

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ**

КВАЛІФІКАЦІЙНА РОБОТА
на тему: «ІНТЕЛЕКТУАЛЬНА СИСТЕМА
ВІДЕОСПОСТЕРЕЖЕННЯ НА ОСНОВІ МАШИННОГО
НАВЧАННЯ»

на здобуття освітнього ступеня магістра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

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

_____ (підпис)	<u>Володимир ГАЛЕТА</u> Ім'я, ПРИЗВИЩЕ здобувача
-------------------	---

Виконав:	здобувач(ка) вищої освіти гр. <u>КСДМ-62</u> <u>Володимир ГАЛЕТА</u> Ім'я, ПРИЗВИЩЕ
Керівник:	<u>Артем АНТОНЕНКО</u> Ім'я, ПРИЗВИЩЕ
Рецензент:	_____ Ім'я, ПРИЗВИЩЕ

науковий ступінь,
вчене звання

науковий ступінь,
вчене звання

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
Навчально-науковий інститут Інформаційних технологій

Кафедра Комп'ютерної інженерії

Ступінь вищої освіти Магістр

Спеціальність 123 «Комп'ютерна інженерія»

Освітньо-професійна програма Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ

Завідувач кафедри Наталія ЛАЩЕВСЬКА

_____ Ім'я, ПРІЗВИЩЕ
«_____» _____ 2024р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Галета Володимир Сергійович

(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Інтелектуальна система відеоспостереження на основі машинного навчання»

керівник кваліфікаційної роботи: Артем АНТОНЕНКО, канд.техн.наук, доцент,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від
«15» жовтня 2024р. №320

2. Строк подання кваліфікаційної роботи: «29» грудня 2024р.

3. Вихідні дані до кваліфікаційної роботи: Науково-технічна література, технологічні рамки та протоколи, дизайн і архітектура системи, технічні характеристики пристрою та вимоги, інтеграція та функціональність, оцінка та бенчмаркінг.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Теоретичні основи інтелектуальних систем відеоспостереження
2. Хмарні обчислення та Fog Computing у відеоспостереженні
3. Розробка та реалізація інтелектуальної децентралізованої системи відеоспостереження
4. Впровадження систем відеоспостереження у різних умовах

5. Перелік ілюстративного матеріалу: презентація

1. Мета, об'єкт, предмет дослідження
2. Актуальність роботи
3. Проблеми традиційних систем відеоспостереження та необхідність інтелектуальних рішень
4. Хмарні та туманні обчислення з використанням методів машинного навчання
5. Архітектура інтелектуальної системи відеоспостереження
6. Розміщення камер відеоспостереження у різних локаціях
7. Мережева інфраструктура та резервування
8. Забезпечення резервуванням основної камери відеоспостереження
9. Демонстрація функціональних можливостей додатка від виробника
10. Власний сервер для реалізації закритого локального спостереження

11. Proxmoх та Home Assistant: інтеграція motionEye для моніторингу
 12. Кошторис реалізації інтелектуальної системи відеоспостереження
 13. Порівняльний аналіз традиційних систем відеоспостереження та запропонованого рішення
 14. Висновки
 15. Публікації та апробація роботи
6. Дата видачі завдання «01» вересня 2024р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	10.10-12.10.2024	
2	Обробка матеріалу	12.10-15.10.2024	
3	Розробка теоретичної частини	15.10-18.10.2024	
4	Хмарні обчислення та Fog computing у відеоспостереженні	18.10-22.10.2024	
5	Розробка та реалізація інтелектуальної децентралізованої системи відеоспостереження	22.10-26.10.2024	
6	Впровадження систем відеоспостереження в різних умовах експлуатації	26.10-30.11.2024	
7	Висновки за результатами аналізу	30.11-02.12.2024	
8	Розробка презентації	02.12-08.12.2024	
9	Передзахист	09.12-11.12.2024	
10	Здача в деканат	20.12-29.12.2024	

Здобувач вищої освіти

(підпис)

Володимир ГАЛЕТА
(Ім'я, ПРІЗВИЩЕ)

Керівник кваліфікаційної роботи

(підпис)

Артем АНТОНЕНКО
(Ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістр: 137 стор., 62 рис., 9 табл., 49 джерел.

Мета роботи – розробити і впровадити інтелектуальну децентралізовану систему відеоспостереження, яка використовує машинне навчання, хмарні обчислення та платформи Fog Computing для забезпечення надійного спостереження в урбанізованих і важкодоступних регіонах.

Об'єкт дослідження – система відеоспостереження з використанням технологій машинного навчання.

Предмет дослідження – методи та технології побудови децентралізованих систем відеоспостереження для різних умов середовища, що базуються на інтелектуальних обчисленнях та розподілених обчислювальних платформах.

Короткий зміст роботи: У роботі розглянуто розробку та впровадження інтелектуальних децентралізованих систем відеоспостереження, що поєднують технології машинного навчання, хмарного обчислення та Fog Computing.

Проаналізовано сучасні тенденції та обмеження систем відеоспостереження, а також рішення, які підвищують їх продуктивність і надійність. Машинне навчання автоматизує аналіз відеоданих, покращуючи точність виявлення об'єктів і аномалій. Хмарні обчислення забезпечують масштабовану обробку великих обсягів даних, а Fog Computing мінімізує затримки, розташовуючи обчислювальні ресурси ближче до джерел даних. Запропонована архітектура дає змогу ефективно використовувати такі системи в різних умовах.

КЛЮЧОВІ СЛОВА: ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ, ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ, МАШИННЕ НАВЧАННЯ, ХМАРНІ ОБЧИСЛЕННЯ, FOG COMPUTING, АНАЛІЗ ВІДЕОДАНИХ, БЕЗПЕКА, УРБАНІЗОВАНІ МІСЦЕВОСТІ, ВАЖКОДОСТУПНІ МІСЦЕВОСТІ, РОЗПОДІЛЕНІ ОБЧИСЛЕННЯ, МОНІТОРИНГ.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 137 pages, 62 figures, 9 tables, 49 sources.

The purpose of the work is to develop and implement an intelligent decentralized video surveillance system that uses machine learning, cloud computing, and Fog Computing platforms to provide reliable surveillance in urbanized and hard-to-reach regions.

The object of the research is video surveillance system using machine learning.

The subject of research is methods and technologies for building decentralized video surveillance systems for various environmental conditions based on intelligent computing and distributed computing platforms.

Summary of the work: The paper discusses the development and implementation of intelligent decentralized video surveillance systems that combine machine learning, cloud computing, and Fog Computing technologies.

The current trends and limitations of video surveillance systems are analyzed, as well as solutions that increase their performance and reliability. Machine learning automates the analysis of video data, improving the accuracy of object and anomaly detection. Cloud computing provides scalable processing of large amounts of data, and Fog Computing minimizes delays by placing computing resources closer to data sources. The proposed architecture allows for the effective use of such systems in various conditions.

KEY WORDS: INTELLIGENT VIDEO SURVEILLANCE SYSTEMS, DECENTRALIZED SYSTEMS, MACHINE LEARNING, CLOUD COMPUTING, FOG COMPUTING, VIDEO DATA ANALYSIS, SECURITY, URBANIZED LOCATIONS, HARD-TO-ACCESS LOCATIONS, DISTRIBUTED COMPUTING, MONITORING.

ЗМІСТ

ВСТУП.....	9
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ.....	10
1.1 Визначення та класифікація систем відеоспостереження	10
1.2 Проблеми та обмеження традиційних централізованих систем	17
1.3 Тенденції розвитку інтелектуальних децентралізованих систем.....	24
1.4 Переваги та виклики використання інтелектуальних децентралізованих систем відеоспостереження	31
РОЗДІЛ 2 ХМАРНІ ОБЧИСЛЕННЯ ТА FOG COMPUTING У ВІДЕОСПОСТЕРЕЖЕННІ.....	40
2.1 Архітектура хмарних обчислень у відеоспостереженні	40
2.2 Концепція Fog Computing та її основні характеристики.....	48
2.3 Порівняння рішень на основі хмарних і Fog-обчислень для розподіленої обробки даних.....	53
РОЗДІЛ 3 РОЗРОБКА ТА РЕАЛІЗАЦІЯ ІНТЕЛЕКТУАЛЬНОЇ ДЕЦЕНТРАЛІЗОВАНОЇ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ	60
3.1 Компоненти інтелектуальних децентралізованих систем.	60
3.2 Інтеграція машинного навчання у систему відеоаналізу	81
3.3 Забезпечення безпеки та захисту даних у децентралізованих системах	88
3.4 Розподіл обчислювальних ресурсів між вузлами системи	94
РОЗДІЛ 4 ВПРОВАДЖЕННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ В РІЗНИХ УМОВАХ ЕКСПЛУАТАЦІЇ	100
4.1 Використання систем в урбанізованих зонах.....	100
4.2 Особливості впровадження у важкодоступних та віддалених місцевостях ...	105
4.3 Оцінка ефективності децентралізованих систем у різних середовищах.....	108
4.4 Економічні та технічні переваги децентралізованих систем.....	112
ВИСНОВКИ.....	117
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	118
Додаток А. Технічні характеристики, функціональні можливості IP камер та додатка від TP-Link серії TAPO.....	123
Додаток Б. Порівняння технічних характеристик та кошторис локального та хмарного сховища від TP-Link.....	126
Додаток В. Порівняння технічних характеристик маршрутизаторів від TP-Link серії Archer.....	128
Додаток Г. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація).....	129

ВСТУП

Швидкий прогрес у сфері технологій кардинально трансформував системи відеоспостереження, розширивши горизонти їхнього застосування. Раніше ці системи залежали від централізованого управління, потребували складної інженерної інфраструктури і значних ресурсів для розгортання та обслуговування. Висока вартість прокладання коаксіальних і живильних кабелів робила класичні системи громіздкими, особливо у випадку впровадження у кількох локаціях одночасно.

Децентралізація значно підвищила ефективність відеоспостереження. Завдяки IP-камерам, сучасні системи більше не залежать від централізованих вузлів для збереження та обробки даних, що дозволяє управляти ними з будь-якої точки світу через інтернет. Це зменшує навантаження на мережу і дає змогу адаптувати системи під індивідуальні потреби користувачів, спрощуючи налаштування та експлуатацію.

Ще однією суттєвою перевагою є використання хмарних обчислень, які дозволяють зберігати й обробляти дані на віддалених серверах. Інтеграція технологій машинного навчання відкриває нові можливості для автоматизації, такі як розпізнавання облич, детекція руху чи аналіз подій у реальному часі. Це значно підвищує ефективність систем у різноманітних сценаріях, від моніторингу великих міських зон до забезпечення безпеки критичних об'єктів.

Інноваційні технології, зокрема Fog Computing, дозволяють обробляти дані на проміжних вузлах, що зменшує затримки і знижує залежність від стабільного інтернет-з'єднання. Сучасні децентралізовані системи відеоспостереження стали невід'ємною частиною інфраструктури розумних міст, забезпечуючи швидкий і гнучкий контроль з мінімальними ресурсами для управління та налаштування.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

1.1 Визначення та класифікація систем відеоспостереження

Аналогові системи відеоспостереження (див. рис.1.1), які з самого початку широко використовувалися, базуються на застосуванні коаксіальних кабелів для з'єднання камер з відеореєстратором. Ці системи функціонують виключно локально, без підключення до мережі Інтернет, що обмежує їхні можливості. Основною характеристикою аналогового відеоспостереження є те, що вся інфраструктура налаштована в одному місці, і всі дані передаються до централізованого відеореєстратора, що дозволяє переглядати відео лише на підключених локальних моніторах, без можливості віддаленого доступу через Інтернет. Такі системи мають певні недоліки. По-перше, коаксіальні кабелі мають обмеження щодо довжини, що ускладнює масштабування системи, коли кількість камер збільшується. Для вирішення проблем із передачею сигналу можна використовувати підсилювачі, однак це призводить до зростання затримки та погіршення якості зображення.



Рисунок 1.1 – Демонтована несправна аналогова камера відеоспостереження
«LUXCAM»

Встановлення аналогових систем також потребує участі кваліфікованих спеціалістів, оскільки для правильної роботи потрібно заздалегідь продумати розташування камер і підготувати необхідну інфраструктуру. Без цих підготовчих етапів встановлення аналогової системи може бути складним і часозатратним процесом.

До того ж, аналогові камери мають досить низьку роздільну здатність через обмеження самої технології. Максимальна роздільна здатність для таких систем зазвичай становить 720x576 пікселів або 576р у співвідношенні сторін 4:3, що значно впливає на якість зображення. Через таку низьку роздільну здатність важко розпізнавати дрібні деталі, наприклад, обличчя людей чи номери автомобілів, що може суттєво знизити ефективність системи в ситуаціях, коли важливо отримати чітке відео з високим рівнем деталізації. Аналогові системи відеоспостереження мають обмеження у масштабуванні, складності встановлення, низькій роздільній здатності, а також відсутності можливості віддаленого доступу до відео, що робить їх менш ефективними порівняно з сучасними цифровими або мережевими рішеннями.

Протягом тривалого часу аналогові системи відеоспостереження залишалися основними технологіями в цій сфері. Однак із розвитком технологій та через обмеження аналогових систем відбулося поступове впровадження цифрових систем відеоспостереження. Відмінність цифрових систем полягає у використанні не аналогових, а аналого-цифрових перетворювачів (АЦП), які перетворюють інформацію з аналогового формату у цифровий – у вигляді нулів та одиниць, що дозволяє зберігати дані не в аналоговій формі, а у вигляді цифрових бітів, що значно підвищує ефективність обробки, збереження та передачі інформації. Основна зміна відбулася через відмову від магнітних носіїв, на які записувалась аналогова інформація. Натомість почали використовувати цифрові носії, які дозволяють зберігати значно більше інформації в порівнянні з попередніми аналоговими носіями. Цифрова інформація, яка зберігається у вигляді бінарних даних, значно краще підходить для обробки і дозволяє оптимізувати використання сховищ даних. Сучасні цифрові відеореєстратори можуть зберігати відео на

внутрішні або зовнішні жорсткі диски з великим об'ємом пам'яті, що дає змогу записувати величезну кількість даних на тривалі періоди часу (див. рис.1.2).



Рисунок 1.2 – Полусправний відеореєстратор «TVT TD-2308SE-SL» та демонтований жорсткий диск «Western Digital Blue 500GB»

Цифрові системи відеоспостереження (див. рис.1.3), які нині є найпоширенішими у світі, мають безліч переваг. Вони не тільки забезпечують покращену якість збереження відео та аудіо, але й підтримують високу роздільну здатність, яка може досягати 1, 2, 5, 10 або навіть 16 мегапікселів. У деяких випадках роздільна здатність таких систем досягає 4K і навіть вищих значень. Проте варто розуміти, що з підвищенням роздільної здатності збільшується об'єм даних, які необхідно зберігати, тому використовуються жорсткі диски з великою ємністю. У реальних умовах для більшості задач відеоспостереження достатньо роздільної здатності в межах 1-4 мегапікселів, що дозволяє отримувати чітке зображення, з якого можна розпізнати обличчя, номери автомобілів та інші деталі. Ще одним важливим аспектом цифрових систем є те, що вони дозволяють підключати велику кількість камер (4, 8, 16 та більше) до одного відеореєстратора. Усі камери одночасно фіксують відео та передають його на жорсткий диск відеореєстратора, що значно спрощує процес зберігання даних і управління системою.



Рисунок 1.3 – Стоп-кадр запису зі цифрових камер відеоспостереження «Xiaomi YI Home» зі роздільною здатністю 1280X720 (720P) або 1 МП

З приходом цифрових технологій з'явилася можливість використовувати мережеве з'єднання, що суттєво збільшило пропускну здатність і дозволило підключати камери безпосередньо до ПК або комутаторів через Ethernet-кабелі або патч-корди. Це нововведення не лише поліпшило якість відеофіксації, але й сприяло розвитку більш масштабованих систем відеоспостереження, що дозволяють ефективно охоплювати більші площі та інтегрувати більшу кількість камер.

Гібридні системи відеоспостереження представляють собою унікальне рішення, що поєднує в собі як аналогові, так і цифрові технології. Виходячи з назви, можна зрозуміти, що ці системи здатні одночасно працювати з обома типами камер, що робить їх досить гнучкими для різних умов. Основу таких систем становлять гібридні відеореєстратори (DVR), які можуть виконувати перетворення аналогового сигналу в цифровий, а також працювати безпосередньо з цифровими камерами, записуючи відео на внутрішні або зовнішні носії даних, включаючи ПК. Така технологія є досить зручною, особливо в тих випадках, коли є необхідність використовувати аналогові камери на ділянках, де не потрібно прокладати довгі коаксіальні кабелі для передачі зображення на віддалені точки. Наприклад, у близьких до системи відеоспостереження місцях можна встановлювати аналогові камери, а для більш віддалених об'єктів використовувати IP-камери. Цифрові IP-камери підключаються до мережі Інтернет і можуть взаємодіяти з гібридним

відеореєстратором через локальну мережу, що забезпечує можливість встановлення камер на більші відстані, ніж дозволяють коаксіальні підключення, які мають певні технічні обмеження. Натомість для IP-камер використовуються Ethernet-кабелі або патч-корди зі роз'ємами RG45, що спрощує прокладання кабелів і дозволяє використовувати існуючу мережеву інфраструктуру (маршрутизатори, комутатори).

Додатковою перевагою гібридних систем є їх універсальність і простота підключення. Такі камери можуть одночасно обслуговувати не тільки систему відеоспостереження, але й інші мережеві потреби. Наприклад, використання існуючих дротів заземлення в будинках для підключення інтернету через електричні розетки – це цікавий приклад такого підходу, який можна порівняти з гібридною відеосистемою. У цьому випадку використання заземляючого дроту як провідника для передачі інтернет-сигналу дозволяє уникнути додаткових витрат на прокладання нових ліній. Такі гібридні системи дозволяють плавно перейти від повністю аналогових систем відеоспостереження до сучасних рішень, просто замінивши окремі компоненти, як-от відеореєстратор, на гібридний, що значно полегшує процес модернізації системи без необхідності заміни всіх аналогових камер. До того ж, використання технології PoE (Power over Ethernet) дозволяє жити камери через Ethernet-кабелі або патч-корди без необхідності прокладання окремих ліній живлення (див. рис.1.4) [1].



Рисунок 1.4 – Використання патч-корду у якості живлення на камерах відеоспостереження від виробника Reolink

Гібридні системи відеоспостереження є зручним і економічно ефективним рішенням для тих, хто вже використовує аналогові системи, але прагне підвищити їх функціональність і масштабованість за рахунок цифрових технологій.

На сьогоднішній день ми поступово переходимо до використання сучасних інтелектуальних систем відеоспостереження, які базуються на децентралізації – управління такою системою більше не прив'язане до певної центральної точки, як це було раніше. Традиційні децентралізовані системи вже дозволяють підключати камери до мережі Інтернет і керувати ними з віддаленого місця. Однак, інтелектуальні децентралізовані системи відеоспостереження пропонують значно ширший функціонал, усуваючи потребу в додаткових компонентах, таких як відеореєстратори, коаксіальні кабелі чи Ethernet-кабелі або патч-корди, які були характерними для попередніх рішень.

Інтелектуальні децентралізовані системи складаються лише з камер, які самостійно виконують всі необхідні функції, не потребуючи додаткових допоміжних елементів для своєї роботи. Такі камери можуть використовувати безпроводні технології зв'язку, зокрема Wi-Fi або GSM, що значно спрощує їх використання та управління та надає змогу швидко налаштувати і управляти системою відеоспостереження з будь-якого куточка світу через мобільний додаток або спеціалізоване програмне забезпечення для ПК.

Однією з основних переваг таких камер є їх автономність, мобільність і простота у встановленні. Вони не вимагають прокладання складних мережевих структур, а все, що потрібно для їх роботи – це доступ до електромережі та безпроводний зв'язок (див. рис.1.5).



Рисунок 1.5 – Камери відеоспостереження Xiaomi Yi Home 720p з автономним живленням від портативних зарядних пристроїв

Камери легко масштабуються, оскільки можуть використовувати Wi-Fi або GSM для передачі даних, що дозволяє розміщувати їх у важкодоступних або віддалених місцях без необхідності прокладання фізичних з'єднань. Якщо потрібно підключити велику кількість таких камер в одній мережі, можна використовувати потужні маршрутизатори, такі як Ubiquiti або Mikrotik, або простіші рішення від Asus чи TP-Link, які підтримують технологію Mesh-систем, що дозволяє створювати стійку безшовну мережу з плавним переходом між точками доступу, аналогічно до мобільного зв'язку, забезпечуючи надійний зв'язок навіть у великих приміщеннях.

Інтелектуальні децентралізовані системи відеоспостереження можуть інтегрувати функції машинного навчання і хмарних сервісів, що дозволяє автоматизувати процеси аналізу даних. Наприклад, камери можуть розпізнавати рух, відрізняти людей від тварин, реагувати на плач дитини або інші специфічні події, автоматично надсилаючи сповіщення на ваш смартфон. Окрім цього такі системи можуть працювати у повністю автономному режимі завдяки використанню джерел безперебійного живлення або альтернативних джерел, таких як сонячні панелі, що дозволяє використовувати їх навіть у випадках перебоїв з електропостачанням. Розумні камери, які можуть передавати дані безпосередньо в хмару, зберігають відео навіть у разі пошкодження або знищення самої камери,

забезпечуючи додатковий рівень безпеки, що особливо корисно, якщо знаходитись далеко від об'єкта, за яким ведеться відеонагляд, іноді буде потрібен віддалений доступ до відеозаписів.

1.2 Проблеми та обмеження традиційних централізованих систем

Традиційні централізовані системи відеоспостереження мають ряд суттєвих недоліків, які стали ще більш очевидними з розвитком нових технологій:

- обмежена пропускна здатність;
- високі вразливість до відмов і кіберзагроз;
- труднощі в масштабуванні;
- велика кількість провідних з'єднань;
- складна інфраструктура,
- необхідність постійної технічної підтримки;
- обмежена функціональність.

Централізовані системи зазвичай використовуються великими компаніями, однак вони обмежують можливості доступу до відео поза межами корпоративної мережі (див. рис.1.6) [2]. Такий підхід може бути виправданий з точки зору безпеки, але коли кількість камер збільшується, система швидко досягає своїх фізичних і технічних меж. Прокладання кабелів для підключення камер, особливо на великих відстанях, стає трудомістким процесом, і це стосується як цифрових систем, що використовують Ethernet-кабелі або патч-корди, так і аналогових систем, які мають ще більше обмежень .

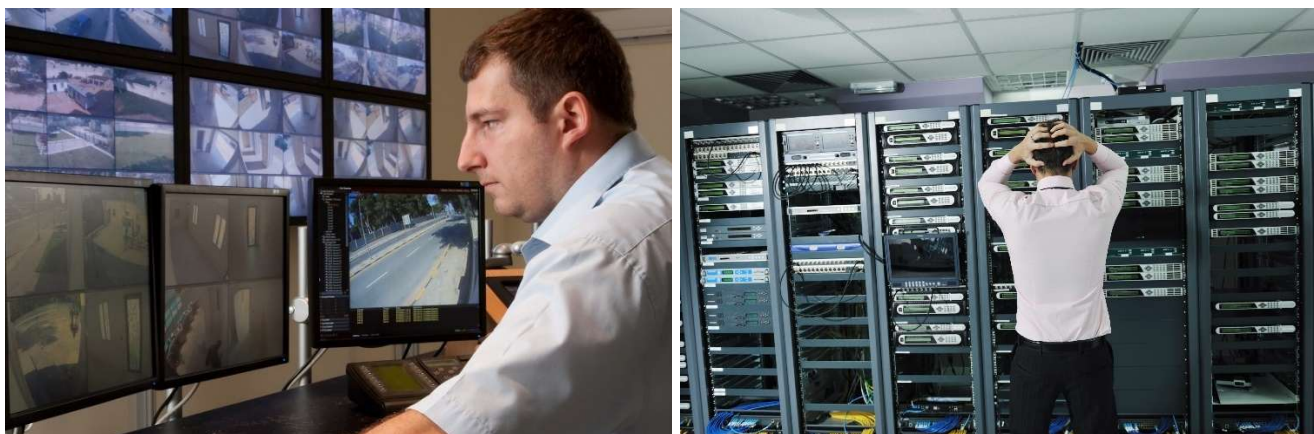


Рисунок 1.6 – Складнощі з постійним моніторингом та обслуговуванням традиційних систем відеоспостереження

Обмежений доступ на рівні закритої мережі. Одним із ключових недоліків централізованих систем є їх залежність від єдиного центру управління – у випадку відсутності або втрати критичних відеоданих, значна кількість часу витрачається на пошук потрібного фрагмента запису, особливо якщо невідомо точний час інциденту. Така залежність від централізованого керування також призводить до того, що в разі виходу з ладу центрального вузла система втрачає свою ефективність, а відновлення даних або подій може бути вкрай складним.

Використання застарілих технологій. Більшість традиційних систем відеоспостереження, які використовують застарілі камери, не мають здатності виявляти рух або автоматично записувати його протягом певного часу, що призводить до того, що важлива інформація може бути втрачена. Деякі камери взагалі не підтримують запис звуку, що ще більше ускладнює можливість отримання повної картини подій. Наприклад, якщо оператор залишає пост спостереження, або зосереджує увагу на чомусь іншому, важливий момент може бути пропущено – це може мати серйозні наслідки для системи, яка не здатна самостійно фіксувати все, що відбувається в режимі реального часу. Робота операторів, що контролюють такі системи, є виснажливою – людина змушена постійно сидіти перед численними моніторами і безперервно стежити за ситуацією в різних місцях, що є не лише важким, але й неефективним з точки зору використання часу та ресурсів (див. рис.1.6) [2]. Через це стало очевидним, що

сучасні системи відеоспостереження повинні еволюціонувати. Хоча централізація має свої переваги, коли всі дані зберігаються та обробляються в одному місці, така концепція є застарілою і потребує змін для ефективнішого управління сучасними системами безпеки.

Існують системи відеоспостереження, які мають функції фіксації подій або виявлення руху, проте більшість із них використовують застарілі технології, що вже давно не відповідають вимогам сучасних умов. Попри те, що світова індустрія пропонує більш сучасні рішення для централізованих систем, такі системи все ще мають ряд суттєвих проблем. Наприклад, навіть інтерфейс керування системою відеоспостереження часто є незручним для користувачів, які не мають досвіду роботи з такими технологіями. Налаштування і підтримка системи можуть вимагати спеціаліста – це призводить до додаткових витрат на догляд за такими людьми, навіть якщо система повністю належить приватній особі або компанії.

Окрім постійного моніторингу з боку оператора, необхідно також утримувати технічного спеціаліста, який буде відповідальний за налаштування, обслуговування і вирішення технічних проблем системи. Тобто, окрім оператора, компанії потрібно наймати окрему людину, яка регулярно буде приходити для обслуговування обладнання. Така потреба у технічному супроводі і постійному контролі з боку кількох працівників суттєво збільшує витрати на утримання системи відеоспостереження.

Обмежена мобільність. Однією з важливих проблем, які виникають під час використання централізованих систем відеоспостереження, є їх складність у перенесенні з одного приміщення до іншого. Уявімо ситуацію, коли орендується приміщення для власних потреб, де немає встановлених систем відеоспостереження, але наявна мінімальна інфраструктура, така як мережеві підключення та електроживлення. Спершу будуємо в цьому приміщенні власну систему, далі встановлюємо нове обладнання, включаючи камери спостереження, але стикаємося з проблемою, коли потрібно буде змінити місце оренди. При переїзді виникає необхідність демонтажу всієї інфраструктури, повертаючи приміщення до початкового стану.

Такий етап має на меті демонтаж системи відеоспостереження, які зазвичай обладнані великою кількістю з'єднувальних кабелів та мають громіздкі конструкції. Якщо демонтажем займається людина, що не спеціалізується на відеоспостереженні, вона може пошкодити обладнання або втратити важливі компоненти. призводить до додаткових витрат і проблем, що нагадує ситуацію, коли нам постійно потрібен технік для обслуговування системи. Такі системи є малопридатними для постійного демонтажу і перенесення в інші місця, що робить їх незручними для компаній або осіб, які часто змінюють орендовані приміщення. Встановлення, підтримка та демонтаж таких камер потребує значних зусиль (див. рис.1.7) [3] і ресурсів, що робить централізовані системи відеоспостереження недоцільними в умовах тимчасової оренди.



