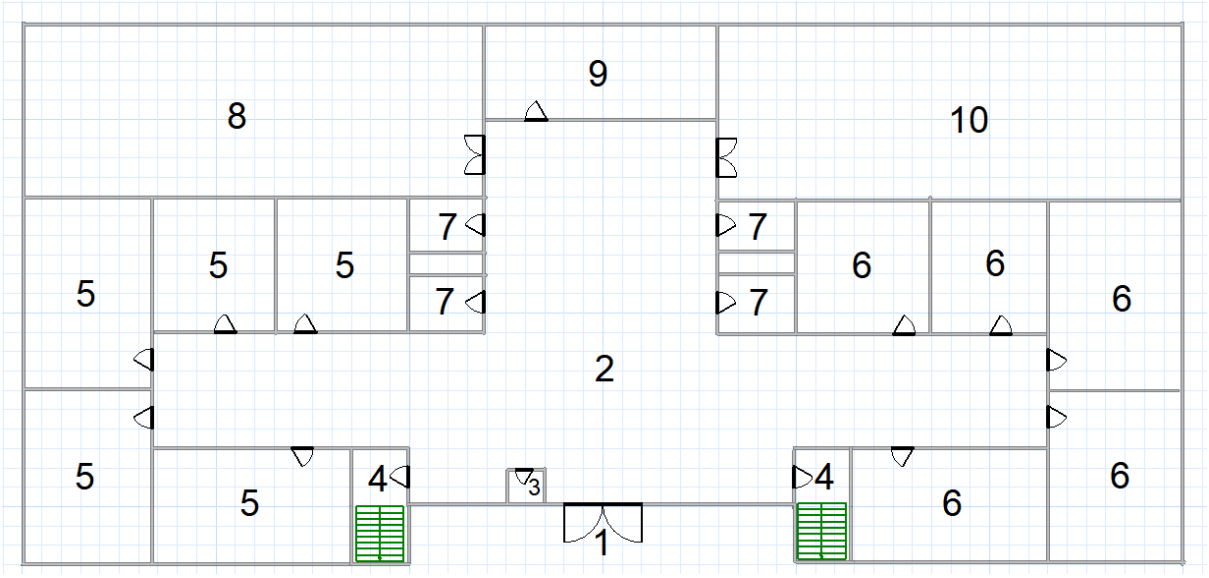

Рисунок 2.1 - Загальна схема першого поверху Калуського ліцею

На рисунку 2.1 показано схематичне планування першого поверху. Основні функціональні зони позначено цифрами від 1 до 10:

1. Вхід у ліцей - основна точка доступу до навчального закладу. Контроль цієї зони є критично важливим для фіксації всіх вхідних/вихідних подій, у тому числі відвідувань сторонніми особами.

2. Головний вестибюль. Тут перебуває значна кількість учнів у перервах та під час початку/завершення навчального дня.

3. Кімната охорони - приміщення, у якому встановлюється основне обладнання системи відеоспостереження:

- сервер із ПЗ Partizan CMS;
- PoE-комутатор для живлення IP-камер;
- джерело безперебійного живлення (UPS);
- монітор, клавіатура, мишка для охоронця.

Така конфігурація забезпечує локальне зберігання відео, доступ до архівів, віддалене адміністрування та живлення камер по одному кабелю (Ethernet + живлення через PoE).

4. Входи до сходів на 2 поверх - критичні точки, що дають вертикальний доступ між поверхами. Потребують постійного візуального нагляду, щоб уникнути несанкціонованих переміщень або конфліктів.

5. Адміністративні кабінети - приміщення, де працюють директор, заступники, секретаріат, учительська. Як центр управління освітнім процесом, ця зона потребує особливого контролю (особливо поза робочим часом).

6. Навчальні кабінети для учнів - аудиторії, де проходить основна частина навчального процесу. Моніторинг переміщень у коридорах біля них є важливим з точки зору безпеки та дисципліни.

7. Туалети - згідно з правовими обмеженнями, відеоспостереження всередині санітарних зон не допускається. Однак можливо вести спостереження за входами до цих приміщень.

8. Їдальня - місце з масовим скупченням учнів у години обіду. Нагляд забезпечує дисципліну, а також може бути корисним для вирішення конфліктних ситуацій.

9. Гардеробна - зона, де зберігається особистий одяг учнів. Є ризиковою зоною щодо крадіжок, тому потребує фіксації всіх переміщень.

10. Актовий зал - багатофункціональне приміщення для проведення загальношкільних заходів, концертів, зборів. Під час подій - підвищений ризик втрати речей або конфліктів.

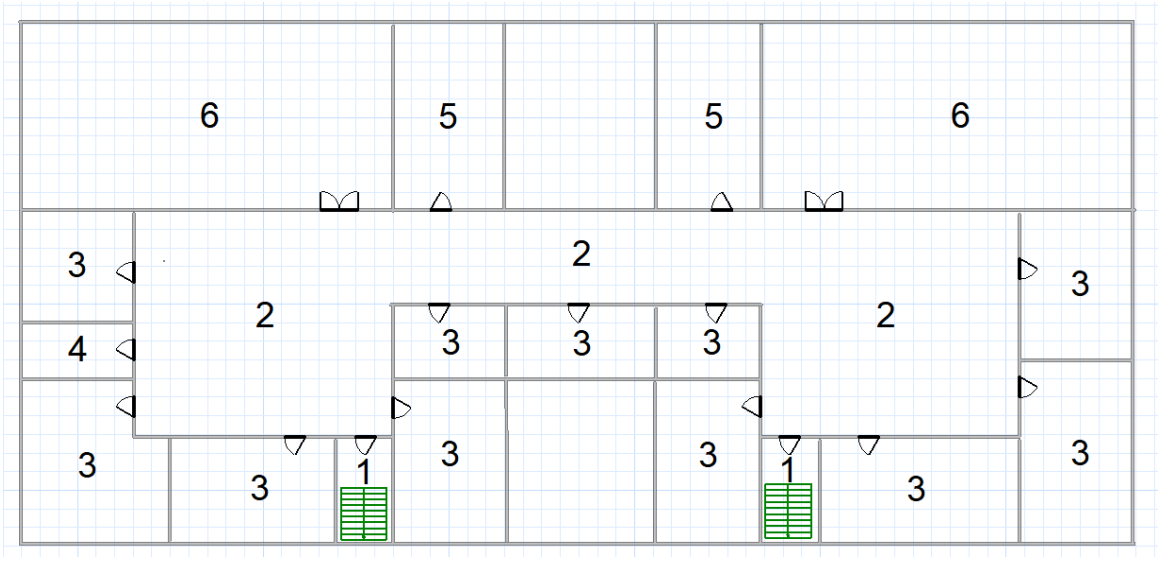

Рисунок 2.2 - Загальна схема другого поверху Калуського ліцею

Другий поверх є продовженням навчального простору, однак із певними додатковими функціональними приміщеннями, зокрема для фізичного виховання. На схемі позначено:

1. Сходи між поверхами - забезпечують вертикальні переміщення між 1, 2 та 3 поверхами. Саме в цій зоні найчастіше трапляються конфлікти або порушення дисципліни, тому тут також доцільно встановлювати камери.

2. Коридор другого поверху - головна транспортна артерія між навчальними кабінетами, спортивними приміщеннями та адміністративними зонами. Забезпечення відеонагляду тут дозволяє фіксувати усі переміщення та контролювати масову поведінку учнів.

3. Навчальні кабінети - класи, де відбувається освітній процес. Камери встановлюються не всередині, а в коридорі поблизу дверей до цих приміщень.

4. Технічна кімната - спеціально відведене приміщення для розміщення інфраструктурного мережевого обладнання:

- сервер із ПЗ Partizan CMS;
- PoE-комутатор для живлення IP-камер 2-го і 3-го поверху;
- джерело безперебійного живлення (UPS);
- монітор, клавіатура, мишка.

5. Дві роздягальні - приміщення для перевдягання перед заняттями фізкультурою. Встановлення камер усередині заборонене, але доцільно контролювати вхідні двері.

6. Два спортивні зали - використовуються для фізичного виховання. Тут можуть траплятись як нещасні випадки, так і порушення дисципліни. Відеоспостереження дозволяє фіксувати всі дії під час занять.

Таким чином, аналіз просторової структури ліцею на обох поверхах дозволяє спроєктувати систему відеоспостереження, яка охоплює ключові зони ризику, забезпечує контроль за вертикальними і горизонтальними маршрутами пересування, дозволяє обмежити доступ до критичних приміщень та створює умови для безпечного і контрольованого освітнього процесу.

На рисунках 2.3-2.17 подано покрокове розміщення камер та пояснення щодо вибору кожної позиції і напрямку спостереження.

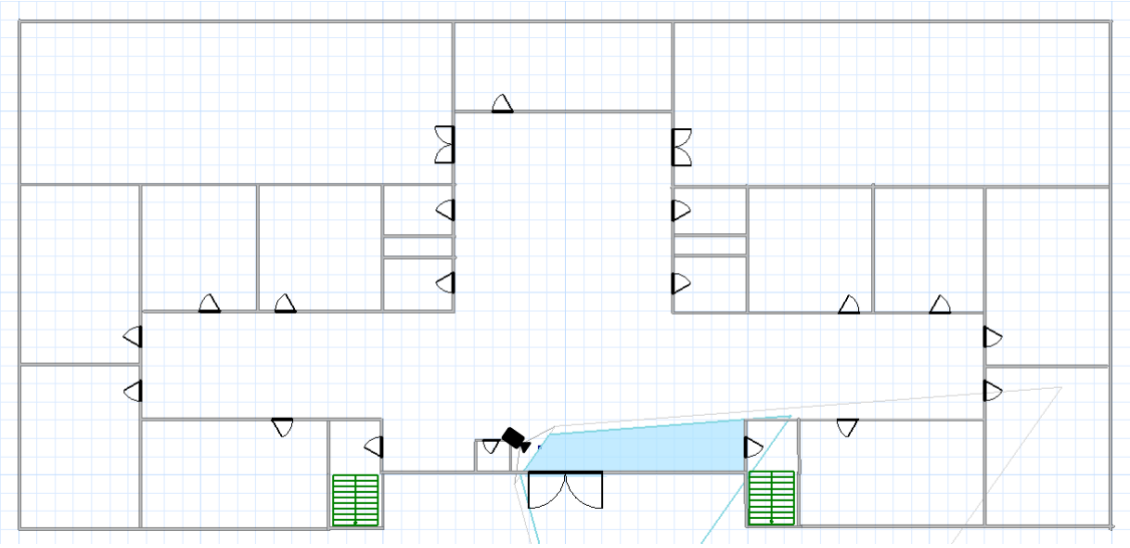

Рисунок 2.3 – Камера №1.1: Вхід у ліцей + сходи (праве крило)

Перша камера розташована навпроти головного вхоіду і орієнтована так, щоб охопити всю зону перед дверима, а також частково - вхід на сходи в правому крилі. Це дозволяє:

- чітко фіксувати всіх осіб, які заходять або виходять;
- виявляти спроби несанкціонованого проникнення;
- бачити маршрути переміщення одразу після входу в ліцей.

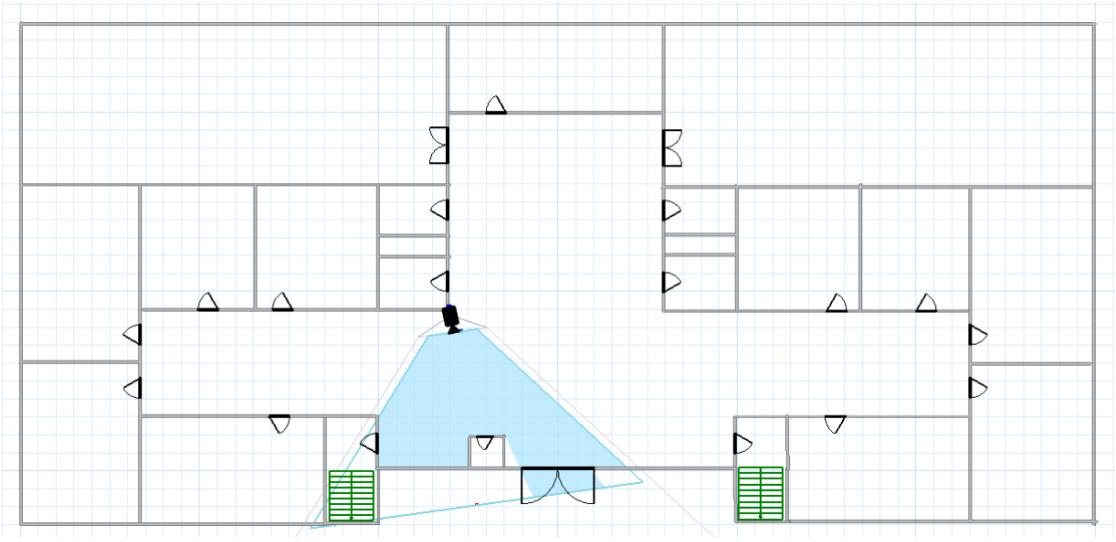

Рисунок 2.4 – Камера №1.2: Кімната охорони + сходи (ліве крило) + головний вхід

Камера охоплює одразу три важливі точки:

- вхід у кімнату охорони;

- сходи у лівому крилі;
- частину головного входу.

Це важливо для:

- захисту доступу до технічного вузла СВС;
- моніторингу потоків учнів по коридору;
- підтримки візуального контакту з обома сходовими маршами.

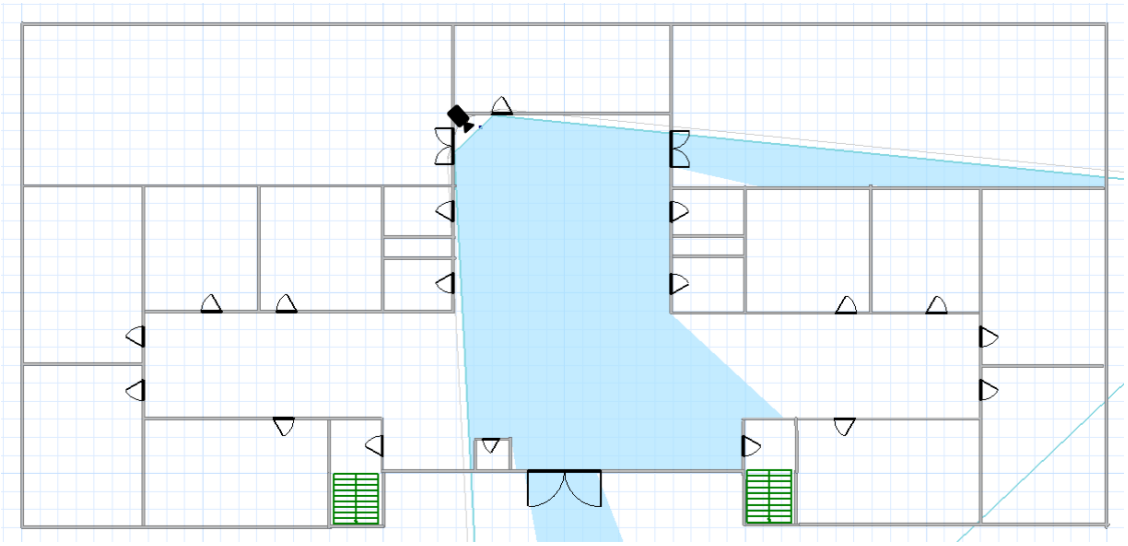

Рисунок 2.5 – Камера №1.3: Їдальня, гардероб, актовий зал + додаткові зони

Одна з найважливіших камер: розміщена у центральній зоні, вона фіксує:

- вхід у їдальню;
- гардеробну;
- вхід в актовий зал;
- також частково - туалети, головний вхід, охоронну зону, сходи.

Це багатозональне охоплення дозволяє:

- вести спостереження у годинах пік (перед уроками, обід);
- запобігати крадіжкам речей із гардеробу;
- мати доказову базу у разі конфліктів під час масових заходів.

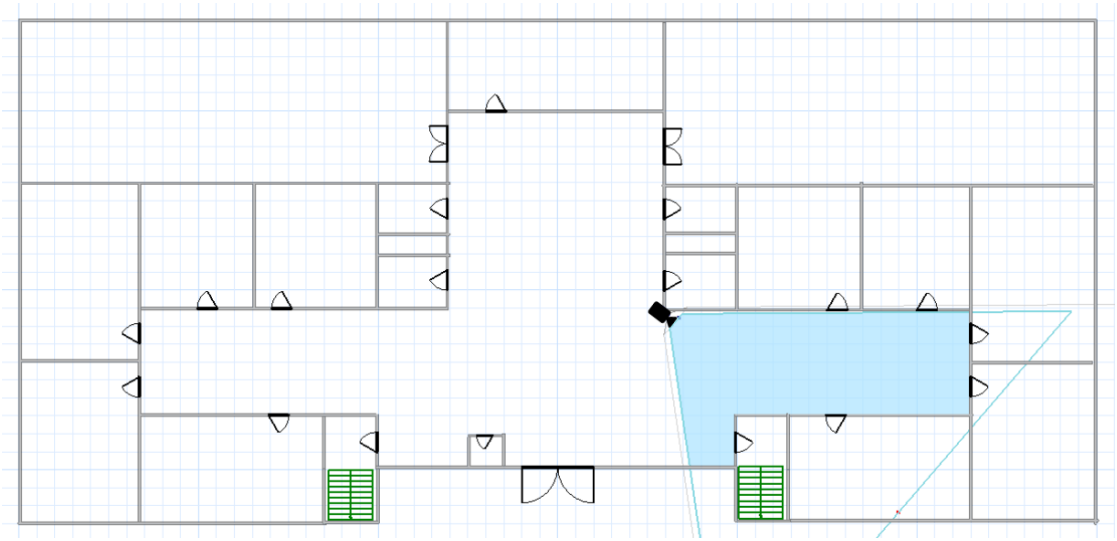

Рисунок 2.6 – Камера №1.4: Праве крило - сходи + кабінети

Ця камера розміщена в правому коридорі, орієнтована на:

- вхід на праві сходи;
- двері навчальних кабінетів.

Фіксує активність учнів у навчальний і позаурочний час, забезпечує контроль за вертикальними переміщеннями і дисципліною в коридорі.

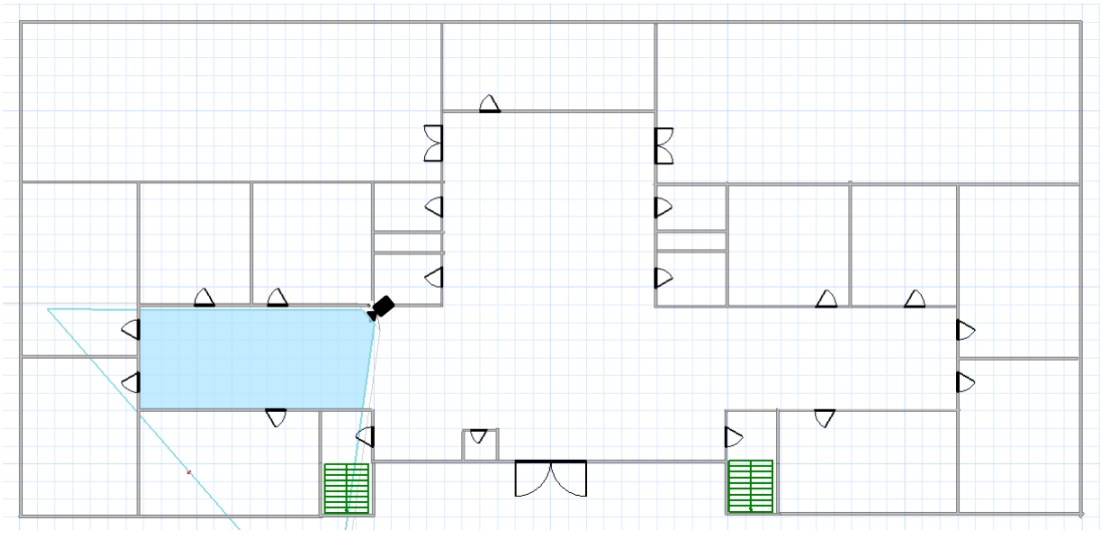

Рисунок 2.7 – Камера №1.5: Ліве крило - навчальні кабінети

Симетрична до попередньої, ця камера охоплює:

- коридор лівого крила;
- двері кабінетів;
- рух у напрямку лівої сходової клітки.

Обидві камери (1.4 і 1.5) створюють повноцінну систему контролю обох крил будівлі.

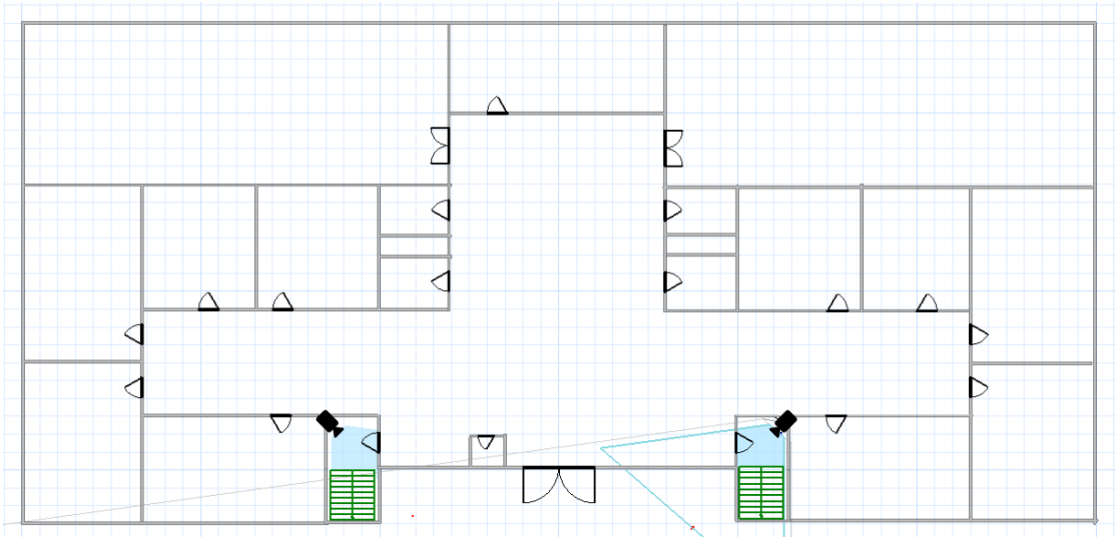

Рисунок 2.8 – Камера №1.6 і 1.7: Всередині сходових ніш

Камери встановлені безпосередньо в просторі, де починаються сходи:

- одна для правого крила, одна для лівого.

Це дозволяє:

- фіксувати рухи по вертикалі (наверх, вниз);
- контролювати поведінку в місцях, де часто трапляються конфлікти або порушення.

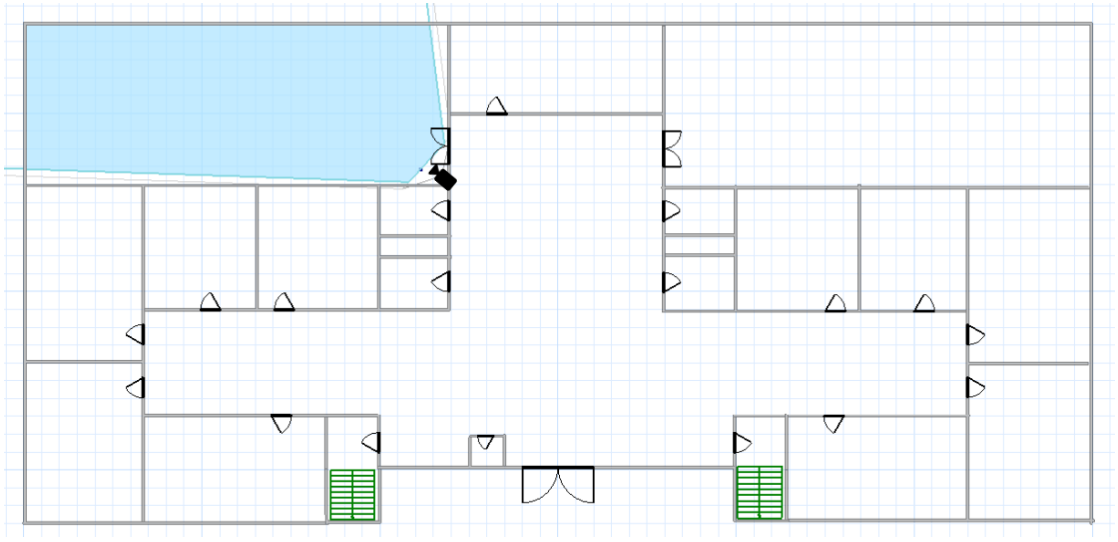

Рисунок 2.9 – Камера №1.8: Їдальня

Встановлена ближче до входу в їдальню і спрямована всередину приміщення. Мета:

- зафіксувати поведінку учнів під час обіду;
- уникнути пошкоджень майна, розлитої їжі тощо;
- мати повний огляд під час великої кількості учнів.

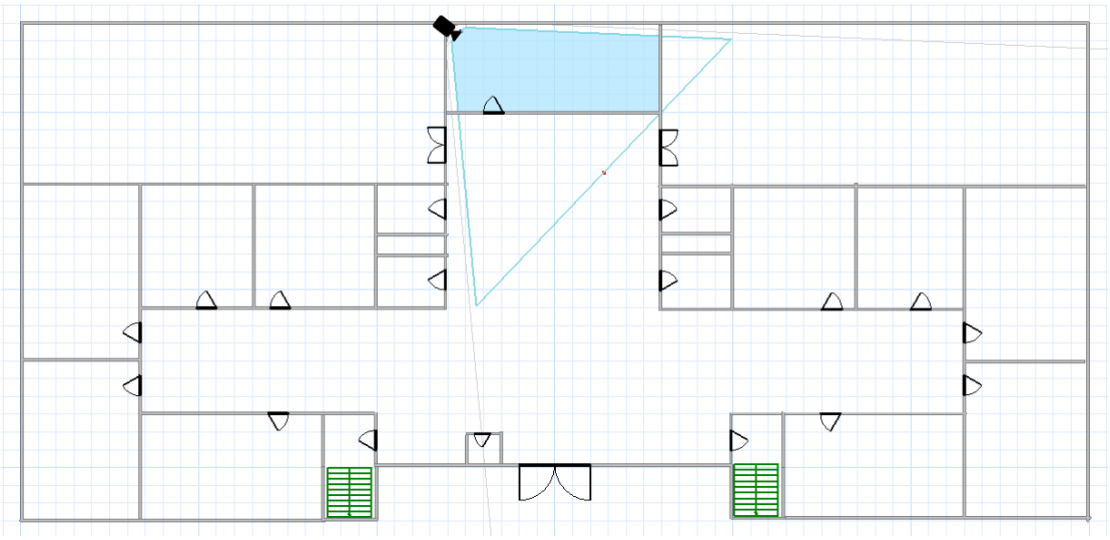

Рисунок 2.10 – Камера №1.9: Гардероб

Спрямована всередину гардеробу:

- важливо через скупчення особистих речей;
- допомагає адміністрації в разі втрат або конфліктів.

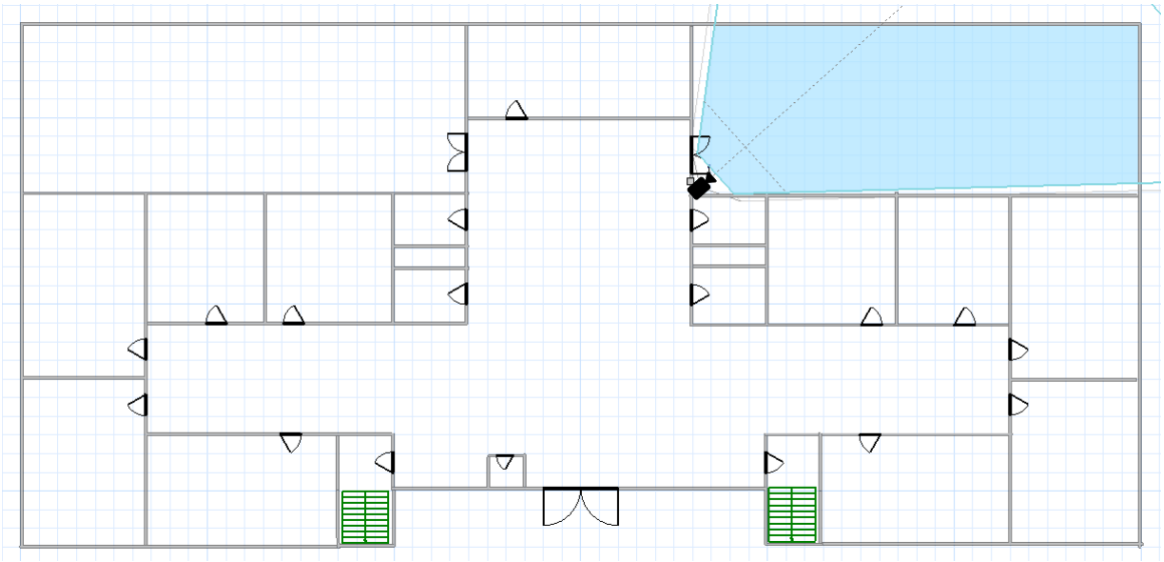

Рисунок 2.11 – Камера №1.10: Актовий зал

Спрямована всередину залу, дозволяє:

- контролювати підготовку до подій;

- вести запис заходів (може бути джерелом архівного відео);
- забезпечити безпеку під час загальношкільних подій.

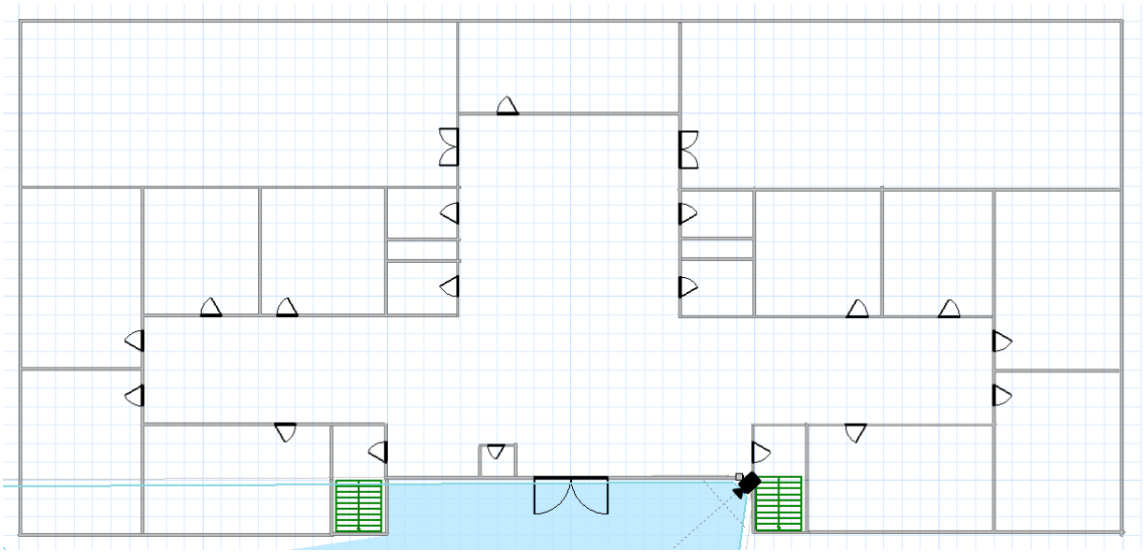

Рисунок 2.12 – Камера №1.11: Зовнішнє спостереження за входом

Камера встановлена на вулиці, біля входу, спрямована на:

- фіксацію облич усіх, хто входить;
- спостереження за територією перед ліцеєм;
- контроль нічних інцидентів або сторонніх осіб.

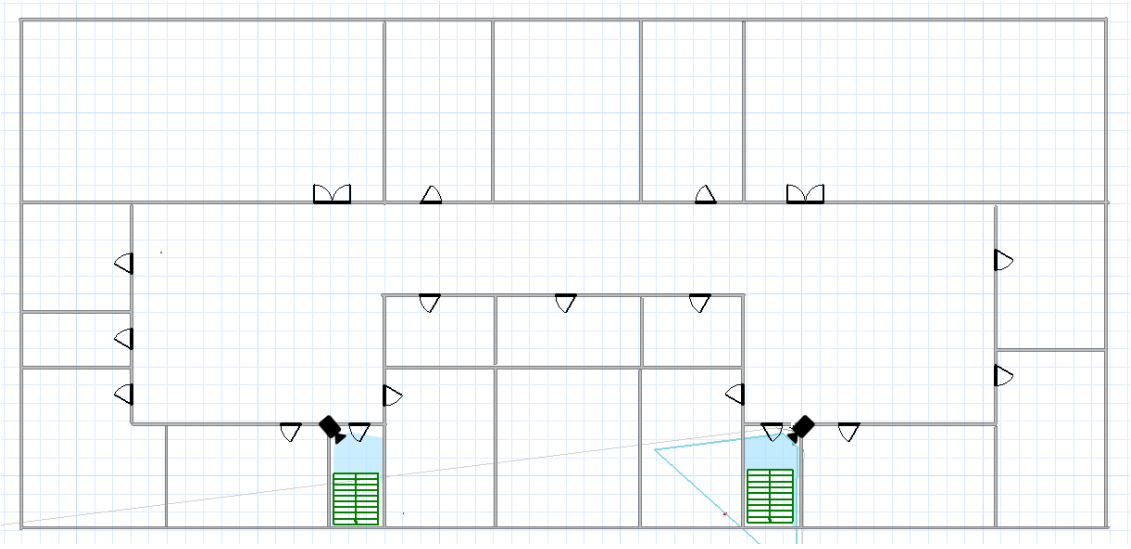

Рисунок 2.13 – Камера №2.1 і 2.2: Сходи з першого на другий поверх (праве і ліве крило)

Обидві камери встановлені в аналогічних місцях, як і на першому поверсі - в зоні сходових майданчиків, на виході зі сходів. Вони:

- фіксують усіх, хто піднімається на другий поверх;
- забезпечують безперервний відеонагляд між поверхами;
- працюють у тандемі з камерами, встановленими на першому поверсі в аналогічних точках (камери 1.6 і 1.7), що створює вертикальне відеопокриття.

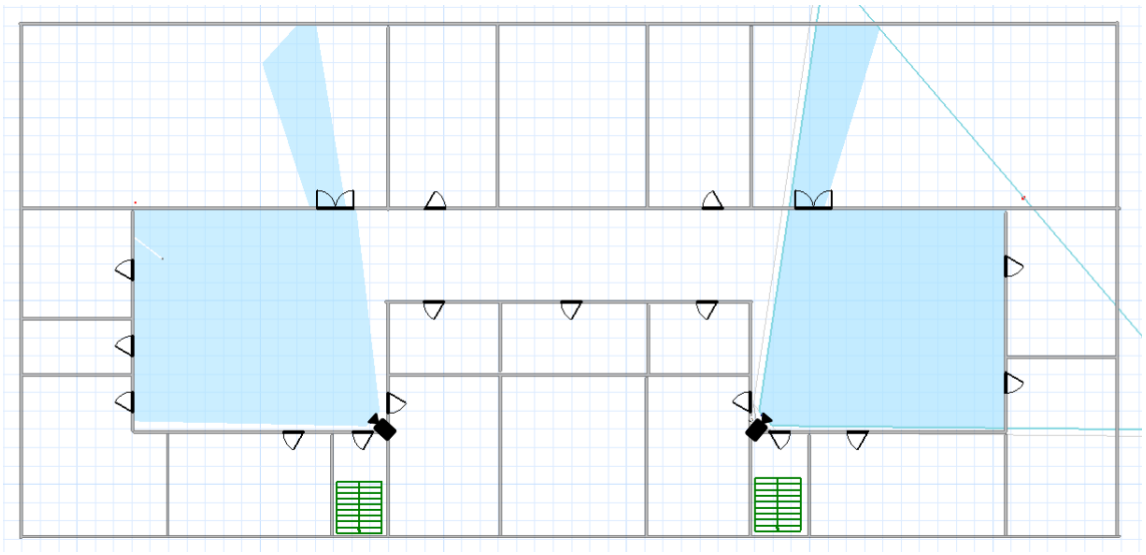

Рисунок 2.14 – Камера №2.3 і 2.4: Вихід зі сходів + спортзал + технічна кімната

Ці дві камери (рис.2.14) охоплюють більші площі у відповідних крилах:

- ліва камера: фіксує вихід зі сходів, кабінети в лівому крилі, вхід до технічної кімнати (де розміщене мережеве обладнання), а також вхід до спортзалу;
- права камера: фіксує аналогічно вихід зі сходів у правому крилі, навчальні кабінети та вхід до правого спортзалу.

Обґрунтування:

- забезпечується контроль у разі несанкціонованого доступу до технічної кімнати;
- покриття маршрутів пересування учнів до кабінетів і спортивних залів.

Ці дві камери (рис.2.15) орієнтовані так, щоб:

- ліва камера: охопити коридор перед навчальними кабінетами, вхід до технічної кімнати, лівий спортзал і роздягальню;
- права камера: відповідно фіксує праву роздягальню, кабінети в правому крилі, вхід до правого спортзалу.

Це важливі точки, оскільки:

- роздягальні - це зони ризику (особисті речі, конфлікти);
- вхід до спортзалу - місце великого трафіку під час уроків фізкультури;
- технічна кімната потребує захисту (мережеве обладнання).