Рисунок 1.7 – Велика кількість деталей призводить до складності у підтримці та мобільності традиційних систем відеоспостереження

Централізовані системи більше підходять для підприємств, які володіють приміщеннями на довготривалу перспективу. Якщо компанія не планує змінювати місце розташування протягом багатьох років (10-15 років і більше), то вкладення у встановлення стаціонарної системи відеоспостереження може бути виправданим. У таких випадках система обростає інфраструктурою та служить довгий час, забезпечуючи належний рівень безпеки. Однак для компаній, які часто орендують приміщення і мають обмежений термін використання, централізовані системи відеоспостереження не є економічно вигідними. Постійне перенесення системи з одного місця в інше буде надто затратним і складним процесом. Тому, для

тимчасових проєктів та оренди приміщень, більш доцільно використовувати мобільні та гнучкі рішення для відеоспостереження, які не вимагатимуть значних витрат на демонтаж та перенесення.

Системи відеоспостереження зазвичай встановлюються на тривалий період часу, протягом якого вони мають ефективно виконувати свою основну функцію – відеофіксацію певної території або об'єкта. Важливо, щоб цей об'єкт не змінювався часто, оскільки часті переналаштування та переміщення системи можуть негативно вплинути на фінансову та економічну частину діяльності. Постійне налаштування та переустановка централізованих систем відеоспостереження є недоцільним рішенням, тому їх краще використовувати на довготривалій основі, коли об'єкт є постійним або мало змінюється. Якщо ж планується короткотривала оренда приміщення, після якої обладнання необхідно буде перенести в інше місце, централізовані системи відеоспостереження стають менш ефективними. В таких випадках доцільніше розглянути альтернативні, «мобільні» системи відеоспостереження, які легко демонтуються та встановлюються в нових локаціях без суттєвих фінансових втрат.

Вразливість до кібератак. Ще однією проблемою є вразливість систем відеоспостереження до кібератак. Навіть якщо ми говоримо про закриті системи, вони не є абсолютно захищеними – у разі, якщо стороння особа отримає прохід в систему, наприклад, через фізичне підключення до мережі, використовуючи флешку чи інші пристрої – можлива інфекція вірусом або втрата важливих даних. Якщо відеореєстратор, до якого підключена система відеоспостереження, постраждає від зловмисного програмного забезпечення, що може призвести до втрати відеозаписів за кілька годин чи навіть днів, тому важливо забезпечити безпеку об'єкта. У разі, якщо немає резервних копій даних на зовнішніх сховищах, відеозаписи можуть бути втрачені назавжди.

Традиційні централізовані системи відеоспостереження часто функціонують за принципом циклічного запису – старі записи видаляються, щоб звільнити місце для нових. У більшості випадків користувачі таких систем не зосереджують увагу

на необхідності регулярного резервного копіювання даних, що робить систему вразливою до атак або втрат даних через збої.

Зловмисники, отримавши доступ до таких систем, можуть легко маніпулювати даними, якщо система не має належного рівня захисту (див. рис.1.8) [4]. Хоча файли, які записує відеореєстратор, зазвичай зашифровані і не використовують стандартні формати, такі як MP4 або MKV, це не забезпечує повного захисту. Ці файли шифруються спеціальним програмним забезпеченням, розробленим для роботи з відеоспостереженням, однак при фізичному доступі до жорсткого диска або при недостатньому захисті мережі, зловмисники можуть обійти ці заходи і заволодіти відеоданими.



Рисунок 1.8 – Несанкціонований доступ через «людський» фактор

Висока ймовірність виходу системи із ладу. Крім кіберзагроз, централізовані системи відеоспостереження також мають значну ймовірність виходу з ладу через складність своєї архітектури. Вони складаються з численних компонентів, включаючи відеореєстратори, жорсткі диски, мережеве обладнання та камери, які підключаються за допомогою коаксіальних кабелів або пачкордів. Кожен з цих компонентів може з часом вийти з ладу, що негативно вплине на загальну працездатність системи. Наприклад, камери підключаються до відеореєстратора через кабелі, і якщо якийсь кабель пошкоджується або втрачається з'єднання, система не зможе отримувати сигнал від цієї камери – у таких випадках відеореєстратор повідомить про втрату сигналу, і в результаті ми отримаємо частково непрацюючу систему. Оскільки камера не має своєї автономної системи

зберігання даних і є просто «очима» системи, вона потребує постійного підключення до відеореєстратора для запису відео, що створює додаткові уразливості: будь-який збій у мережі або пошкодження кабелю може вивести з ладу окрему камеру або навіть всю систему (див. рис.1.9) [5].

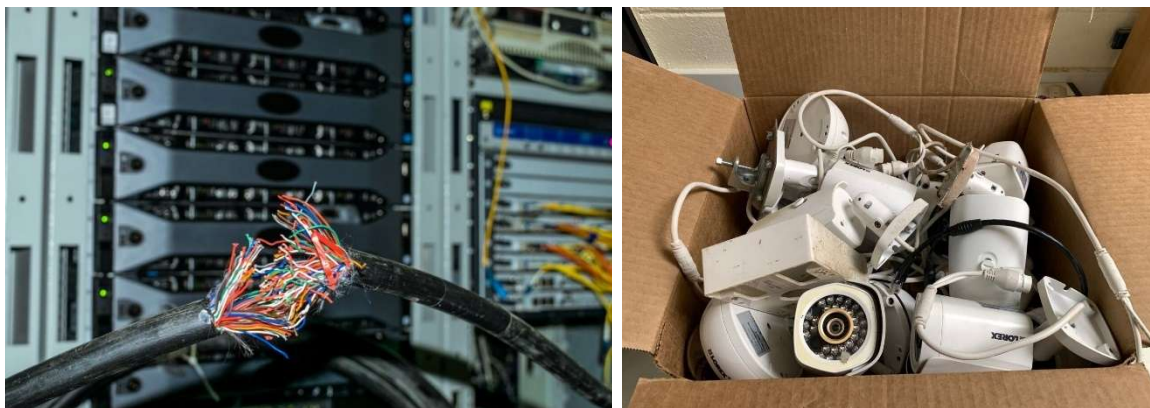


Рисунок 1.9 – Велика кількість деталей призводить до складності у підтримці та мобільності традиційних систем відеоспостереження

Також до цієї проблеми додається використання великої кількості кабелів, що розгортаються у системах відеоспостереження. Якщо один з кабелів пошкоджується або виходить з ладу, може бути складно знайти точку проблеми через велику кількість з'єднань. Іноді це можна вирішити шляхом перемикання на інший кабель, але це тимчасове рішення. Згодом пошкоджений кабель все одно потрібно замінити, що вимагає часу і додаткових витрат на обслуговування.

Такі проблеми з відмовами особливо актуальні для старіших систем відеоспостереження, які з часом стають менш надійними через знос обладнання та застарілість технологій та наштовхує до припливу кількості ремонтів та налаштувань, що ускладнює підтримку таких систем. Коли система «старіє», будь-яка проблема може призвести до серйозних збоїв, особливо якщо мережеві кабелі або камери виходять з ладу, а діагностика проблеми займає багато часу через велику кількість обладнання.

З огляду на стрімкий розвиток технологій, традиційні системи відеоспостереження поступово втрачають свою актуальність, оскільки новіші

рішення пропонують більшу гнучкість і надійність. Використання сучасних технологій, таких як Power over Ethernet (PoE), значно зменшує кількість кабелів і підвищує надійність систем, оскільки живлення і передача даних здійснюються через один кабель. Тому важливо не стояти на місці, а постійно впроваджувати новітні технології, щоб забезпечити максимальну ефективність і надійність систем відеоспостереження.

1.3 Тенденції розвитку інтелектуальних децентралізованих систем

Аналізуючи традиційну централізовану систему відеоспостереження та порівнюючи її з сучасними технологіями (див. рис.1.10), стає зрозуміло, що такі системи поступово втрачають свою актуальність. Така застаріла архітектура вимагала тривалого часу на обслуговування та постійного технічного нагляду для вирішення проблем, таких як втрата сигналу або погана якість зображення. Хоча така система могла забезпечувати досить якісну картинку, яка іноді навіть перевищувала можливості новіших рішень, її підтримка часто була невиправдано дорогою та складною – це призводило до необхідності наймати додатковий персонал, відповідальний за налаштування, обслуговування і моніторинг системи, що збільшувало витрати на її експлуатацію.



Рисунок 1.10 – Порівняння традиційної (лише як периферійний пристрій) та інтелектуальної камер (повністю автономна система) відеоспостереження

Мінімізація втручань з боку спеціалістів. Сьогодні, коли багато людей працюють віддалено, або навпаки, існує тенденція автоматизації багатьох процесів, технології значно змінили підходи до управління системами відеоспостереження. Посади, які раніше передбачали присутність операторів для контролю за системами, поступово скорочуються або трансформуються через впровадження інтелектуальних рішень. Наприклад, тепер можна використовувати відеоспостереження без необхідності залучення оператора на постійній основі – система може працювати автономно, з мінімальним втручанням людини [.

Спрощений інтерфейс та налаштування. Встановлення новітніх систем відеоспостереження дозволяє користувачам самостійно виконувати необхідні налаштування чи переміщення камер без потреби в залученні спеціалістів (див. рис.1.11), що значно скорочує витрати на підтримку системи та виключає необхідність оплати роботи додаткового персоналу. Технології стали більш доступними та зручними у використанні, що дозволяє уникнути зайвих витрат і витратити ресурси на впровадження більш сучасних рішень, таких як системи розумного міста (Smart City), які включають різноманітні датчики і сенсори для моніторингу та управління міською інфраструктурою [44].

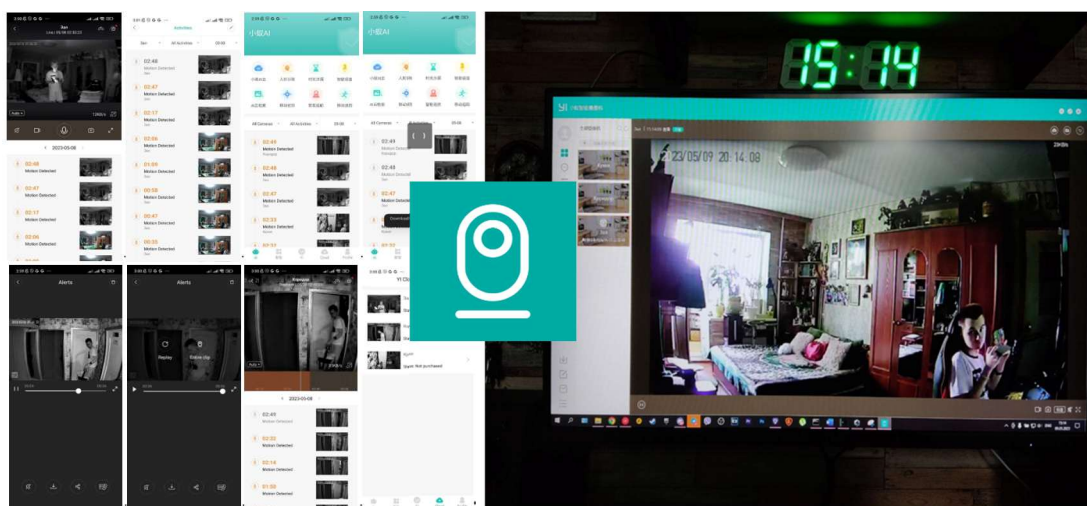


Рисунок 1.11 – Інтеграція спрощених інтерфейсів для керування інтелектуальними децентралізованими системами відеоспостереження на різних платформах

Покращення завдяки інтеграції новітніх технологій. Нова система відеоспостереження, яка може здатися спрощеною або «дитячою» на перший погляд, насправді забезпечує потужний функціонал (див. рис.1.12). Вона дозволяє використовувати передові технології для значно ширшого спектра завдань, не вимагаючи великих інвестицій на її підтримку, що надало можливість заощадити кошти, які можна спрямувати на інші, більш інноваційні проєкти, такі як впровадження IoT-технологій або модернізація інших елементів інфраструктури – все це призвело до того, що багато компаній почали замислюватися, чи дійсно варто використовувати великі, складні та громіздкі системи відеоспостереження. Хоча такі системи все ще актуальні в певних галузях, де є підвищені вимоги до безпеки даних, наприклад, у фінансових установах або компаніях, що працюють з конфіденційною інформацією, вони не завжди виправдані в інших ситуаціях. Деякі організації усвідомили, що для них достатньо простіших та ефективніших рішень.

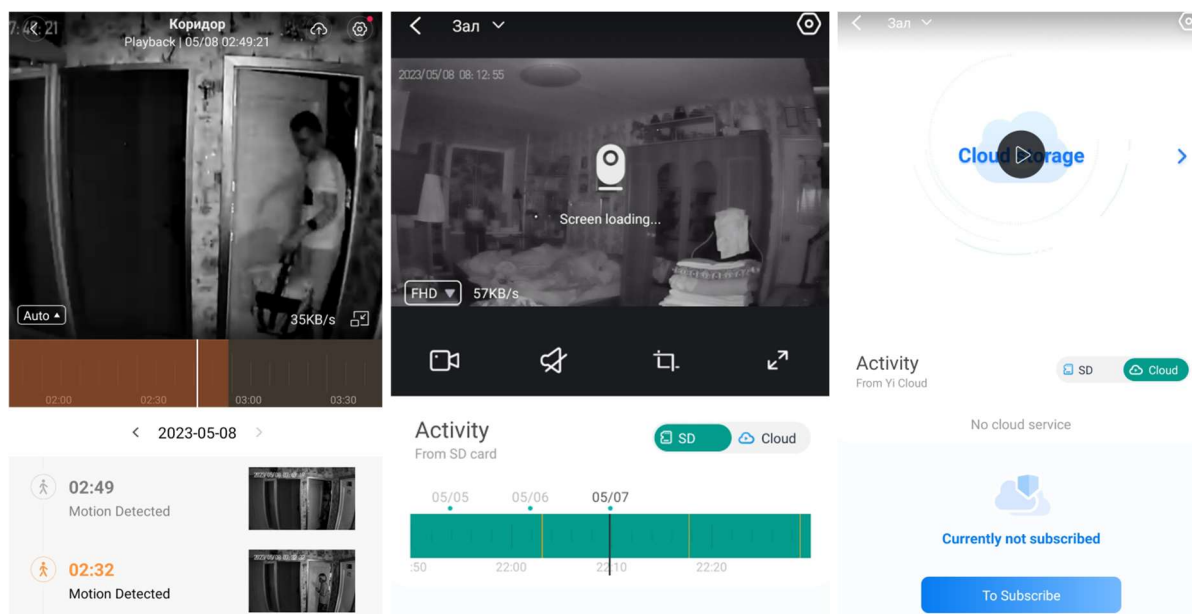


Рисунок 1.12 – Використання нових технологій у поїднанні зі зручним додатком (камери відеоспостереження Xiaomi YI Home 720 та додаток YI Home)

Справді, великі підприємства, такі як гіпермаркети або торгові центри, продовжують використовувати традиційні централізовані системи відеоспостереження через масштаб їхніх об'єктів. Проте для менших магазинів або

мережевих точок, таких як пекарні чи магазини техніки на кшталт «Дніпро-М», централізована система відеоспостереження вже є надмірною. Їм немає сенсу мати складну мережу камер і окремого персоналу для постійного моніторингу кожного невеликого магазину.

Мінімізація провідних комунікацій. З розвитком технологій ситуація змінилася. Наприклад, технологія Wi-Fi зазнала значних покращень – від початкової повільної передачі даних до сучасних стандартів, які дозволяють використовувати безпроводні рішення замість традиційних провідних, що суттєво знизило потребу в складних монтажах і мережних підключеннях, і водночас підвищило зручність у використанні (див. рис.1.13). Завдяки безперервному розвитку інженери все частіше враховують потреби споживачів, надаючи їм легкі у використанні системи відеоспостереження, які можуть працювати без постійної підтримки та не вимагати значних інвестицій в обслуговування.



Рисунок 1.13 – Повністю автономні системи відеоспостереження в межах одного пристрою (зліва направо: Xiaomi Yi Home 720p та Tuuya C18)

Інтеграція в межах одного пристрою. Сучасні системи відеоспостереження здатні працювати автономно, що дозволяє зменшити залежність від централізованих рішень і зробити їх більш мобільними, компактними і функціональними (див. рис.1.13). Вони можуть бути простими у використанні навіть для некваліфікованих користувачів, а їхнє налаштування займає мінімум

часу та зусиль. Такі системи можна впровадити практично будь-де, зберігаючи високу якість роботи, при цьому зменшуючи кількість технічних завдань, які раніше були необхідні для підтримки великих централізованих мереж.

Як підсумок, можна дійшли до точки, коли системи відеоспостереження можуть стати простими, мінімалістичними та легко керованими (див. рис.1.13), забезпечуючи всі необхідні функції без потреби в складному технічному обслуговуванні. У сучасних реаліях технологічного прогресу це робить їх ідеальним рішенням для багатьох компаній, дозволяючи їм оптимізувати витрати та спростити процеси.

«Ультимативний» функціонал. Сучасна система відеоспостереження може бути оснащена розширеними можливостями завдяки інтеграції з сервісами виробника та додатковими технологіями, такими як хмарні обчислення та машинне навчання. Ці інновації дозволяють не лише підвищити функціональність системи, але й суттєво знизити потребу в людському втручанні. Наприклад, використання інтегрованих датчиків дозволяє автоматизувати багато процесів, які раніше потребували участі оператора. Такі датчики можуть виконувати різні завдання, як-от визначення руху, ідентифікація того, хто або що саме рухається (чи це людина, тварина, чи просто пил), а також розпізнавання звуків, таких як плач дитини або інші специфічні шуми. Завдяки цьому система здатна працювати в режимі 24/7, забезпечуючи постійний нагляд за об'єктом без потреби в окремій людині, яка б контролювала всі процеси (див. рис.1.12).

Окрім цього, всі дані, які збираються системою відеоспостереження, можуть автоматично надсилатися на ваш смартфон, який завжди знаходиться поруч. Такий підхід робить систему неймовірно зручною та мобільною. Більшість користувачів смартфонів проводять на своїх пристроях від години до кількох годин щодня, що дає змогу без проблем інтегрувати функціонал відеоспостереження в їх повсякденне життя.

Централізоване керування децентралізованими системами. Додавання мобільного додатку, який керуватиме системою відеоспостереження, дозволяє створити справді інтелектуальну систему, здатну працювати автономно та

надавати вичерпну інформацію в будь-який момент (див. рис.1.12). Така система фактично є інтелектуальною децентралізованою платформою, що дозволяє контролювати і керувати відеоспостереженням дистанційно, без залучення сторонніх фахівців, що забезпечить максимальну зручність і ефективність, оптимізуючи як роботу самої системи, так і витрати на її обслуговування.

Системи відеоспостереження, що працюють на основі інтелектуальних технологій, вже не перший рік використовуються в усьому світі. Однак вони здебільшого призначені для некомерційних цілей, таких як нагляд за домашніми улюбленцями або дітьми у дитячих кімнатах. Ці системи дозволяють в реальному часі контролювати, що відбувається в приміщенні, включаючи спостереження за рухами та звуками. Наприклад, власники можуть отримувати push-сповіщення на свої смартфони, якщо дитина заплакала або якщо зафіксовано будь-які незвичні рухи. Користувачі отримують доступ до відеоданих, що відбуваються в цей момент часу або ж можуть повертатися назад, аби проаналізувати події за допомогою спеціального інтерфейсу, що показує детекцію рухів, звуків чи інших активностей. Система може зафіксувати моменти, коли пройшла людина чи з'явилася тварина.

Щоб забезпечити надійність, в разі несправності камери, вся інформація може зберігатися у хмарі виробника, що дозволяє користувачам отримувати доступ до записів через мобільний додаток, навіть якщо з камерою сталося щось непередбачуване. Однак слід зазначити, що це забезпечує лише частковий спокій. Проблеми можуть виникнути в ситуаціях, коли камеру можуть пошкодити або вкрасти. При цьому важливо усвідомлювати, що камера відеоспостереження є лише кінцевим пристроєм в системі, аналогічно до мишки чи клавіатури в ПК. Якщо пошкодити камеру, вона просто перестане записувати, але всі зібрані дані повинні зберігатися на відеореєстраторі або в хмарі.

Важливим нюансом інтелектуальних децентралізованих систем відеоспостереження є те, що вони зазвичай функціонують на основі однієї компактної камери. Така камера може бути розташована в будь-якому зручному місці, забезпечуючи при цьому простоту використання та доступність, що

відкриває нові можливості для моніторингу, оскільки немає потреби в складних системах з безліччю камер. Усе управління відбувається через одну інтегровану камеру, що підвищує зручність і ефективність відеоспостереження в різних умовах.

«Мінімалістичність» у сторону компактності та зручності. Повертаючись до концепції системи відеоспостереження, варто зазначити, що вона може базуватися на єдиній камері, що є досить зручним рішенням, що звільняє користувача від необхідності турбуватися про деталі (див. рис.1.13). Все, що потрібно зробити – це забезпечити належну мережеву інфраструктуру для підключення, щоб мати можливість отримувати доступ до системи відеоспостереження з будь-якої точки світу, за умови стабільного інтернет-з'єднання. У деяких випадках можливе створення безпроводної локальної мережі без підключення до інтернету через провайдера, що дозволяє здійснювати спостереження в рамках закритої мережі.

Такий підхід особливо корисний не тільки для великих компаній, а й для приватних підприємців, які орендують великі приміщення або мають кілька роздрібних магазинів, наприклад, пекарні чи магазини електроніки та інструментів. Вони не потребують традиційних та громіздких систем відеоспостереження, адже можуть використовувати компактні камери з усіма необхідними функціями. Ці камери, незважаючи на свою просту зовнішність, оснащені всіма необхідними технологіями, що дозволяє масштабувати систему, розміщуючи їх у численних точках продажу.

Зменшення фінансових втрат за рахунок скорочення робочих місць. Однією з переваг такого підходу є можливість централізованого управління з однієї локації, що дозволяє найняти лише одну людину для обробки та моніторингу даних, зібраних з усіх камер. Така особа може займатися аналітикою, що зібралася за допомогою додаткового програмного забезпечення, замість того, щоб наймати окремих працівників для кожного магазину, що особливо вигідно, оскільки навіть при втраті або несправності камери, дані все ще можуть зберігатися в хмарі.

Інтеграція нових практик щодо відеоспостереження. Багато камер обладнані датчиками руху та інфрачервоними датчиками, що підвищує їхню

ефективність. Більшість сучасних камер також використовують технології машинного навчання, що дозволяє їм розпізнавати певні об'єкти, звуки (наприклад, плач дитини) та відрізняти людей від тварин (див. рис.1.12) – все це робить систему відеоспостереження дуже зручною, зручною та інтелектуальною, забезпечуючи при цьому децентралізований підхід до моніторингу.

1.4 Переваги та виклики використання інтелектуальних децентралізованих систем відеоспостереження

Переваги використання інтелектуальних децентралізованих систем відеоспостереження є досить суттєвими, серед яких варто виділити кілька ключових аспектів:

- використання машинного навчання;
- використання хмарних обчислень;
- компактні розміри в межах одного пристрою;
- висока енергоефективність;
- використання безпроводних технологій;
- використання альтернативних джерел живлення.

Використання машинного навчання. Таке рішення дозволяє програмному забезпеченню камер не лише фіксувати відео, а й розпізнавати специфічні об'єкти та події. Наприклад, система може відрізнити, чи проходить повз людина, чи це тварина, або ж виявити плач дитини по аудіо-детекції, що стає можливим завдяки створенню моделей машинного навчання, які навчаються на великій кількості даних і покращують свою здатність до ідентифікації об'єктів. Виробники вбудовують у камери спеціальні програми та алгоритми, які реалізують машинне навчання, щоб пристрої могли визначати, що саме перед ними. Чи це людина, чи, наприклад, пил, або навіть рух листка – система навчена не реагувати на незначні

зміни, зосереджуючи увагу на важливих подіях. Камери самостійно відбирають ключові фрагменти відео для подальшого зберігання, що робить їх функціонування ефективнішим. Цей підхід також дозволяє системам аналізувати зібрані дані за тривалий період – від днів до місяців. Камери не лише фіксують відео, а й здатні сповіщати користувачів про виявлені рухи, що особливо важливо уночі або в умовах, коли є ризик несанкціонованого доступу до об'єкта, що суттєво зменшує потребу у постійному моніторингу камер.

Машинне навчання у таких системах значно підвищує ефективність відеофіксації та оптимізує витрати на зберігання даних. Наприклад, камери можуть працювати не в режимі цілодобового запису, а активуватися лише при виявленні руху, що дозволяє економити місце на носії інформації. Багато сучасних камер мають можливість запису на карту Micro SD. Для карти пам'яті об'ємом 128 ГБ при якості запису Full HD можна зберігати дані більше ніж два тижні. Однак, за рахунок функції активації запису лише при виявленні руху, цей термін можна значно подовжити – до двох-трьох місяців, залежно від частоти фіксацій, що робить такі системи відеоспостереження більш гнучкими та економічними, а також зручними у використанні для різних типів об'єктів.

Використання хмарних обчислень. Ще однією значною перевагою інтелектуальних децентралізованих систем відеоспостереження є можливість використання хмарних обчислень – це, зокрема, означає, що багато процесів, які раніше виконувалися локально на камері або відеореєстратору, тепер реалізуються безпосередньо в хмарі. Хмарні сервіси (див. рис.1.12), що надаються виробниками, дозволяють зберігати записи відеофіксації без необхідності постійного зберігання всього відео, що займає великий обсяг пам'яті. Завдяки хмарним рішенням, система відеоспостереження може фіксувати лише ті фрагменти, де зафіксовано рух, а не безперервно зберігати весь запис, що суттєво знижує обсяги даних, які потрібно зберігати, що, в свою чергу, зменшує витрати на зберігання як для виробника, так і для користувача.

Багато виробників надають доступ до хмарних сервісів за підпискою, яка може бути безкоштовною або платною, залежно від рівня сервісу. Хмарні

обчислення – це не лише просте зберігання даних на серверах, а й виконання численних процесів обробки та передачі даних, які раніше здійснювалися локально. Таке рішення дозволяє камерам споживати менше енергії (див. рис.1.12): сучасні пристрої зазвичай споживають до одного ватта потужності, що зменшує витрати на електроенергію. У разі відключення електроенергії доступ до хмарного сховища залишається можливим, за умови, що сервери постачальника послуг функціонують, що дозволить користувачам у будь-який момент отримати доступ до відеозаписів, зокрема, у ситуаціях, коли виникає необхідність перевірити певні події. Однак, якщо постачальник послуг не забезпечує стабільний доступ до своїх хмарних рішень, це може свідчити про недоліки у їхній системі – у такому разі користувачам варто шукати альтернативні рішення, які, можливо, будуть дорожчими, але зможуть надати більшу надійність.

Компактні розміри в межах одного пристрою. Серед численних переваг інтелектуальних децентралізованих систем відеоспостереження важливу роль відіграють їх компактні розміри, що сприяє зручності установки (див. рис.1.12). Такі камери часто використовуються в приватних будинках, квартирах, а також у магазинах і підприємствах, які не бажають витратити час і ресурси на складні централізовані системи відеоспостереження, що потребують спеціального технічного обслуговування та постійного контролю.

Завдяки своїй простоті установки і зручності використання, ці системи є привабливими для багатьох користувачів. Процес встановлення таких камер не займає багато часу, і немає необхідності залучати спеціалістів для їх налаштування, що наштовхує на те, що навіть людина, яка не має глибоких технічних знань, може впровадити систему відеоспостереження. Все, що потрібно, це розмістити камеру у відповідному місці і підключити її до необхідної інфраструктури.

Камери можуть бути підключені до локальної мережі, використовуючи Ethernet-кабелі або патч-корд для з'єднання з маршрутизатором або комутатором, або ж вони можуть працювати через безпроводне з'єднання Wi-Fi (див. рис.1.12), яке надасть додаткову гнучкість при виборі місця для установки, адже користувач може легко переміщати камери без значних труднощів. Як приклад, можна просто

відключити камеру від одного маршрутизатора та підключити до іншого, якщо SSID та пароль встановити як у попередньому, що робить цю систему дуже зручною у використанні та налаштуванні.

Висока енергоефективність. Камери відеоспостереження, які входять до складу інтелектуальних децентралізованих систем, характеризуються надзвичайно низьким споживанням електроенергії (див. рис.1.14), що робить їх ідеальними для підключення до джерел безперебійного живлення (ДБЖ), включаючи ті, що живляться від альтернативних джерел енергії, таких як сонячні панелі чи вітрові генератори. У ситуаціях, коли постачання електроенергії стає ненадійним, ці альтернативні джерела можуть забезпечити безперервну роботу системи.