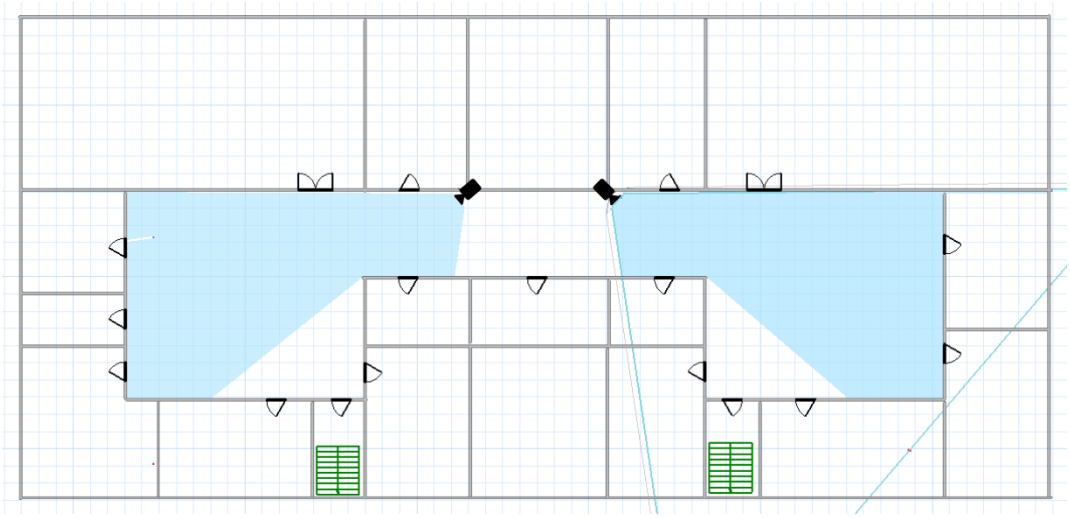

Рисунок 2.15 – Камера №2.5 і 2.6: Кабінети + роздягальні + спортзали

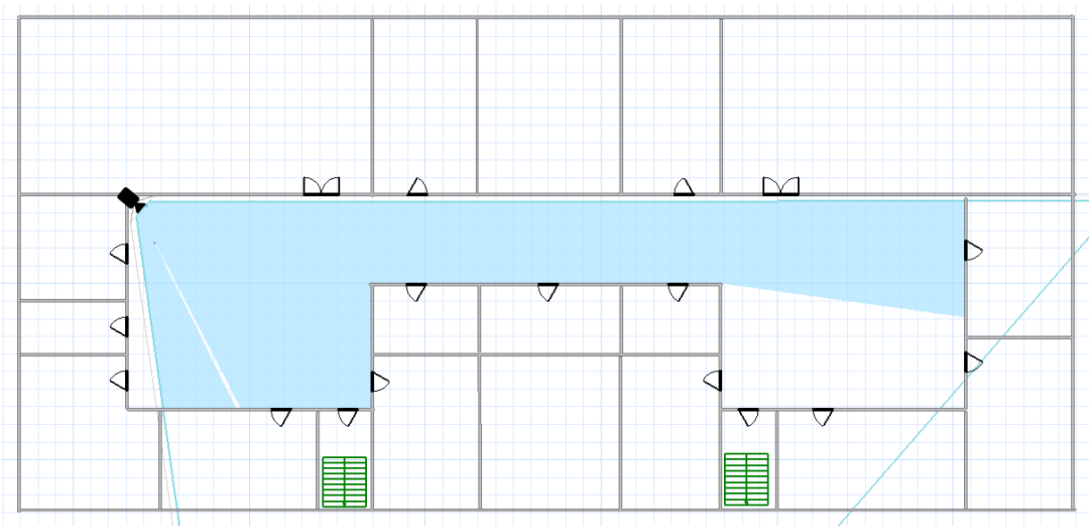

Рисунок 2.16 – Камера №2.7: Центральний коридор другого поверху

Ця камера (рис.2.16) встановлена в центральному перехідному коридорі, забезпечує:

- ширококутове охоплення обох крил (ліва та права частина другого поверху);
- фіксує входи до роздягалень, кабінетів, спортзалів, вихід на сходи та технічну кімнату.

Обґрунтування:

- усуває можливі “мертві зони”;
- дає повну панораму дій на другому поверсі;
- працює як резервний вузол огляду для дублювання критичних зон.

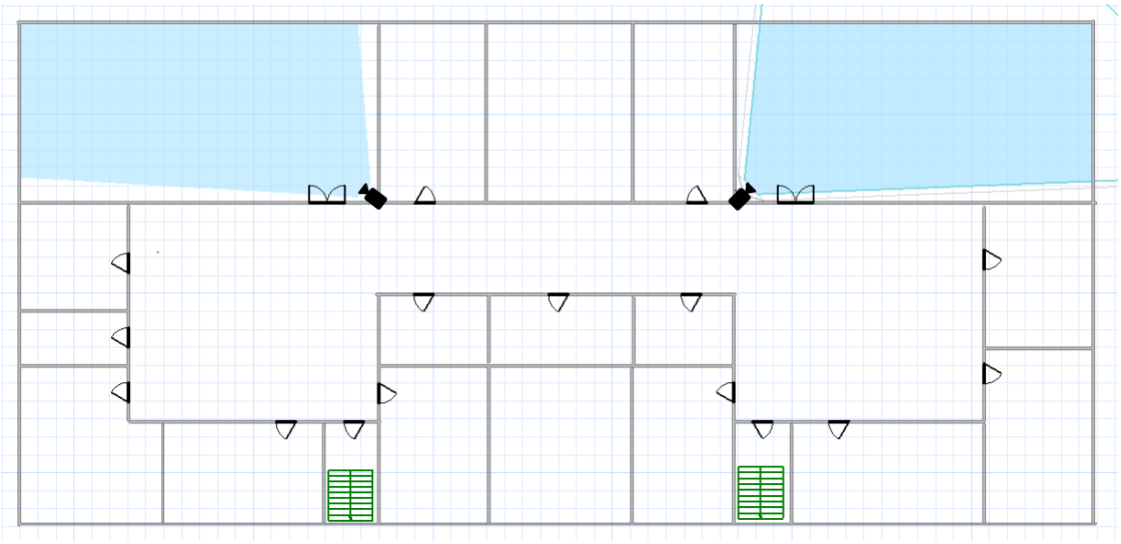

Рисунок 2.17 – Камера №2.8 і 2.9: Усередині спортивних залів

Останній рисунок і найбільш специфічні камери (рис. 2.17):

- кожна камера встановлена всередині свого спортзалу (лівого й правого);
- орієнтована на центральну частину зали та зону входу/виходу.

Призначення:

- контроль безпеки під час занять;
- фіксація нещасних випадків, конфліктів, неправомірної поведінки;
- підтримка дисципліни та можливість аналізу спортивних активностей.

Слід зазначити, що будівля Калуського ліцею має також третій поверх, архітектурно схожий на другий. Спортивні зали в ліцеї займають два рівні - другий і третій поверх, отже, система відеоспостереження має враховувати вертикальну структуру будівлі.

На третьому поверсі передбачається аналогічна схема розміщення камер, як і на другому, з однією відмінністю - на третьому поверсі не встановлюються камери в спортивних залах, оскільки вони вже повністю охоплюються камерами з другого рівня. Відповідно, на третьому поверсі буде встановлено ще 7 камер, що забезпечать контроль:

- виходів зі сходів;
- коридору;
- входів до кабінетів;
- службових і технічних приміщень.

Таким чином, загальна кількість камер у системі відеоспостереження складе 27 одиниць, з яких:

- 11 розміщені на першому поверсі;
- 9 - на другому поверсі;
- 7 - на третьому поверсі.

На основі аналізу архітектури будівлі Калуського ліцею та з урахуванням зон ризику, місць масового скупчення учнів і маршрутів пересування, сформовано структуру системи відеоспостереження, яка охоплює всі критично важливі ділянки.

Загальна система з 27 камер дозволяє здійснювати:

- контроль над усіма входами та виходами з будівлі;
- спостереження за переміщенням учнів між поверхами;
- моніторинг навчальних, адміністративних, технічних приміщень;
- нагляд у зонах загального користування - гардеробі, їдальні, актовому залі, спортивних залах.

Такий підхід гарантує повноцінний візуальний контроль за всіма безпековими процесами в закладі, підвищує рівень дисципліни та дозволяє швидко реагувати на інциденти або порушення. Крім того, система залишається масштабованою, з можливістю інтеграції зовнішніх камер або розширення аналітичного функціоналу в майбутньому.

Для забезпечення ефективного функціонування системи відеоспостереження у Калуському ліцеї була розроблена структурна схема, яка відображає взаємозв'язок між основними компонентами системи: відеокамерами, мережевим обладнанням, відеореєстратором, серверною частиною та програмним забезпеченням для управління і моніторингу.

Основною метою побудови системи відеоспостереження є створення централізованої, надійної та розподіленої інфраструктури відеоконтролю, яка забезпечує постійний моніторинг ситуації в приміщеннях Калуського ліцею, запис і архівування відеоінформації, а також локальний і віддалений доступ до архівів у межах дозволених прав.

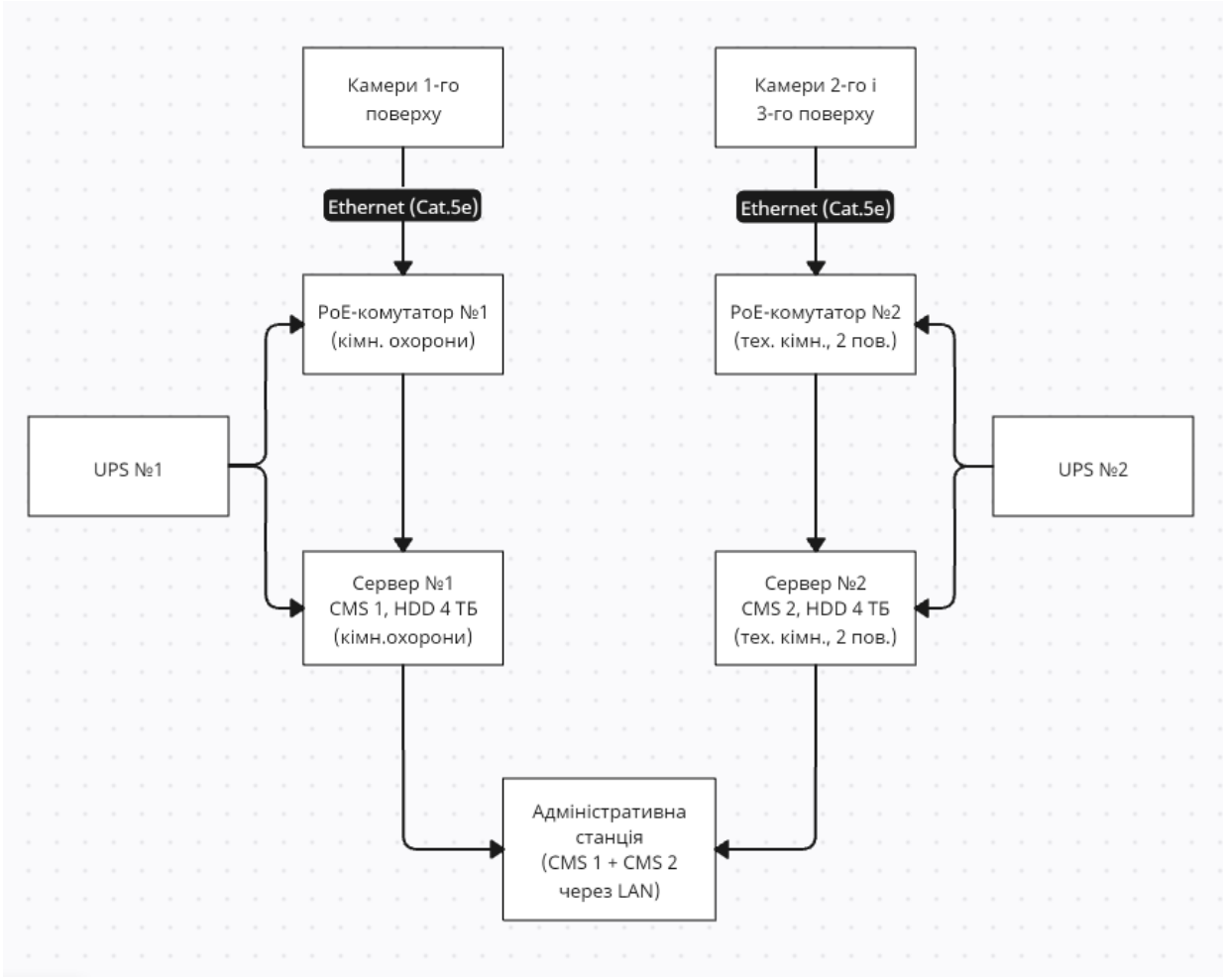

Рисунок 2.18 – Структурна схема системи відеоспостереження

Структурна схема системи відеоспостереження (рисунок 2.18) демонструє загальну архітектуру побудови системи в межах навчального закладу. В її основі

- розподілене підключення IP-камер до серверів з обробки та зберігання відеоданих, що дає змогу ефективно охопити всі критичні зони будівлі. Для кожної групи камер передбачено окремий вузол керування та архівації, що дозволяє оптимально розподілити навантаження між поверхами й забезпечити стабільність роботи.

Такий підхід дозволяє реалізувати масштабовану систему з можливістю подальшого розширення, інтеграції додаткових функцій (наприклад, аналітики подій, розпізнавання облич) та централізованого контролю за ситуацією в режимі реального часу. Система орієнтована на максимальну зручність адміністрування, гнучкість у конфігурації та відповідність реальним потребам освітнього процесу.

Для кращого розуміння функціональних можливостей розробленої системи відеоспостереження було побудовано діаграму прецедентів (рисунок 2.19), яка відображає основні дії користувачів у системі.

Рисунок 2.19 – Діаграма прецедентів для системи відеоспостереження

У системі є два типи користувачів: адміністратор та охоронець. Обидва мають доступ до функцій перегляду відео — як у реальному часі, так і до архівних записів. Адміністратор додатково виконує дії з управління користувачами, налаштування системи та видалення записів. Таким чином, обсяг повноважень адміністратора ширший, ніж у охоронця, але базові функції доступні обом.

Також побудовано діаграму послідовностей для одного з ключових сценаріїв — перегляд архівного відео. Вона демонструє взаємодію між компонентами системи в часі, що особливо важливо для розуміння логіки функціонування системи на рівні запитів.

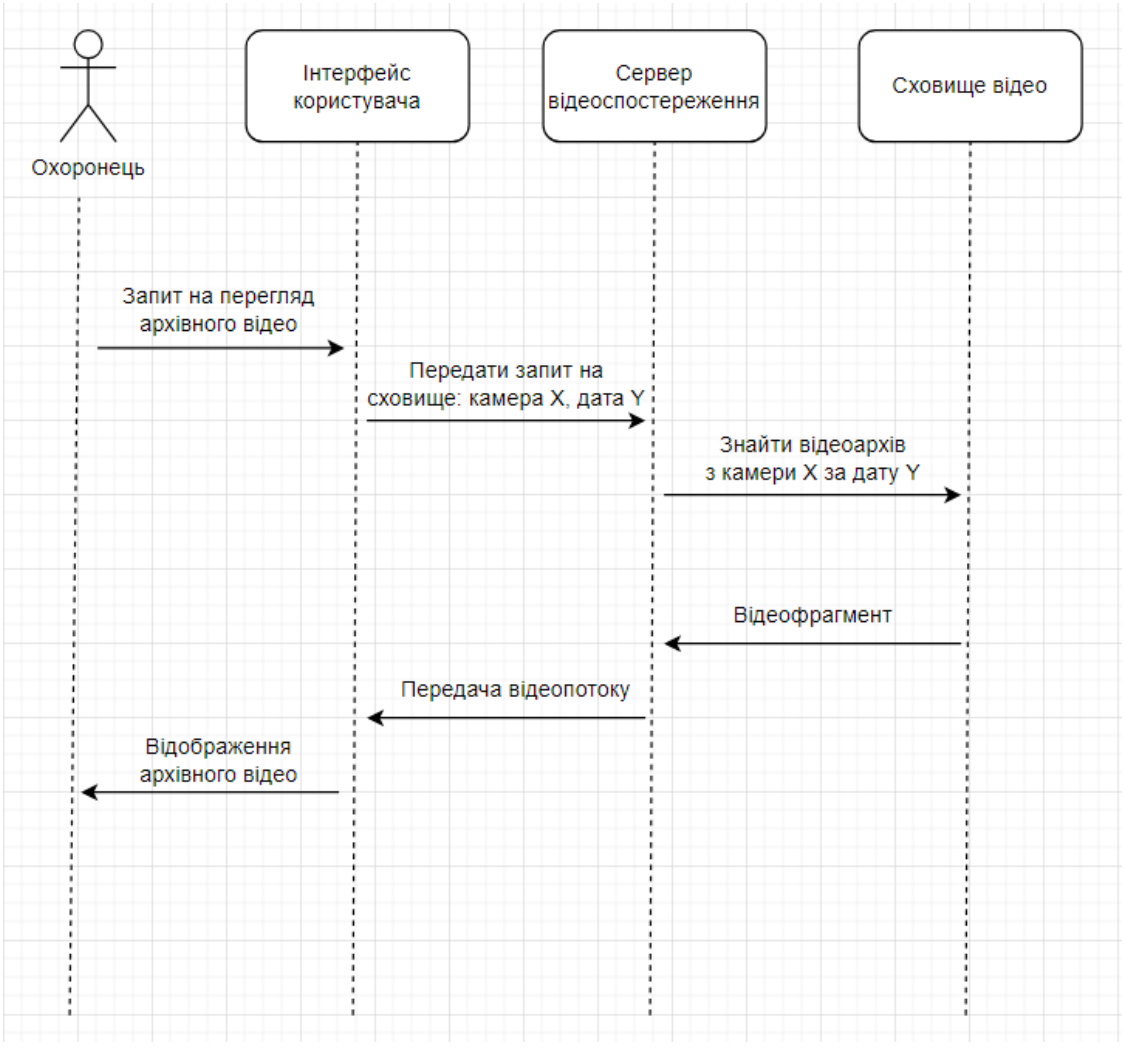

Рисунок 2.20 – Діаграма послідовності сценарію “Перегляд архівного відео”

Процес починається з того, що охоронець через інтерфейс програми надсилає запит на перегляд архівного відео. Інтерфейс передає цей запит до

сервера відеоспостереження, зазначаючи камеру та дату. Сервер звертається до сховища відео з метою знайти відповідний архів. Після знаходження відеофрагмента, дані передаються назад на сервер, який транслює відеопотік до інтерфейсу користувача. В результаті, на стороні користувача відображається запитане архівне відео.

Дана діаграма дозволяє наочно продемонструвати, як відбувається комунікація між складовими системи під час запиту архіву.

Одним з ключових компонентів будь-якої сучасної системи відеоспостереження є інформаційна база, що забезпечує облік користувачів, камер, подій та відеоархівів. Для системи, спроєктованої в межах цієї роботи, реалізовано просту, але ефективну реляційну модель бази даних, яка відповідає вимогам до масштабованості, безпеки та зручності обслуговування.

Базу даних побудовано на основі чотирьох логічно взаємопов'язаних таблиць: Користувачі (табл. 2.1), Камери (табл. 2.2), Відеоархів (табл. 2.3), Журнал подій (табл. 2.4). Вони охоплюють основні об'єкти системи відеоспостереження й дозволяють зберігати метаінформацію про всі дії, що відбуваються в системі.

Таблиця 2.1 – Структура таблиці «Користувачі»

Поле	Тип	Призначення
id	INTEGER	Первинний ключ
login	TEXT	Ім'я користувача
password_hash	TEXT	Хеш пароля для авторизації
role	TEXT	Роль користувача (адміністратор, охоронець)

Ця таблиця забезпечує контроль доступу до системи. Залежно від ролі, користувач отримує різні права: наприклад, охоронець — лише на перегляд відео, а адміністратор — на керування системою.

Таблиця 2.2 – Структура таблиці «Камери»

Поле	Тип	Призначення
id	INTEGER	Унікальний ідентифікатор камери
name	TEXT	Назва камери
location	TEXT	Поверх або приміщення встановлення
ip_address	TEXT	Мережева IP-адреса камери

Інформація про камери використовується при відображенні потоку, збереженні архівів та формуванні запитів на пошук.

Таблиця 2.3 – Структура таблиці «Відеоархів»

Поле	Тип	Призначення
id	INTEGER	Первинний ключ
camera_id	INTEGER	Зв’язок із камерою (зовнішній ключ)
date_start	DATETIME	Час початку запису
date_end	DATETIME	Час завершення запису
file_path	TEXT	Шлях до відеофайлу на сервері

Ця таблиця виконує функцію індексації відеофайлів. Самі записи зберігаються на жорсткому диску з доступом через локальну мережу.

Таблиця 2.4 – Структура таблиці «Журнал подій»

Поле	Тип	Призначення
id	INTEGER	Первинний ключ
user_id	INTEGER	Зв’язок із користувачем (зовнішній ключ)
event_time	DATETIME	Час події
event_type	TEXT	Тип дії (вхід, експорт відео, перегляд архіву)
description	TEXT	Опис події

Журнал подій виконує функцію моніторингу дій усіх користувачів системи. Це підвищує прозорість та дозволяє виявити спроби несанкціонованого доступу або зловживання.

Таблиця Відеоархів має зовнішній ключ camera_id, який посилається на таблицю Камери, а Журнал подій пов’язаний через поле користувач_id із таблицею Користувачі. Така структура дозволяє реалізувати цілісність даних і підтримувати логічні зв’язки між об’єктами.

У межах реалізації проєкту було обрано використання вбудованої бази даних, яка інтегрована в програмне забезпечення системи відеоспостереження. Такий підхід дозволяє уникнути складної серверної інфраструктури, зменшити витрати на впровадження та забезпечити достатній рівень продуктивності для невеликої локальної мережі навчального закладу.

У якості сховища даних обрано формат SQLite — легку реляційну базу даних, що не потребує окремого сервера та зберігається у вигляді одного файлу на диску. Це дозволяє безпосередньо вбудувати логіку роботи з базою даних у

програмний інтерфейс і уникнути мережевих затримок при запитах. З технічного погляду, база даних ініціалізується під час першого запуску програми, а її оновлення відбувається автоматично при додаванні нових камер, збереженні відео або фіксації дій користувачів.

Такий підхід має низку переваг:

- мінімальні ресурси для запуску. Не потрібно встановлювати або адмініструвати окрему СУБД;
- висока швидкодія при локальному використанні. Усі запити виконуються миттєво, без звернення до зовнішніх серверів;
- простота резервного копіювання. Достатньо скопіювати один файл бази даних;
- інтеграція в логіку ПЗ. Усі запити формуються й виконуються програмно, відповідно до подій інтерфейсу.

Разом із тим, для забезпечення безпеки доступу до інформації, файл бази даних зберігається на захищеному розділі жорсткого диска. У системі передбачено обмеження прав на доступ до цього файлу: лише адміністратор ОС та сама програма мають дозвіл на читання й запис. За необхідності можна додатково застосовувати повнодискове шифрування (наприклад, BitLocker у Windows).

Завдяки продуманій структурі таблиць та зв’язків між ними, система забезпечує:

- зручне управління правами доступу;
- швидкий пошук відеозаписів за датою, подією чи користувачем;
- збереження логів активності для аудиту;
- можливість масштабування — наприклад, додавання нових камер чи нових рівнів користувачів без зміни структури.

Використання вбудованої бази даних дає змогу розгорнути повноцінну систему відеоспостереження на одному комп’ютері без зовнішніх залежностей, що ідеально підходить для навчального закладу з обмеженим бюджетом та чітко визначеним переліком вимог до безпеки. Такий підхід дозволяє зробити систему

максимально автономною, надійною й простою в адмініструванні, що повністю відповідає цілям цього проєкту.

2.2 Загальні вимоги до системи

Система відеоспостереження для Калуського ліцею ім. Д. Бахматюка має забезпечити надійний захист навчального закладу, підвищити рівень безпеки учнів і співробітників, а також сприяти збереженню майна. Ці вимоги враховують специфіку навчального закладу, необхідність захисту персональних даних та забезпечення ефективного функціонування системи в різних умовах.

Система повинна забезпечувати безперервне відеоспостереження за визначеними зонами ліцею (вхідні групи, коридори, спортивний зал, прилегла територія) в режимі реального часу. Важливо, щоб система автоматично записувала відео з камер спостереження та зберігала його на надійному носії. Обсяг сховища має бути достатнім для зберігання відеоархіву протягом заданого періоду (наприклад, 30 днів).

Система може включати функції інтелектуального аналізу відео, такі як розпізнавання облич, виявлення руху, перетин лінії, залишення об'єкта, для автоматичного виявлення та реагування на підозрілі події. Також важливим є забезпечення можливості віддаленого перегляду відео в режимі реального часу та перегляду архівних записів з авторизованих пристроїв (комп'ютер, смартфон, планшет) через захищене з'єднання. Для зручності керування, система повинна мати інтуїтивно зрозумілий інтерфейс для керування налаштуваннями, користувачами, камерами, архівом та іншими функціями.

З точки зору безпеки, система повинна забезпечувати конфіденційність відеоданих та захист від несанкціонованого доступу, перегляду, копіювання чи зміни. Доступ до системи повинен бути обмежений для авторизованих користувачів за допомогою надійних механізмів аутентифікації (пароль, біометрія, двофакторна аутентифікація). Відеодані, що передаються та зберігаються, повинні бути зашифровані для захисту від перехоплення та

несанкціонованого доступу. Система також повинна забезпечувати цілісність відеоданих та захист від підробки, зміни чи видалення, а також вести журнал дій користувачів для відстеження та аналізу подій, пов'язаних з безпекою.

Важливими технічними вимогами є забезпечення високої якості відеозображення (роздільна здатність, частота кадрів, чутливість) для чіткої ідентифікації об'єктів та подій, надійність та стабільність роботи системи з мінімальним часом простою, а також масштабованість архітектури системи для можливості додавання нових камер або збільшення обсягу сховища в майбутньому. Сумісність з існуючою мережевою інфраструктурою ліцею та енергоефективність системи для зниження витрат на електроенергію також є важливими аспектами.

Вимоги до умов експлуатації включають здатність обладнання системи працювати в заданому діапазоні температур (в залежності від місця встановлення – внутрішнє чи зовнішнє), захищеність від вологи та пилу, забезпечення якісного відеозображення в різних умовах освітлення (день, ніч, темрява) та стійкість до вібрації.

Нарешті, система повинна відповідати вимогам законодавства України щодо захисту персональних даних та відеоспостереження, а також галузевим стандартам та рекомендаціям щодо проектування та встановлення систем відеоспостереження.

Цей перелік вимог є відправною точкою для проектування та розробки комп'ютерної системи відеоспостереження для Калуського ліцею ім. Д. Бахматюка. Під час проектування необхідно враховувати специфічні потреби та особливості навчального закладу, а також можливі ризики та загрози.

2.3 Вибір обладнання

Вибір апаратного забезпечення для системи відеоспостереження Калуського ліцею базується на аналізі ключових вимог до системи: забезпечення безпеки на території, можливість перегляду подій у реальному часі та зберігання

відеоархівів щонайменше протягом 14 днів. Враховувались такі критерії: вартість, якість зображення, надійність, простота інтеграції та масштабованість системи.

У цьому розділі здійснено обґрунтований вибір основних компонентів: IP-камер, мережевого обладнання, відеореєстратора/сервера та накопичувачів.

Вибір IP-камер

Вимоги до камер:

- роздільна здатність: не менше 2 Мп (Full HD) для чіткого розпізнавання осіб;
- нічне бачення: ІЧ-підсвітка до 20–30 м;
- кут огляду: не менше 90°;
- зовнішнє та внутрішнє використання: камери з класом захисту IP66;
- підтримка PoE: для мінімізації витрат на прокладання живлення;
- функції: детекція руху, компенсація заднього світла, WDR.

Для вибору потрібної камери, потрібно їх порівняти (таблиця 2.5).

Таблиця 2.5 - Порівняльна таблиця IP-камер

Параметр	Dahua IPC-HDW1230T1	Hikvision DS-2CD1023G0-I	Partizan IPO-2SP SE
Роздільна здатність	2 Мп	2 Мп	2 Мп
Кут огляду	103°	106°	90°
ІЧ-підсвітка	до 30 м	до 30 м	до 20 м
Захист корпусу	IP67	IP66	IP66
Підтримка PoE	Так	Так	Так
Середня ціна (грн)	~1 600	~1 700	~1 200

Обґрунтування вибору:

Для реалізації проєкту обрано IP-камери Partizan IPO-2SP SE, які забезпечують високу якість зображення, надійну роботу в умовах освітніх закладів та мають оптимальне співвідношення ціна/якість.

Загалом встановлено 27 камер, з яких:

- 11 камер - на 1-му поверсі (вхід, охорона, коридори, їдальня, актовий зал, гардероб тощо);

- 16 камер - на 2-му та 3-му поверхах (кабінети, сходи, спортзали, технічна кімната).

Серверне та мережеве обладнання

Для забезпечення стабільного функціонування відеосистеми було обрано два незалежні комплекси обладнання (таблиця 2.6), по одному на кожну частину будівлі (1 поверх / 2+3 поверхи):

Таблиця 2.6 – Вибране обладнання

Компонент	Кількість	Характеристики
1	**2**	**3**
Сервер (ПК)	2	Intel Core i5, 8/16 ГБ RAM, HDD 4 ТБ WD Purple
PoE-комутатор	2	PoE-Link PL-2016GG-2SF
Джерело безперебійного живлення (UPS)	2	Потужність ~700 ВА, резерв ≥30 хвилин
Мережеве з’єднання	2	Gigabit Ethernet, прокладка кабелів Cat.5e
Монітор охорони	2	FullHD, 21.5+ дюйма
Клавіатура/мишка	2	USB, провідні

Накопичувачі та архівування

З метою зберігання відеозаписів протягом не менше 14 діб при середній якості (1080p, 15 FPS), встановлено жорсткі диски:

- 2 × HDD WD Purple 4TB - по одному на кожен сервер;
- всі записи ведуться у циклічному режимі з автоматичним перезаписом;
- підтримка детекції руху знижує обсяг непотрібного відеоархіву.

Вибране обладнання забезпечує:

- масштабованість - можливість додати нові камери за потреби;
- низьке енергоспоживання - камери PoE споживають до 5 Вт;
- низькі експлуатаційні витрати - завдяки безкоштовному ПЗ та доступному обладнанню;
- простоту монтажу та обслуговування - немає потреби в окремому живленні для кожної камери;

- відповідність вимогам закладу освіти - система безпечна, економічна та ефективна.

Основні компоненти системи відеоспостереження описані в таблиці 2.7.

Таблиця 2.7 – Вибрані компоненти для системи відеоспостереження

№	Компонент	Модель / Тип	Кількість	Призначення
1	2	3	4	5
1	IP-камера	Partizan IPO-2SP SE	27	Відеоспостереження по всьому ліцею
2	Сервер ПК (відеореєстратор)	Intel Core i5, 8/16 ГБ RAM, 4 ТБ HDD	2	Обробка і зберігання відео
3	PoE-комутатор	PoE-Link PL-2016GG-2SF	2	Передача даних і живлення камер по одному кабелю
4	Джерело безперебійного живлення (UPS)	Powercom / LogicPower 700 ВА	2	Захист від відключень живлення
5	Програмне забезпечення	Partizan CMS	2 інсталяції	Керування камерами, архів, віддалений доступ
6	Монітор	21.5" FullHD	2	Виведення відео в охороні
7	Миша + клавіатура	USB	2	Керування ПЗ

Загальні характеристики системи:

- кількість відеоканалів: 27;
- розміщення серверів:
- перший поверх: сервер №1 (кімната охорони);
- другий і третій поверхи: сервер №2 (технічна кімната);
- мережеве з’єднання: Gigabit Ethernet по поверхах;
- тип запису: безперервний + за подією (рух);
- тривалість зберігання відео: 14–30 днів;
- можливість віддаленого доступу: через Partizan CMS-клієнт або браузер у локальній мережі;
- інтерфейс користувача: простий, доступний для охоронця або IT-адміністратора.

На основі аналізу технічних потреб, особливостей інфраструктури навчального закладу та економічної доцільності, було сформовано оптимальний склад обладнання системи відеоспостереження. Основу системи становлять 27 IP-камер Partizan IPO-2SP SE, об’єднані в єдину мережу за допомогою PoE-комутаторів і двох серверів, що розташовані в охоронній кімнаті та технічному приміщенні.

Така система повністю відповідає вимогам безпеки для навчального закладу, забезпечує контроль над переміщенням учнів і персоналу, а також мінімізує ризики втручань сторонніх осіб або несанкціонованих дій усередині будівлі.

2.4 Вибір програмного забезпечення

Вибір програмного забезпечення є важливим етапом при проектуванні системи відеоспостереження, оскільки саме воно забезпечує управління, моніторинг, аналіз та зберігання відеоданих. На ринку існує велика кількість різноманітних програмних продуктів, які відрізняються функціональністю, вартістю, вимогами до апаратного забезпечення та зручністю використання. Розглянемо декілька популярних варіантів, які можуть бути використані для системи відеоспостереження Калуського ліцею.

XProject Go – це програмне забезпечення для відеоспостереження, розроблене компанією Milestone, провідним постачальником у цій галузі. Однак, початкова версія продукту має суттєво обмежений функціонал, що ускладнює оцінку повної функціональності. Наприклад, перша платна версія XProject Go підтримує до 26 камер, надає можливість необмеженого зберігання відеоархіву та функцію веб-відеоспостереження. На противагу цьому, найбільш повнофункціональний варіант, XProject Corporate, не має обмежень щодо обсягу відеоархіву та кількості камер, а також підтримує інтеграцію стороннього ПЗ, розширені аналітичні функції, такі як розпізнавання осіб та номерів автомобілів, налаштування зон приватності та аналітичний пошук в архіві за подіями.

Програма XProject Go вирізняється підтримкою широкого спектру відеокамер – понад 900 моделей від більш ніж 80 виробників, а також можливістю використання USB-камер. Для підключення аналогових камер передбачена підтримка IP-декодерів. Програма використовує сучасні та ефективні кодеки стиснення відео, такі як H.264, MPEG4, ASP та MxPEG. Детектор руху має гнучкі налаштування чутливості та зон відповідальності. Для коректної роботи програми рекомендується ПК з процесором від 2,4 ГГц та 2 Гб оперативної пам'яті. Користувачам, які використовують продукт більше 30 днів, необхідно пройти безкоштовну реєстрацію на сайті розробника. XProject Go сумісна з операційними системами Windows XP, Vista, 7 і 10, та має багатомовний інтерфейс.

XProtect Go – це безкоштовна версія провідного програмного забезпечення для управління відео, розроблена для малого бізнесу та домашнього використання. Вона дозволяє оцінити переваги IP-відео та відкритої платформи Milestone без початкових фінансових витрат. Зручні опції переходу на платні версії роблять її чудовим вибором для початку використання надійного IP-відеоспостереження з можливістю подальшого розширення.

SecuritySpy – це програмне забезпечення для відеоспостереження, розроблене для Mac, яке дозволяє швидко та легко створити комплексну та ефективну систему відеоспостереження для дому чи бізнесу [26]. Завдяки функціям виявлення руху, сповіщенням електронною поштою, підтримці стандарту ONVIF та можливості керування PTZ-камерами, SecuritySpy перетворює будь-який Mac на повноцінну станцію відеоспостереження, наприклад, з кількома великими екранами для центру моніторингу безпеки.

SecuritySpy також ідеально підходить для віддаленого керування, оскільки має безпечний веб-інтерфейс з повним набором функцій, що дозволяє отримувати доступ до системи спостереження та керувати нею через Інтернет або локальну мережу. SecuritySpy має інтуїтивно зрозумілий інтерфейс користувача, що робить його простим у використанні. Для створення системи відеоспостереження з нуля потрібні лише SecuritySpy, Mac та IP-камери. Якщо

вже є аналогові камери, SecuritySpy може використовувати їх разом із сучасними IP-камерами, забезпечуючи плавний перехід до цифрової системи. Гнучкість SecuritySpy дозволяє створити систему, яка відповідає індивідуальним потребам, незалежно від кількості камер. SecuritySpy інтегрується практично з усіма IP-камерами на ринку [25].

Основні функції SecuritySpy:

- одночасне відображення та запис відео з багатьох камер;
- підтримка сумісних з Mac пристроїв відео- та аудіовходу;
- сумісність з IP-відеокамерами, зокрема ONVIF, Axis, Sony, Canon, D-Link, Dahua, Hikvision та іншими. SecuritySpy інтегрується практично з усіма IP-камерами на ринку [26].

ZoneMinder має модульну структуру, де кожен компонент активується лише за потреби, що оптимізує використання ресурсів і підвищує ефективність системи [27]. Навіть на застарілому комп'ютері Pentium II можна під'єднати декілька пристроїв запису і відстежувати камери зі швидкістю до 25 кадрів в секунду на пристрій, але ця швидкість зменшується вдвічі з кожною додатковою камерою на тому ж пристрої. Додаткові камери на окремих пристроях можуть підтримувати 25 кадрів в секунду.