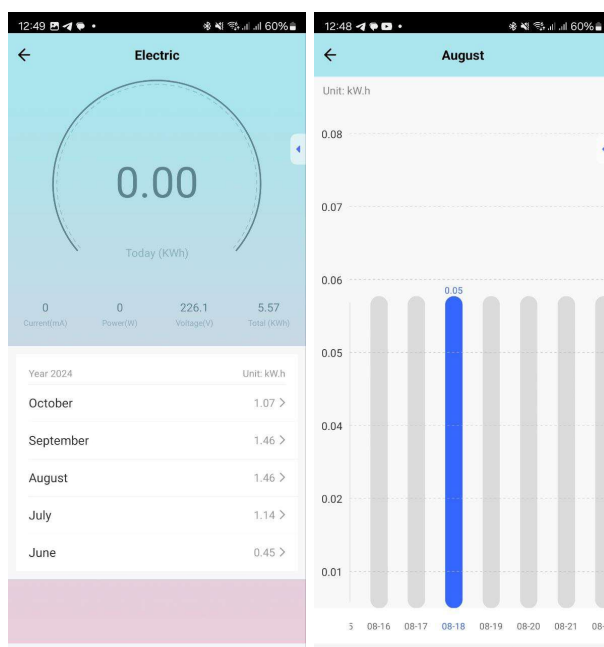


Рисунок 1.14 – Рівень споживання електроенергії однієї інтелектуальної камери відеоспостереження (за допомогою додатка Smart Life та розумної розетки)

Використання безпроводних технологій. Надана можливість підключення до маршрутизатора або модему, який, в свою чергу, може бути з'єднаний з зовнішньою антеною, або взагалі – інтеграція USIM карти (SIM-карта для модемів та маршрутизаторів) робить системи відеоспостереження ще більш функціональними, особливо у віддалених сільських районах.

Використання альтренативних джерел живлення. Використовуючи альтернативні джерела живлення, такі камери можуть функціонувати автономно – сонячні панелі можуть бути інтегровані в систему, забезпечуючи енергію, яка зберігатиметься у спеціальних збірках зі акумуляторів для подальшого живлення (див. рис.1.15). Вже доступні моделі камер з вбудованими сонячними панелями, що дозволяє їм безпосередньо заряджатися від сонячної енергії.

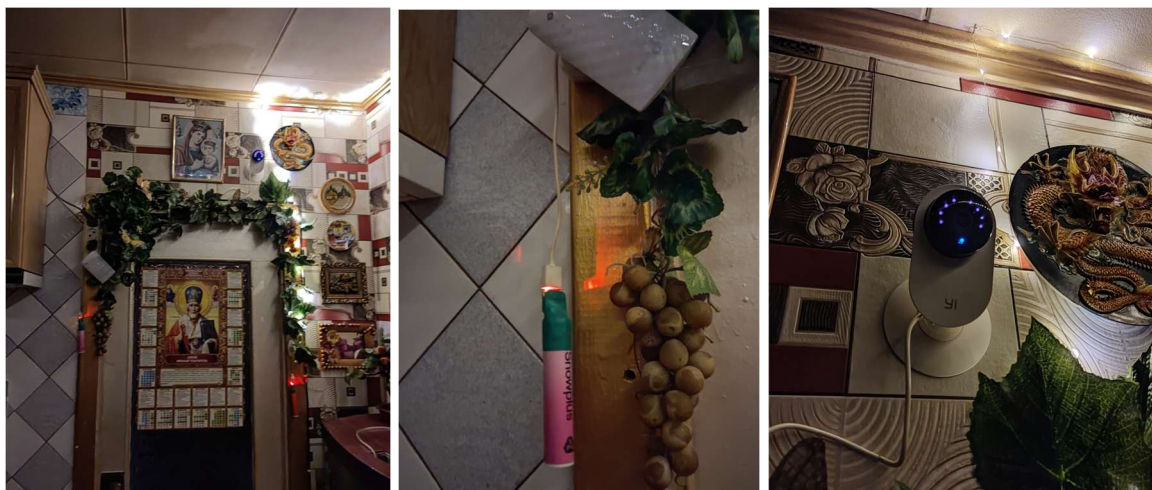


Рисунок 1.15 – Використання альтренативних джерел для працездатності інтелектуальних систем відеоспостереження (на основі вторинної сировини)

До недоліків інтелектуальних децентралізованих систем відеоспостереження можна віднести наступні ключові аспекти:

- вразливість до кібератак;
- фізичне пошкодження;
- використання флеш-пам'яті як головного носія;
- використання моделі децентралізації (для конфіденційності та приватності);
- потреба у забезпеченні додаткових механізмів безпеки.

Вразливість до кібератак. Оскільки такі системи використовують сервіси сторонніх постачальників, існує ризик несанкціонованого доступу через слабкі місця захищеного каналу передачі даних або зламу облікового запису користувача,

який контролює ці камери, що призводить до витоку даних, а й навіть унеможлиблює контроль над самою системою відеоспостереження (див. рис.1.8).

Фізичне пошкодження. Ще одним вагомим недоліком є можливість втрати відеоданих у разі фізичного пошкодження або крадіжки камери (див. рис.1.13) – якщо власник не використовує хмарне сховище для зберігання відео, дані, записані на камері, можуть бути безповоротно втрачені. У традиційних системах відеоспостереження зазвичай є центральний відеореєстратор, що зберігає записи з усіх камер, тому навіть при виході з ладу однієї камери, інші продовжують функціонувати, і дані зберігаються на централізованому пристрої. Попри це, перевагою сучасних децентралізованих камер є їх відносно низька вартість. Навіть у разі втрати однієї з камер через злом або крадіжку, заміна не вимагає вагомих економічних витрат. Якщо ж при цьому використовується хмарне сховище, яке надає виробник системи, власник може без труднощів переглянути події, зафіксовані до моменту інциденту, що значно підвищує безпеку та ефективність таких систем.

Використання флеш-пам'яті як головного носія. Одним із недоліків відеокамер спостереження, якщо не використовувати хмарні сервіси, є те, що вони зазвичай зберігають дані на флеш-картах пам'яті, які мають значно менший ресурс, ніж жорсткі диски (див. рис.1.16). Якщо придбати карту пам'яті, призначену для смартфонів або інших пристроїв, які не мають постійного навантаження на збереження даних, вона може швидко вийти з ладу при використанні в камерах, які постійно перезаписують відео у циклічному режимі. Флеш-пам'ять швидко зношується при частому перезаписуванні, особливо якщо відео записується безперервно 24/7, то така карта пам'яті може вийти з ладу менш ніж за рік. Щоб уникнути цього, користувачі часто налаштовують камери на запис лише за подіями або в певні проміжки часу, що дозволяє знизити навантаження на карту пам'яті та продовжити її термін служби.

Хоча USB-накопичувачі й побудовані на схожій технології (їх краще, їх також не можна використовувати так само надійно, як жорсткі диски, через їхній обмежений ресурс. На цей аргумент існує контраргумент – коли ми говоримо про

карти пам'яті, спеціально створені для постійного перезапису даних, наприклад, у відеореєстраторах автомобілів чи системах відеоспостереження, де використовуються локальні носії для зберігання інформації, ці карти мають підвищену вартість.



Рисунок 1.16 – Накопичувачі даних зі збільшеним ресурсом запису/перезапису (зліва направо: microSDXC Western Digital Purple SC QD101 256GB, HDD Western Digital Purple 4TB та SSD Western Digital Red SA500 1TB)

Однак це виправдано, оскільки вони володіють значно більшим ресурсом циклів запису, що дозволяє їм довше служити в умовах постійного перезапису, що стосується і традиційних систем відеоспостереження, особливо в більш дорогих комплектах, де замість звичайних жорстких дисків для ПК чи ноутбуків (форм-фактор 3,5 або 2,5 дюйма) використовуються спеціальні жорсткі диски. Такі диски розроблені для обробки великих обсягів даних і безперервного циклу запису й перезапису інформації та мають збільшений ресурс саме для потреб відеоспостереження (див. рис.1.16).

Серед відомих виробників подібних рішень можна виділити:

- Western Digital (HDD та SSD);
- Seagate (HDD та SSD);
- Samsung (HDD раніше, тепер лише SSD);
- Kingston (лише SSD);
- Cricial (Micron) (лише SSD).

Твердотільні накопичувачі (SSD) також можуть використовуватися в цих системах, але для потреб постійного запису й перезапису даних часто зручніше використовувати жорсткі диски (HDD), з огляду на їхню більшу економічність і пристосованість для таких завдань (див. рис.1.16).

Використання моделі децентралізації. Ще одним недоліком систем відеоспостереження, що використовують модель децентралізації (див. рис.1.11), є проблема управління доступом. Такі системи дозволяють керувати камерами з одного місця, але також надають можливість отримувати до них доступ з будь-якої точки, що створює потенційні ризики для безпеки. Одним із цих ризиків є те, що стороння особа може отримати доступ до вашого облікового запису, навіть без вашого відома. Наприклад, якщо хтось має доступ до вашого акаунта або якщо свідомо чи випадково поділилися даними для входу з іншими, це може дозволити сторонній особі контролювати камери спостереження.

Особливо важливою є проблема, що доступ до камер за допомогою одного акаунта дозволяє не лише переглядати записане (див. рис.1.11), але й здійснювати дії, які можуть загрожувати безпеці системи. Така особа може стерти всі дані, що зберігаються на карті пам'яті, або відключити функцію запису, про що не дізнаєтесь, поки не виявите проблему, а в гіршому випадку будете вважати, що камери продовжують записувати все належним чином, тоді як хтось уже змінив налаштування на свою користь. Такі моменти відкривають можливості для злочинних дій, оскільки зловмисник може діяти непомітно для нас.

Щоб запобігти таким ризикам, рекомендується регулярно змінювати паролі на обліковому записі, особливо якщо доступ до камер надається іншим людям, наприклад, для налаштування або технічної підтримки. Якщо цього не робити, ризикуєте тим, що камери відеоспостереження використовуватимуть не лише ви, але й сторонні особи, які можуть мати доступ до записів або навіть змінювати налаштування.

Потреба у забезпеченні додаткових механізмів безпеки. Також важливо використовувати складні та надійні паролі для забезпечення конфіденційності й захисту вашої системи від небажаного втручання (див. рис.1.8). Наприклад, якщо

використовуєте систему відеоспостереження вдома і постійно ведете відеонагляд, варто пам'ятати, що будь-який несанкціонований доступ до камер є порушенням вашої приватності, що є не лише етичною проблемою, але може кримінально каратися за законів.

Для того, щоб мінімізувати ризики, необхідно регулярно змінювати паролі на своїх облікових записах і камерах – це краще розглядати не стільки як недолік систем відеоспостереження, скільки як вимушену міру безпеки, бо будь-що, що має вихід в інтернет, стає потенційною мішенню для хакерських атак.

Якщо хтось «зламає» обліковий запис, до якого підключені камери, або навіть ваш маршрутизатор, зловмисник може отримати доступ до відеопотоку, якщо не було захищено належним чином налаштування свого маршрутизатора, наприклад, неправильно перенаправили порти чи не встановили надійний пароль, зловмисник може отримати доступ до камер через відкриту IP-адресу, просканувавши перед цим відкриті порти та дізнатись, що використовується у мережі система відеоспостереження. Для цього зловмиснику навіть не потрібен ваш обліковий запис, оскільки доступ до маршрутизатора може відкрити можливість переглядати відео з камер. Хоча у нього можуть бути певні обмеження щодо доступу до інших функцій, але він все ж зможе отримати зображення з камер, що є серйозною загрозою для конфіденційності.

Для запобігання таким ситуаціям важливо регулярно змінювати паролі та ретельно налаштовувати захист не тільки камер, але й маршрутизатора. Якщо планується керувати відеоспостереженням ззовні, тобто через інтернет, варто звернути увагу на правильну переадресацію портів та забезпечити безпеку мережових з'єднань. Якщо ж вам необхідний тільки локальний доступ до камер, доцільніше не підключати їх до загальної мережі Wi-Fi або використовувати окремий маршрутизатор, що не підключений до інтернету, що дозволить забезпечити більший захист від зовнішніх загроз і уникнути ризиків, пов'язаних з потенційними зламами. Тож при виборі камер відеоспостереження варто враховувати не лише функціональні можливості, але й питання безпеки, особливо якщо планується підключення до інтернету.

РОЗДІЛ 2 ХМАРНІ ОБЧИСЛЕННЯ ТА FOG COMPUTING У ВІДЕОСПОСТЕРЕЖЕННІ

2.1 Архітектура хмарних обчислень у відеоспостереженні

Архітектура хмарних обчислень у системах відеоспостереження має велику гнучкість і різноманітність, оскільки ці системи не обмежуються лише функціями самих камер відеоспостереження – інтелектуальні децентралізовані системи відеоспостереження можуть виконувати кілька ролей. Наприклад, камери можуть функціонувати як кінцеві пристрої, що лише захоплюють зображення та передають його для подальшої обробки, або ж вони здатні виконувати обробку частини даних безпосередньо на пристрої, зберігати деяку інформацію на внутрішніх носіях, як-от карти пам'яті, і контролювати певні процеси.

Навіть найбільш автономні камери відеоспостереження потребують розвиненої інфраструктури для опрацювання відеоданих. Коли виникають перебої в електроживленні або інтернет-з'єднанні, частина функцій таких камер може стати недоступною або неефективною. Тому за функціонуванням кожної такої інтелектуальної камери стоїть складна система, яка забезпечує її інтеграцію в загальну мережу, хоча камери можуть виконувати певні завдання самостійно, обробка та управління більшістю процесів відбуваються за допомогою хмарних обчислень.

Більшість сучасних камер відеоспостереження, особливо тих, що є відносно недорогими, базуються на використанні хмарної архітектури. Вони зазвичай інтегруються з мобільними додатками, що дозволяють користувачам дистанційно контролювати та керувати камерами. Крім мобільних додатків, існують також веб-інтерфейси та програмне забезпечення для ПК, що надають додаткові можливості для керування системами. Проте слід розуміти, що ці додатки не є повністю автономними – за ними стоїть потужна архітектура хмарних обчислень, яка

обробляє дані та забезпечує роботу системи на стороні виробника, що особливо важливо для рішень, які ми купуємо «під ключ» і використовуємо у своїх системах відеоспостереження (див. рис.2.1) [6].

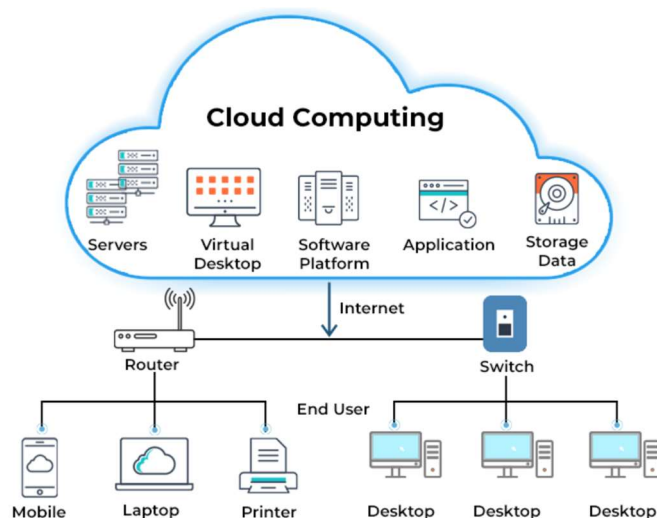


Рисунок 2.1 – Архітектура хмарних обчислень

Архітектура хмарних обчислень у відеоспостереженні включає комплекс ключових компонентів, які забезпечують роботу таких систем:

- серверна інфраструктура;
- мережева інфраструктура;
- мережеві протоколи;
- зберігання та обробка даних;
- віддалений доступ.

Серверна інфраструктура. Одним із прикладів таких серверних інфраструктур є платформи гігантів, таких як Amazon, Microsoft і Google (див. рис.2.2). Amazon надає свої серверні потужності через платформу Amazon Web Services (AWS), Microsoft використовує платформу Azure, а Google – Google Cloud відповідно. Ці хмарні платформи забезпечують не лише зберігання великих обсягів відеоданих, але й їхню обробку, що дозволяє швидко реагувати на події, записувати відео та виконувати аналітичні функції [7].



Рисунок 2.2 – Технологічні гіганти у сфері хмарних обчислень
(Amazon – AWS, Google – Google Cloud, Microsoft – Azure)

Більшість готових рішень камер відеоспостереження, доступних на ринку за порівняно низькою ціною, часто використовують інфраструктуру самого виробника або опираються на серверні ресурси таких компаній, як Amazon, Microsoft або Google (див. рис.2.2) [7]. Проте кінцевий користувач може не знати, на якій саме платформі побудована ця інфраструктура, оскільки він взаємодіє безпосередньо з хмарою, яку надає виробник камер відеоспостереження.

За таку послугу користувач зазвичай платить підписку або інші платежі безпосередньо виробнику камер, а не самій Amazon, Microsoft або Google. Якщо користувач вирішить не сплачувати за додаткові послуги чи підписку, доступний функціонал камер буде обмеженим. Наприклад, камери можуть лише записувати відео на локальні носії даних, або мати доступ до базових функцій хмари виробника, де відеодані можуть передаватися в зашифрованому вигляді. Навіть у разі невикористання підписки виробник все одно може збирати певні дані для підтримки функціонування камер.

Мережева інфраструктура. Для повної роботи цих камер зазвичай потрібне стабільне підключення до інтернету, що дозволяє використовувати всі можливості хмарної інфраструктури (див. рис.2.1) [6]. Однак є варіант локального використання таких камер, при якому їх можна підключити до локальної мережі, не використовуючи інтернет, що дозволить камерам працювати з обмеженим функціоналом, але без необхідності постійного підключення до хмарних сервісів.

Мережеві протоколи. У будь-якій архітектурі хмарних обчислень для систем відеоспостереження присутні важливі компоненти, які часто залишаються непомітними для кінцевого користувача, особливо якщо він взаємодіє лише через мобільний додаток, веб-інтерфейс або програму на ПК (див. рис.2.1) [6]. Навіть найпростіші системи відеоспостереження використовують мережеві протоколи для передачі даних, що може відбуватися як локально в межах однієї мережі, так і до хмарного сховища виробника.

Одним із найбільш поширених протоколів для передачі відеоданих – це пряме потокове передавання RTSP (Real-Time Streaming Protocol) , який часто застосовується для локальної передачі даних (див. рис.2.3) [8]. За допомогою цього протоколу відеопотік передається в межах локальної мережі, і тільки користувачі цієї мережі можуть отримувати доступ до відео. Для використання цього протоколу необхідно налаштувати відповідні порти на маршрутизаторі, наприклад, стандартний порт 554, який забезпечує передачу даних за протоколом RTSP. Якщо у нас є статична IP-адреса (біла IP-адреса), налаштування перекидування портів дозволяє переглядати відео з камер відеоспостереження навіть ззовні, через інтернет.

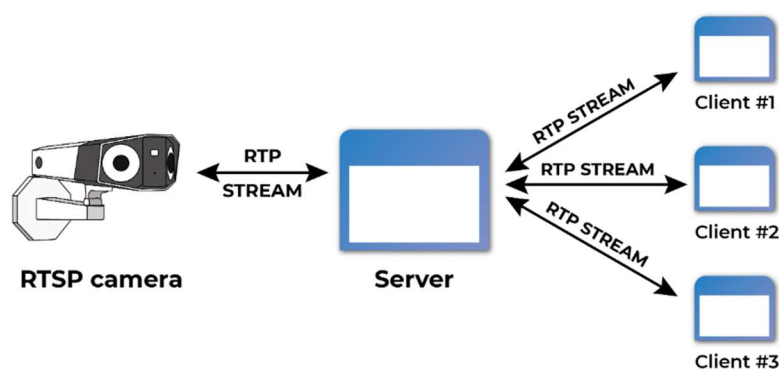


Рисунок 2.3 – Передача даних через RTSP протокол до кінцевих пристроїв

Якщо ж йдеться про використання хмарної інфраструктури для зберігання та передачі відео, то тут використовуються інші протоколи, зокрема HTTP або HTTPS, які забезпечують безпечну передачу відео до хмари (використовує ті ж самі

методи, що RTSP, тільки краще) (див. рис.2.3) [9]. Це стосується тих випадків, коли користувач взаємодіє із системою відеоспостереження через мобільний додаток або веб-інтерфейс, не налаштовуючи самостійно RTSP. Дані передаються на сервери виробника, і вже звідти користувач може отримати доступ до відео. Часто такі хмарні рішення базуються на інфраструктурі потужних серверів, таких як Amazon, Microsoft чи Google (див. рис.2.2) [7], що дозволяє отримати надійний і стабільний сервіс, але вимагає додаткових витрат.

Для більшості користувачів, які купують прості системи відеоспостереження, використання потужних серверів від відомих компаній може виявитися надмірно дорогим. У таких випадках доцільно використовувати спрощену хмарну інфраструктуру, яку надає сам виробник камер. Хоча такі рішення можуть бути обмеженими за функціоналом, вони часто задовольняють потреби тих користувачів, які не хочуть занурюватися у технічні деталі, але потребують стабільної та надійної роботи системи без додаткових налаштувань або великих витрат на підтримку власної інфраструктури.

Зберігання та обробка даних. Для кінцевого користувача цей процес залишається абсолютно непомітним, адже взаємодія відбувається через спеціальний додаток виробника камер відеоспостереження. Користувач не «бачить», як саме дані зберігаються та обробляються у хмарі. Якщо порівнювати з традиційними локальними системами відеоспостереження, де відео зберігається безпосередньо на відеореєстраторі або жорсткому диску, то у випадку інтелектуальних децентралізованих камер часто використовується локальне сховище у вигляді карти пам'яті.

Коли йдеться про хмарні обчислення, застосовуються зовсім інші методи зберігання та обробки даних (див. рис.2.1) [6]. Для роботи з великими обсягами відео можуть використовуватися технології на основі NoSQL баз даних, такі як MongoDB або Cassandra (див. рис.2.4). Ці рішення дозволяють ефективно обробляти великі масиви даних і забезпечують швидкий доступ до відеоінформації, що є критично важливим для систем відеоспостереження [10].



Рисунок 2.4 – Базы даних Cassandra та MongoDB

Віддалений доступ. На відміну від традиційних локальних систем відеоспостереження, де все зосереджено в одному фізичному місці і неможливо здійснювати доступ поза мережею, хмарна інфраструктура надає можливість керувати системою звідки завгодно.

За допомогою хмарної архітектури (див. рис.2.2) [7], яка включає серверні потужності та мережеві протоколи (див. рис.2.3) [8, 9], дані з камер відеоспостереження можуть передаватися, зберігатися та оброблятися у хмарі. Їм ж, в свою чергу, надається доступ до відеоданих та управляти системою за допомогою веб-додатків, мобільних клієнтів або спеціальних програм, тобто дозволить здійснювати віддалений моніторинг і управління відеоспостереженням у реальному часі, незалежно від фізичного розташування камер. Таке рішення є надзвичайно зручним і гнучким, адже забезпечує надійний контроль і доступ до системи в будь-який момент, що значно підвищує ефективність управління відеоданими в сучасних умовах.

Використання сторонніх хмарних сервісів. Якщо ж говорити про віддалений доступ до відеоспостереження, особливо у контексті використання потужних серверних рішень від таких компаній, як Amazon, Microsoft чи Google (див. рис.2.2), і варто зазначити, що такі платформи забезпечують високий рівень захисту та масштабованості [7]. Наприклад, якщо у нас є достатньо ресурсів і прагнемо побудувати власну інфраструктуру для відеоспостереження, можна скористатися рішеннями від Amazon, такими як платформа Amazon Kinesis Video Streams – це

спеціалізоване API, яке надає керування, стеження та обробку відеоданих через хмарні сервери Amazon (див. рис.2.5) [11].

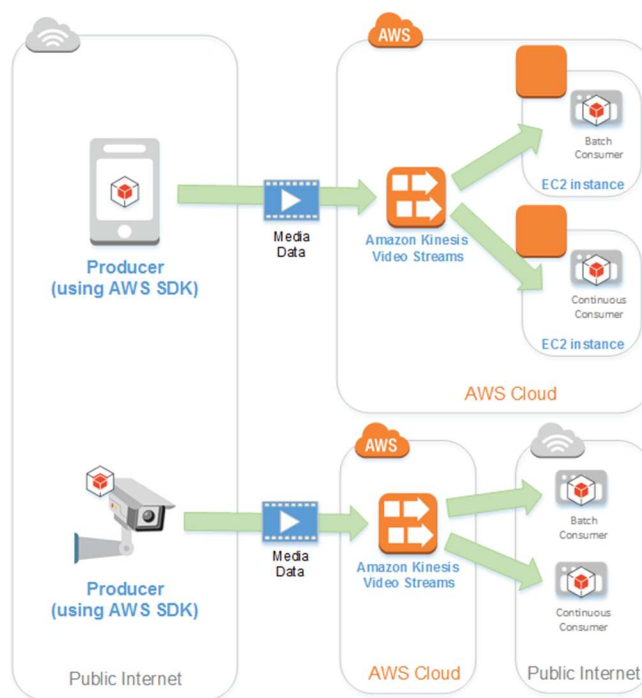


Рисунок 2.5 – Сервіс Amazon Kinesis Video Streams
(для захоплення великих обсягів відеоданих)

Amazon Kinesis Video Streams (див. рис.2.5) є потужним інструментом для захоплення, обробки та зберігання великих обсягів медіапотоків, що дозволяє не лише організувати надійний віддалений доступ до відео, але й забезпечує високий рівень захисту даних. Дане рішення особливо корисне, якщо не маєте великого досвіду в налаштуванні відеоспостереження або не довіряєте стандартним рішенням виробників дешевших систем. Використання серверів Amazon дає впевненість у надійному збереженні і захисті ваших даних (див. рис.2.5) [11], оскільки компанія пропонує ультимативні заходи безпеки, що особливо важливо для організацій, які потребують високого рівня конфіденційності та контролю за відеопотоками.

Amazon Kinesis Video Streams відкриває можливості для аналітики та інтеграції з системами машинного навчання (див. рис.2.5) [11]. Наприклад, можна використовувати ці можливості для розширення функціональності своєї системи

відеоспостереження – додати детекцію рухів, розпізнавання облич, виявлення людей або тварин, а також інші спеціалізовані алгоритми на основі машинного навчання, такі як визначення плачу дитини. Якщо не бажаєте розробляти власне рішення для цих завдань – Amazon Kinesis Video Streams стане ефективним варіантом, хоча й не найдешевшим.

Такі рішення, як Amazon Kinesis Video Streams (див. рис.2.5), є ідеальними для великих урбанізованих проєктів, зокрема для впровадження розумних дорожніх камер у масштабах міста. У столиці, де встановлюється велика кількість камер і є постійний рух людей, транспортних засобів, а також необхідність розпізнавання облич та аналізу подій, традиційні рішення можуть бути недостатніми.

Використання хмарних сервісів від виробника. Використовуючи сотні камер, такі системи можуть навчатися за допомогою алгоритмів машинного навчання для автоматизації процесів спостереження та реагування на певні події, такі як виявлення нестандартних ситуацій, транспортних заторів чи інших критичних моментів. Якщо ж йдеться про невеликі об'єкти, наприклад, мережі магазинів, де встановлюється лише кілька камер для базового відеоспостереження, такі комплексні рішення можуть бути надлишковими. У таких випадках можна використовувати простіші варіанти, які надаються безпосередньо виробниками обладнання.

Багато виробників уже мають власні додатки, веб-інтерфейси або програмні рішення для управління відеокамерами (див. рис.1.11), що дозволить уникнути розробки власної інфраструктури, якщо немає потреби в масштабуванні системи відеоспостереження до рівня «розумного міста».

У будь-якому разі, вибір рішення залежить від масштабу проєкту. Для невеликих систем з кількома камерами достатньо використання базових програмних рішень від виробників. Але якщо система відеоспостереження має обслуговувати велику кількість камер і забезпечувати складну аналітику в реальному часі, варто звернути увагу на масштабовані хмарні платформи, такі як Amazon Kinesis Video Streams, які забезпечують високу надійність, захист та

можливість глибокого аналізу даних. Таке рішення чудово підходить для тих, хто хоче отримати максимальний рівень безпеки, функціональності та надійності, навіть якщо їхня початкова система відеоспостереження є відносно простою.

Хоча рішення коштує недешево, його масштабованість та можливості інтеграції з аналітичними інструментами і алгоритмами машинного навчання роблять його ідеальним для тих, хто готовий інвестувати в більш складні та потужні системи відеоспостереження.

2.2 Концепція Fog Computing та її основні характеристики

Окрім хмарних обчислень, для відеоспостереження доцільно розглянути концепцію Fog Computing (туманні обчислення) (див. рис.2.6). Хоча ця архітектура не була розроблена виключно для відеоспостереження, вона ефективно застосовується навіть у дешевих системах.