Завдяки зручному та всеосяжному веб-інтерфейсу на основі PHP, ZoneMinder є ефективним і корисни. Користувач може контролювати камери з будь-якого місця, використовуючи комп'ютер або мобільний телефон з доступом до Інтернету, і налаштовувати веб-інтерфейс відповідно до доступної пропускної здатності. Веб-інтерфейс дозволяє переглядати, архівувати та видаляти події, записані камерами, і взаємодіє з основними демонами для забезпечення повної співпраці. ZoneMinder можна встановити як системну службу для віддаленого перезавантаження системи.

Ключовими функціями ZoneMinder є захоплення та аналіз зображень, а також набір налаштовуваних параметрів, які мінімізують кількість помилкових спрацьовувань і втрату відеоматеріалу. Можна визначити "зони" для кожної камери з різною чутливістю та функціональністю [28]. Це дозволяє виключати

зони, які не потрібно відстежувати, або визначати області, які будуть сигналізувати при перевищенні певних порогів у поєднанні з іншими зонами.

Partizan CMS – це професійне програмне забезпечення для централізованого управління системами відеоспостереження Partizan. Воно дозволяє об'єднати в єдину систему велику кількість IP-камер та відеореєстраторів, забезпечуючи зручний моніторинг, керування та адміністрування [22, 23].

Основні можливості Partizan CMS:

- підтримка великої кількості камер: можливість підключення та управління великою кількістю IP-камер різних моделей;
- централізований моніторинг: перегляд відео в реальному часі з декількох камер на одному екрані;
- запис та відтворення відео: запис відеопотоку з камер на жорсткий диск або в хмарне сховище, а також відтворення архівних записів;
- інтелектуальний аналіз відео: розпізнавання руху, виявлення облич, перетин лінії, вторгнення в зону та інші аналітичні функції;
- віддалений доступ: перегляд відео та управління системою з будь-якої точки світу через Інтернет;
- керування користувачами та правами доступу: розмежування прав доступу для різних користувачів системи;
- інтеграція з іншими системами безпеки: можливість інтеграції з системами контролю доступу, охоронною сигналізацією тощо.

iSpy – це безкоштовне програмне забезпечення з відкритим кодом для систем відеоспостереження, яке працює на платформі Windows. Воно має широкий набір функцій і підтримує велику кількість IP-камер, веб-камер та інших відеопристроїв.

Основні можливості iSpy:

- підтримка різних джерел відео: IP-камери, веб-камери, мікрофони, робочий стіл;
- детекція руху: автоматичний запис відео при виявленні руху в кадрі;

- сповіщення: відправка email-повідомлень або SMS-повідомлень при виявленні руху;

- віддалений доступ: перегляд відео та управління системою через Інтернет;

- запис та відтворення відео: запис відео на жорсткий диск, а також відтворення архівних записів;

- інтеграція з IoT-пристроями: можливість інтеграції з різними IoT-пристроями, такими як датчики температури, вологості тощо.

Shinobi – це ще одне безкоштовне програмне забезпечення з відкритим кодом для систем відеоспостереження, яке відрізняється гнучкістю та можливістю налаштування. Воно працює на платформах Linux, Windows та macOS.

Основні можливості Shinobi:

- підтримка різних джерел відео: IP-камери, веб-камери, локальні відеофайли;

- детекція руху: виявлення руху в кадрі з використанням різних алгоритмів;

- запис та відтворення відео: запис відео на жорсткий диск, в хмарне сховище або на FTP-сервер;

- віддалений доступ: перегляд відео та управління системою через веб-інтерфейс;

- керування користувачами та правами доступу: розмежування прав доступу для різних користувачів системи;

- інтеграція з іншими системами: можливість інтеграції з різними системами через API.

Shinobi є хорошим вибором для досвідчених користувачів, які потребують гнучкого та налаштовуваного рішення для відеоспостереження.

При виборі програмного забезпечення для системи відеоспостереження Калуського ліцею необхідно враховувати такі фактори:

- кількість камер, які необхідно підключити до системи;

- необхідний функціонал (моніторинг, запис, аналіз, віддалений доступ);
- вимоги до апаратного забезпечення;
- вартість програмного забезпечення;
- зручність використання та наявність технічної підтримки;
- вимоги до безпеки та захисту даних.

У таблиці 2.8 наведено порівняльну характеристику шести рішень: Milestone XProtect, Shinobi, SecuritySpy, ZoneMinder, Luxriot EVO та Partizan CMS. Аналіз проводився за ключовими критеріями: ліцензія, підтримка камер, наявність аналітики, вимоги до обладнання, вартість, а також можливість масштабування.

Таблиця 2.8 - Порівняльна характеристика програмного забезпечення для відеоспостереження

Критерій	Milestone XProtect	Shinobi	SecuritySpy	ZoneMinder	Luxriot EVO	Partizan CMS
Тип ліцензії	Комерційна / безкоштовна версія	Open-source (MIT)	Комерційна	Open-source (GPL)	Комерційна	Безкоштовна для Partizan
Платформи	Windows Server	Linux, Windows, Docker	macOS	Linux	Windows	Windows
Підтримка IP-камер	ONVIF, RTSP	ONVIF, RTSP	ONVIF, RTSP	RTSP, MJPEG	ONVIF, RTSP	Лише Partizan
Мобільний доступ	Офіц. застосунок	Веб і моб. браузер	Застосунок для iOS	Через сторонні сервіси	Офіційний застосунок	Офіційний застосунок
Аналітика / інтелект	Високий рівень	Детекція руху, події	Обмежено	Рух, події	AI-модулі, інциденти	Лише базовий перегляд
Масштабованість	Дуже висока (1000+ камер)	Висока (100+ камер)	Обмежена (~64 камер)	Обмежена (~50 камер)	Дуже висока	Обмежена (Тільки Partizan)
Ціна	Безкоштовно до 8 камер	Безкоштовно	Від $50 за камеру	Безкоштовно	Платна, залежить від пакету	Безкоштовно
Оновлення / підтримка	Офіційна підтримка, SLA	Активна спільнота	Платна підтримка	Обмежена спільнота	Офіційна, корпоративна	Офіційна (лише Partizan)

Кінець таблиці 2.8

Переваги	Потужна система, інтеграції	Гнучкість, сучасний дизайн	Простота для Mac	Класика open-source	Корпоративний рівень	Простота, інтеграція з Partizan
Недоліки	Дорога комерційна ліцензія	Потребує базових знань Linux	Лише для macOS	Застарілий інтерфейс	Висока вартість	Лише для камер Partizan
Загальна оцінка	Професійне рішення	Оптимальний для Linux	Зручно для Mac	Мінімальний рівень	Для підприємств	Варіант лише для власного бренду

На основі проведеного порівняльного аналізу програмного забезпечення для відеоспостереження, з урахуванням функціональності, сумісності з обраним обладнанням, вимог до системних ресурсів та бюджету навчального закладу, оптимальним вибором є Partizan CMS. Це програмне забезпечення має низку суттєвих переваг: воно є безкоштовним для використання з камерами бренду Partizan, має простий у користуванні інтерфейс, підтримує базові функції запису та перегляду в реальному часі, забезпечує зберігання архіву на локальному сервері, а також дозволяє адміністратору здійснювати базове налаштування камер і доступу.

Partizan CMS - це централізована платформа для роботи з відеопотоками від камер бренду Partizan, яка дозволяє здійснювати як онлайн-моніторинг, так і керування архівом, налаштування камер, пошук за подіями та доступ до записів із різних пристроїв. У нашому випадку система використовується для одночасної роботи з 27 камерами, поділеними на дві серверні групи (1 поверх / 2+3 поверхи), кожна з яких керується окремим ПК із встановленим ПЗ.

Обґрунтування вибору

Причини, що визначили вибір саме Partizan CMS, полягають не лише у технічній сумісності з камерами Partizan, але й у комплексі економічних, функціональних та адміністративних факторів.

По-перше, ПЗ є повністю безкоштовним у разі використання камер бренду Partizan, що дозволяє уникнути витрат на придбання ліцензій або підписки, як це

часто трапляється з комерційними рішеннями. Для закладу освіти, який обмежений у фінансуванні, цей чинник є особливо важливим.

По-друге, простота інсталяції та підтримки дозволяє обслуговувати систему без залучення висококваліфікованого IT-персоналу. Встановлення ПЗ можливе на звичайні персональні комп'ютери під управлінням Windows, а інтерфейс адаптований для користувачів без спеціальної технічної освіти.

По-третє, Partizan CMS надає повний набір необхідних функцій - перегляд в реальному часі, запис, відтворення архіву, створення скріншотів, експорт відео, налаштування детекції руху тощо - без обмежень, що зустрічаються у базових або безкоштовних версіях конкурентів.

Масштабованість та розподілена архітектура

Завдяки гнучкій архітектурі, Partizan CMS дозволяє легко масштабувати систему відеоспостереження - як горизонтально (додавання нових камер), так і вертикально (розподіл завдань між кількома комп'ютерами). В умовах Калуського ліцею це реалізовано у вигляді двох незалежних CMS-серверів, кожен з яких відповідає за окремі поверхи:

- сервер 1, розташований у кімнаті охорони, обслуговує 11 камер першого поверху;
- сервер 2, розміщений у технічній кімнаті другого поверху, обслуговує 16 камер, встановлених на другому та третьому поверхах.

Кожен сервер працює автономно, але в межах загальної локальної мережі, що дозволяє адміністраторам переглядати відео з обох CMS-серверів за допомогою центрального клієнтського застосунку Partizan або браузерного інтерфейсу. Це особливо зручно в контексті охоронної служби: для перегляду камер не потрібно перемикати фізичні кабелі або користуватись сторонніми додатками - доступ до всіх потоків централізований.

У разі збільшення кількості камер у майбутньому (наприклад, встановлення зовнішніх камер або камер на подвір'ї), система зможе легко масштабуватись за рахунок додавання третього сервера або збільшення потужності існуючих. Partizan CMS не обмежує кількість інсталяцій у межах

одного закладу, що робить її придатною як для невеликих конфігурацій, так і для систем професійного рівня.

Підтримка серверного обладнання

Partizan CMS невимоглива до ресурсів системи. При коректному налаштуванні параметрів відео (зокрема, частоти кадрів та роздільної здатності), один ПК може обробляти відео від 12–16 камер без суттєвих затримок. У даному проєкті використано два ПК з процесорами Intel Core i5 та 8–16 ГБ оперативної пам’яті, що є достатнім для безперебійної роботи в освітньому закладі. Жорсткі диски на 4 ТБ дозволяють зберігати відеоархів тривалістю до 2–4 тижнів при налаштуванні запису за детекцією руху.

Завдяки простоті налаштування, системний адміністратор або відповідальна особа з охорони може самостійно:

- додавати нові камери;
- змінювати розклад запису;
- створювати облікові записи з обмеженими правами;
- оновлювати програмне забезпечення без втрати даних.

У результаті аналізу функціональних можливостей, ліцензійної політики, сумісності з обраним обладнанням, вимог до серверних ресурсів та простоти адміністрування, програмне забезпечення Partizan CMS було обрано як оптимальне рішення для реалізації системи відеоспостереження в Калуському ліцеї.

Цей вибір забезпечує повну сумісність із камерами Partizan IPO-2SP SE, дозволяє реалізувати контроль за всіма поверхами закладу, дає змогу розділити навантаження на два ПК, зберігає відеоархіви локально та не вимагає жодних додаткових витрат на ліцензії чи навчання персоналу. Система є масштабованою, стабільною, керованою і повністю відповідає вимогам безпеки сучасного навчального середовища.

2.5 Алгоритм роботи системи

Система відеоспостереження, реалізована у Калуському ліцеї, функціонує на основі цифрової архітектури з використанням IP-камер, PoE-комутаторів, серверного обладнання та програмного забезпечення Partizan CMS. Програмна логіка побудована так, щоб забезпечити постійний відеоконтроль, централізоване зберігання даних, фільтрацію за подіями, зручний доступ до архівів, а також адміністрування прав доступу до системи.

Умовно логіку роботи можна поділити на звичайний (робочий) режим, обробку подій та реакцію з боку адміністратора/системи.

Звичайний режим роботи системи

У щоденному режимі, коли не зафіксовано аномальних подій чи загроз, система працює за наступним сценарієм:

1. Постійний відеомоніторинг

27 IP-камер Partizan IPO-2SP SE, розміщених на всіх трьох поверхах ліцею, здійснюють постійне відеоспостереження у своїх зонах охоплення. Вони підключені до PoE-комутаторів, які, окрім передачі даних, забезпечують електроживлення через кабель Ethernet. Відеопотік надходить на два локальні сервери:

- сервер №1 – обробляє 11 камер першого поверху;
- сервер №2 – обробляє 16 камер з другого та третього поверхів.

2. Передача відеопотоку та його обробка

Кожна камера передає відеосигнал у цифровому форматі (RTSP) безпосередньо до Partizan CMS, встановленого на відповідному ПК. Частота кадрів, роздільна здатність та кодування налаштовуються окремо для кожної камери відповідно до вимог до архіву та пропускної здатності мережі.

3. Запис відео на жорсткий диск

Усі потоки записуються на жорсткі диски обсягом 4 ТБ на кожному сервері. В залежності від налаштувань, запис може здійснюватися в

безперервному режимі або лише за подією (наприклад, при виявленні руху). У типовій конфігурації обрано комбінований режим:

- у години навчального процесу відео записується безперервно;
- у позаурочний час - тільки при активації тригера руху.

4. Зберігання архівів і циклічний перезапис

Partizan CMS автоматично управляє простором на диску: коли він заповнюється, найстаріші фрагменти архіву видаляються, а на їх місце записується нове відео. У середньому, при розумних налаштуваннях якості, архів охоплює 14–30 днів запису з кожної камери.

5. Віддалений та локальний доступ

Охоронці або адміністратори мають змогу переглядати відео з камер в реальному часі, а також отримувати доступ до архіву. Це можливо як локально (на комп'ютері в охоронній кімнаті), так і віддалено через мережу, за умови наявності облікових даних і прав доступу. Підтримується також мобільний клієнт для смартфонів.

6. Виявлення руху

Partizan CMS підтримує вбудовану систему детекції руху, яка працює на рівні програмного забезпечення. Для кожної камери можна задати:

- зону спостереження (наприклад, двері, вхід у клас, сходи);
- чутливість (розмір об'єкта, швидкість);
- час реагування (ніч, післяурочний час тощо).

У разі фіксації руху система автоматично:

- починає запис (якщо був вимкнений);
- може надіслати сповіщення (на пошту або в CMS-інтерфейс);
- позначає відеофайл спеціальним маркером, що значно спрощує подальший пошук.

Ця функція особливо ефективна у вечірній час, коли рух у закладі повинен бути мінімальним, а також у зонах із обмеженим доступом (наприклад, технічна кімната, адміністративні кабінети, сходи між поверхами).

7. Аналіз подій та пошук в архіві

Partizan CMS дозволяє зручно переглядати архівні записи, фільтруючи події за:

- датою й часом;
- типом події (наприклад, зафіксовано рух);
- конкретною камерою.

Завдяки цьому оператор охорони або відповідальна особа може оперативно переглянути фрагмент відео без потреби вивчати багатогодинний запис. Часто це дозволяє знайти порушення або інциденти вже впродовж кількох хвилин.

8. Користувацькі ролі

Partizan CMS підтримує створення облікових записів із розмежуванням прав доступу:

- адміністратор - має повний контроль: додає/видаляє камери, налаштовує параметри запису, створює користувачів;
- оператор - переглядає відео, архів, не має права змінювати налаштування;
- гість - може переглядати тільки визначені камери без доступу до архіву або конфігурацій.

Усі дії користувачів логуються. Це дозволяє проводити аудит дій та уникнути несанкціонованих змін у конфігурації системи.

9. Захист даних

Забезпечується кількома рівнями:

- аутентифікація через логін і пароль;
- обмеження доступу до серверів - фізично сервери розміщені в контрольованих приміщеннях (кімната охорони і технічна кімната);
- локальне зберігання без виходу в публічний інтернет, що мінімізує ризики злому.

Система відеоспостереження, реалізована на базі Partizan CMS, дозволяє створити гнучке, надійне та безпечне середовище моніторингу для трьох

поверхів ліцею. Принципова логіка роботи побудована таким чином, щоб забезпечити:

- безперервне спостереження в режимі реального часу;
- автоматичне реагування на події за допомогою детекції руху;
- централізоване зберігання відеоархіву з можливістю швидкого доступу до ключових записів;
- просте та захищене адміністрування, що не потребує додаткових ліцензій чи складних технічних знань.

Завдяки розподіленій архітектурі (два сервери), система не лише відповідає поточним потребам навчального закладу, а й є готовою до подальшого масштабування без суттєвих витрат.

2.6 Безпечне зберігання даних

Впровадження системи відеоспостереження в Калуському ліцеї ім. Д. Бахматюка вимагає особливої уваги до питань конфіденційності та захисту інформації. Це зумовлено тим, що система збирає та обробляє великий обсяг персональних даних, включаючи зображення учнів та співробітників, записи їх пересування та інші відомості, що можуть бути використані для ідентифікації особи. Неналежне поводження з цими даними може призвести до порушення прав людини, розголошення особистої інформації та інших негативних наслідків.

Обробка персональних даних у системі відеоспостереження повинна здійснюватися на основі таких принципів:

- законність, справедливість та прозорість: обробка даних повинна здійснюватися на законних підставах, бути справедливою та прозорою для суб'єктів даних;
- обмеження цілі: дані повинні збиратися лише для чітко визначених, законних цілей і не повинні оброблятися у спосіб, несумісний з цими цілями. У випадку ліцею, такими цілями можуть бути забезпечення безпеки учнів та

співробітників, запобігання правопорушенням та контроль за дотриманням правил внутрішнього розпорядку;

- мінімізація даних: обсяг даних, що збираються, повинен бути мінімальним, достатнім для досягнення визначених цілей. Не слід збирати дані, які не є необхідними для функціонування системи відеоспостереження;

- точність: дані повинні бути точними та актуальними. Необхідно вживати заходів для забезпечення того, щоб неточні або неповні дані були виправлені або видалені;

- обмеження зберігання: дані повинні зберігатися протягом обмеженого періоду часу, необхідного для досягнення цілей обробки. Після закінчення цього періоду дані повинні бути безпечно видалені;

- цілісність та конфіденційність: дані повинні оброблятися таким чином, щоб забезпечити їх цілісність та конфіденційність, включаючи захист від несанкціонованого доступу, використання, розголошення, знищення або пошкодження.

Для забезпечення конфіденційності та захисту інформації в системі відеоспостереження необхідно вжити комплекс технічних та організаційних заходів, зокрема:

- контроль доступу: доступ до відеозаписів повинен бути обмежений колом осіб, які мають відповідні повноваження та несуть відповідальність за безпеку ліцею. Необхідно використовувати надійні механізми аутентифікації та авторизації, такі як паролі, біометричні дані або електронні сертифікати;

- шифрування даних: відеозаписи повинні зберігатися в зашифрованому вигляді, щоб унеможливити їх перегляд у разі несанкціонованого доступу;

- захист мережі: система відеоспостереження повинна бути захищена від несанкціонованого доступу ззовні за допомогою міжмережевого екрана (firewall) та інших засобів захисту мережі;

- моніторинг та аудит: необхідно здійснювати моніторинг та аудит дій користувачів системи відеоспостереження для виявлення та запобігання порушенням політики безпеки;

- навчання та підвищення обізнаності: співробітники, які мають доступ до системи відеоспостереження, повинні проходити навчання з питань захисту персональних даних та інформаційної безпеки;
- регулярні перевірки безпеки: необхідно регулярно проводити перевірки безпеки системи відеоспостереження для виявлення та усунення вразливостей.

Інформування суб'єктів даних

Учні, співробітники та інші особи, які перебувають у зоні відеоспостереження, повинні бути проінформовані про факт здійснення відеозапису, цілі обробки даних та їхні права. Для цього необхідно розмістити відповідні інформаційні знаки на території ліцею та надати інформацію про відеоспостереження на веб-сайті ліцею та в інших публічних місцях.

Відповідальність

Необхідно визначити відповідальних осіб за забезпечення конфіденційності та захисту інформації в системі відеоспостереження. Ці особи повинні здійснювати контроль за дотриманням вимог законодавства та політики безпеки, а також реагувати на порушення та інциденти безпеки.

Впровадження цих вимог дозволить забезпечити належний рівень конфіденційності та захисту інформації в системі відеоспостереження Калуського ліцею ім. Д. Бахматюка, а також створити безпечне та комфортне середовище для навчання та роботи.

Методи збереження та резервного копіювання

Локальне збереження даних

Локальне збереження передбачає використання фізичних серверів, розташованих безпосередньо в ліцеї.

Вимоги до обладнання:

- сервери повинні мати достатню обчислювальну потужність, великий обсяг дискового простору, а також підтримку RAID-масивів для забезпечення відмовостійкості;

- організація дискового простору: важливо правильно організувати дисковий простір, розділивши його на окремі томи для операційної системи, програмного забезпечення та відеоархіву;

- моніторинг: необхідно встановити систему моніторингу, яка буде відстежувати стан серверів, дискового простору, температуру та інші важливі параметри.

Резервне копіювання даних

Регулярне створення резервних копій є важливим для захисту від втрати даних:

- періодичність: важливість даних та допустимий час їх відновлення визначають періодичність резервного копіювання. Рекомендується щоденне резервне копіювання критично важливих даних та щотижневе – повного обсягу відеоархіву;

- методи: існують різні методи резервного копіювання, такі як повне, інкрементне та диференційне копіювання. Вибір залежить від обсягу даних, швидкості копіювання та доступного дискового простору;

- зберігання: резервні копії необхідно зберігати у безпечному місці, окремо від основних серверів. Рекомендується використовувати декілька місць зберігання, включаючи локальне сховище та віддалене хмарне сховище;

- автоматизація: варто автоматизувати процес резервного копіювання за допомогою спеціалізованого програмного забезпечення.

Хмарне зберігання даних

Хмарне зберігання стає все більш популярним варіантом для резервного копіювання:

- переваги: хмарні сховища забезпечують відмовостійкість, масштабованість та доступність даних з будь-якого місця;

- безпека: при використанні хмарного сховища необхідно забезпечити захист даних, вибираючи надійного постачальника хмарних послуг, який відповідає вимогам законодавства про захист персональних даних.

Перевірка та відновлення даних

Регулярна перевірка цілісності резервних копій та тестування процедур відновлення даних є критично важливими:

- періодичність перевірок: необхідно регулярно проводити тестове відновлення даних з резервних копій, щоб переконатися, що вони придатні для використання;

- інструменти перевірки: існують спеціалізовані інструменти для перевірки цілісності даних.

Безпека даних

Захист даних від несанкціонованого доступу є важливим аспектом збереження та резервного копіювання:

- шифрування: рекомендується використовувати шифрування даних як при зберіганні, так і при передачі;

- контроль доступу: необхідно встановити чіткі правила доступу до даних та обмежити доступ лише для авторизованих користувачів;

- аудит: важливо вести аудит усіх операцій з даними, щоб мати можливість відстежити будь-які несанкціоновані дії.

Відповідність нормативним вимогам

При збереженні та резервному копіюванні даних необхідно враховувати вимоги законодавства про захист персональних даних:

- GDPR: якщо система відеоспостереження обробляє персональні дані громадян ЄС, необхідно дотримуватися вимог GDPR;

- локальне законодавство: необхідно враховувати вимоги місцевого законодавства про захист персональних даних;

Рекомендації:

- використовуйте комбінацію локального та хмарного зберігання для забезпечення максимальної надійності [24];

- автоматизуйте процеси збереження та резервного копіювання;

- регулярно перевіряйте цілісність резервних копій та тестуйте процедури відновлення даних;

- забезпечте захист даних від несанкціонованого доступу;

- дотримуйтесь вимог законодавства про захист персональних даних.

Впровадження цих методів дозволить створити надійну та безпечну систему збереження та резервного копіювання даних для системи відеоспостереження Калуського ліцею ім. Д. Бахматюка.

Шифрування, контроль доступу та аудит дій користувачів

Забезпечення конфіденційності, цілісності та доступності відеоданих є критично важливим елементом при впровадженні системи відеоспостереження в освітніх закладах. Особливо актуальним це стає у зв’язку з вимогами Закону України "Про захист персональних даних", а також міжнародними практиками щодо обробки візуальної інформації, яка може ідентифікувати особу.

Шифрування відеоданих

Одним із найбільш ефективних способів захисту відеоінформації від несанкціонованого доступу є шифрування. У контексті IP-відеоспостереження доцільно використовувати як транспортне шифрування, так і шифрування на рівні зберігання.

Транспортне шифрування забезпечується використанням протоколів HTTPS, SSL/TLS та VPN-тунелів. Це дозволяє захистити відеопотоки під час передавання з камер до сервера або до пристрою перегляду. Найбільш надійними вважаються VPN-з’єднання на основі OpenVPN або IPSec, які не лише шифрують потік, а й аутентифікують пристрої в мережі.

Шифрування відеоархівів на диску може здійснюватися програмними методами - шляхом встановлення криптографічного шару шифрування файлової системи (наприклад, LUKS у Linux або BitLocker у Windows). Такий підхід особливо доцільний у випадках, коли фізичний доступ до сервера не може бути на 100% виключений. Крім того, деякі сучасні відеореєстратори мають вбудовані функції апаратного шифрування потоків на рівні камери.

Контроль і розмежування доступу

Безпечна система відеоспостереження не повинна надавати доступ до всіх функцій усім користувачам. Тому важливо впровадити ієрархічну модель прав доступу, де кожен користувач має обмеження відповідно до своєї ролі.

У типовій структурі школи доцільно виділити такі рівні доступу:

- адміністратор системи - має повний контроль: налаштування, додавання/видалення камер, керування правами інших користувачів, очищення архіву;
- охоронець/черговий адміністратор - має доступ до перегляду живих потоків та обмеженого архіву без можливості змінювати конфігурацію системи;

Усі користувачі повинні проходити аутентифікацію при вході в систему. Рекомендується використовувати складні паролі, а при можливості - двофакторну аутентифікацію (2FA). Операційна система сервера має також бути налаштована на блокування облікового запису після певної кількості невдалих спроб входу.

Аудит дій користувачів

Не менш важливою складовою безпеки є прозорість і відслідковуваність усіх дій, які виконуються в системі відеоспостереження. Для цього впроваджується журналювання подій, яке охоплює:

- час і дату входу та виходу користувача із системи;
- IP-адресу, з якої відбувся доступ;
- переглянуті відеоархіви;
- зміну конфігураційних параметрів;
- додавання чи видалення користувачів або камер;
- спроби несанкціонованого доступу.

Всі ці події зберігаються у зашифрованому журналі подій із прив’язкою до користувача. Адміністратор системи має можливість регулярно переглядати лог-файли та виявляти підозрілі дії (наприклад, систематичні нічні входи або спроби змінити конфігурацію).

Для зручності управління аудитом рекомендується інтегрувати систему відеоспостереження з системою централізованого логування (наприклад, syslog-сервером або ELK Stack), яка дозволяє гнучко аналізувати й фільтрувати дані, а також створювати сповіщення про підозрілі дії в реальному часі.

Захист відеоінформації в навчальному закладі - це не лише питання технічної реалізації, а й дотримання етичних та правових норм. Шифрування, розмежування доступу та аудит - це три опори надійної, безпечної і контрольованої системи відеоспостереження.

Запровадження таких механізмів дозволяє:

- виключити витік конфіденційної інформації;
- забезпечити правовий захист у разі інцидентів;
- підтримувати довіру до системи з боку батьків, учнів та персоналу.

Урахування цих аспектів на етапі проєктування та впровадження системи є запорукою її ефективності та безпечного функціонування в умовах освітнього закладу.

Висновок до розділу

У другому розділі було здійснено проєктування комп'ютерної системи відеоспостереження для Калуського ліцею імені Дмитра Бахматюка з урахуванням особливостей архітектури будівлі та вимог до безпеки. Визначено цілі системи, обрано оптимальні місця для розміщення відеокамер та сформовано загальну структурну схему системи.

Було обґрунтовано вибір обладнання, що відповідає технічним, функціональним та економічним вимогам навчального закладу. Система базується на IP-камерах з підтримкою PoE, що спрощує монтаж і знижує витрати на прокладання кабелів. Для зберігання відеоінформації передбачено сервер із достатнім обсягом пам'яті та можливістю розширення.

Також розроблено логіку функціонування системи з урахуванням сценаріїв використання: архівація, віддалений доступ, обмеження прав користувачів, збереження конфіденційності. Описано алгоритм взаємодії між пристроями, способи передачі даних та принципи безпечного зберігання відеоархіву.

Запропоноване рішення є гнучким, масштабованим і відповідає сучасним технічним вимогам до систем відеоспостереження.

3 НАЛАШТУВАННЯ ТА ОБСЛУГОВУВАННЯ СИСТЕМИ

3.1 Правила використання та встановлення обладнання

При використанні обладнання слід дотримуватись наступних правил:

- не підключайте камеру до нестабільного джерела живлення - це може спричинити коротке замикання, загоряння або ураження струмом;
- переконайтесь, що напруга живлення та температурні умови відповідають технічним вимогам пристрою;
- використовуйте грозозахисне обладнання для захисту камери від перенапруг під час грози;
- не розбирайте камеру самостійно - це призведе до втрати гарантії та може пошкодити пристрій;
- якщо камера отримує нестабільну або занадто низьку напругу, вона може перезавантажуватись або вимикатися;
- під час встановлення камери на металеву поверхню обов’язково забезпечте електричну ізоляцію між корпусом пристрою та металом, щоб уникнути електричних перешкод або збоїв.

Правила встановлення необхідного обладнання:

- для полегшення монтажу в комплекті камери є клейкий шаблон із позначенням місць для свердління отворів;
- при встановленні камери на металеву поверхню необхідно забезпечити електричну ізоляцію корпусу камери від металу та кріпильних елементів;
- категорично заборонено заземлювати корпус камери або будь-які її компоненти, а також інші елементи системи відеоспостереження;
- використовуйте шестигранні ключі для регулювання кута нахилу, повороту об’єктива, а також для налаштування поля зору та фокусування;
- якщо в мережі є активний dhcp-сервер, рекомендується дозволити йому автоматично призначати ip-адресу камері. у разі його відсутності - попередньо вручну налаштуйте адреси відповідно до параметрів мережі;

- обов’язково змініть стандартний (порожній) пароль доступу до ip-камери, скориставшись програмою Partizan Device Manager;

- запишіть встановлений пароль і збережіть його у надійному місці - у разі втрати відновити доступ можна лише через сервісний центр Partizan.

3.2 Програмний продукт Partizan Device Manager

За допомогою Partizan Device Manager можна отримати доступ для конфігурації IP-камер за допомогою IP-адреси або MAC-адреси пристрою. Вигляд меню програми Partizan Device Manager зображений на рисунку 3.1.

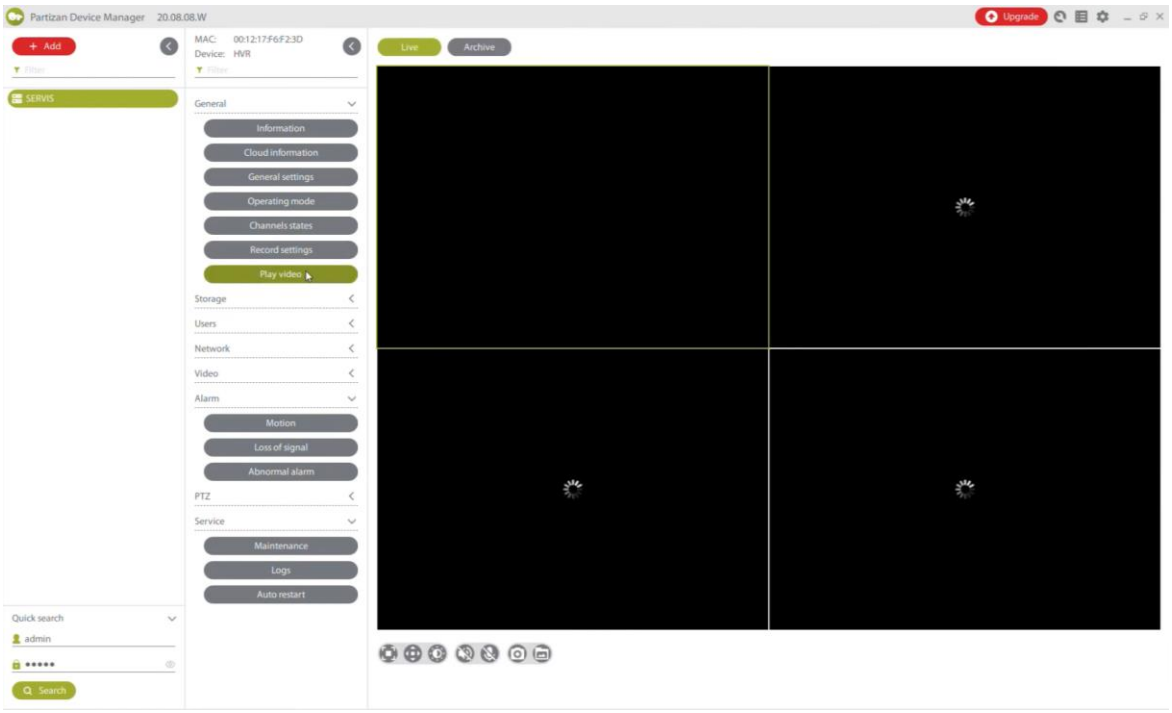

Рисунок 3.1 – Меню Partizan Device Manager

Можливості Partizan Device Manager:

- програма автоматично знаходить усі пристрої Partizan, підключені до локальної мережі;

- додати обладнання можна вручну, ввівши його IP-адресу або MAC-адресу;

- відображається основна інформація про пристрій, зокрема дата та версія прошивки, Partizan ID і MAC-адреса;
- є можливість змінити пароль доступу до пристрою;
- програма дозволяє переглядати відео у реальному часі;
- підтримується оновлення прошивки та скидання налаштувань до заводських;
- мережеві параметри пристрою можна налаштовувати як автоматично, так і вручну.

Додавання пристроїв за IP-адресою або MAC-адресою

Для додавання пристрою необхідно натиснути на кнопку «Додати», після чого в новому меню потрібно вибрати параметр додавання (IP або MAC), після чого задати параметри пристрою до якого бажаєте підключитись (рисунок 3.2).

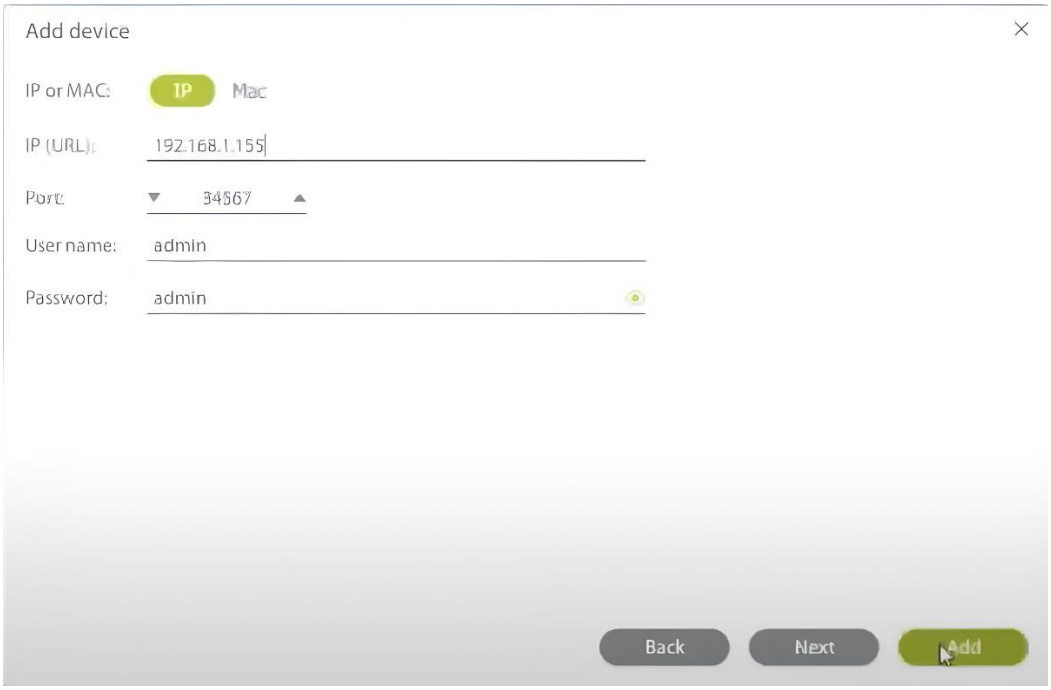

Рисунок 3.2 – Меню ручного додавання

Налаштування камери по DHCP

В Partizan Device Manager можна увімкнути підключення камери по DHCP. Це дозволить камері автоматично отримати IP-адресу та інші параметри для роботи в мережі. Служба DHCP дозволяє уникнути помилок налаштування та

необхідності вручну вносити мережеві параметри для кожної камери. Крім того, DHCP допомагає запобігти конфлікту адрес, викликані використанням раніше призначеної IP-адреси при налаштуванні нового IP-пристрою Partizan (рисунок 3.3).