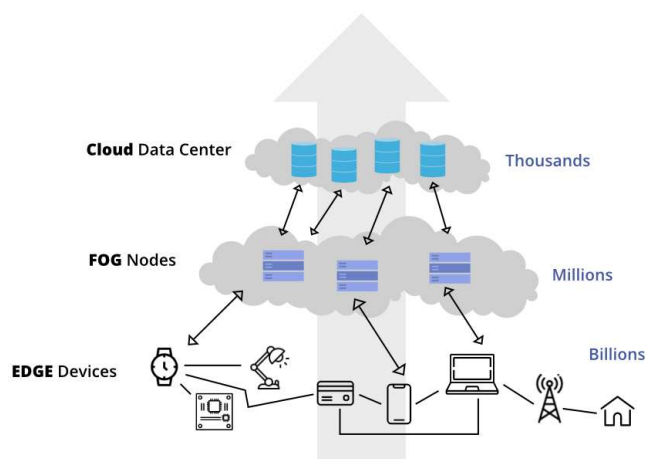


Рисунок 2.6 – Концепція Fog Computing (туманні обчислення)

Основна перевага Fog Computing полягає в можливості обробки даних на рівні пристроїв, ближче до місця їх створення (див. рис.2.6) [12, 13], що особливо важливо для оптимізації відеопотоків. Якщо всі камери відеоспостереження

надавали б лише хмарні рішення для зберігання та обробки даних, це б вимагало великих ресурсів від хмарних серверів. Багато виробників впроваджують Fog Computing як альтернативу повністю хмарним рішенням, дозволяючи користувачам отримувати основні функції без оплати підписок. Наприклад, камери можуть безкоштовно надавати можливість отримувати сповіщення в додатках або отримувати доступ до невеликих відеофрагментів, записаних на картку пам'яті.

Концепція Fog Computing дозволяє виконувати частину обчислень на рівні самої камери, зменшуючи затримки та оптимізуючи трафік між камерами та центральними серверами (див. рис.2.6) [12, 13]. Для відеоспостереження це означає, що значна частина обробки відеопотоків відбувається локально – камери можуть записувати відео на локальні носії, такі як карти пам'яті, і забезпечувати віддалений доступ до цих записів через додатки. Таким чином, користувач має можливість переглядати відео та керувати записами в будь-який момент часу, зберігаючи лише необхідні фрагменти, наприклад, ті, де відбувся рух або інша подія.

Основна частина відеоданих зазвичай не зберігається на хмарних серверах, оскільки це б створювало надмірне навантаження на інфраструктуру. Натомість на хмарних серверах зберігаються лише короткі відеофрагменти, пов'язані з важливими подіями, що знижує потребу в великих обчислювальних ресурсах і забезпечує стабільний доступ до системи відеоспостереження, що є ключовою перевагою Fog Computing: оптимізація трафіку і мінімізація затримок при передачі даних, що головне у справній роботі системи в умовах звичайного інтернет-з'єднання або стандартного маршрутизатора (див. рис.2.6) [12, 13].

Завдяки Fog Computing (див. рис.2.6), камери відеоспостереження можуть ефективно функціонувати в умовах обмеженої пропускної здатності, а хмарна інфраструктура виробника не перевантажується обробкою великих обсягів відеоданих, що дозволяє камерам забезпечувати надійну роботу та зручний віддалений доступ до відеозаписів, навіть у системах з мінімальною кількістю обладнання.

Основні особливості систем відеоспостереження можна деталізувати, поділивши їх на ключові аспекти:

- децентралізоване опрацювання даних;
- опрацювання даних у режимі реального часу;
- децентралізоване зберігання даних;
- енергоефективні протоколи передачі даних.

Децентралізоване опрацювання даних. В нинішніх системах відеоспостереження, як, наприклад, при використанні технології Fog Computing, обробка даних здійснюється на різних рівнях інфраструктури, починаючи від камер відеоспостереження і продовжуючи через локальні вузли, такі як шлюзи або маршрутизатори, що знаходяться безпосередньо на об'єкті. Такий підхід дозволяє зменшити навантаження на хмарні ресурси виробника серверів та інших віддалених систем зберігання даних (див. рис.2.6) [12, 13].

Вузли обробки даних – це локальні пристрої, наприклад, камери з інтегрованими процесорами, маршрутизатори та інші периферійні пристрої. Вони є важливими осередками для попередньої обробки інформації (див. рис.2.6) [12]. Наприклад, у системі відеоспостереження камера, яка має інтегрований процесор, може виконувати обробку даних самостійно – це можуть бути операції зі збереження відео. Вона може працювати навіть за відсутності підключення до Інтернету, аналогічно до відеореєстратора в автомобілі, що означає, що обробка і збереження даних можуть відбуватися локально, без необхідності залучення хмарних рішень.

Такий підхід є надзвичайно ефективним, особливо коли Інтернет-з'єднання відсутнє – у таких системах використовуються протоколи для розподіленої обробки даних, що дозволяє забезпечити ефективний обмін інформацією між пристроями. Наприклад, протокол Message Queuing Telemetry Transport (MQTT) забезпечує ефективну передачу даних з мінімальним енергоспоживанням, що є особливо важливим для пристроїв з обмеженими ресурсами. Інший приклад – протокол CoAP (Constrained Application Protocol), який також є енергоефективним і підходить для роботи в умовах обмежених ресурсів [14]. Як приклад, одна камера

може працювати значно довше від резервного живлення, ніж маршрутизатор, оскільки виконує свої задачі дуже енергоефективно, роблячи інтелектуальні децентралізовані системи відеоспостереження не лише продуктивними, але й енергоефективними, що є великим плюсом. Завдяки цьому, такі камери можуть працювати з джерелами безперебійного живлення навіть у випадках відсутності електроенергії.

Розподілена обробка даних в системах відеоспостереження, як було зазначено, здійснюється на різних рівнях інфраструктури (див. рис.2.6) [12, 13] – від самих камер до локальних вузлів, таких як шлюзи або маршрутизатори, то такий підхід надає значні переваги. Наприклад, камери можуть самостійно аналізувати відео на предмет виявлення руху і передавати на сервер лише результати обробки, а не весь відеопотік, що суттєво знижує трафік даних і, що важливо, зменшує затримку передачі інформації та дозволяє отримувати оперативний доступ до відеоматеріалів без зайвих затримок, що особливо корисно в ситуаціях, де потрібна швидка реакція. Цим самим розподілена обробка даних забезпечує енергоефективність системи – дозволяє впроваджувати відеоспостереження навіть у важкодоступних місцях, де енергоресурси обмежені. Завдяки цьому, такі камери можуть працювати від резервних джерел живлення тривалий час, знижуючи загальне споживання енергії.

Обробка даних у режимі реального часу. Технологія Fog Computing дозволяє обробляти відео безпосередньо на місці, ближче до джерела даних, що значно зменшує час затримки (див. рис.2.6) [12, 13] між генерацією відео та реакцією системи, що надзвичайно важливо для завдань, де потрібна миттєва реакція, наприклад, для виявлення руху або аномальної поведінки. У випадку несанкціонованого доступу система може швидко відреагувати – відразу повідомити охорону або активувати захисні механізми.

Був випадок зі використанням камери відеоспостереження, що працювала в екосистемі Тіуа: коли хтось намагався перехопити відеодані через веб-інтерфейс за допомогою HTTP-протоколу, система миттєво припиняла відеоспостереження і виводила сповіщення про помилку несанкціонованого

доступу та автоматично блокувало подальший запис відео до перезавантаження системи. Така реакція демонструє швидку й ефективну роботу навіть у бюджетних рішеннях відеоспостереження.

Децентралізоване зберігання даних. Дозволяє децентралізовано зберігати дані не тільки на самих камерах відеоспостереження, які мають локальні сховища (наприклад, карти пам'яті), але й на периферійних пристроях, таких як мікросервери або локальні вузли, що особливо актуально для короткострокового зберігання відео, зменшуючи потребу в постійному доступі до хмарних сервісів (див. рис.1.12, 1.13, 2.6) [14].

Такий підхід стає надзвичайно корисним у віддалених або важкодоступних місцевостях, де інтернет-з'єднання може бути нестабільним або відсутнім. Наприклад, використання периферійних пристроїв з великим обсягом пам'яті дозволяє накопичувати відео безпосередньо на місці й відправляти його в хмару лише в разі потреби. У деяких випадках хмарне зберігання може бути взагалі не потрібним, оскільки всі відеодані можуть зберігатися локально на мікросерверах чи NAS (Network-Attached Storage), що надасть змогу зменшити залежність від централізованих хмарних рішень, що підвищує автономність і стабільність систем відеоспостереження [46, 47].

Енергоефективні протоколи передачі даних. Особливе значення в концепції Fog Computing мають протоколи зв'язку, які забезпечують ефективну передачу даних із мінімальним енергоспоживанням. Наприклад, протокол IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) використовується для IP-мереж з низьким енергоспоживанням і застосовується для підключення пристроїв Інтернету речей (IoT) [15], включаючи камери відеоспостереження. Хоча версія IPv6 ще не повністю замінила IPv4 через брак постійних IP-адрес, динамічна адресація, яка надається провайдерами, дозволяє продовжувати використовувати IPv4 до її повного вичерпання.

Ще одним ефективним протоколом є Zigbee, який також часто використовується для енергоефективного з'єднання периферійних пристроїв у розподілених системах [16]. Цей протокол популярний серед пристроїв розумного

будинку, таких як датчики температури, вологості, протікання води, відкриття дверей тощо. Завдяки своїй енергоефективності ці пристрої можуть працювати на одній батареї від кількох місяців до року, що надає їх практичними для тривалого використання без необхідності постійної заміни джерел живлення.

2.3 Порівняння рішень на основі хмарних і Fog-обчислень для розподіленої обробки даних

Під час вибору між хмарними та Fog Computing рішеннями для обробки даних у системах відеоспостереження, ключову роль відіграють вимоги до швидкості обробки, інфраструктурні можливості та специфіка середовища, де вони застосовуються. Обоє рішення (див. рис. 2.7) мають за та проти, і повинні оцінюватися відповідно до завдань системи відеоспостереження.

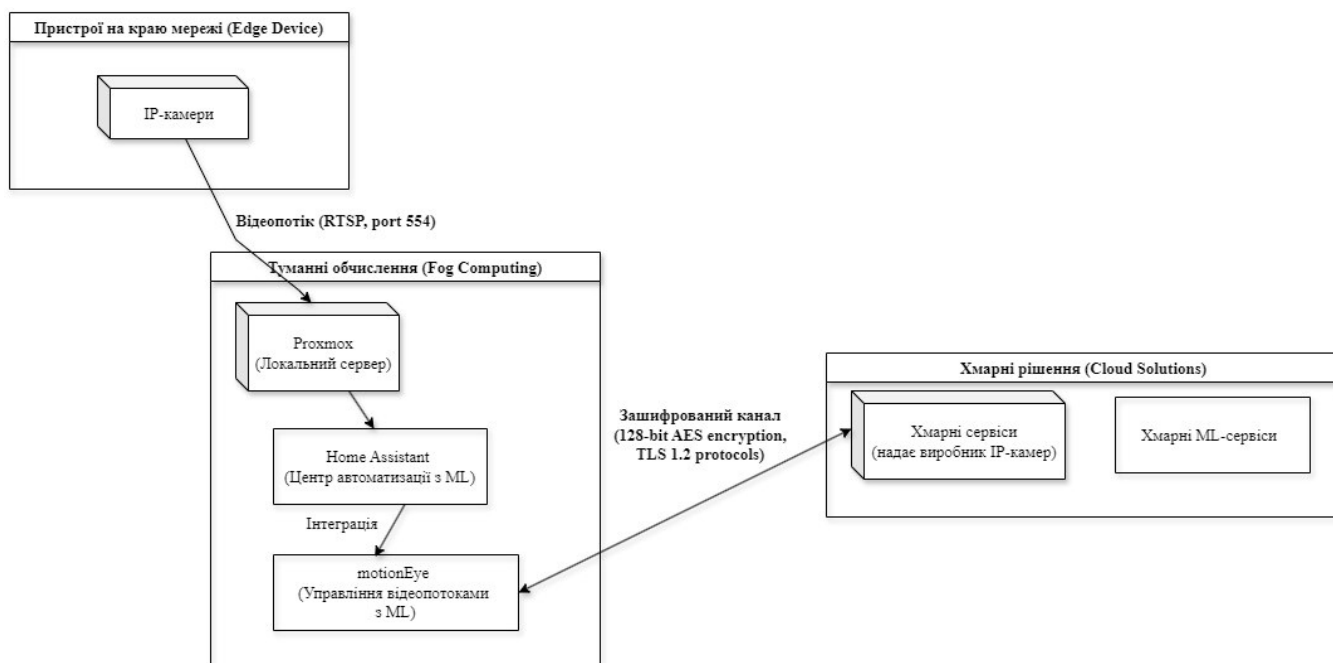


Рисунок 2.7 – Fog-Cloud архітектура для інтелектуального відеоспостереження

Перший критерій – час відгуку. Один із головних показників, що впливає на вибір між хмарними та Fog Computing рішеннями – це час відгуку. У хмарних рішеннях усі дані, включаючи відео з камер спостереження, передаються на віддалені сервери для обробки та зберігання, що означає, що дані повинні пройти через кілька мережевих вузлів до центру обробки, що може спричиняти затримки (див. рис.2.6) [12, 13, 17].

Для завдань, де потрібна миттєва реакція в реальному часі, таких як виявлення руху або розпізнавання облич, ці затримки можуть істотно вплинути на оперативність роботи системи. Як приклад, у хмарних рішеннях відео з камер, розташованих на значній відстані, передається до центрального хмарного сервера для обробки. Цей процес може зайняти кілька секунд, перш ніж результати обробки будуть доступні для реагування. Якщо користувач знаходиться далеко від камер, кількасекундна затримка може бути несуттєвою, оскільки безпосереднє реагування на місці події неможливе.

Натомість Fog Computing дозволяє обробляти дані на місцевих вузлах, таких як маршрутизатори або периферійні пристрої, що розташовані ближче до камер відеоспостереження, що надає можливість значно зменшити затримки, оскільки дані обробляються на місці, без потреби відправляти їх на віддалені сервери (див. рис.2.6) [12, 13, 17]. Такий підхід критично важливий для застосувань, де необхідна миттєва реакція на події, наприклад, для виявлення небезпеки чи контролю доступу.

Камери, оснащені інтегрованими процесорами, що працюють за принципом Fog Computing, можуть самостійно аналізувати відеопотік на місці та оперативно передавати інформацію про загрози службі безпеки, не відправляючи всі дані на хмару. Таке рішення на базі Fog Computing мають явну перевагу в сценаріях, де критично важливий мінімальний час відгуку, наприклад, у системах безпеки, що потребують негайної реакції.

Проте, у випадках, коли оперативність не є ключовою, наприклад, коли користувач знаходиться далеко від місця події і може реагувати з певною затримкою, хмарні рішення можуть виявитися доцільнішими. Вони забезпечують

централізовану обробку даних та доступ до них з будь-якої точки, що є зручним у випадку віддаленого контролю за ситуацією.

Другий критерій – інфраструктура. Якщо розглядати питання інфраструктури, то хмарні рішення вимагають стабільного та високошвидкісного інтернет-з'єднання для надсилання даних на віддалені сервери, що особливо важливо для відеопотоків у реальному часі, коли йдеться про відео у високій роздільній здатності, як-от HD або 4K (див. рис.2.1, 2.6) [6, 12, 13, 17].

Для безперебійної роботи таких систем потрібна висока пропускна здатність мережі, оскільки передача великих відеопотоків потребує швидкого каналу. У разі виникнення перебоїв або збоїв у з'єднанні, існує можливість знищення всіх даних чи «зіпсування» роботи цілої системи відеоспостереження. Наприклад, у великих містах, де доступ до високошвидкісного інтернету є загальнодоступним і стабільним, хмарні рішення можуть бути ефективними, оскільки інфраструктура відповідає вимогам таких систем.

Однак у віддалених регіонах, де інтернет-з'єднання нестабільне, наприклад, при використанні мобільного інтернету або в умовах низької якості зв'язку, хмарна архітектура може бути менш надійною. У таких випадках збої у з'єднанні можуть впливати на роботу системи відеоспостереження, знижуючи її ефективність і надійність.

Натомість рішення на основі Fog Computing можуть ефективно працювати навіть у середовищах з низькою пропускною здатністю або в умовах періодичних збоїв з'єднання, яке можливе завдяки тому, що обробка даних здійснюється локально, на периферійних пристроях, таких як маршрутизатори або самі камери. Таким чином, на хмару передаються лише вже оброблені дані, а не весь відеопотік, що значно знижує вимоги до інтернет-з'єднання.

Такий підхід особливо доцільний для віддалених або важкодоступних районів, де інфраструктура інтернету недостатньо розвинена або взагалі відсутній зв'язок. Fog Computing рішення забезпечують стабільну роботу системи відеоспостереження, мінімізуючи залежність від якості та стабільності інтернет-з'єднання (див. рис.2.1, 2.6) [6, 12, 13, 17]. Наприклад, навіть у ситуаціях, коли

доступ до інтернету відсутній або нестабільний, обробка даних на місці дозволяє системі продовжувати працювати без перебоїв.

Третій критерій – масштабованість. Масштабованість є одним із ключових факторів при виборі між хмарними та Fog Computing рішеннями. Хмарні обчислення мають очевидну перевагу в цьому питанні – завдяки своїй архітектурі, вони здатні обробляти великі обсяги даних з різних джерел та об'єднувати їх у єдине централізоване сховище, що надасть можливість швидко та ефективно масштабувати систему відеоспостереження, додаючи нові камери, збільшуючи обсяг зберігання даних або розширюючи потужності для обробки (див. рис.2.1, 2.6) [6, 12, 13, 17]. Наприклад, якщо зростає кількість камер, користувач може просто замовити більше ресурсів у хмарного провайдера, що не потребує значних зусиль із налаштування.

У деяких випадках, навіть підписка на хмарні сервіси для великої кількості камер може бути вигіднішою з фінансової точки зору, ніж для меншої кількості пристроїв, що робить хмарні рішення зручнішими як для виробників, так і для користувачів. До того ж, централізоване управління дозволяє легше контролювати всі камери навіть у випадку, якщо вони розташовані в різних місцях.

На відміну від хмарних рішень, масштабованість Fog Computing обмежена локальними обчислювальними ресурсами (див. рис.2.1, 2.6) [6, 12, 13, 17]. У такій архітектурі кожен периферійний вузол має власні обмеження щодо обробки даних, що ускладнює процес додавання нових пристроїв або збільшення потужностей. Для розширення системи на базі Fog Computing може знадобитися встановлення додаткових апаратних компонентів, модернізація існуючого обладнання або налаштування нової локальної інфраструктури, що є більш складним і витратним процесом, порівняно з хмарними рішеннями. Наприклад, при додаванні нових камер у систему відеоспостереження на базі Fog Computing потрібно збільшувати локальні обчислювальні ресурси – це може бути додавання оперативної пам'яті, обсягу сховища (твердотільних або жорстких дисків), або встановлення додаткових вузлів обробки. У випадку, якщо система працює на основі міні-ПК чи віртуальних

машин, доведеться збільшувати ресурси цих пристроїв для належного функціонування.

Найбільш ефективною стратегією може бути поєднання обох підходів, використовуючи хмарні рішення для центральної обробки та зберігання великих обсягів даних, а Fog Computing – для обробки на периферії з мінімальною затримкою. Така гібридна модель дозволить отримати переваги обох технологій і забезпечить ефективне управління як інфраструктурою, так і витратами, оптимізуючи використання індивідуально до конкретних потреб системи відеоспостереження (див. рис.2.1, 2.6) [6, 12, 13, 17].

Четвертий критерій – приклади. Хмарні рішення дають можливість доступу до відеоматеріалів з будь-якої точки світу, що є особливо корисним у випадках, коли немає доступу до локальної мережі. Однак, важливо враховувати те, що хмарні рішення зазвичай вимагають додаткових витрат на підписку. Тому для тих, хто не потребує високого рівня інтеграції або постійного доступу до даних, буде достатньо можливостей, які надає камера та її локальна інфраструктура – в такому випадку камери можуть працювати незалежно, записуючи дані локально та надсилаючи основні сповіщення без використання складних хмарних функцій (див. рис.2.1) [6].

До того ж, Fog Computing рішення також можуть вимагати створення локальної інфраструктури, яка буде обробляти дані на місці та може бути корисним для тих, хто хоче зберігати контроль над процесами обробки даних і мінімізувати залежність від інтернет-з'єднання (див. рис. 2.6) [12, 13, 17].

До хмарних рішень у сфері відеоспостереження можна віднести різні камери, зокрема такі, які пропонують повністю автономні і незалежні інтелектуальні системи відеоспостереження. Більшість таких камер, а також ті, які ще виробляються, як приклад, екосистемою Тіуа (див. рис.1.13, 1.12), про яку було згадано раніше, яка націлена на постійне використання своїх хмарних сервісів. Ці сервіси необхідні для отримання сповіщень про рух або інших подій у режимі реального часу.

У своїй попередній бакалаврській роботі було розглядано впровадження камер відеоспостереження в приватні будинки чи квартири на базі рішень від виробника Xiaomi – Yi Home 720p (див. рис.1.3, 1.5, 1.11, 1.12, 1.13, 1.15). Ці камери були доступними за ціною та мали велику підтримку з боку користувачів, які активно розширювали їх функціонал, і мали в собі як і повністю хмарні рішення, але після «перепрошивки» – отримали Fog рішення. Вони проіснували досить довго й досі залишаються актуальними.

Одним із прикладів популярних хмарних рішень є сервіс Amazon Kinesis Video Streams (див. рис.2.5, 2.7) [11], який надає значні переваги завдяки використанню передової інфраструктури компанії Amazon. Таке рішення забезпечує користувачам гнучку масштабованість, особливо коли йдеться про великі системи відеоспостереження, такі як міські мережі камер. Масштабування такої системи є ключовою перевагою хмарних рішень, оскільки додавання нових камер та збільшення обробки даних можливе за допомогою простого замовлення додаткових ресурсів у хмарного провайдера.

Якщо ж система потребує ще більшого рівня інтеграції та можливостей, існують інші хмарні платформи, наприклад, Google Cloud і IoT Core, які дозволяють зберігати й обробляти дані з різних IoT-пристроїв, включаючи камери. Google Cloud також підтримує аналітику в реальному часі та пропонує тісну інтеграцію з іншими сервісами, що забезпечує додаткову гнучкість у використанні і можливість оптимізувати процеси [18]. Ще одним потужним рішенням є Microsoft Azure IoT Hub, хмарна платформа для управління IoT-пристроями, що включає можливості зберігання великих обсягів відеоданих та проведення аналітики [19]. Така платформа також орієнтована на масштабованість, зручність моніторингу та обробки відеопотоків із багатьох камер.

До того ж, туманні обчислення мають власні переваги – Cisco Fog Computing пропонує рішення, яке спеціалізується на обробці даних на периферії, зокрема для відеоспостереження, де важлива швидка локальна обробка [20]. Використання енергоефективних протоколів, таких як MQTT та CoAP, дозволяє ефективніше передавати дані та мінімізувати енергоспоживання, знижуючи затримки при

обробці відео, роблячи такі рішення оптимальними для ситуацій, де критичні швидкість і локальна обробка даних. Ще один приклад Fog-рішень – це NVIDIA Metropolis, яке використовує потужності графічних процесорів (GPU) для інтелектуальної обробки відеопотоків на основі штучного інтелекту та машинного навчання [21]. Така платформа дозволяє здійснювати складну відеоаналітику в реальному часі, без необхідності передавати всі дані на віддалені сервери.



Рисунок 2.7 – Хмарні та Fog- рішення

(зліва направо: Google IoT Core, Microsoft Azure IoT Data Hub,
NVIDIA Metropolis, Amazon Kinesis Video Streams)

РОЗДІЛ 3 РОЗРОБКА ТА РЕАЛІЗАЦІЯ ІНТЕЛЕКТУАЛЬНОЇ ДЕЦЕНТРАЛІЗОВАНОЇ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ

3.1 Компоненти інтелектуальних децентралізованих систем

Щоб краще зрозуміти, що таке інтелектуальна децентралізована система відеоспостереження, необхідно детально розглянути її компоненти, принципи роботи та основні можливості. Така система складається з лише з однієї ключової частини – камер, що мають власні процесори та інші комплектуючі, які дозволяють їм функціонувати автономно, навіть за умови відсутності електроенергії.

При виборі інтелектуальної децентралізованої системи відеоспостереження важливо зважати на кінцеві цілі її використання. Якщо необхідно забезпечити віддалений контроль за певною ділянкою без глибокого занурення у технічні деталі, можна вибрати простіші варіанти систем. Проте, якщо потрібна більш складна інфраструктура, варто звернути увагу на рішення, які пропонують розширені можливості керування та інтеграції з іншими системами.

Коли обирається система відеоспостереження, слід розуміти, що різні виробники пропонують власні екосистеми, подібно до того, як це роблять технологічні компанії (наприклад, Apple, Samsung чи Xiaomi) (див. рис.3.1) [22]. Тому не рекомендується «змішувати» обладнання від різних виробників, адже кожен бренд створює свою екосистему, що передбачає узгоджене функціонування всіх компонентів. Зазвичай такі системи мають власне програмне забезпечення для управління, яке найчастіше призначене для смартфонів, що дозволить користувачам легко отримувати доступ до відеопотоків з будь-якого місця та в будь-який час, адже смартфони завжди під рукою.



Рисунок 3.1 – Порівняння екосистем Apple та Google

При виборі виробника також слід враховувати додаткові послуги, які можуть надаватися. Наприклад, деякі системи пропонують хмарне зберігання даних на платній основі. Якщо користувач не планує вкладати кошти у подібні сервіси, можна обрати камери з можливістю локального зберігання інформації на карті пам'яті.

Якщо потрібно інтегрувати систему або камери відеоспостереження у вже існуюче середовище, наприклад, до існуючого серверу чи програмного забезпечення, то є інший підхід. В такому випадку важливо не стільки обирати камери від конкретного виробника з їхніми екосистемами та сервісами, скільки забезпечити сумісність із вже наявними інструментами, такими як власний сервер або програмні рішення для отримання контролю зі одного місця.

Цей підхід дає змогу використовувати більш доступні камери без дорогих підписок на хмарні сервіси – зберігати дані локально, на власному сервері, маючи повний контроль над інфраструктурою – це ідеальне рішення для тих, хто не хоче залежати від сторонніх сервісів або прагне максимальної безпеки і конфіденційності даних. Камери можуть бути підключені через локальну мережу, і у такому випадку ви отримаєте більше гнучкості в управлінні даними.

Для більшості випадків користувачі надають перевагу першому варіанту – коли все обладнання від одного виробника інтегровано в просту та інтуїтивно зрозумілу систему (див. рис.3.1) [22], що зручно, оскільки не потрібно

замислюватися про налаштування мережевої інфраструктури або конфігурацію серверів.

Є два основні підходи до використання систем відеоспостереження:

1. Перший підхід полягає у придбанні камер однієї екосистеми, що забезпечує інтеграцію з хмарними сервісами: рішення підходить для тих, хто не має спеціальних вимог щодо захисту або конфіденційності і готовий користуватися послугами виробника для зберігання даних. Хмарні сервіси також надають додатковий захист у випадку пошкодження камер, адже всі записи будуть збережені на серверах виробника.

2. Другий підхід підходить для тих, хто має технічні навички або потребує більшої автономії та контролю: полягає у створенні власного серверу для підключення різних камер від різних виробників за допомогою протоколу RTSP (див. рис.2.3) [8, 9]. Такий сервер дозволяє об'єднати всі камери в одну систему, незалежно від їхнього виробника, що дає можливість централізованого керування та підвищує гнучкість.

Використання різних камер від різних виробників дозволяє створити більш гнучку та масштабовану систему. Наприклад, можливе використання автономних камер, які живляться від сонячних панелей, разом із камерами, що підключені до локальної мережі. За допомогою інтеграцій, таких як Home Assistant (див. рис.3.2) [23], можна об'єднати всі ці пристрої в одну екосистему та керувати ними з одного додатку, що значно зручніше, ніж використовувати кілька різних додатків для кожної камери.



Рисунок 3.2 – Платформа Home Assistant та хаб Home Assistant Yellow

Другий варіант є трохи складнішим і дорожчим у налаштуванні, але він забезпечує повний контроль над системою відеоспостереження та лише підходить для тих, хто хоче зберігати великі обсяги даних локально, не залежати від хмарних сервісів і забезпечити конфіденційність. Проте, якщо технічні можливості або бюджет обмежені, можна зупинитися на першому варіанті, використовуючи інфраструктуру та сервіси виробника камер. У цьому випадку варто розглянути компоненти, які можна використовувати для обох варіантів (див. рис.3.3).

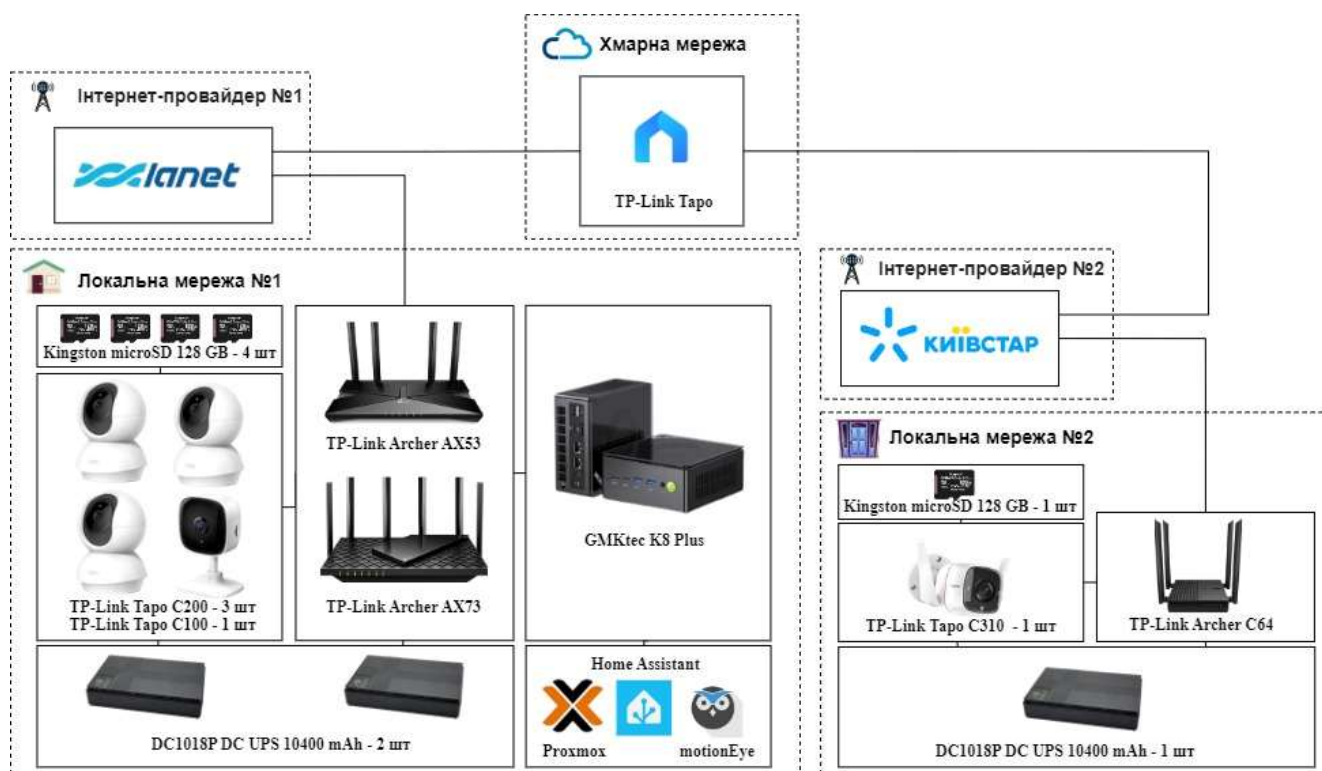


Рисунок 3.3 – Схема інтелектуальної системи відеоспостереження з резервуванням, локальним та хмарним сервісами

Для першого варіанту з використанням лише готових рішень від виробника систем відеоспостереження:

- камери відеоспостереження;
- мобільний пристрій;
- дешевий маршрутизатор;
- застосунок від виробника;
- сервіси виробника (на безкоштовній/платній основі).

Для другого варіанту з використанням сторонніх рішень для систем відеоспостереження:

- камери відеоспостереження;
- мобільний пристрій / ПК;
- дорогий маршрутизатор;
- локальний сервер;
- ПЗ з відкритим кодом;
- технічні навички.

Вибір камер відеоспостереження – TP-Link Taro. Основним компонентом будь-якої децентралізованої системи відеоспостереження є самі камери. Вони підходять як для сценарію з локальним сервером, так і для варіанту з використанням хмарних сервісів виробника камер. Для демонстрації реальної інтеграції інтелектуальної децентралізованої системи відеоспостереження було вирішено використати камери від одного виробника – TP-Link, який відомий своїм мережевим обладнанням. Обрані камери належать до екосистеми TP-Link серії Таро, яка, крім камер, також включає розумні розетки, датчики, системи освітлення та інші інтелектуальні пристрої.

Було обрано дві моделі камер: Таро С100 та Таро С210, а також одну зовнішню камеру Таро С310 (див. рис.3.4). (Додаток А) Перші дві моделі мають різні функціональні можливості. Таро С100 – це стаціонарні камери без механізмів повороту, призначені для фіксованого спостереження за певною ділянкою. Попри свою простоту, вони мають низку корисних функцій, що відрізняють їх від традиційних камер відеоспостереження. Таро С210, на відміну від попередньої

моделі, має трьохосовий поворотний механізм, що дозволяє змінювати напрямок огляду камери за допомогою додатку – для відстеження ситуацій у різних частинах приміщення.



Рисунок 3.4 – Інтелектуальні камери відеоспостереження TP-Link серії Таро
(зліва направо: Таро C310, Таро C210, Таро C110)

Дані камери дають можливість спостерігати не тільки за однією точкою, а й оперативно змінювати напрямок спостереження. Також, крім внутрішніх камер відеоспостереження було встановлено одну зовнішню камеру Таро C310 для моніторингу прибудинкової території. Така камера має підвищений захист від впливу навколишнього середовища: вона стійка до пилу, води та екстремальних температур, що робить її ідеальною для зовнішнього використання.

Загалом було встановлено 5 камер, які розташовані у різних місцях та виконують різні завдання. Наприклад, частина камер забезпечує моніторинг безпеки всередині квартири, а зовнішня камера слугує для нагляду за територією біля будинку (див. рис.3.5). Деякі камери відеоспостереження знаходяться не в одній локації, що забезпечує зручний контроль з одного місця. Камери працюють через безпроводне з'єднання Wi-Fi на частоті 2,4 ГГц, що дозволяє їх інтегрувати в мережу без необхідності прокладання додаткових кабелів, а також, за можливістю (притаманне зовнішнім камерам) – підключення за допомогою Ethernet-кабелю або патч-корду.

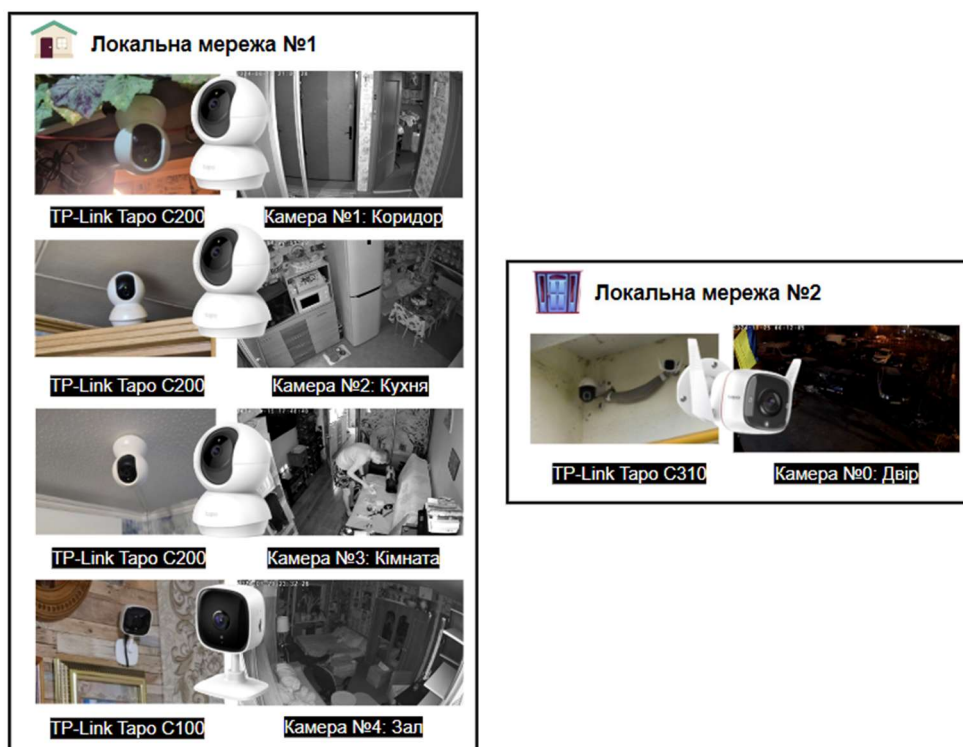


Рисунок 3.5 – Розташування системи відеоспостереження

Камери відеоспостереження TP-Link серії Таро є чудовим прикладом того, як можна створити інтелектуальну систему відеоспостереження, використовуючи різні типи обладнання, які інтегруються в єдину екосистему. Важливо зазначити, що раніше використовувалися камери Xiaomi YI Home 720p 2015 року випуску (див. рис.1.5). Хоча вони виконували свої функції, їхній функціонал був обмеженим, а також вони були призначені для китайського ринку та перепрошиті для роботи в Україні – саме тому було прийнято рішення перейти на європейські камери TP-Link серії Таро, які забезпечують кращу якість і сучасніші можливості інтеграції.

Камери відеоспостереження TP-Link Таро C210, оснащені поворотним механізмом, здебільшого використовуються в місцях із високою активністю або там, де необхідно спостерігати за кількома зонами одночасно. Завдяки можливості повороту ці камери дозволяють відмовитися від використання кількох камер для охоплення різних точок. Окрім базових функцій відеоспостереження, Таро C210 має інтелектуальні можливості, такі як детекція руху, розпізнавання людини, тварини або дитячого плачу. Її також можна налаштувати на виявлення руху в

конкретних зонах огляду, ігноруючи інші ділянки, щоб уникнути непотрібних сповіщень від несуттєвих рухів. До того ж, камера може автоматично реагувати на рух, наприклад, активувати сирену, оскільки обладнана двонаправленим зв'язком – мікрофоном і динаміком, дозволить не лише прослуховувати, що відбувається у приміщенні, але й спілкуватися через камеру за допомогою мобільного телефону. Така функція може бути корисною для попередження чи відлякування небажаних осіб, оскільки камера забезпечує безпеку, а двосторонній зв'язок дозволяє оперативно реагувати на події [45]. (Додаток А)

Усі ці моделі підтримують роздільну здатність Full HD (1080p), яка є достатньою для більшості сценаріїв спостереження (див. рис.3.4) . Проте камери Таро С210 і Таро С310 можуть знімати з роздільною здатністю до 2К, що покращує якість зображення, але водночас потребує більше ресурсів для збереження та обробки даних. Кожна з цих камер має 3-мегапіксельну матрицю, що забезпечує достатньо високу деталізацію зображення для основних завдань відеоспостереження (див. рис.3.6).

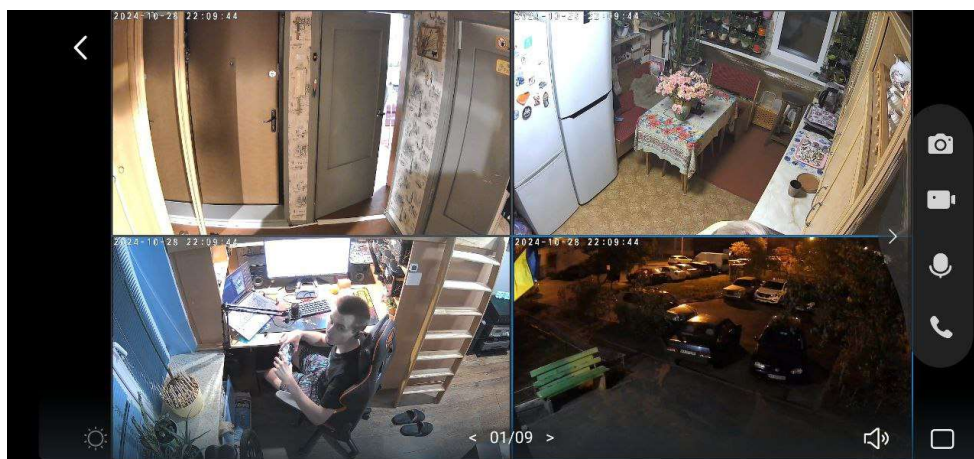


Рисунок 3.6 – Одночасний перегляд зі 4 камер відеоспостереження TP-Link серії Таро в різних локаціях (9 зон – 32 камери максимум)

Для спостереження цього цілком достатньо, оскільки камери зазвичай розміщені стаціонарно, і їх основне завдання – фіксувати рух навколо (див. рис.3.4). Завдяки низькій частоті кадрів і достатній якості зображення (Full HD або 2K), такі камери можуть записувати тривалий час на локальне сховище. Наприклад, якщо

взяти камеру з 128 ГБ пам'яті, як на одному з прикладів використання, то цього об'єму вистачає на два тижні безперервного запису відео 24/7 (див. рис.3.7). Протягом цього часу камера постійно записує відео на карту пам'яті без перерв, і при цьому не виникає проблем з відтворенням або зберіганням даних.

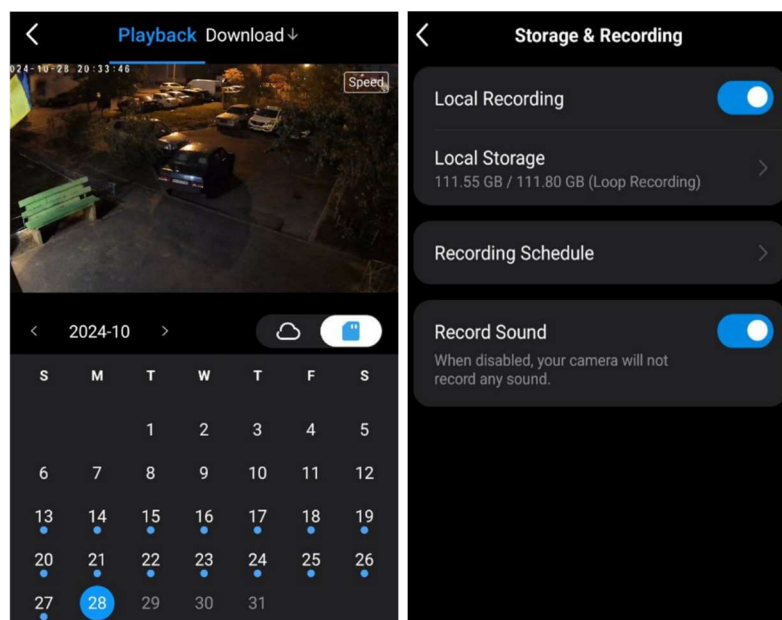


Рисунок 3.7 – Локальне сховище у камер відеоспостереження TP-Link серії Таро (карта пам'яті на 128 ГБ – 15,5 днів запису відео)

Проте варто пам'ятати, що карти пам'яті зменшений ресурс, до того ж якщо вони вже використовуються для постійного перезапису даних. Це означає, що зазвичай через рік чи півтора карту пам'яті потрібно замінити. Такий досвід підтверджується попереднім використанням камер від Хіаомі, де після кількох років експлуатації карти пам'яті починали працювати некоректно, потребували частого форматування або заміни – це пов'язано з тим, що карти пам'яті не призначені для постійного перезапису даних, а більше для зберігання файлів.

Для тих, хто планує встановлення системи відеоспостереження, варто розглянути можливість використання хмарного сховища замість або на додаток до локального сховища на картах пам'яті (див. рис.3.7-3.8). Хмарне сховище пропонує додаткові переваги:

- доступ до відеозаписів з будь-якого місця;

- незалежність від обмежень локального сховища (до 1 місяця записів);
- короткі звіти за 1 день.

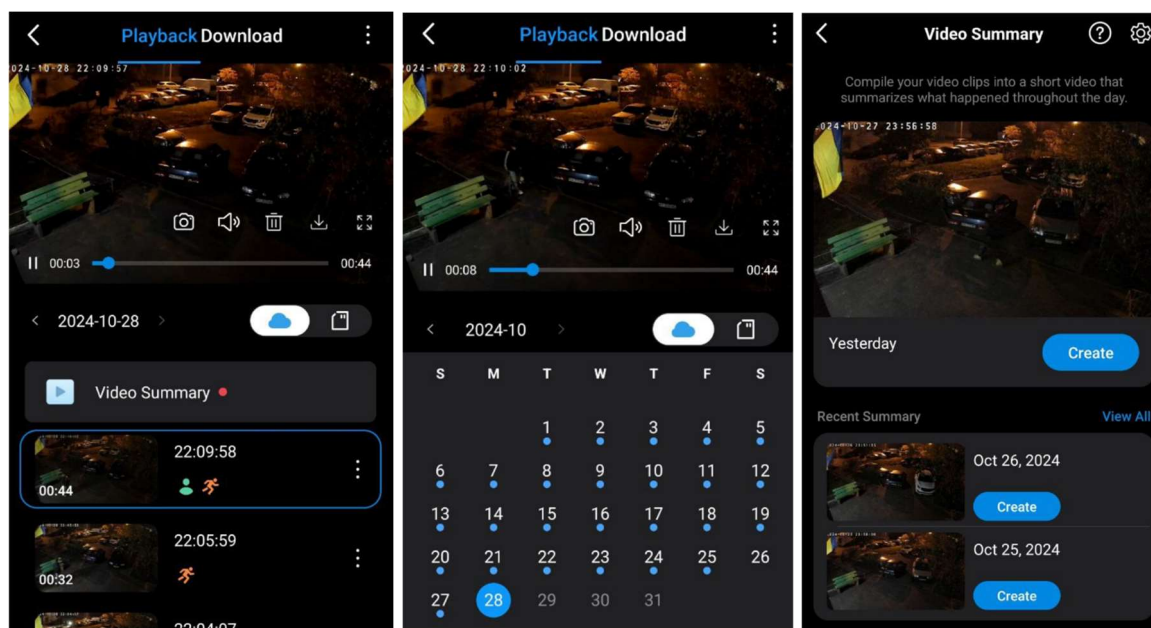


Рисунок 3.8 – Хмарне сховище у камер відеоспостереження TP-Link серії Таро (1 місяць записів та короткі відеозвіти за день)

Системи відеоспостереження мають багато функцій, і їхній функціонал значною мірою залежить від програмного забезпечення, яке надають виробники. В основному, цей функціонал реалізується через спеціальні додатки для мобільних пристроїв або ПК. Основна увага зосереджена на мобільних додатках, оскільки більшість користувачів сьогодні мають смартфони, і це робить використання таких додатків максимально зручним. Проте деякі виробники, наприклад Dahua та її суббренди, такі як IMOU, пропонують також версії програм для ПК, що може стати вирішальним фактором для тих, хто хоче керувати камерами з ПК (див. рис.3.9).

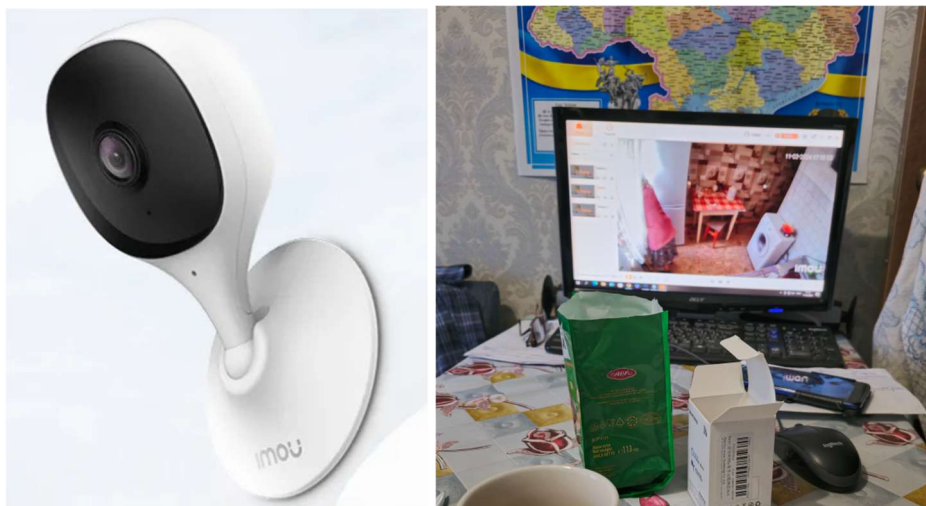


Рисунок 3.9 – Інтелектуальна камера відеоспостереження Imou Cue 2E
(додаток Imou Life для Windows, macOS, Android, iOS)

Програмне забезпечення від виробника – Таро. Найважливіше, що робить ці камери відеоспостереження по-справжньому «інтелектуальними» – це можливість дистанційного керування через мобільний додаток, що дозволить керувати камерою і переглядати відео з будь-якого куточка світу, що значно підвищує ефективність і зручність використання таких систем відеоспостереження.

Додаток Таро (див. рис.3.10) дозволяє керувати камерами відеоспостереження з будь-якої точки світу, не обмежуючись лише локальною мережею, що досягається за допомогою інфраструктури самого виробника, який використовує хмарні сервіси і забезпечує захищене з'єднання даних через SSL шифрування. Хоча при такому підході існує невелика затримка при передачі даних, це надає широкий спектр можливостей, зокрема віддалене керування камерами.

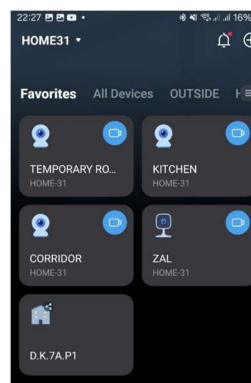


Рисунок 3.10 – Додаток Таро (лише для Android, iOS)

Функціонал додатку Таро включає такі можливості:

- налаштування та отримання push-сповіщень (у разі детектування);
- віддалений доступ з будь-якої мережі;
- перегляд відео в реальному часі (локальний та/або хмара);
- керування записом (локально);
- зберіганням даних (локальний та/або хмара);
- двостороннього зв'язок (інтегровані мікрофон та динамік);
- поширення камер відеоспостереження іншим особам (до 5 користувачів).

Додаток не є складним, але надає всі необхідні інструменти для зручного управління: від налаштувань сповіщень і перегляду відео до двостороннього зв'язку і віддаленого доступу в режимі реального часу, що дозволить ефективно керувати системою відеоспостереження навіть на великих відстанях, забезпечуючи повний контроль і безпеку незалежно від місця розташування камер.

Система відеоспостереження, побудована на продукції одного виробника, забезпечує інтеграцію камер у єдину екосистему, що значно спрощує керування. Наприклад, у випадку з TP-Link, камери можуть працювати в різних місцях, бути підключеними до різних мереж, але при цьому всі вони будуть доступні через один додаток. Навіть якщо камери встановлені на відстані кількох кілометрів одна від одної, користувач має змогу керувати ними віддалено через інтеграції.

Використання міжнародних камер, які призначені для європейського ринку, також забезпечує безперебійність їх роботи в Україні – це підтверджується досвідом попередніх досліджень, де було зазначено, що навіть бюджетні камери можуть надавати достатній функціонал для спостереження. Однак трохи дорожчі моделі забезпечують кращу якість і більші можливості, що робить їх оптимальними для використання в довготривалій перспективі. Використовуючи міжнародні, зокрема європейські, камери відеоспостереження, ми отримуємо надійність і сумісність із нашими умовами без будь-яких проблем, що було підтверджено попередніми дослідженнями.

Раніше акцент робився на тому, що навіть найдешевші бюджетні моделі можуть ефективно працювати, забезпечуючи базові функції. Однак у цьому випадку ми використовуємо дещо дорожчі камери, які мають кращий функціонал і орієнтовані на міжнародний ринок, зокрема на Європу. Додаток Таро (див. рис.3.10), який використовується для керування камерами, не є складним, проте він надає можливість підключити всі пристрої до єдиної системи управління.

Двохстороння система зв'язку. Однією з корисних функцій цих камер є підтримка двостороннього зв'язку, оскільки в них є інтегровані мікрофон і динамік, що дозволяє спілкуватися через камери так, як це робиться під час телефонної розмови. Додаток дозволяє налаштовувати push-сповіщення, що надходитимуть на телефон у залежності від конкретних подій. Наприклад, якщо камера встановлена в місці з мінімальним рухом, можна вимкнути сповіщення на час, коли там перебувають люди, а в ситуаціях, коли приміщення, наприклад магазин або будинок, зачинене, можна активувати сповіщення про рух, і додаток надішле сповіщення у разі виявлення активності (Додаток А).

Сховище зберігання даних – локальне. Камери також записують відео на локальне сховище, що є безкоштовною опцією. Завдяки цьому користувачі можуть переглядати як реальний потік, так і відео з невеликою затримкою.

Система може працювати через один додаток, навіть якщо камери підключені до різних мереж або встановлені в різних місцях, що є зручним для тих, хто, як у власному випадку, використовує камери в кількох об'єктах – як удома, так і поза ним. Планується, у найближчому майбутньому, встановлення камер відеоспостереження у віддаленому будинку, що знаходиться за 500–600 км, і все це буде інтегровано в межах одного додатку для віддаленого доступу.

Сховище зберігання даних – хмарне. Хмарні сервіси дозволяють зберігати дані від камер у захищеному середовищі, що гарантує доступ навіть у випадку втрати фізичного носія, наприклад, через крадіжку або пошкодження камери, що особливо важливо, коли йдеться про збереження важливих записів. У випадку відключення електроенергії, камери можуть передавати дані в хмару, забезпечуючи доступ до останніх записів, зроблених перед відключенням – завдяки

цьому користувачі отримують постійний контроль навіть тоді, коли камера тимчасово не працює в онлайн-режимі.

Виробник камер відеоспостереження TP-Link пропонує користувачам два основні тарифні плани для зберігання даних:

- річний план (зі знижкою);
- місячний план (без знижки).

Однією з ключових функцій є надання хмарного сховища, де всі відеозаписи зберігаються протягом 1 місяця – ці записи включають короткі відеоролики, що створюються під час детекції руху або присутності людей перед камерою. Дані зберігаються на серверах TP-Link, що є надзвичайно корисним у випадках втрати з'єднання з камерою. Навіть якщо камера перестане працювати, наприклад, через пошкодження або втрату зв'язку з інтернетом, записи залишаться доступними в хмарі, що досить важливо для ситуацій, коли камера може бути знищена або викрадена зловмисниками, оскільки всі дані залишаються захищеними в хмарному сховищі, і користувач зможе переглянути, що відбувалося до моменту втрати зв'язку [24]. (Додаток Б)

Окрім цього, TP-Link надає ще одну зручну функцію – щоденний підсумковий відеоролик (див. рис.3.11) [24]. Цей відеоролик, що триває близько хвилини, автоматично створюється на основі всіх моментів руху, зафіксованих протягом дня – це значно спрощує процес перегляду записів, оскільки не потрібно переглядати всі матеріали повністю. У такий спосіб зручно коли камера розташована в місці з нечастими рухами, і користувачеві не потрібно витрачати багато часу на пошук потрібних моментів.

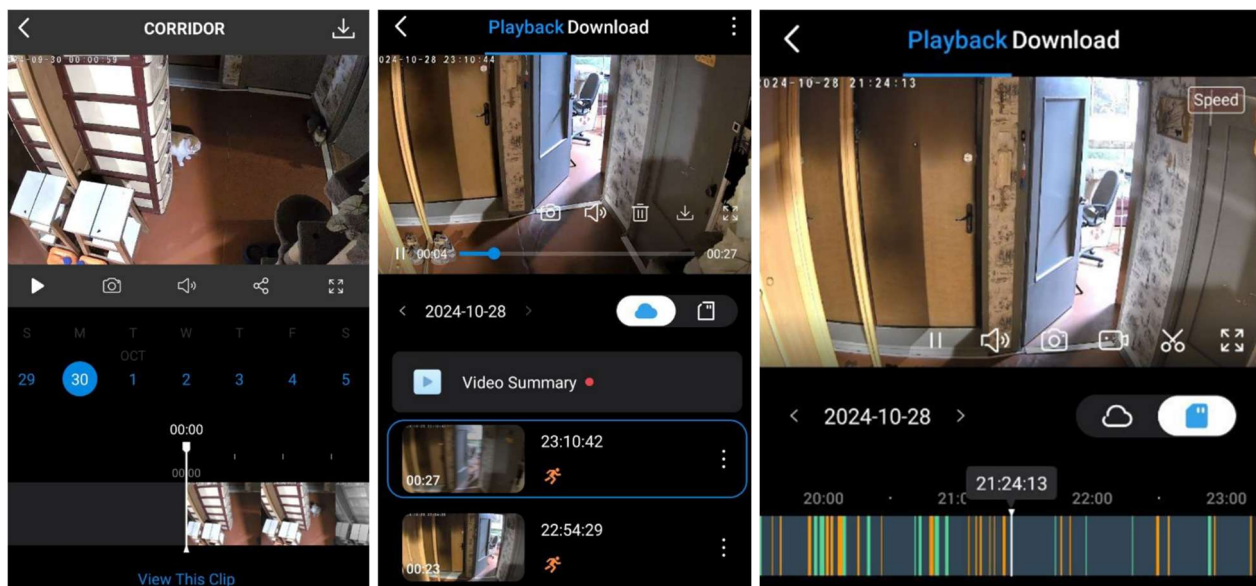


Рисунок 3.11 – Порівняння хмарного та локального сховища
(підсумковий ролик у хмарному, зручна часова шкала у локальному)

Що стосується локального сховища, воно також має свої переваги: камери TP-Link дозволяють зберігати записи на карті пам'яті, де користувач може переглядати записи безпосередньо. Локальне сховище дозволяє швидко переміщатися по записах за допомогою зручної шкали часу, що полегшує доступ до необхідних моментів. До того ж, записи можна переглядати навіть у випадку відсутності інтернету, що забезпечує постійний доступ до даних (див. рис.3.8) [24].