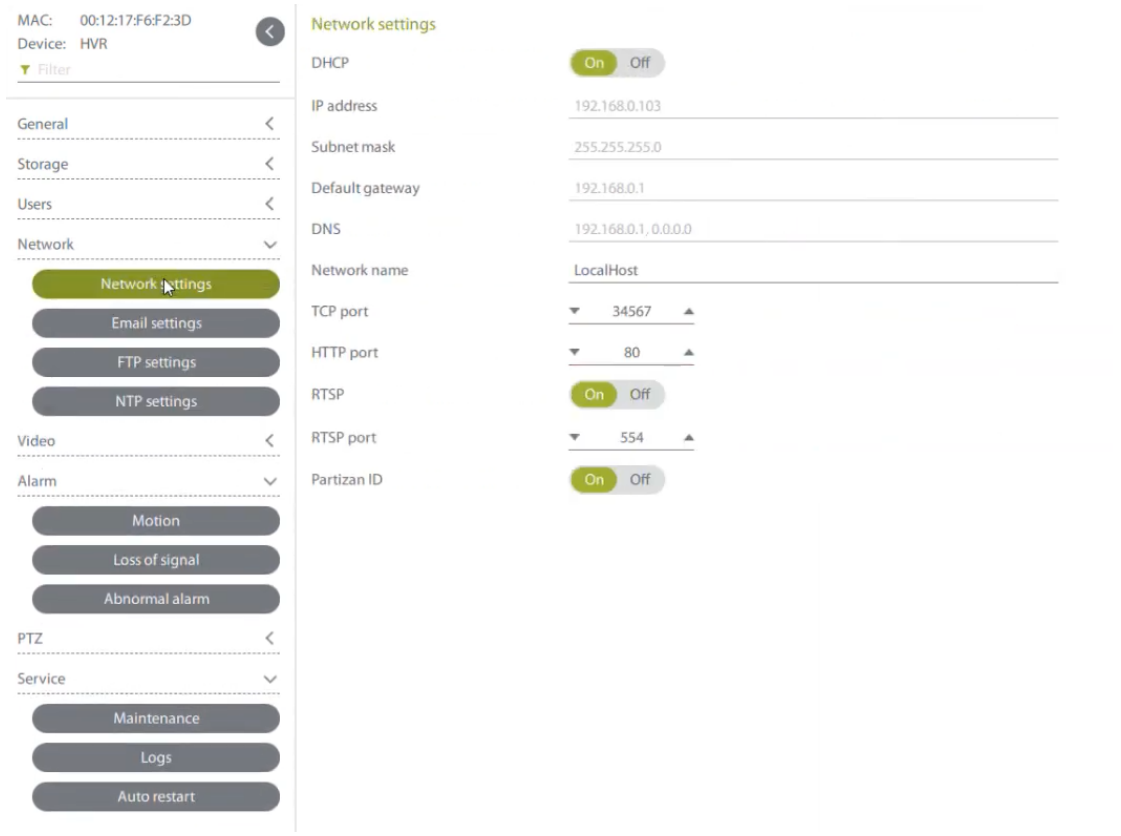

Рисунок 3.3 – Меню налаштування по DHCP

Централізоване оновлення прошивки

На основі програми Partizan Device Manager створено спеціальний сервіс для оновлення прошивок пристроїв.

Прошивки поділяються на два типи:

- стандартна прошивка - забезпечує сумісність із додатками Partizan Pro, Partizan CMS та Partizan ACM;
- хмарна прошивка - підтримує спеціальний протокол для роботи з хмарним сервісом Partizan Cloud Storage, включно із записом та переглядом відео в хмарних застосунках для ПК і мобільних пристроїв.

Перед початком користування потрібно визначити, для чого буде використовуватись пристрій, і встановити відповідну прошивку:

- камера зі стандартною прошивкою не працює з хмарним сервісом Partizan Cloud Storage;
- камера з хмарною прошивкою не підтримує стандартні програми на кшталт Partizan Pro, оскільки призначена виключно для хмарних застосунків.

У Partizan Device Manager сервіс оновлення представлений у вкладці «Обслуговування» у вигляді двох окремих кнопок - кожна відповідає за встановлення одного з типів прошивки. Після вибору кнопки потрібна версія прошивки автоматично завантажується з сервера та встановлюється, якщо вона доступна. Після інсталяції пристрій перезапускається, при цьому його налаштування залишаються без змін.

Якщо прошивка для конкретної моделі відсутня у базі, запит автоматично надсилається до Департаменту Розробки компанії Partizan Security. У такому разі прошивка буде створена та додана в базу протягом трьох робочих днів.

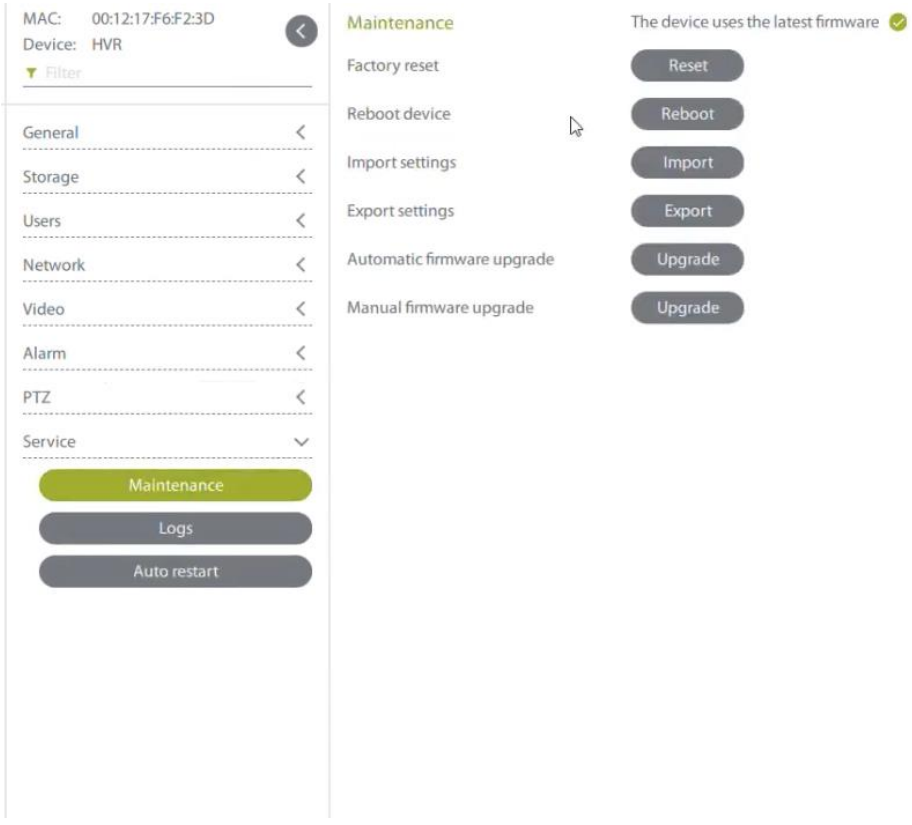

Рисунок 3.4 – Розділ обслуговування

Щоб зробити скидання до заводських налаштувань, необхідно зайти в розділ обслуговування (рисунок 3.4) і вибрати пункт «Обнулення до заводських налаштувань».

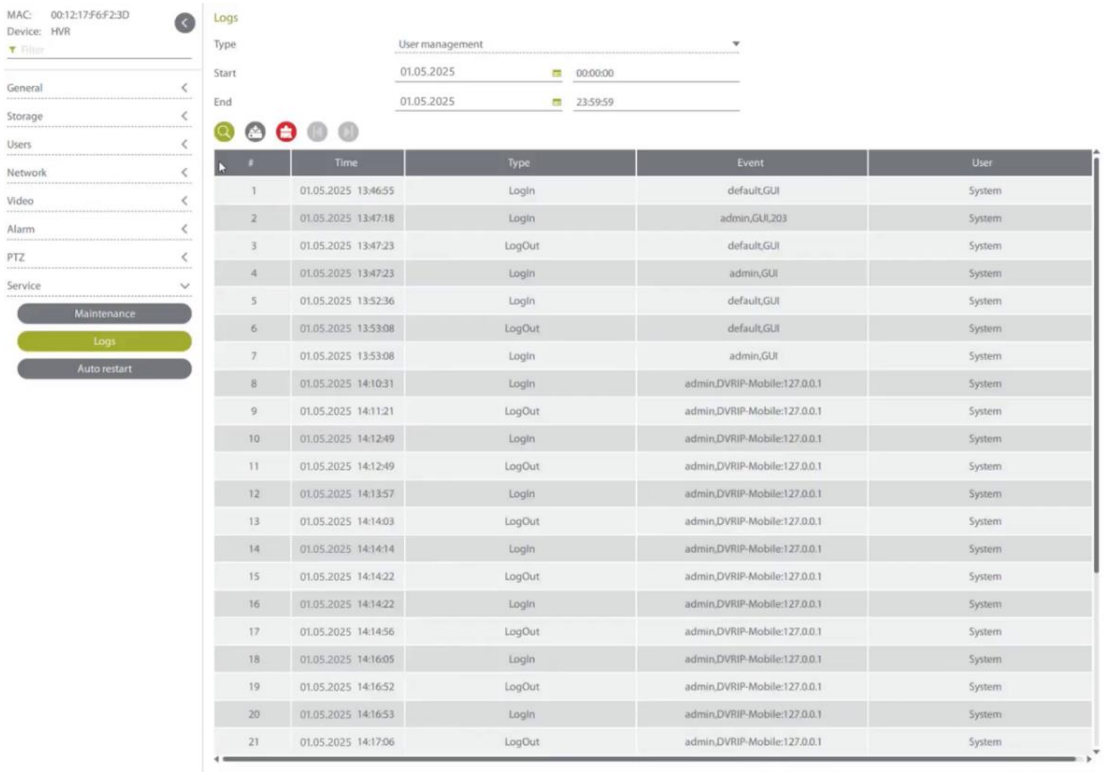

Рисунок 3.5 – Журнал подій

На рисунку 3.5 зображено інтерфейс журналу подій. У вікні відображаються записи про дії користувачів, зокрема час входу та виходу із системи, тип підключення (через інтерфейс або мобільний застосунок) і обліковий запис, з якого виконувалась дія.

Інтерфейс дозволяє фільтрувати події за типом, датою та часом, що дає змогу швидко знаходити потрібну інформацію. Такий журнал є важливою частиною системи безпеки, оскільки дає змогу контролювати доступ та аналізувати дії користувачів у разі інцидентів.

Також програмне забезпечення передбачає роботу з вбудованою базою даних, яка автоматично обслуговується через графічний інтерфейс адміністратора. Це забезпечує простоту експлуатації, швидкодію, а також виключає необхідність безпосередньої роботи з SQL-запитами з боку персоналу.

У процесі налаштування системи використовується кілька рівнів параметрів (таблиця 3.1), які охоплюють різні аспекти її роботи:

Таблиця 3.1 – Рівні конфігурації системи відеоспостереження

Рівень	Що налаштовується	Як відбувається
Програмне забезпечення	Ролі, доступи, журнал подій	Через GUI або config-файли
База даних	Структура, зв’язки, зберігання	SQL-запити, внутрішній API
Мережа	IP-адреси камер	DHCP, ручне налаштування
Безпека	Паролі, шифрування, резервні копії	Хешування, ролі БД, автоматизація

База даних системи включає чотири основні таблиці. Нижче подано їх короткий опис та приклади наповнення (таблиця 3.2-3.5).

Таблиця 3.2 – Користувачі

id	логін	роль	хеш_паролю
1	admin	адміністратор	********
2	guard1	охоронець	********

Призначення: зберігання облікових записів та ролей користувачів. Через інтерфейс адміністратор може створити нового користувача, вказати роль, а система автоматично захешує пароль.

Таблиця 3.3 – Камери

id	назва	поверх	ip_адреса
1	Вхід	1	192.168.1.10
2	Коридор 2 поверх	2	192.168.1.11

Призначення: облік підключених IP-камер, їх назв та місць встановлення. Налаштування камер виконується через GUI: IP-адреса вноситься вручну або автоматично сканується мережею.

Таблиця 3.4 – Відеоархів

id	камера_id	дата	час_початку	час_завершення	шлях_до_файлу
1	1	2025-06-09	08:00:00	08:10:00	/videos/door1_0800.mp4
2	2	2025-06-09	08:00:00	08:15:00	/videos/hall2_0800.mp4

Призначення: автоматичне індексування відеофрагментів, що записуються системою. Шлях до файлу генерується автоматично.

Таблиця 3.5 – Журнал подій

id	користувач_id	тип_події	дата_час
1	1	вхід в систему	2025-06-09 07:50:00
2	2	перегляд відео	2025-06-09 08:20:00

Призначення: фіксація дій користувачів у системі — з метою аудиту, безпеки та виявлення порушень.

У системі передбачено набір базових дій, які виконує адміністратор через графічний інтерфейс, з відповідним внесенням даних у базу (табл. 3.6):

Таблиця 3.6 – Дії адміністратора та їх реалізація в БД

Дія	Реалізація
Створення користувача	GUI → запис у таблицю Користувачі
Додавання камери	GUI → запис у таблицю Камери
Налаштування архіву	GUI → автозапис у Відеоархів
Перевірка дій	Перегляд вмісту Журнал_подій
Обмеження доступу	Призначення ролей або прав доступу в GUI

Варто зазначити, що навіть якщо адміністратор не працює з SQL-запитами безпосередньо, усі його дії всередині програми викликають відповідні SQL-команди, які оновлюють записи у базі.

Для захисту даних передбачено хешування паролів, обмеження доступу на рівні ОС і можливість планування резервного копіювання файлу БД. Це дозволяє відновити інформацію у разі збою без втрати критичних даних.

У сукупності описані дії та механізми дозволяють ефективно керувати системою відеоспостереження без необхідності глибокої технічної підготовки адміністратора, забезпечуючи зручність, безпеку й надійність усіх процесів взаємодії з базою даних і програмою в цілому.

3.3 Вирішення типових несправностей

У разі виникнення проблем з роботою обладнання рекомендується скористатися наступними вказівками:

- щоб визначити невідому IP-адресу камери, дізнатись її серійний номер (Partizan ID) або MAC-адресу, скористайтеся програмою Partizan Device Manager;

- якщо IP-камери, підключені до однієї мережі, не працюють одночасно, але окремо функціонують коректно - перевірте, щоб у кожної з них була унікальна IP-адреса, а не стандартна заводська;

- якщо камера постійно перезавантажується, перевірте, чи відповідає джерело живлення вимогам камери та чи не втрачається потужність на довгих кабелях. Спробуйте підключити камеру до іншого блоку живлення або використати коротший кабель;

- якщо система працює нестабільно, зображення мають шуми чи спотворення - це може бути спричинено заземленням елементів відеоспостереження. Перевірте й усуньте можливі точки заземлення: корпуси камер, обплетення коаксіального кабелю, кабелі живлення дисплея, підключеного до відеореєстратора;

- розмите чи нечітке зображення може бути наслідком неправильно налаштованого об’єктива або забруднення лінз. Очистьте лінзи засобом для оптики й налаштуйте фокус вручну;

- якщо зовнішня лінза запотіла - витріть її м’якою тканиною з оптичним засобом. Якщо це трапляється регулярно, варто замінити камеру на модель, розраховану на роботу в умовах підвищеної вологості;

- у випадку запотівання внутрішніх лінз зверніться до сервісного центру - можливо, порушена герметичність корпусу, і потрібно замінити вологопоглинаючий елемент;

- якщо проблема не вирішується жодним із вказаних способів, зверніться до служби технічної підтримки Partizan для подальшої діагностики та допомоги.

Висновок до розділу

У третьому розділі розглянуто практичні аспекти встановлення, налаштування та обслуговування комп’ютерної системи відеоспостереження для Калуського ліцею ім. Д. Бахматюка.

Здійснено аналіз правил встановлення обладнання, враховано електротехнічні вимоги, зокрема необхідність електричної ізоляції камер від металевих поверхонь, стабільного живлення та захисту від перенапруг. Детально описано інструкції з монтажу, підключення і налаштування IP-камер, зокрема використання шаблонів для точного розміщення, а також засоби регулювання об’єктива й фокусування.

Окрема увага приділена програмному забезпеченню Partizan Device Manager, яке використовується для автоматичного виявлення камер у мережі, зміни налаштувань, оновлення прошивок, роботою з базами даних, налаштування мережевих параметрів, ведення журналу подій і безпечної роботи з обліковими даними.

У розділі також подано рекомендації щодо виявлення та усунення типових несправностей, зокрема проблем із живленням, IP-конфліктами, запотіванням об’єктивів, а також ситуацій, що виникають через неправильну експлуатацію або порушення технічних вимог.

В результаті було доведено, що правильна інсталяція та обслуговування системи є критично важливими чинниками її надійної роботи. Виявлені особливості й запропоновані рішення забезпечують стабільність, безперервність відеоспостереження та відповідність вимогам безпеки навчального середовища.

4 ОЦІНКА ЕФЕКТИВНОСТІ ТА МАСШТАБУВАННЯ СИСТЕМИ

4.1 Оцінка ризиків без відеоспостереження

Відсутність системи відеоспостереження у сучасному освітньому закладі створює низку серйозних ризиків - як для фізичної безпеки учнів та працівників, так і для матеріального забезпечення установи, її репутації, а також правового захисту у разі інцидентів. Особливо критичним це є в умовах зростання рівня суспільної тривожності, зростання підліткової агресії, випадків вандалізму, проникнення сторонніх осіб на територію шкіл та зниження загального рівня дисципліни.

Фізична безпека учнів і персоналу

Одним із головних завдань системи відеонагляду є превенція ситуацій, що становлять загрозу життю або здоров'ю. Без відеофіксації адміністрація втрачає можливість оперативно реагувати на:

- випадки агресії між учнями, булінг, конфлікти або бійки;
- ситуації, коли учні травмуються в коридорах, сходах чи спортзалі без свідків;
- проникнення сторонніх осіб у будівлю, зокрема під час навчального процесу або після завершення занять;
- ризики пов'язані з несанкціонованим залишенням території закладу учнями під час уроків або перерв.

Відсутність камер у місцях загального користування - таких як входи, коридори, хол, спортзал, внутрішнє подвір'я - позбавляє керівництво ключового інструмента контролю і стримування подібних ситуацій.

Матеріальні збитки та вандалізм

У шкільних будівлях часто фіксуються випадки псування шкільного майна - розбиття вікон, ламання меблів, зіпсовані стіни, крадіжки обладнання або техніки. Без системи спостереження практично неможливо виявити винуватців, оскільки:

- більшість інцидентів відбувається у віддалених або неконтрольованих зонах;
- учні рідко зізнаються у вчиненому правопорушенні без прямих доказів;
- свідки, навіть якщо є, не завжди готові повідомляти правду.

Це призводить до фінансових втрат, відсутності відповідальності і підриву дисципліни.