Однак варто зазначити, що інтерфейс для роботи з хмарним сховищем може бути дещо менш зручним порівняно з локальним: при використанні хмарного сховища користувачеві доводиться довше чекати на відображення записів у додатку, особливо якщо він шукає конкретний час або день (див. рис.3.11). Водночас хмарне сховище надає додатковий рівень безпеки у випадку втрати доступу до локальних даних (див. рис.3.8) [24, 46, 47].

Альтернатива інфраструктури виробника – вибір сервера на базі міні-ПК GMKtec K8 Plus. Одним із важливих варіантів є використання власного сервера для зберігання даних, що забезпечує вищий рівень конфіденційності та контролю. Наприклад, встановивши власний сервер, можна забезпечити зберігання відеоданих на своїй стороні, без необхідності надавати доступ до цих даних виробнику камери або іншим стороннім сервісам, що підходить для ситуацій, коли

потрібна максимальна конфіденційність та безпека, і немає потреби у підключенні камер відеоспостереження безпосередньо до інтернету або є бажання «контролювати», які дані передаються в мережу.

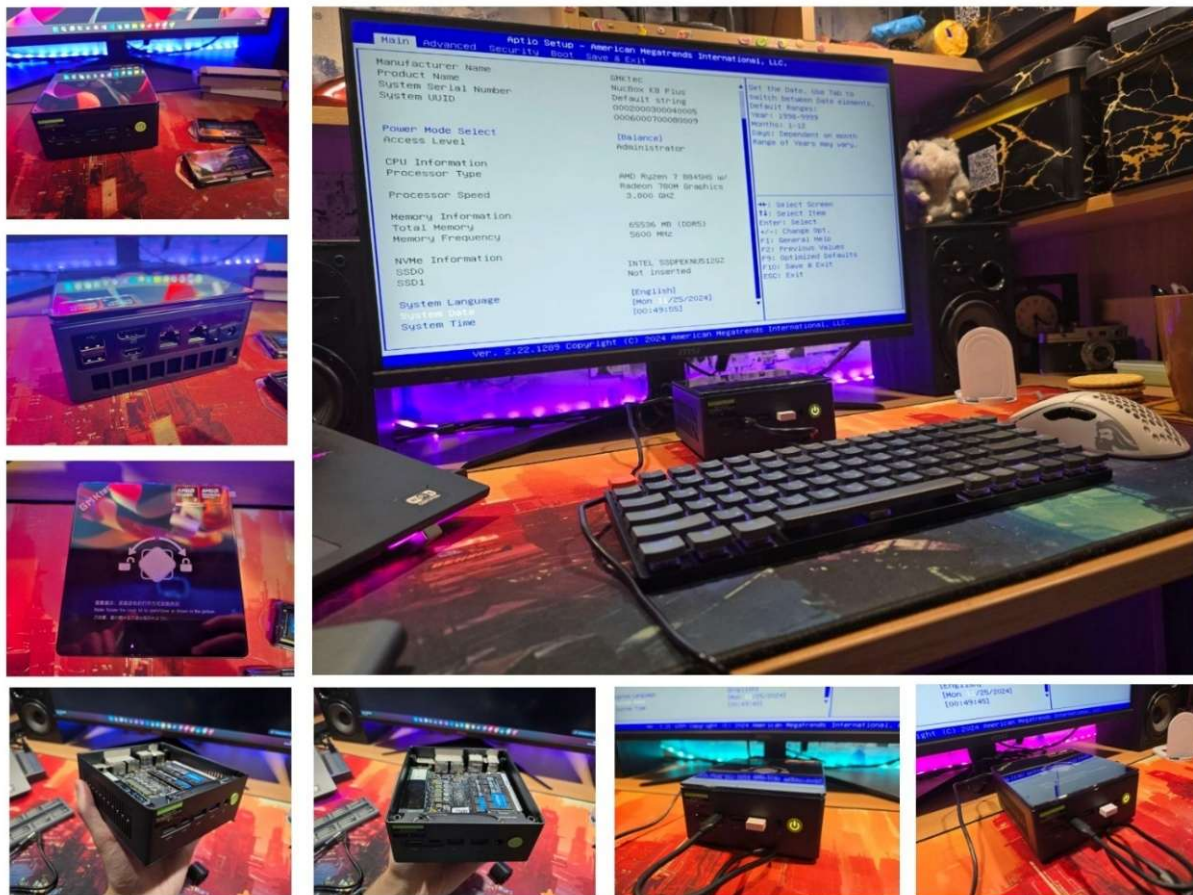


Рисунок 3.12 – Сервер на базі міні-ПК GMKtec NucBox K8 Plus та його інтерфейс

Використання власного сервера, на базі міні-ПК GMKtec NucBox K8 Plus (див. рис.3.12, табл. 2.1) [32] також дозволяє розширити можливості зберігання даних, особливо якщо у нас є великий обсяг сховища, наприклад, кілька терабайтів і більше, що надає можливість зберігати набагато більше відеозаписів, ніж на одній карті пам'яті, і мати до них швидкий доступ без затримок, що іноді виникають при використанні хмарних сервісів.

Таблиця 3.1 – Технічні характеристики міні-ПК GMKtec K8 Plus

Характеристика	GMKtec K8 Plus
Процесор	AMD Ryzen 7 8845HS (8 ядер, 16 потоків)
Оперативна пам'ять	До 96 ГБ DDR5, частота до 5600 МГц (2 слоти)
Накопичувачі	Підтримка до 2x M.2 2280 PCIe 4.0 SSD (до 8 ТБ)
Графіка	Вбудована графіка Radeon 780M, можливість підключення eGPU через OCuLink
Порти	2x USB 4.0, HDMI, DisplayPort, 2x Ethernet (2.5 Гбіт/с), Wi-Fi, Bluetooth 5.2
Підтримка дисплеїв	До 4 дисплеїв одночасно
Розміри	135 x 125 x 58 мм
Операційна система	Підтримка Windows 11 Pro (опціонально)
Ціна	Від \$389.99

Виробник TP-Link надає можливість використовувати камери серії Таро поза межами власних хмарних сервісів та додатків. Наприклад, в камерах передбачено використання протоколу RTSP (Real-Time Streaming Protocol) (див. рис.2.3) [8, 9], який дозволяє інтегрувати камери в інші системи та передавати відео на ПК або сервер для запису або подальшої обробки, незалежно від того, чи використовуються хмарні сервіси від TP-Link (див. рис.3.13-3.14) [25].

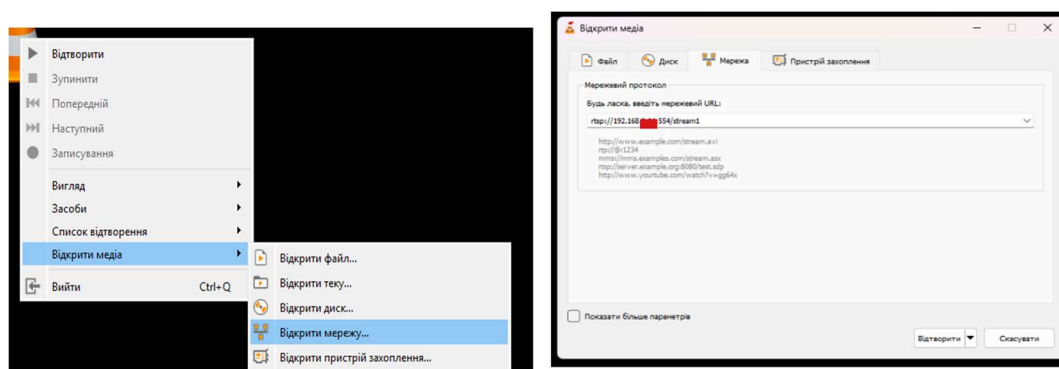


Рисунок 3.13 – Перевірка доступності однієї із камер у програмі VLC

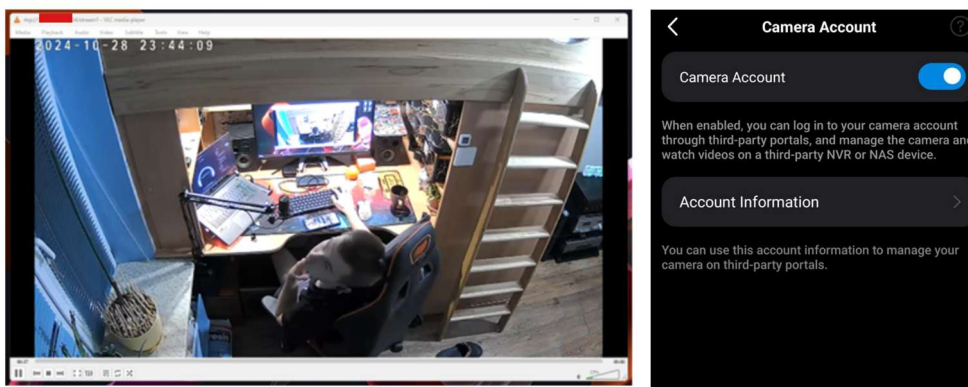


Рисунок 3.14 – Обхід хмарних сервісів TP-Link через протокол RTSP (порт 554) (попередньо має бути створено акаунт у додатку TP-Link Таро для отримання доступу до RTSP потоку)

Протокол RTSP може бути додатково захищений паролем, що збільшує рівень безпеки передачі даних. Використання цього протоколу в локальній мережі може бути достатнім для забезпечення приватності та захисту відео, оскільки всі дані залишаються всередині вашої мережі, але якщо планується передача даних за межі локальної мережі, варто звернути увагу на додаткові заходи безпеки, щоб уникнути компрометації даних [25].

Завдяки використанню протоколу передачі даних RTSP (див. рис.2.3) [8, 9], можливо інтегрувати камери відеоспостереження не тільки від виробника TP-Link, але й від будь-яких інших виробників, які підтримують цей протокол, у різні програми, додатки чи веб-сервери. Одним із варіантів використання цього протоколу є підключення камер через IP-адресу та порт RTSP (554), що дозволяє легко налаштувати їх для інтеграції з різними серверами чи системами (див. рис.3.13-3.14) [25].

Альтернатива ПЗ виробника – Home Assistant та доповнення MotionEye. Якщо ми прагнемо більш гнучкого та масштабного рішення для об'єднання камер відеоспостереження та розумних пристроїв, важливо розглянути альтернативний підхід. Він полягає у використанні сервера або інфраструктури, на яку можна встановити спеціальну операційну систему або образ для Docker Compose.

Одним із найкращих варіантів для цього є Home Assistant – платформа для керування розумним будинком. Вона дозволяє інтегрувати як камери

відеоспостереження, так і різноманітні датчики, об'єднавши їх у єдину систему. За допомогою Home Assistant можна використовувати «аддон» MotionEye для відеоспостереження та інші «аддони» для керування датчиками, що працюють за протоколами Zigbee, MQTT та іншими. У такому випадку всі пристрої, включно з камерами та датчиками різних виробників, можна керувати та відслідковувати з одного налаштованого інтерфейсу – наприклад, через планшет або веб-сторінку, що дозволить створити централізовану панель керування, на якій відображатимуться всі дані з камер і датчиків у будинку або навіть поза його межами (див. рис.3.15-3.16) [26, 27].

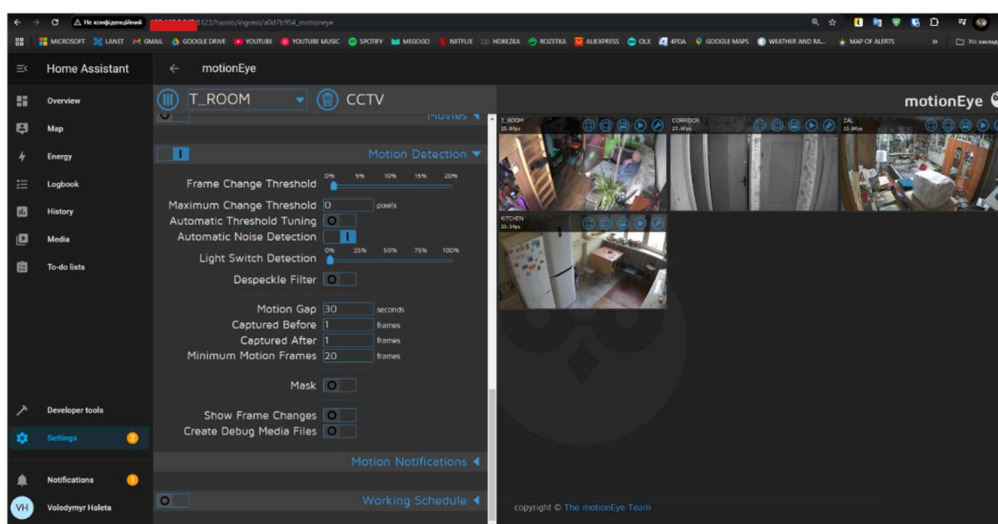


Рисунок 3.15 – Налаштування детекції на рух у сервісі Home Assistant через доповнення motionEye

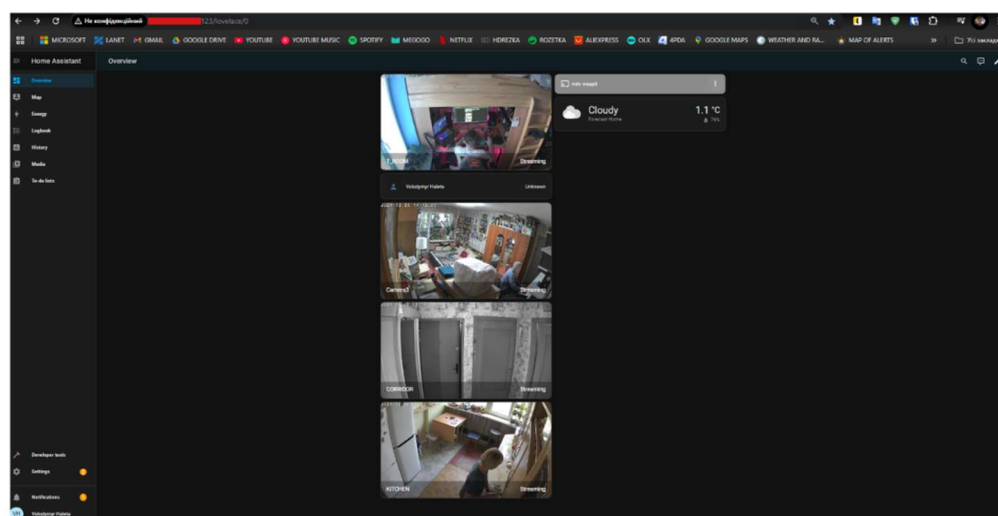


Рисунок 3.16 – Інтеграція камер з доповнення motionEye у інтерактивний дашборд веб-додатка Home Assistant

Завдяки використанню камер відеоспостереження як частини розумного будинку, можна навіть відмовитися від окремих датчиків руху – камери здатні самостійно виявляти рух у зоні їхнього огляду та виконувати різні автоматизовані дії, такі як вмикання чи вимикання світла. Такі рішення, як описані вище, дозволяють створювати розширені інтеграції, що виходять за межі традиційного підходу до розумного будинку, які відкривають нові можливості для використання інфраструктури не лише в приватних будинках, а й у більших масштабах, наприклад, у міських або сільських місцевостях, а також для об'єднання цих територій в єдину мережу (див. рис.3.12) [26, 27].

Вибір розширеної мережевої інфраструктури – TP-Link Archer. Можливість створення мереж на основі технології OneMesh або EasyMesh від TP-Link дозволяла об'єднувати кілька маршрутизаторів в єдину систему. Система EasyMesh дозволяє з'єднувати кілька маршрутизаторів або підсилювачів сигналу, створюючи єдине мережеве покриття з високою пропускну здатністю, а також використанням провідного «бекхола», що дозволяє обходити перешкоди, такі як залізобетонні стіни.

У такий спосіб, основний маршрутизатор TP-Link Archer AX73, який використовується у цьому проєкті, володіє досить високими характеристиками та підтримкою Wi-Fi 6, що забезпечує кращу швидкість передачі даних та більшу пропускну спроможність у порівнянні зі старішими стандартами. Другий маршрутизатор TP-Link Archer AX53, який виконує роль «сателіта», також підтримує Wi-Fi 6 (див. рис.3.17). (Додаток В)



Рисунок 3.17 – Маршрутизатори TP-Link Archer AX73 та AX53
(з'єднані у EasyMesh – провідним бекхолом)

Маршрутизатори TP-Link пропонують зручне віддалене керування через мобільний додаток Tether, що дозволяє користувачам не лише керувати маршрутизаторами з будь-якої точки світу, але й налаштовувати мережу, контролювати підключені пристрої та слідкувати за роботою системи.

До того ж, до головного маршрутизатора TP-Link Archer AX73 підключено джерело безперебійного живлення (див. рис.3.18), яке дозволяє працюючи лише від нього, пропрацювати 4 години 10 хвилин (зі оптичним терміналом), що зручно, якщо потрібно віддалено підключатися до будинку, використовуючи додатки від виробника.

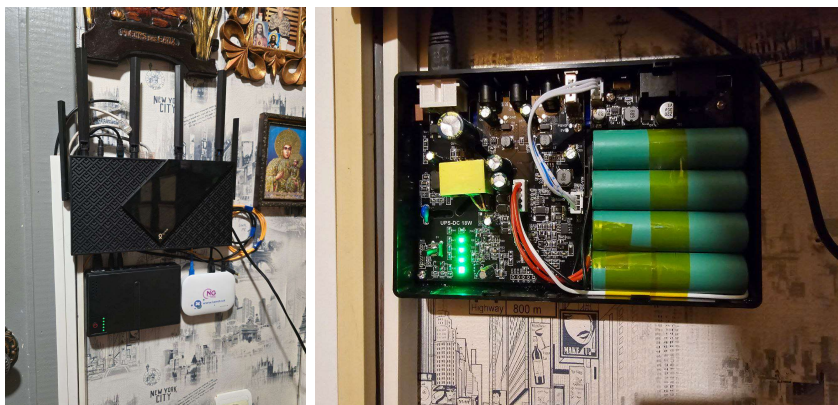


Рисунок 3.18 – Резервування мережевої інфраструктури завдяки DC1018P DC UPS 10400 mAh (~4 години 10 хвилин)

На даний момент у системі підключено близько 30 пристроїв (див. рис.3.19-3.20), але це число пов'язане зі розумним будинком, який використовує лише технологію Wi-Fi, але зменшиться внаслідок впровадження технології розумного будинку на базі протоколу Zigbee та розгортання власного сервера Home Assistant [26, 27].

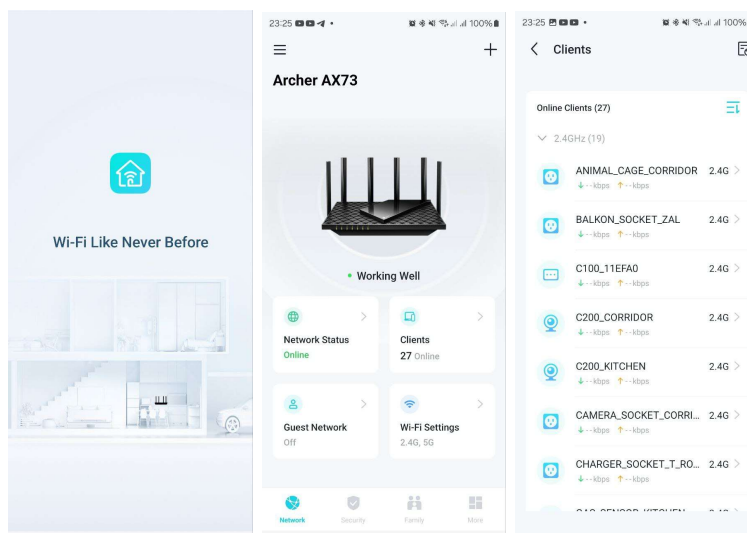


Рисунок 3.19 – Додаток Tether для маршрутизаторів TP-Link

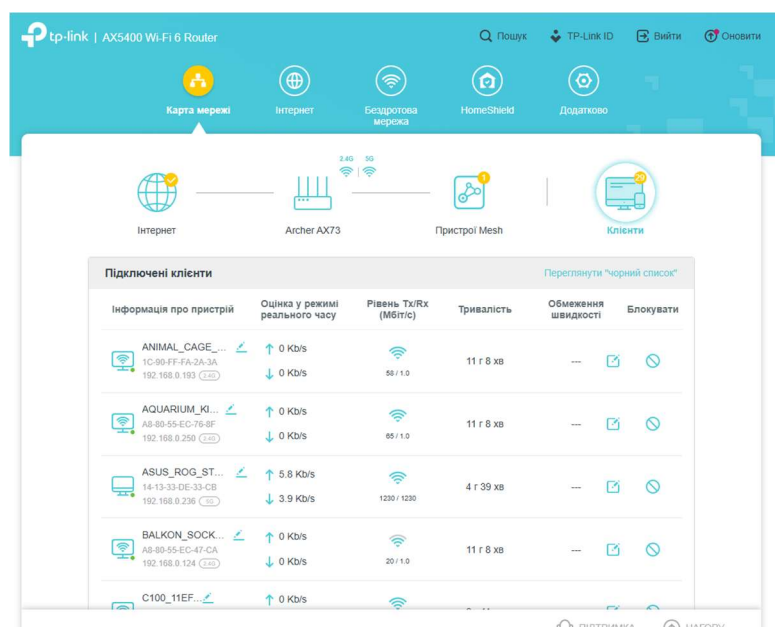


Рисунок 3.20 – Веб-сервіс TP-Link для маршрутизаторів TP-Link

3.2 Інтеграція машинного навчання у систему відеоаналізу

Розглядаючи детальніше інтеграцію технологій машинного навчання у системи відеоспостереження або інтелектуальні децентралізовані системи, стає очевидним, що цей підхід, хоч і є складнішим, але значно універсальнішим і

підходить для великих проєктів, де використовується велика кількість камер, об'єднаних у єдину систему.

Інтеграція машинного навчання у таких системах буде надзвичайно корисною, оскільки вона допомагає відфільтровувати зайві або помилкові спрацювання, які часто трапляються під час відеоспостереження (див. рис.3.21).

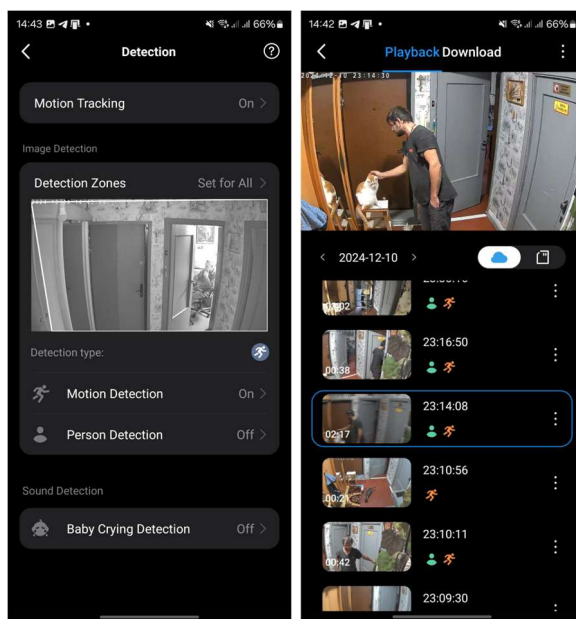


Рисунок 3.21 – Функції на основі машинного навчання у камер відеоспостереження (трекінг по зонам, детекція по руху, виявлення людини та плачу дитини)

Наприклад, стандартні хмарні сервіси чи сама камера можуть фіксувати рухи, які насправді не мають значення, як-от рухи дерев чи тіней, що в нічний час часто можуть викликати фальшиві спрацювання. Хоча у додатку Таро можна налаштувати зону виявлення руху для камери (див. рис.3.22), щоб обмежити область моніторингу, все ж є ймовірність помилкових сповіщень, коли камера реєструє рух, якого насправді немає, що особливо актуально у сутінках, коли тіні або рухи дрібних об'єктів можуть помилково розпізнаватися як рух людини. У таких ситуаціях, стандартні можливості камер стають недостатніми, і необхідно застосовувати більш складні рішення.

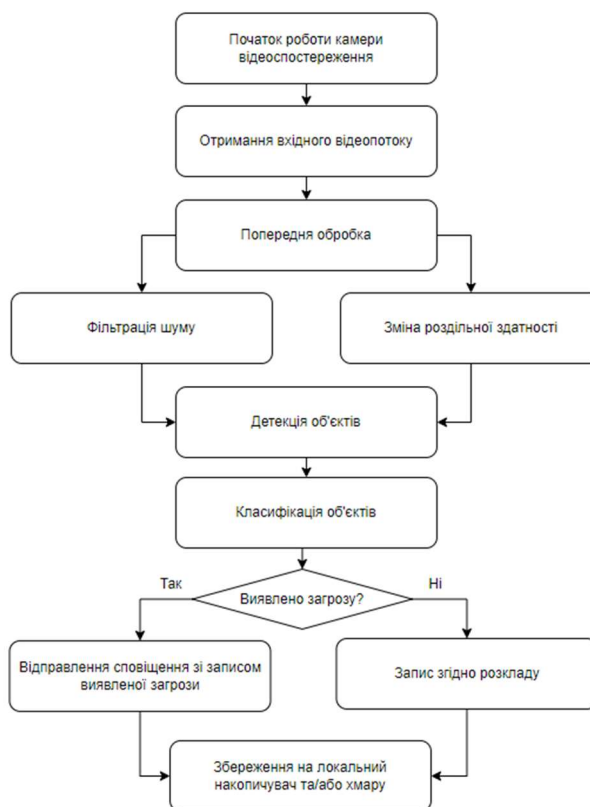


Рисунок 3.22 – Схема роботи машинного навчання на предмет шаблонної детекції та класифікації об’єктів

Інтеграція машинного навчання у системи відеоспостереження не тільки допомагає уникати фальшивих спрацювань, але й дозволяє автоматизувати важливі процеси. Наприклад, камери можуть бути використані не лише для спостереження, але й для взаємодії з іншими елементами розумного будинку або міста – це може бути автоматичне ввімкнення світла, коли виявляється людина в зоні дії камери, або активізація інших систем безпеки.

Сьогодні, інтелектуальні камери відеоспостереження активно використовуються в розумних містах для автоматичного виявлення різних порушень. Наприклад, камери можуть фіксувати швидкість автомобілів, розпізнавати номери транспортних засобів та автоматично надсилати дані до відповідних служб, які, у свою чергу, можуть надсилати водіям штрафи за перевищення швидкості або інші порушення. Ці камери, завдяки алгоритмам машинного навчання, можуть аизначити машину, фіксувати їх швидкість і передавати дані у реальному часі.

Інтелектуальні децентралізовані системи відеоспостереження стають все більш популярними завдяки своїй здатності самостійно обробляти великий обсяг інформації та застосовувати машинне навчання для підвищення ефективності моніторингу, що надає можливість не лише автоматизувати процеси в рамках розумного будинку або міста, але й підвищити загальну безпеку, інтегруючи камери з іншими системами, такими як датчики руху, освітлення, або ж системи контролю за трафіком.

Використання Home Assistant як єдина система. Home Assistant – це система, яка дозволяє встановлювати різноманітні доповнення або «аддони», що діють як контейнери, подібно до тих, що працюють через Docker. Розгорнути Home Assistant можна у різний спосіб, найпопулярніші з них – як ОС сервера, за допомогою віртуалізації, а також за допомогою контейнеризації через Docker Compose. Навіть якщо не було розгорнуто систему через Docker, Home Assistant все одно використовує контейнери для своїх «аддонів», що забезпечує їхню гнучкість – додавання, видалення або вимикання цих «аддонів» в будь-який момент, як це зазвичай робиться у контейнеризованих середовищах, але не надає можливість гнучко оновлювати та встановлювати «аддони», якщо Home Assistant було розгорнуто через Docker Compose [29].

Використання Home Assistant дозволяє об'єднувати відеоспостереження з іншими елементами розумного будинку або міста, такими як датчики руху, освітлення, безпека тощо в одну єдину систему (див. рис.3.15-3.16) [23, 26, 27].

Доповнення до Home Assistant – MotionEye. Якщо розглянути можливості машинного навчання в системі відеоаналізу, то це дозволяє уникати зайвих сповіщень про випадкові рухи, такі як рух дерев або тіні, які часто викликають помилкові тривоги. Одним із таких рішень є доповнення або «аддон» – MotionEye для Home Assistant (див. рис.3.15) [27], який також можна встановити як контейнер через Docker Compose чи обрати у списку «аддонів», якщо використовувався інший метод розгортання Home Assistant OS [29]. MotionEye дозволяє налаштовувати детекцію руху, як це роблять більшість комерційних додатків для камер відеоспостереження, але з додатковою перевагою – можливістю інтеграції великої

кількості камер від різних виробників, незалежно від того, чи камери знаходяться в одній мережі, чи мають доступ до інтернету, їх можна підключати і керувати ними навіть на великій відстані (див. рис.3.15-3.16) [27].

Крім базової детекції руху, MotionEye дозволяє моментально отримувати зображення або короткі відеофрагменти з камер у разі виявлення активності. Однак, без додаткового навчання системи, ця функція може призводити до надмірної кількості сповіщень, якщо камера фіксує непотрібні рухи, такі як випадкові об'єкти або тіні (див. рис.3.11) [27]. Щоб уникнути цього, система машинного навчання може бути навчена розпізнавати лише певні об'єкти, такі як автомобілі або люди в конкретних зонах спостереження.

MotionEye, як і всі «аддони» для Home Assistant, використовують YAML-файли для збереження конфігурацій. Мова YAML, яка застосовується для конфігураційних файлів, дозволяє створювати гнучкі і легко масштабовані рішення. Завдяки цьому, всі налаштування можуть зберігатися на міні-ПК або іншому сервері, що забезпечує постійне збереження важливих параметрів. У разі потреби, конфігурації можна легко експортувати та відновити на іншому пристрої. Приклад конфігураційного файлу, який можна використовувати для налаштування контейнера MotionEye (див. рис.3.23-3.24).

```
version: '3'
services:
  motioneye:
    image: ccrisan/motioneye:master-armhf
    container_name: motioneye
    ports:
      - "8765:8765"
    volumes:
      - /etc/motioneye:/etc/motioneye
      - /var/lib/motioneye:/var/lib/motioneye
    restart: unless-stopped
```

Рисунок 3.23 – Фрагмент конфігураційного файлу YAML
(для розгортання у вигляді контейнера через Docker Compose)

Один із прикладів використання MotionEye, окрім машинного навчання, – це налаштування запису відео не постійно, а лише в моменти, коли система виявляє рух, що був навчений через інтеграцію з машинним навчання, допомагаючи

економити місце на локальному сховищі та отримувати лише релевантні відеофрагменти. Записані дані можуть зберігатися на міні-ПК, наприклад, GMKtec NucBox K8 Plus (див. рис.3.12) [32], і відправлятися на сторонні сервіси, такі як Telegram-боти, для швидкого отримання сповіщень про події (див. рис.3.24) [40]. Така система працює в режимі автоматизації, дозволяючи налаштовувати різні сценарії дій, що підвищують ефективність та зручність відеоспостереження, забезпечуючи інтеграцію з іншими пристроями та сервісами.

```
automation:
- alias: 'Send alert on motion detection'
  trigger:
    platform: state
    entity_id: camera.motioneye_cam1
    to: 'motion_detected'
  action:
    - service: notify.telegram_bot
      data:
        message: "Виявлено рух на камері!"
        data:
          photo:
            - url: "http://<motioneye_ip>:8765/picture/1/current"
              caption: "Ось фото з камери"
```

Рисунок 3.24 – Фрагмент конфігураційного файлу YAML
(автоматизація: надсилання медіафайлів у Telegram)

Інтеграція машинного навчання з такими платформами, як Home Assistant і MotionEye, дає можливість використовувати сучасні моделі нейронних мереж для автоматизації та покращення функцій відеоаналітики [49, 50].

Одним із таких прикладів є YOLO (You Only Look Once) (див. 3.25) – модель, яка дозволяє розпізнавати та класифікувати об'єкти на відеозаписах, таких як люди, транспортні засоби або інші об'єкти [30, 31].

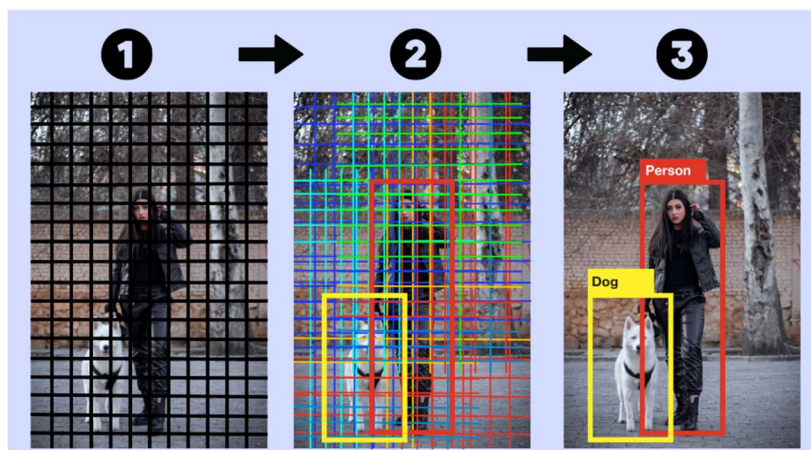


Рисунок 3.25 – Принцип роботи моделі YOLO для розпізнавання та класифікації об'єктів

Застосування цієї моделі на локальних пристроях, наприклад, на міні-ПК GMKtec NucBox K8 Plus (див. рис.3.12) [32], дозволяє значно знизити навантаження на мережу, оскільки обробка даних виконується локально, що зменшить необхідність передачі великих обсягів необроблених даних до хмарних сервісів і підвищує ефективність обробки відеопотоку. До того ж, така інтеграція машинного навчання забезпечує більш точну детекцію подій та класифікацію об'єктів відповідно до налаштувань користувача.

Окрім детекції та класифікації об'єктів, система може аналізувати поведінку, наприклад, виявляти нетипову активність – тривале перебування об'єкта в забороненій зоні або підозрілі маршрути руху. Завдяки можливостям навчання, система може самостійно адаптуватися на основі зібраних даних і автоматично реагувати на аномальні ситуації. Така технологія дозволяє використовувати відеоаналітику не тільки для будинку або прибудинкової території, а й у масштабах розумного міста, де інтелектуальні децентралізовані системи відеоспостереження допомагають управляти великою кількістю пристроїв [49, 50].

3.3 Забезпечення безпеки та захисту даних у децентралізованих системах

Для налаштування віддаленого керування важливою є увага до багатьох аспектів, особливо якщо ми плануємо створити систему, що базуватиметься на власній інфраструктурі. Такий підхід дозволить нам забезпечити кращу керованість системою, розвантажити її та отримати більше функціональних можливостей. Одним із ключових моментів є захист даних, особливо у випадках децентралізованих систем, таких як відеоспостереження. Для цього необхідно впроваджувати методи безпечної відправки та збереження даних, включаючи захищені з'єднання для віддаленого доступу. Наприклад, можна використовувати технології тунелювання через CloudFlare або застосовувати SSL-сертифікати для захисту переданих даних.

Протокол передачі даних RTSP. Якщо йдеться про передачу відеопотоків у цей момент, протокол RTSP є найпоширенішим для цього завдання (див. рис.2.3) [8, 9]. Він дозволяє передавати дані між відеокамерами та серверами або іншими системами відеоспостереження з мінімальною затримкою, що робить його ідеальним для роботи в реальному часі (див. рис.3.13-3.14) [25]. Окрім того, цей протокол підтримує масштабованість, що дозволяє обслуговувати велику кількість клієнтів. Завдяки цьому його можна інтегрувати в різноманітні системи з різними камерами сторонніх виробників, що надає можливість використовувати не тільки фірмові камери, але й сторонні рішення, забезпечуючи віддалений доступ у межах децентралізованої системи.

Домен для віддаленого доступу. Наша мета – створити систему віддаленого доступу до камер відеоспостереження, зокрема таких виробників, як TP-Link серії Таро, забезпечуючи роботу пристроїв у межах локальної мережі та віддаленого доступу. Для цього можна налаштувати захищений домен третього рівня, що дозволить забезпечити безпечне з'єднання без необхідності використання статичної IP-адреси. Таке рішення спрощує доступ до системи ззовні, дозволяючи

користувачам підключатися до камер відеоспостереження через інтернет. Хоча статична IP-адреса є бажаним варіантом, її використання не є обов'язковим.

Важливо розуміти, що такий захищений домен третього рівня забезпечить постійну точку доступу до системи для віддалених користувачів, спрощуючи налаштування і доступ, однак, для захисту цього з'єднання від потенційних атак ми плануємо використовувати SSL-сертифікати (див. рис.3.26) [33, 34]. Вони шифрують трафік і забезпечують безпеку з'єднання, знижуючи ризик компрометації домену. Без SSL-сертифіката система стає вразливою для злоумисників, які можуть легко скомпрометувати незахищений домен.

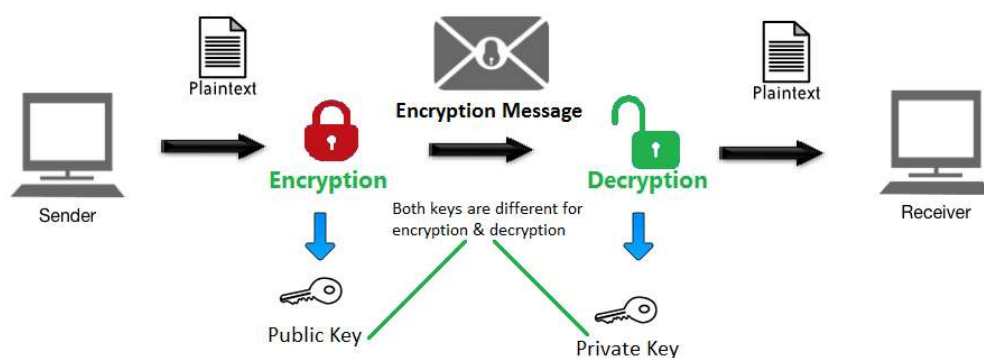


Рисунок 3.26 – Принцип роботи SSL-сертифікації

Отримання домену від виробника мережевого обладнання. Сучасне мережеве обладнання, особливо те, що мають покращений функціонал від виробника, хоча й коштують дорожче, пропонують значно більше можливостей. Наприклад, такі пристрої дозволяють легко інтегруватися з хмарними сервісами, багато з яких вже інтегровані в маршрутизатор. Маршрутизатори, як-от від TP-Link (див. рис.3.17), мають інтегровану підтримку хмарних сервісів, що дає можливість створювати домени третього рівня для віддаленого доступу.

TP-Link пропонує власний сервіс віддаленого доступу через захищене SSL-з'єднання, що дозволяє підключатися до локальної мережі без необхідності в додаткових хмарних сервісах. Наприклад, сервіс TP-Link DDNS дозволяє створювати домени третього рівня, що забезпечують вихід в інтернет і можливість

віддаленого доступу – це є значною перевагою, оскільки дозволяє використовувати зручні рішення для захищеного доступу до домашньої мережі (див. рис.3.27) [35].

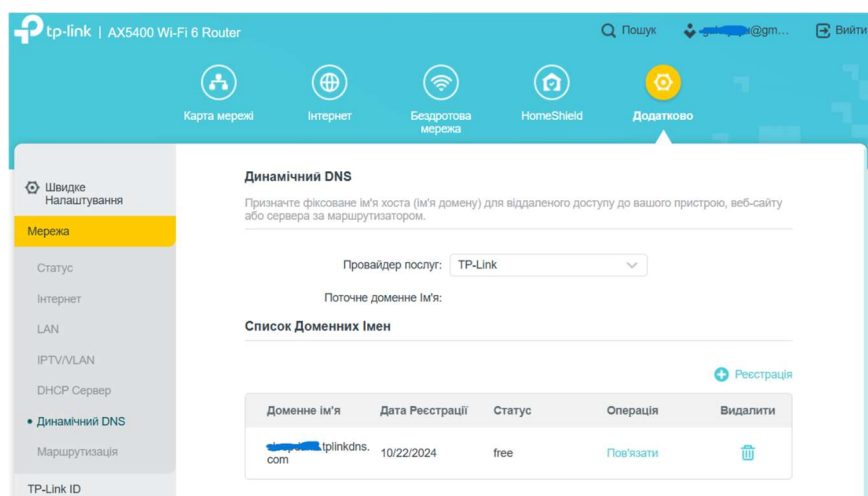


Рисунок 3.27 – Домен третього рівня за допомогою TP-Link

Проте інші виробники, такі як Keenetic, пропонують ще більш розширений функціонал. Їхні маршрутизатори дозволяють створювати домени з додатковими можливостями і розширеним налаштуванням безпеки.

Keenetic, наприклад, пропонує власний сервіс KeenDNS [36], який дозволяє створювати домени третього рівня з більшими можливостями налаштування, що надає змогу не тільки налаштовувати віддалений доступ, але й обмежувати доступ із зовнішніх мереж, забезпечуючи додатковий рівень захисту. Якщо домен відкритий без належного захисту або SSL-сертифіката, зломисники можуть легко скористатися цим, особливо якщо використовуються стандартні паролі. Вони можуть отримати доступ до маршрутизатора і, відповідно, до всієї мережевої інфраструктури, що створює значні ризики, включаючи можливість компрометації мережі або використання її в злочинних цілях.

Більшість користувачів стикаються з тим, що не мають статичних IP-адрес, а використовують динамічні або «сірі» IP-адреси, що може обмежувати деякі можливості налаштування, однак маршрутизатори від таких виробників, як TP-Link або Keenetic, надають інструменти для обходу цих обмежень, дозволяючи

використовувати домени третього рівня для віддаленого доступу. Такі рішення спрощують конфігурацію, роблячи доступ до мережі захищеним і стабільним.

Отримання домену від стороннього постачальника послуг. Якщо маршрутизатор або виробник не надає можливості налаштування домену третього рівня своїми ресурсами, можна скористатися сторонніми сервісами, такими як CloudFlare (див. рис.3.28) [37]. Такий сервіс корисний тим, коли немає статичної IP-адреси, або коли маршрутизатор не підтримує налаштування безпечного віддаленого доступу. Сервіси на зразок CloudFlare надають можливість організувати захищене з'єднання між віддаленими користувачами і локальною системою, наприклад, відеоспостереження, без потреби відкривати порти на маршрутизаторі, що потенційно може створити ризики для безпеки.

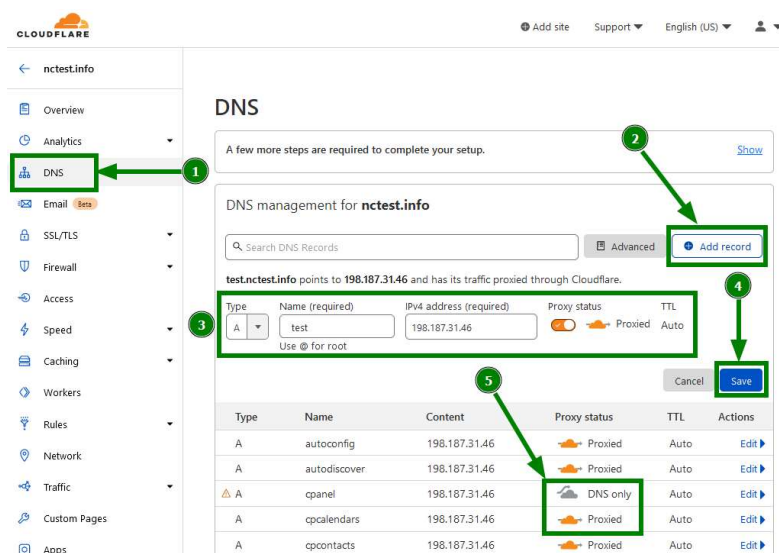


Рисунок 3.28 – Домен третього рівня за допомогою CloudFlare
(покрокова інструкція для реєстрації нового домена)

CloudFlare дозволяє створювати захищені з'єднання через хмарну платформу CloudFlare, забезпечуючи шифрування трафіку та захист даних за допомогою SSL-сертифікатів [37]. Однією з головних переваг цього рішення є те, що для його роботи не потрібна наявність статичної або «білої» IP-адреси, а також відсутня необхідність відкривати порти на маршрутизатор, що робить можливим віддалений

доступ із будь-якої мережі, з високим рівнем захисту завдяки SSL-сертифікатам, які складно зламати.

Після створення домену третього рівня через CloudFlare, його можна легко інтегрувати в систему, наприклад, в Home Assistant за допомогою спеціального «аддона» CloudFlare [38]. Налаштування включає в себе додавання сертифікату SSL для шифрування даних, що запобігає перехопленню та несанкціонованому доступу до конфіденційної інформації, такої як відеоматеріали з камер спостереження, навіть якщо передача відбувається поза межами локальної мережі.

Важливо відзначити, що сертифікати SSL, доступні через CloudFlare, захищають дані на всіх етапах їх передачі, що робить цей підхід дуже ефективним для створення безпечної та надійної інфраструктури віддаленого доступу. Окрім того, це рішення дозволяє зберігати контроль над системою, оскільки виробники камер спостереження, наприклад TP-Link, зазвичай самостійно забезпечують захист даних через свої сервери.

Використовуючи сервіси на кшталт CloudFlare, можливо налаштувати систему під свої потреби, забезпечуючи гнучкий захист і контроль за допомогою домену третього рівня та шифрування SSL, навіть якщо маршрутизатор не підтримує таку функцію безпосередньо. Таке рішення також підходить для реалізації інтелектуальної децентралізованої системи відеоспостереження, забезпечуючи безпечний вихід в інтернет і шифрування на всіх етапах передачі даних, що є гнучким і надійним підходом для віддаленого моніторингу та управління системою спостереження.

Альтернативні методи захисту під час використання віддаленого доступу. Крім використання домену третього рівня та SSL-сертифікату для шифрування даних і захисту трафіку, безпеку системи можна суттєво підвищити за допомогою інших методів, таких як багаторівнева автентифікація і контроль доступу.

Безпека будь-якої системи не обмежується лише шифруванням; важливими аспектами є також захист облікових записів користувачів та лімітувати прихід ресурсам на основі ролей. Наприклад, розглянемо варіант камери відеоспостереження TP-Link серії Таро (див. рис.3.3) (Додаток А), які

використовують хмарну інфраструктуру від виробника. Спочатку треба зареєструватись одним акаунтом, до якого будуть прив'язані всі камери. Навіть якщо планується використовувати власну інфраструктуру для керування камерами, доступ до пристроїв через RTSP (порт 554) – спочатку його потрібно увімкнути за допомогою налаштувань, наданих виробником (див. рис.3.13-3.14) [25].

TP-Link, як і багато інших сучасних виробників, надає можливість двофакторної автентифікації (2FA): це може бути автентифікація через push-сповіщення в мобільному додатку, електронну пошту або інші засоби багаторівневого підтвердження особи.

2FA допомагає отримати надрівень безпеки, бо для авторизації потрібен не лише пароль, а спеціальний код, що постійно міняється, тому такий захист знижує ризик несанкціонованого доступу.

Для генерації цих кодів зазвичай використовуються спеціальні додатки, такі як Google Authenticator або Microsoft Authenticator та інші (див. рис.3.29) [39]. Ці додатки працюють на основі унікального 16-значного ключа, який генерує одноразові коди для підтвердження доступу. Але, важливо розуміти, що якщо цей 16-значний ключ потрапить до рук зловмисника, він зможе налаштувати аутентифікатор на власному пристрої і отримувати ті ж самі коди для доступу. Тому, незважаючи на високий рівень захисту, важливо обережати цей ключ і не передавати його стороннім особам.

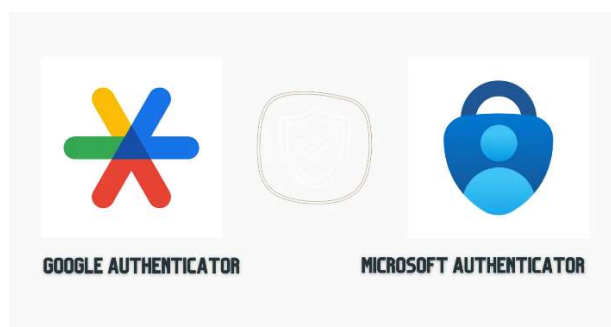


Рисунок 3.29 – Двофакторна автентифікація
(Google Authenticator vs Microsoft Authenticator)

3.4 Розподіл обчислювальних ресурсів між вузлами системи

Розглядаючи більш детально принцип розподілу ресурсів між вузлами системи, то можна побачити, що навіть використання камер TP-Link серії Таро (див. рис.3.4) (Додаток А) включає розподіл завдань між самими камерами та хмарними сервісами виробника, що дозволяє значно зменшити навантаження на інфраструктуру як камери, так і хмару. Наприклад, коли камера працює у режимі запису 24/7 або при виявленні руху, всі обчислювальні процеси, пов'язані із записом та обробкою відео, виконує сама камера, тоді як сповіщення про події передаються на хмарні сервери виробника.

Такий підхід знижує навантаження на хмарні сервіси, зменшує енергоспоживання камер і забезпечує ефективний розподіл ресурсів між системними вузлами. Хмарні сервіси можуть виконувати лише допоміжні функції, наприклад, обробляти базові обчислювальні завдання, а сама камера записує та передає дані або зберігає їх локально, не витрачаючи багато енергії. Камери відеоспостереження TP-Link серії Таро мають значно нижчий бітрейт, меншу кількість кадрів в секунду та нижчу якість зображення порівняно з, наприклад, камерами смартфонів, що також сприяє економії енергії (див. рис.1.14, 3.8, 3.9).

Якщо розглядати сценарій використання не лише хмарної інфраструктури виробника, а й локальних систем, наприклад, інтеграції камер TP-Link серії Таро у домашню систему через протокол RTSP, налаштування безпеки та підключення до Home Assistant через «аддон» MotionEye, то це дозволяє передавати відео потоки на локальні сервери для подальшої обробки та зберігання даних (див. рис.2.3, 3.11, 3.12) [8, 9, 23, 26, 27]. У цьому випадку камера може автономно виконувати детекцію руху та надсилати сповіщення про події на Telegram-бот або інші системи (див. рис.3.24) [40], а обробку відеопотоків можна перенести на центральний вузол системи, наприклад, на міні-ПК на кшталт GMKtec NucBox K8 Plus (див. рис.3.12) [32].

Вузол системи – сервер. Використання таких локальних вузлів, як власний сервер на базі міні-ПК GMKtec NucBox K8 Plus (див. рис.3.12) [32], дозволяє знизити навантаження на камери та хмару, оскільки всі відео-дані зберігаються локально, а обробка та аналіз виконуються на центральному вузлі. Такий вузол може виконувати більш складні завдання, наприклад, обробку відео за допомогою машинного навчання для розпізнавання облич, транспортних засобів чи аналізу інших специфічних подій.

Також такий міні-ПК може виступати єдиним вузлом для всіх підключених камер, що дозволяє зберігати дані централізовано, замість доступу до кожної окремої камери через хмарні сервіси, що робить управління та доступ до записів більш зручним і ефективним. Замість завантаження даних з хмари, які можуть бути обмеженими підпискою та займати час, локальна система на базі міні-ПК дозволяє швидше отримувати доступ до відеоматеріалів і значно знижує загальне навантаження на камери та хмарні ресурси.

Міні-ПК може бути ефективно використаний як локальний обчислювальний вузол у концепції Fog Computing (див. рис.2.6) [12, 13]. Він працює безпосередньо на місці встановлення камер відеоспостереження або навіть поза ним, виконуючи обробку даних локально (див. рис.3.30), що дозволяє зменшити затримки та обсяг переданих даних до хмари, що є важливим для оптимізації системи. Лише значущі події або архіви відео передаються на хмарне зберігання, тоді як локальний вузол здатний обробляти події в реальному часі. Такий підхід дозволяє проводити швидкий аналіз і реакцію на критичні ситуації, не вимагаючи передачі великих обсягів даних через мережу.

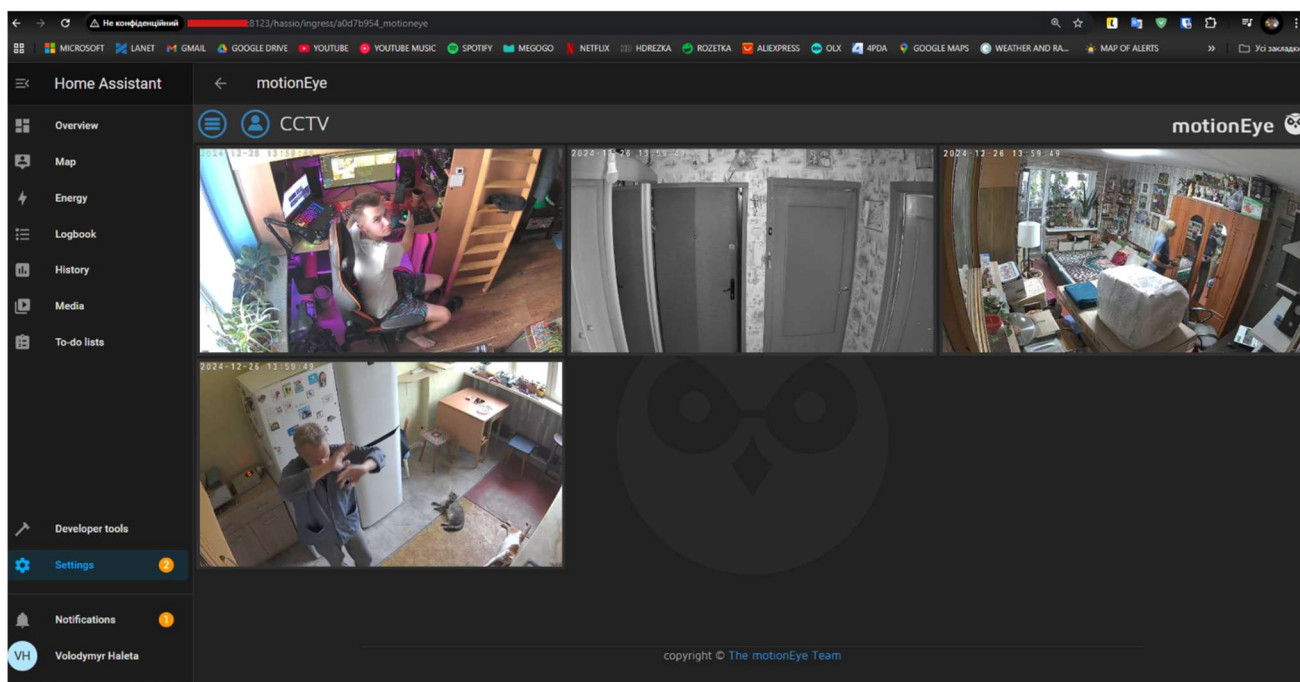


Рисунок 3.30 – Камери відеоспостереження підключенні до сервісу Home Assistant через доповнення motionEye

До того ж, міні-ПК дозволяє зберігати та аналізувати великі обсяги даних за допомогою хмарних сервісів, коли це необхідно, зокрема для довготривалого зберігання відеоматеріалів чи проведення глибшого аналізу. Хмарні сервіси можуть використовуватися не тільки від сторонніх компаній, таких як Amazon, Microsoft, Google, але й можуть бути побудовані на базі локальної інфраструктури, що дає гнучкість і контроль над даними (див. рис.2.1, 2.2) [6, 7]. При цьому системи відеоспостереження зазвичай містять кілька камер, що підключені до наявної інфраструктури, яка може складатися з міні-ПК, локальних серверів (див. рис.3.3, 3.31) або хмарних рішень від виробників.