Порушення внутрішнього порядку та дисципліни

Коли учні знають, що за їхньою поведінкою не спостерігають, рівень порушень дисципліни зростає. Відсутність відеоспостереження провокує такі прояви:

- систематичні запізнення або прогули;
- куріння, вживання енергетичних напоїв або алкоголю на території школи;
- несанкціонований доступ до службових приміщень;
- порушення санітарних правил у туалетах, роздягальнях або технічних кімнатах.

Впровадження системи відеоспостереження має психологічний стримувальний ефект, тому її відсутність - прямий фактор зростання порушень.

Репутаційні та соціальні ризики

Ситуації, пов’язані з насильством, булінгом або небезпекою для дітей, без належної фіксації можуть стати предметом публічного резонансу. У випадках, коли у школі трапляються інциденти, і немає записів камер, ЗМІ або батьки можуть трактувати ситуацію упереджено, звинувачуючи адміністрацію у бездіяльності.

Таким чином, відсутність системи фіксації:

- знижує довіру з боку батьків і громади;
- може викликати негативні висвітлення у пресі або соцмережах;
- послаблює позиції адміністрації при розгляді конфліктів.

Відсутність доказової бази у спірних ситуаціях

Системи відеоспостереження відіграють критичну роль при офіційному розслідуванні подій: травмувань, пожеж, крадіжок, правопорушень тощо. Без відеоархіву:

- адміністрація не може надати доказів правоохоронним органам або страховим компаніям;
- стає складно обґрунтувати дії працівників чи учнів;
- втрачається можливість переглянути хронологію подій;
- рішення часто базуються на свідченнях, що можуть бути неповними або упередженими.

В умовах сучасної правової системи відсутність об'єктивної відеоінформації може призвести до юридичної відповідальності або невиправданих звинувачень.

Ризик втрати контролю за зовнішнім периметром

У багатьох навчальних закладах питання безпеки обмежується внутрішніми приміщеннями. Проте найбільша частка загроз надходить ззовні - під час приходу/виходу учнів, перерв, батьківських зборів, спортивних змагань тощо.

Відсутність камер на подвір'ї або поблизу входу/виходу призводить до:

- неконтрольованого пересування сторонніх осіб;
- конфліктів між учнями або з мешканцями району;
- небезпеки на проїжджій частині чи шкільній стоянці.

Також у разі НС (наприклад, евакуації або пожежі) неможливо відтворити хід подій для подальшого аналізу ефективності дій персоналу.

Аналізуючи всі згадані аспекти, можна зробити висновок, що відсутність відеоспостереження у навчальному закладі створює високий рівень ризику, як для безпеки, так і для управлінських процесів. У сучасних умовах система відеоспостереження не є розкішшю, а - необхідним елементом інфраструктури безпеки, який:

- мінімізує загрози фізичної шкоди;
- забезпечує дисципліну й правопорядок;

- надає юридичну захищеність адміністрації;
- створює прозорість управлінських рішень;
- формує довіру з боку батьків, учнів та громадськості.

4.2 Вартість впровадження та експлуатації системи відеоспостереження

Запровадження системи відеоспостереження передбачає комплекс витрат, пов’язаних не лише з закупівлею обладнання, але й із подальшим налаштуванням, навчанням персоналу, обслуговуванням та енергоспоживанням. Розрахуємо вартість обладнання (табл. 4.1).

Таблиця 4.1 - Вартість обладнання

Найменування	Кількість	Одинична вартість, грн	Загальна вартість, грн
IP-камера Partizan IPO-2SP SE	27	2 600	70 200
PoE-комутатор PoE-Link PL-2016GG-2SF	2	5 700	11 400
Сервер (Intel Core i5, 8/16 ГБ, 4 ТБ HDD)	2	17 000	34 000
Монітор 21.5" Full HD	2	4 000	8 000
Джерело безперебійного живлення (UPS)	2	3 000	6 000
HDD WD Purple 4 ТБ	2	4 000	8 000
Кронштейни, кабель, короб, інше	комплект	-	5 000
Разом	-		142 600 грн

Вартість монтажних робіт

Монтаж системи передбачає прокладання кабельних трас, встановлення камер, кріплення комутатора, налаштування мережі, підключення до електроживлення, фіксацію устаткування та первинне тестування (табл.4.2).

Таблиця 4.2 - Вартість монтажних робіт

Робота	Одиниця виміру	Кількість	Ціна за одиницю	Загальна сума, грн
Монтаж камер	шт.	27	400	10 800
Прокладання кабелю	м	~300 м	20	6 000
Підключення + налаштування системи	фіксовано	1	1 200	1 200
Разом	-	-	-	18 000 грн

Обслуговування системи передбачає: оновлення ПЗ, перевірка працездатності обладнання, очищення камер, заміна кабелів або роз'ємів у разі потреби. Сума початкових витрат розрахована в таблиці 4.3..

Таблиця 4.3 – Сума початкових витрат

Категорія витрат	Вартість, грн
Обладнання	142 600
Монтаж	18 000
Разом	160 600грн

Конфігурація системи відеоспостереження - це повноцінна багатокамерна система із 27 IP-камерами, двома комутаторами PoE, двома серверами для зберігання і обробки відео, а також безперебійним живленням. Для центрального керування обрана програма Partizan CMS, що не потребує додаткових витрат на ліцензію в базовому варіанті. Таким чином, система є масштабованою, економічно ефективною та повністю відповідає потребам навчального закладу.

Вартість впровадження залишається в межах 170 тисяч гривень, що робить її доступною для комунального освітнього закладу за підтримки бюджету або меценатів. Такий підхід дозволяє забезпечити надійний контроль ключових зон, підвищити дисципліну, знизити ризики та покращити загальний рівень безпеки учасників освітнього процесу.

4.3 Пропозиції щодо масштабування системи

Поточна система відеоспостереження у Калуському ліцеї ім. Д. Бахматюка реалізована на основі сучасних IP-технологій із використанням 27 камер Partizan IPO-2SP SE, двох PoE-комутаторів на 16 портів кожен, серверів відеозапису з архівуванням на локальні жорсткі диски, а також централізованого моніторингу через Partizan CMS. Хоча система вже охоплює основні ризикові зони на трьох поверхах будівлі, є низка обґрунтованих напрямків для її подальшого масштабування.

1. Масштабування за кількістю камер

Незважаючи на покриття головних коридорів, входів, сходів, їдальні та актового залу, у ліцеї залишаються зони з обмеженим або відсутнім відеоспостереженням, зокрема:

- допоміжні приміщення (комори, архіви, майстерні);
- технічні зони (роздягальні спортзалу - з зовнішнім відеонаглядом, без порушення приватності);
- зовнішні периметри будівлі (запасні виходи, місця для збору сміття);
- ділянки подвір’я та шкільного майданчика;
- внутрішні входи до серверних або приміщень обслуговуючого персоналу.

Для забезпечення повноцінного відеоконтролю доцільним є встановлення ще 6–8 камер, що дозволить створити цілісну систему, яка унеможливить формування "мертвих зон".

2. Масштабування типів камер

Усі камери, які використовуються на даний момент, є фіксованими (Fixed Bullet) і забезпечують огляд під певним кутом. Проте для гнучкості й інтелектуального нагляду доцільно розглянути встановлення:

- PTZ-камер (Pan-Tilt-Zoom):
- можливість віддалено змінювати напрям зйомки та масштаб;

- ефективно застосовуються у великих приміщеннях, на подвір'ї або в коридорах з розгалуженнями;
- можуть автоматично патрулювати територію за заданими маршрутами.

Fisheye або 360°-камер:

- підходять для холів, вестибюлів або актового залу;
- замінюють 2–3 стандартні камери, охоплюючи повну площу.

Камери з аналітикою (Smart IP):

- виявлення сторонніх осіб;
- підрахунок кількості учнів у приміщеннях;
- виявлення довготривалого перебування без руху, бігу, падіння тощо.

3. Модернізація інфраструктури зберігання даних

Наразі система зберігає відео з усіх 27 камер на локальних HDD обсягом 4 ТБ у двох серверах. Цього вистачає на ≈21–30 діб архіву при стандартній якості та режимі запису «за рухом». У разі розширення системи або потреби у більш тривалому зберіганні відео (наприклад, 60–90 діб), рекомендується:

- заміна або доповнення HDD більшими накопичувачами (6–8 ТБ кожен);
- інтеграція NAS-сервера (мережевого сховища) з підтримкою RAID 1 або RAID 5 - для захисту від втрати даних;
- організація резервного копіювання важливих фрагментів на окремі диски, зовнішні накопичувачі або у хмарне сховище.

Також можливе створення розподіленої схеми запису, де частина камер пише на один сервер, а частина - на другий. Це дає змогу зменшити навантаження і підвищити надійність.

4. Розширення програмної частини

На поточному етапі використовується Partizan CMS - безкоштовне програмне забезпечення для перегляду, запису та керування камерами. Проте у разі збільшення кількості пристроїв або потреби в гнучкому керуванні користувачами та аналітикою доцільно перейти на:

- Axxon Next, Luxriot EVO, iVMS, Milestone XProtect - професійні системи з:

- розширеною відеоаналітикою;
- веденням журналів дій користувачів (аудит);
- інтеграцією з СКД, сигналізацією та іншим обладнанням.

Для шкіл, які мають обмежений бюджет, можна використовувати гібридну схему: базовий контроль через безкоштовне ПЗ, а критичні ділянки - через комерційне аналітичне ядро.

5. Інтеграція з іншими системами безпеки

Сучасні системи відеоспостереження можуть ефективно працювати в зв'язці з іншими засобами охорони, що особливо актуально для освітніх закладів. У перспективі масштабування варто передбачити:

- інтеграцію з системами контролю доступу (СКД):
  - зчитування перепусток, карт учнів/персоналу;
  - прив'язка відеопотоку до події проходу.
- Інтеграцію з охоронною та пожежною сигналізацією:
  - автоматичне виведення зображення при тривозі;
  - фіксація джерела сигналу в реальному часі.
- Автоматичне сповіщення охорони або адміністрації через локальну мережу, мобільний додаток або SMS.

Таке масштабування дозволяє перейти від реактивного контролю до активного керування безпекою, де система сама ініціює реакцію на подію.

Масштабування системи відеоспостереження у Калуському ліцеї можливе як кількісно (додаткові камери), так і якісно (аналітика, інтеграція, модернізація зберігання). Це дозволить:

- охопити всі критичні та допоміжні зони;
- автоматизувати реагування на події;
- підвищити рівень цифрової безпеки;
- забезпечити надійний відеоархів і аудит подій.

Такі заходи логічно поєднуються з цифровізацією освіти та загальнонаціональними стандартами безпеки у закладах освіти.

Висновок до розділу

У четвертому розділі було проведено всебічну оцінку ефективності впровадженої системи відеоспостереження для Калуського ліцею ім. Д. Бахматюка.

На основі аналізу ризиків, пов’язаних із відсутністю відеоспостереження, було обґрунтовано необхідність системного контролю для зниження кількості правопорушень, підвищення дисципліни та забезпечення безпеки учасників освітнього процесу.

Розраховано загальну вартість впровадження та експлуатації системи, що включає витрати на обладнання, монтаж, програмне забезпечення, навчання персоналу, технічне обслуговування та споживання електроенергії. Встановлено, що проєкт є фінансово доцільним і оптимально збалансованим за співвідношенням "вартість – функціональність". При цьому щорічні експлуатаційні витрати залишаються помірними, що дозволяє закладу планувати бюджетне обслуговування системи.

Також розглянуто можливості масштабування - система побудована з урахуванням подальшого розширення як по кількості камер, так і шляхом впровадження аналітичних функцій або підключення зовнішніх зон. Архітектура дозволяє інтеграцію з хмарними сервісами, централізоване адміністрування та модернізацію без суттєвих витрат.

Таким чином, оцінка ефективності підтвердила доцільність впровадженого рішення, його економічну виправданість, відповідність сучасним технічним вимогам та перспективність для подальшого розвитку.

ВИСНОВКИ

У ході виконання дипломної роботи було розроблено та обґрунтовано комп’ютерну систему відеоспостереження для Калуського ліцею імені Дмитра Бахматюка. Розробка здійснювалась з урахуванням сучасних вимог до інформаційної безпеки, нормативно-правової бази України та реальних потреб навчального закладу щодо підвищення рівня безпеки, контролю та нагляду.

На першому етапі дослідження було проаналізовано сучасний стан технологій відеоспостереження, їх класифікацію та практичне застосування в освітній сфері. Окрему увагу приділено нормативно-правовим вимогам, які регулюють використання відеоспостереження в навчальних закладах, зокрема щодо захисту персональних даних і відповідності технічним стандартам.

У другому розділі було виконано проєктування системи з урахуванням особливостей приміщень ліцею, розроблено структурну й логічну схеми, визначено оптимальні місця встановлення камер та сформовано архітектуру зберігання відеоінформації. Обґрунтовано вибір обладнання — IP-камер з живленням через PoE, серверного сховища, мережевого обладнання та джерел безперебійного живлення. Також сформовано логіку роботи системи, включно з можливістю архівації, віддаленого доступу та розмежування прав користувачів.

У третьому розділі розглянуто практичні аспекти встановлення, налаштування та обслуговування системи. Подано детальні рекомендації щодо монтажу камер, підключення мережевого обладнання, налаштування IP-адрес, оновлення прошивок та усунення типових несправностей. Також охарактеризовано функціональні можливості програмного забезпечення для адміністрування системи.

Четвертий розділ містить економічне обґрунтування впровадження. Розраховано загальну вартість реалізації системи — від 161 100 до 167 100 грн залежно від обраного програмного забезпечення, а також визначено щорічні витрати на експлуатацію, які становлять близько 8 250 грн. Аналіз показав, що система є економічно доцільною, фінансово доступною для навчального закладу

та не потребує значних ресурсів для обслуговування. Також проєкт передбачає можливість подальшого розширення без суттєвих змін у базовій структурі.

Таким чином, запропоноване рішення повністю відповідає технічним, функціональним і фінансовим вимогам до сучасної системи відеоспостереження для навчального закладу. Його впровадження дозволить значно підвищити рівень безпеки, дисципліни та прозорості всередині освітнього середовища, а також створює передумови для подальшої цифровізації інфраструктури закладу.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 05.05.2025).
2. Про освіту: Закон України від 05 вересня 2017 року № 2145-VIII. URL: https://zakon.rada.gov.ua/laws/show/2145-19 (дата звернення: 05.05.2025).
3. Про інформацію: Закон України від 02 жовтня 1992 року № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 05.05.2025).
4. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 05.05.2025).
5. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. Geneva: International Organization for Standardization, 2013. 30 с.
6. ONVIF – Open Network Video Interface Forum. URL: https://www.onvif.org (дата звернення: 05.05.2025).
7. ДСТУ ISO/IEC 29100:2016. Інформаційні технології. Методи захисту. Загальна структура захисту приватності. [Чинний від 2017-01-01]. К.: ДП «УкрНДНЦ», 2016. 30 с.
8. ДСТУ EN 62676-1-1:2017. Системи відеоспостереження для застосування в сфері безпеки. Частина 1-1. Системні вимоги. Загальні положення. К.: ДП «УкрНДНЦ», 2017. 48 с.
9. Axis Communications. Solutions for education. URL: https://www.axis.com/en-us/solutions/education (дата звернення: 05.05.2025).
10. Pečar, D., & Podgorelec, D. A review of methods and datasets for video anomaly detection // Informatica Economica. 2022. Vol. 26. pp. 27-36.
11. viisights. Solutions for education campuses. URL: https://www.viisights.com/solutions/education-campuses/ (дата звернення: 05.05.2025).

12. Wang, W., Liu, J., Lin, Z., & et al. MagicVideo-V2: Multi-Stage High-Aesthetic Video Generation. URL: https://arxiv.org/abs/2212.12936 (дата звернення: 05.05.2025)

13. SYSVIDEO. Solutions. URL: http://www.sysvideo.cn/solutions/detail.aspx?id=122 (дата звернення: 05.05.2025).

14. Ibosiola, D., Steer, B. A., García-Recuero, Á., & et al. Movie Pirates of the Caribbean: Exploring Illegal Streaming Cyberlockers // Applied Sciences. 2021. Vol. 11, No. 12. 5571 (Ibosiola et al., 2018).

15. Hanwha Vision America. Markets: Education. URL: https://hanwhavisionamerica.com/markets/education/ (дата звернення: 05.05.2025).

16. Поради щодо проєктування та встановлення систем відеоспостереження. URL: https://100realty.ua/uk/articles/poradi-schodo-proektuvannya-ta-vstanovlennya-sistem-videosposterezhennya (дата звернення: 05.05.2025).

17. Березький О.М., Дубчак Л.О., Мельник Г.М., Батько Ю.М., Піцун О.Й. Методичні рекомендації до виконання кваліфікаційної роботи з освітнього ступеня “Бакалавр” спеціальності 123 «Комп’ютерна інженерія» галузі знань 12 Інформаційні технології. Тернопіль: ЗУНУ, 2024.

18. Особливості проектування систем відеоспостереження. URL: http://tren.com.ua/osoblivosti-proektuvannya-sistem-vid/ (дата звернення: 05.05.2025).

19. Тангієв А.А., Деревецький В.Ю., Гураль В.С. Методи протидії атакам на дистанційний банкінг. Матеріали IX Всеукраїнської науково-практичної конференції молодих вчених «Інформаційні технології – 2024». Київ, 2024. С. 260-261.

20. Омельченко М. Підвищення інформаційної безпеки об’єкту інформаційної діяльності шляхом використання інтегрованої системи безпеки: дипломна робота. Київ, 2021.

21. Чудаков К.С. Корпоративна мережа відеоспостереження у місті: дипломний проект. Київ: НТУУ «КПІ імені І. Сікорського», 2023.

22. Partizan Store. URL: https://partizanstore.eu (дата звернення: 05.05.2025).

23. Partizan Global. URL: https://partizan.global (дата звернення: 05.05.2025).

24. WebCameraCloud. URL: https://webcameracloud.com (дата звернення: дата звернення: 05.05.2025).

25. Ben Software. SecuritySpy. URL: https://bensoftware.com/securityspy/ (дата звернення: 05.05.2025).

26. Ben Software. SecuritySpy User Manual. URL: https://bensoftware.com/securityspy/manual/ (дата звернення: 05.05.2025).

27. ZoneMinder. Features. URL: https://zoneminder.com/features/ (дата звернення: 05.05.2025).

28. ZoneMinder. Define Zone. URL: https://zoneminder.readthedocs.io/en/stable/userguide/definezone.html (дата звернення: 05.05.2025).

БІБЛІОГРАФІЧНА ДОВІДКА

Тема бакалаврської роботи: ***Розробка комп'ютерної системи відеоспостереження для Калуського ліцею ім. Д. Бахматюка з безпечним збереженням даних***

Обсяг пояснювальної записки 88 аркушів:

18 таблиць;

26 рисунків.

Дата завершення роботи: *09 червня 2025р*.

Підпис студента- _____*Балита І.М.*.