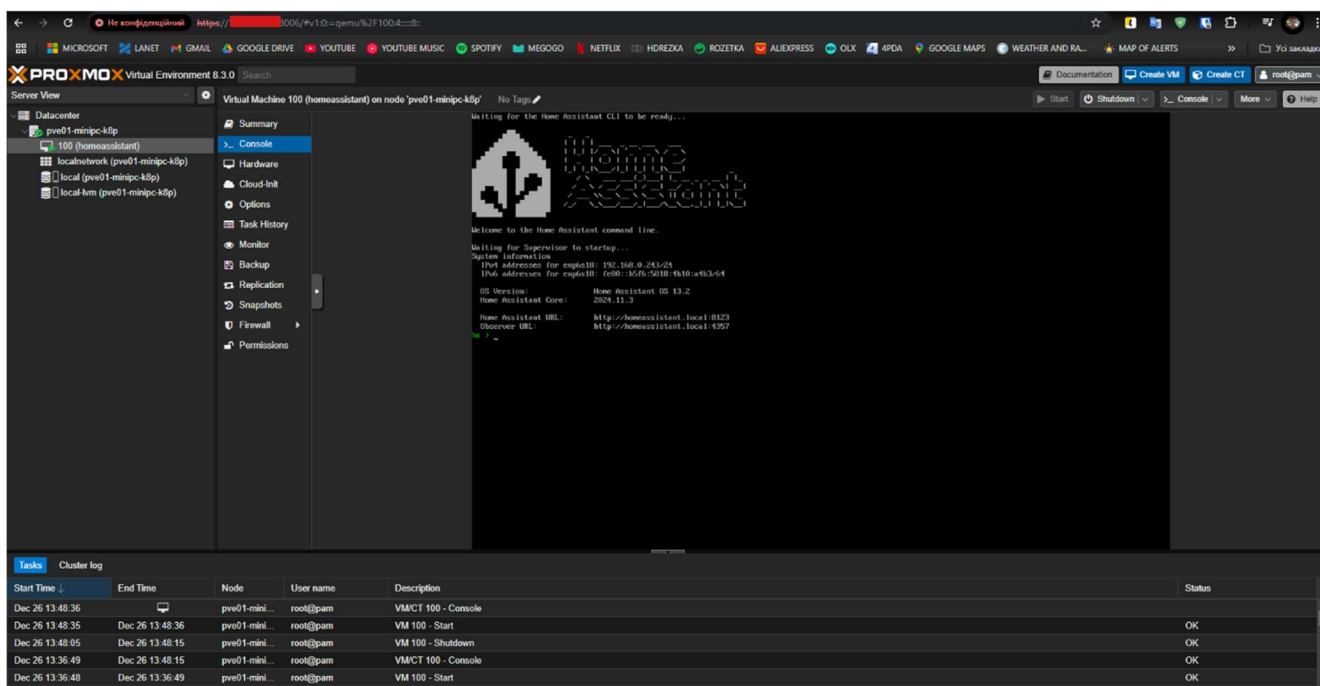


Рисунок 3.31 – Ініційований сервіс Home Assistant на міні-ПК для роботи 24/7

Використання міні-ПК дозволяє розвантажити інфраструктуру, оскільки цей локальний вузол бере на себе значну частину обробки даних (див. рис.3.32), знижуючи навантаження на хмару та камери.

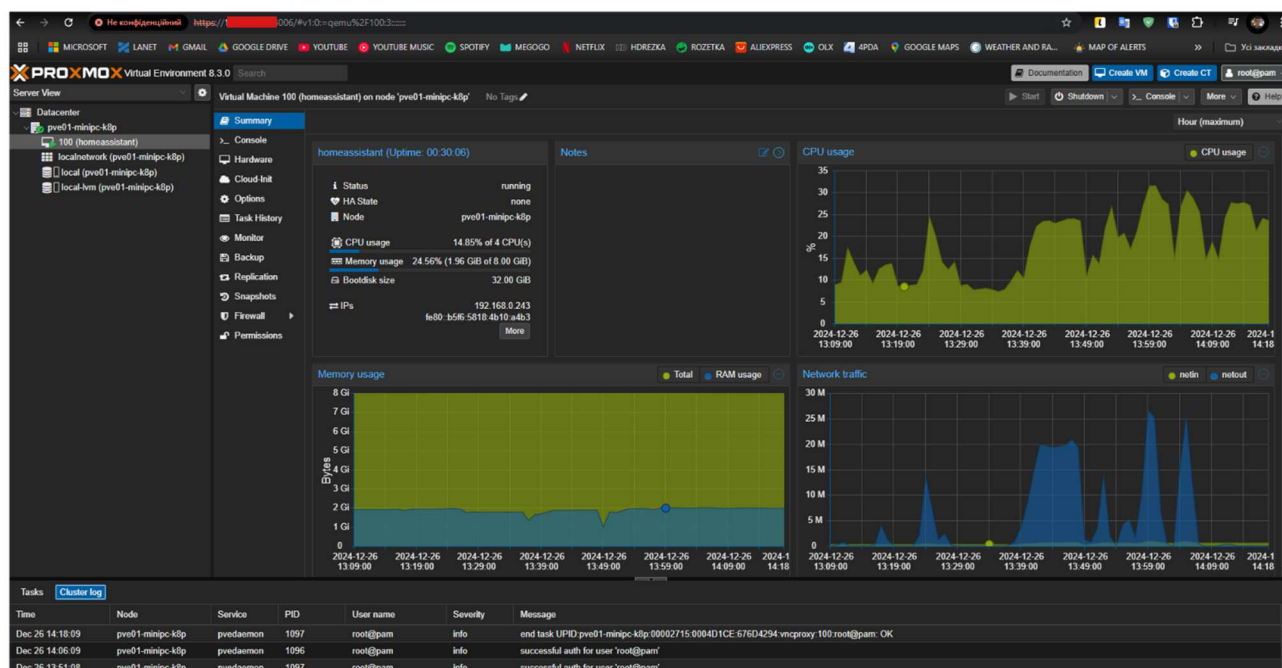


Рисунок 3.32 – Гнучкий контроль над запущеними вузлами завдяки гіпервізору 1-го типу Proxmox

Вузол системи – сховище даних. Ще однією перевагою використання локального сервера є можливість зберігання відео на зовнішніх дисках, що зменшує залежність від обмежених обсягів пам'яті у камерах або від хмарних сховищ, доступ до яких надається лише за підпискою. Використовуючи зовнішні накопичувачі, можливо зберігати дані значно довше, ніж один місяць, як це зазвичай передбачено умовами хмарних сервісів. У випадку з локальними рішеннями, можна зберігати відеоматеріали протягом тривалого часу, наприклад, кілька місяців або навіть рік, залежно від обсягу пам'яті на зовнішньому диску.

Вузол системи – мережеве обладнання. Для стабільної передачі відеоданих важливим аспектом є якісне мережеве обладнання. У випадку великої кількості підключених пристроїв, таких як камери відеоспостереження та інші пристрої розумного будинку, стабільна передача відеопотоків потребує оптимізації мережевих ресурсів. Наприклад, маршрутизатори TP-Link, такі як Archer AX73, можуть підтримувати до 200 пристроїв (див. рис.3.17). (Додаток В).

Таблиця 3.2 – Специфікація обладнання із зазначенням кількості та вартості

№	Найменування обладнання/сервіси	К-сть	Орієнтовна ціна за одиницю (грн)	Загальна вартість (грн)
1	Маршрутизатор TP-Link Archer AX73	1	4 999	4 999
2	Маршрутизатор TP-Link Archer AX53	1	2 799	2 799
3	Маршрутизатор TP-Link Archer C64	1	1 399	1 399
4	Камера відеоспостереження TP-Link Таро C100	1	1 099	1 099

Продовження таблиці 3.2 – Специфікація обладнання із зазначенням кількості та вартості

№	Найменування обладнання/сервіси	К-сть	Орієнтовна ціна за одиницю (грн)	Загальна вартість (грн)
5	Камера відеоспостереження TP-Link Tapo C200	3	1 499	4 497
6	Камера відеоспостереження TP-Link Tapo C310	1	1 999	1 999
7	Карта пам'яті Kingston 128GB microSDXC Class 10 Canvas Select Plus	5	419	2 095
8	TP-Link Tapo Care (підписка на хмарний сервіс)	2	95 (на міс.)	190 (на міс.)
9	Джерело безперебійного живлення DC1018P DC UPS 10400 mAh	3	1 100	3 300
10	Міні-ПК GMKtec K8 Plus	1	15 200 (без комплектації) 29 000 (з)	29 000
11	Гіпервізор 1-го типу Proxmox	1	безкоштовно	безкоштовно
12	Home Assistant OS	1	безкоштовно	безкоштовно
Разом:				51 377 грн

РОЗДІЛ 4 ВПРОВАДЖЕННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ В РІЗНИХ УМОВАХ ЕКСПЛУАТАЦІЇ

4.1 Використання систем в урбанізованих зонах

Інтелектуальні децентралізовані системи відеоспостереження можуть бути особливо корисні для масштабних проєктів, таких як системи «розумного міста». У таких випадках потрібно встановлювати велику кількість камер відеоспостереження, мінімізуючи складність комутацій та з'єднань. Замість традиційного підключення, такі камери можуть використовувати лише живлення, а обробка даних відбуватиметься децентралізовано (див. рис.4.1) [41].



Рисунок 4.1 – Інтелектуальні децентралізовані системи відеоспостереження в урбанізованій місцевості

Важливим аспектом таких систем є те, що відеодані можуть надсилатися на хмарні сервіси, наприклад, Amazon Kinesis (див. рис.2.5, 2.7) [11], або на власні сервери компанії, що дозволяє інтегрувати обробку даних на локальних або хмарних платформах, залежно від потреб проєкту.

Найчастіше такі системи будуть застосовуватися в урбанізованих зонах: на вулицях, площах, громадських місцях і дорогах. В умовах високої щільності інфраструктури та населення, децентралізовані системи забезпечують безпеку, знижуючи навантаження на центральну інфраструктуру. Хоча традиційні системи відеоспостереження теж успішно працюють, вони мають певні обмеження, оскільки управління виконується централізовано, що робить їх вразливими до помилок або збоїв у центральному вузлі (див. рис.1.6) [2].

Децентралізовані інтелектуальні системи, які можуть використовувати, наприклад, потужні хмарні рішення від Amazon Kinesis (див. рис.2.5, 2.7) [11] або власні сервери (див. рис.3.12) [32], дозволяють обробляти дані з багатьох камер ефективніше. Це також зручно для масштабних проєктів, де потрібна автоматизація та можливість аналізу великих обсягів даних в режимі реального часу через єдиний інтерфейс, такий як веб-додаток або інше інтегроване рішення.

Камери відеоспостереження, що встановлюються в громадських місцях, давно забезпечують безпеку та спостереження за об'єктами. Однак у централізованих систем є певні недоліки, адже в разі помилки або неправильної конфігурації у центрі управління може виникнути ризик втрати доступу до відео в критичних ситуаціях (див. рис.1.6) [2]. Впровадження децентралізованих систем допоможе уникнути таких проблем, оскільки кожна камера може бути частиною автономної обчислювальної структури, а обробка даних може виконуватися локально або на хмарних серверах.

Іноді можна зіткнутися з проблемою недоступності даних з певних камер у системах відеоспостереження, або в деяких місцях можуть використовуватися муляжі замість справжніх камер. Такі «псевдокамери» не виконують функції відеоспостереження і не можуть забезпечити належну безпеку (див. рис.4.2).



Рисунок 4.2 – «Псевдокамери» або «муляж» камер відеоспостереження

Саме тому важливо впроваджувати глобальні рішення, наприклад, створювати великі інтелектуальні децентралізовані системи відеоспостереження, що передбачає побудову системи, що складається з безлічі автономних підсистем відеоспостереження, де кожна камера або система працює незалежно одна від одної (див. рис.4.1) [41].

Ці системи не обов'язково будуть під'єднані до однієї локальної мережі, але вони зможуть передавати дані до загальної мережі з використанням надійного захисту. Таким чином, кожна камера, встановлена на вулицях, може функціонувати як частина уніфікованої системи (див. рис.4.1) [41]. Якщо всі ці камери будуть інтегровані в єдину систему, вони зможуть обробляти дані в реальному часі, надаючи можливості для аналітики та прогнозування подій зі використанням найновіших методів машинного навчання, що дозволить підвищити ефективність відеоспостереження і значно покращити його функціонування.

Глобальні системи відеоспостереження можуть функціонувати повсюдно – в містах, громадських місцях, і навіть у важкодоступних локаціях, що дозволить збирати та аналізувати дані з різних джерел у централізованому пункті управління, з якого можна здійснювати моніторинг та контролювати всі підключені системи (див. рис.4.1) [41]. Використовуючи такі можливості, система зможе функціонувати подібно до пошукової системи, як, наприклад, Google, що дозволить швидко знайти необхідні моменти у відеозаписах.

Нині існуючі системи відеоспостереження часто не пов'язані між собою, і це створює певні незручності. Якщо виникає інцидент, і камера була налаштована неправильно, дані можуть бути втрачені, що ускладнює розслідування. Для уникнення таких ситуацій необхідно впроваджувати не лише камери, але й забезпечити їх надійний захист. Камери можуть бути підключені до локальних мереж або передавати дані через захищені зовнішні мережі до контрольного пункту.

Камери можуть передавати свої дані безпроводними методами, наприклад, через Wi-Fi, але це потребує розгортання точок доступу в необхідних місцях. Також можна інтегрувати камери з мобільною інфраструктурою, наприклад, використовуючи мобільний інтернет або технології на основі GSM для передачі даних, як це роблять мобільні вишки. Проте це може бути ресурсомістким рішенням для мобільних операторів, тому краще використовувати альтернативні інфраструктурні рішення, зокрема, для реалізації масштабних проєктів у великих містах. Для міст можна також розгорнути мережі через Ethernet-кабелі, але це потребує встановлення кабельної інфраструктури. Однак безпроводні технології, такі як Wi-Fi, також залишаються перспективними, за умови правильної організації та захисту мереж.

У ситуаціях, коли можливі перебої в електропостачанні або часті відключення електроенергії, надзвичайно важливо забезпечити постійне та безперебійне живлення для систем відеоспостереження. Для цього можна використовувати альтернативні джерела енергії, такі як сонячні панелі або вітрякові установки, які здатні забезпечити автономність роботи системи навіть за відсутності основного джерела живлення. Також, крім альтернативних джерел, можна впровадити рішення на основі джерел безперебійного живлення (ДБЖ), які складаються з акумуляторних батарей і контролерів заряду.

Під час нормальної роботи міської електромережі система живиться від основного джерела електроенергії, при цьому акумулятори ДБЖ залишаються зарядженими. У разі відключення електроенергії, система автоматично перемикається на акумулятори, що дає змогу безперебійно продовжувати роботу

камер відеоспостереження. Камери відеоспостереження, особливо ті, що використовуються в інтелектуальних децентралізованих системах, споживають мінімальну кількість електроенергії, оскільки є енергоефективними пристроями. Наприклад, одна така камера може споживати лише кілька ват енергії (див. рис.1.14), що навіть менше, ніж типовий маршрутизатор.

Таким чином, навіть невеликий ДБЖ з чотирма акумуляторами може забезпечувати живлення для такої камери до 20 годин безперервної роботи. При цьому час зарядки акумуляторів може становити лише кілька годин, що дозволяє забезпечити значну автономність системи в умовах відсутності живлення, що робить такі рішення дуже ефективними (див. рис.4.3-4.4).



Рисунок 4.3 – Забезпечення автономності інтелектуальній камері відеоспостереження у якості ДБЖ (максимальне споживання 5.4 Вт, ~20 годин автономності зі ДБЖ)

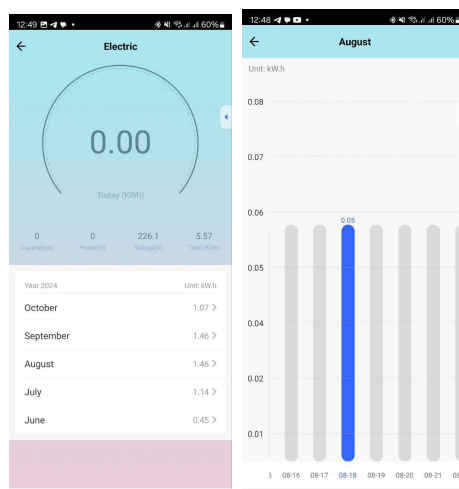


Рисунок 4.4 – Рівень споживання електроенергії однієї інтелектуальної камери відеоспостереження (за допомогою додатка Smart Life та розумної розетки)

4.2 Особливості впровадження у важкодоступних та віддалених місцевостях

Коли йдеться про впровадження проєктів у масштабних урбанізованих умовах, такі проєкти вимагають більш ретельного планування та використання різноманітних рішень, як готових, так і адаптованих під конкретні потреби інфраструктури. Інвестиції в інфраструктуру є необхідними, і для цього існують різні підходи до впровадження систем відеоспостереження, зокрема інтелектуальних децентралізованих камер, особливо в умовах віддалених або важкодоступних місцевостей.

Проєкти такого типу можуть бути значно меншими за масштабом у порівнянні з великими міськими системами, що охоплюють сотні або тисячі камер. У віддалених районах може бути необхідність встановити лише одну або кілька камер, які функціонуватимуть локально. Такі системи можуть використовувати як хмарні технології, надані виробниками камер відеоспостереження, так і локальні рішення, наприклад, сервери на базі міні-ПК. У таких системах можуть бути встановлені 10-15 камер, але навіть менша кількість може бути достатньою для задоволення потреб в окремих регіонах.

Особливості впровадження інтелектуальних децентралізованих камер полягають у тому, що вони не потребують таких великих обчислювальних ресурсів або складної інфраструктури, як традиційні камери, що підключаються до відеореєстраторів через коаксіальні кабелі та мережеве обладнання.

Інтелектуальні системи можуть функціонувати автономно, передаючи дані безпосередньо в хмару або на локальний сервер, що значно спрощує процес впровадження. Як приклад, використання таких камер у важкодоступних місцях, як-от ліфти, є ефективним рішенням. Ліфт – це місце, де складно встановити традиційні відеореєстратори чи прокласти додаткові кабелі. В таких умовах інтелектуальна камера, яка працює автономно, може забезпечити всі необхідні

функції відеоспостереження без складних додаткових налаштувань інфраструктури (див. рис.4.5) [42, 48].



Рисунок 4.5 – Інтелектуальні децентралізовані системи відеоспостереження у важкодоступних та віддалених місцевостях

Для таких умов оптимальним рішенням буде створення безпроводною мережі із застосуванням точок доступу, які можна розташувати вздовж шахти ліфта – ці точки будуть забезпечувати стабільне з'єднання під час руху ліфта, що дозволить отримувати безперервний відеосигнал з кабіни (див. рис.4.5) [42, 48]. Використання міні-ПК для обробки даних на місці може бути недоречним, оскільки можна використовувати віддалені сервери та послуги виробників камер, які забезпечують обробку та зберігання даних на своїх хмарних платформах.

Такі рішення можна застосовувати не лише у рухомих ліфтах, а й у важкодоступних місцевостях, таких як сільські райони або навіть гірські території, де фізичний доступ до камер може бути обмеженим. У таких випадках також можна використовувати системи безперебійного живлення (ДБЖ) для забезпечення роботи камер у випадку перебоїв з електропостачанням (див. рис.4.3). Камери відеоспостереження, оснащені інтелектуальними функціями, можуть автоматично переключатися на резервне живлення та передавати аварійні сигнали у разі виникнення критичних ситуацій, наприклад, коли людина застрягла в ліфті.

Такі системи можуть працювати автоматично, зокрема надсилати екстрені сповіщення до відповідних служб у випадку виявлення небезпеки, що схоже на

рішення, де застосовуються для фіксації порушень правил дорожнього руху, коли камери автоматично фіксують перевищення швидкості та надсилають сповіщення порушникам. У випадку з ліфтами система може автоматично викликати аварійні служби для визволення людини, якщо та «застрягла».

Камери можна також встановлювати в інших важкодоступних місцях, як-от гірські райони, де високий рівень ризику для туристів. В таких умовах інтелектуальні камери можуть передавати інформацію про аномальну поведінку чи стан місцевості різко змінюється, наприклад, якщо турист занадто довго перебуває на одному місці або демонструє незвичну активність, і такі системи можуть автоматично надсилати екстрені сигнали для виклику рятувальних служб (див. рис.4.6) [43].

Завдяки енергоефективності (див. рис.1.14), компактності та можливості працювати на основі безпроводних технологій, інтелектуальні камери відеоспостереження можна легко впроваджувати у важкодоступних місцях. Для передачі даних можна використовувати інфраструктуру мобільних операторів, зокрема LTE – це зробить такі системи ефективними навіть у віддалених регіонах, де немає необхідності у встановленні великої кількості камер або будівництві складної мережевої інфраструктури (див. рис.4.6) [43].

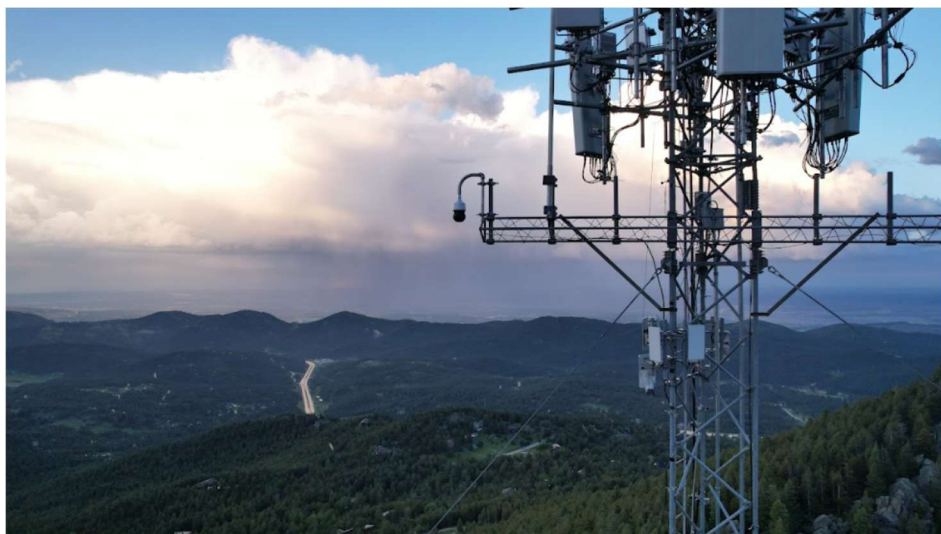


Рисунок 4.6 – Інтелектуальні децентралізовані системи відеоспостереження у важкодоступних та віддалених місцевостях зі використанням LTE

4.3 Оцінка ефективності децентралізованих систем у різних середовищах

Інтелектуальні децентралізовані системи відеоспостереження мають універсальні характеристики, які дозволяють їм бути ефективними в різних середовищах – від міських зон до віддалених і важкодоступних місць, таких як сільська місцевість. Оцінюючи ефективність таких систем, важливо враховувати ключові показники, серед яких споживання електроенергії, продуктивність і надійність під час різних навантажень.

Мінімальне споживання енергії. Енергоспоживання відеоспостережних систем стає критично важливим фактором, особливо у віддалених регіонах, де є обмежений доступ до енергоресурсів або можливі часті перебої з постачанням електрики. У таких умовах використання енергоефективних камер відеоспостереження стає важливим рішенням для забезпечення стабільної роботи системи. Камери споживають мінімальну кількість енергії, що підтверджується багатьма прикладами високої енергоефективності цих пристроїв. До того ж, такі системи можна оснастити безперебійними джерелами живлення (ДБЖ), що дозволяє їм працювати до 20 годин лише від кількох акумуляторів ємністю 2700–2800 мАг, що особливо важливо під час перебоїв у постачанні електроенергії (див. рис.1.14).

Для оптимізації роботи системи можна використовувати міні-ПК як обчислювальні вузли (див. рис.3.12) [32] або як частини розподілених систем обробки даних (Fog Computing) (див. рис.2.6) [12, 13]. Вони допомагають зменшити навантаження на хмарні сервери або на самі камери, однак їх споживання електроенергії, хоч і мінімальне, все ж вище, ніж у самих камер (див. рис.1.14). Тому в деяких випадках, зокрема при автономній роботі в умовах віддалених регіонів, можна покладатися на готові хмарні рішення, запропоновані провайдерами, такими як Amazon або виробниками самих камер (див. рис.2.5) [11].

Системи відеоспостереження навіть під час пікових навантажень споживають незначну кількість енергії, тобто камери споживають всього кілька ватів енергії, навіть при постійному записі, що дозволяє їм працювати автономно протягом тривалого часу. Завдяки такій низькій енергоємності, інтелектуальні децентралізовані системи можуть успішно використовуватися в умовах віддалених і важкодоступних місць, забезпечуючи високу ефективність роботи з мінімальними витратами на енергоресурси.

«Модульність» систем. Продуктивність інтелектуальних децентралізованих систем відеоспостереження значною мірою залежить від вибору інфраструктури: чи це буде інфраструктура, надана виробником, чи власні ресурси для обробки даних. Якщо система повністю базується на рішеннях виробника, то її продуктивність багато в чому залежатиме від постійного доступу до Інтернету для передачі та отримання даних – у такій моделі існує ризик виникнення затримок через віддалену обробку даних у хмарі. Наприклад, при використанні хмарних сервісів на кшталт Amazon Kinesis затримка може бути помітною, що вплине на швидкість обробки інформації та прийняття рішень (див. рис.2.5, 2.7) [11].

Альтернативою може бути використання локальних обчислювальних потужностей, таких як міні-ПК (див. рис.3.12) [32], які дозволяють виконувати обробку даних поблизу системи відеоспостереження, що дозволяє значно покращити прямий, без затримок, зв'язок та підняти загальну швидкість системи, особливо в реальному часі. Такі рішення, що використовують локальні сервери для обробки та аналізу даних, є частиною концепції Fog Computing (див. рис.2.6) [12, 13]. Вони дозволяють аналізувати відео, вести моніторинг і приймати рішення практично миттєво, що є перевагою перед виключно хмарними рішеннями.

Локальне зберігання даних також є важливим аспектом. Наприклад, відеодані можуть зберігатися як на локальних серверах або міні-ПК (див. рис.3.12) [32], так і в хмарі (див. рис.2.5, 2.7) [11]. Однак, використання хмарних сервісів передбачає необхідність постійного доступу до Інтернету, тоді як при локальному зберіганні ця потреба може бути мінімізована або взагалі виключена, що особливо важливо

для віддалених регіонів або ситуацій, коли Інтернет-з'єднання нестабільне або відсутнє.

Варто також зазначити, що використання лише хмарних рішень може потребувати додаткових витрат на платні сервіси або розширені функції, які не доступні безкоштовно після купівлі обладнання. Якщо користувач не хоче створювати власну інфраструктуру, але потребує додаткових можливостей, він буде змушений оплачувати додаткові сервіси виробника [24]. (Додаток В)

Щоб забезпечити високу продуктивність системи, а також збалансувати навантаження між різними компонентами, доцільно використовувати гібридний підхід, що поєднує локальні та хмарні рішення. Локальні рішення можуть забезпечувати обробку даних і зберігання на місці, особливо у випадках, коли доступ до Інтернету обмежений або відсутній. Хмарні ж рішення забезпечують віддалений доступ, відеофіксацію, push-сповіщення та інші функції, коли користувач знаходиться далеко від об'єкта відеоспостереження, що дозволяє не перевантажувати ані локальні, ані хмарні ресурси, забезпечуючи оптимальну продуктивність системи відеоспостереження. (див. рис.3.7-3.8, 3.11) (Додаток В)

Одним із ключових показників ефективності децентралізованих систем відеоспостереження в різних середовищах є надійність – це критичний аспект, особливо для систем, які працюють цілодобово в режимі 24/7, де обробка відеоданих повинна бути безперервною. Оцінка надійності передбачає не лише захист системи від зовнішніх загроз, а й забезпечення резервування даних для запобігання втратам інформації у разі непередбачених ситуацій (див. рис. 3.8). (Додаток В)

Якщо використовувати хмарні рішення від виробника систем відеоспостереження, вони часто включають готові інструменти для захисту та резервного копіювання даних. Наприклад, за підпискою можна зберігати відеодані у хмарних сховищах, що дозволить захистити інформацію в разі пошкодження або виходу з ладу камер через технічні несправності чи навіть фізичні пошкодження злоумисниками. Такі хмарні сервіси забезпечують зручність і надійність у контексті резервного зберігання відео (див. рис. 3.8). (Додаток В)

Однак, у випадку локальної обробки даних, наприклад, за допомогою технології Fog Computing на базі міні-ПК, також можна організувати резервне зберігання відеоданих, що робить систему більш стійкою до збоїв у хмарній інфраструктурі або проблем з Інтернет-з'єднанням (див. рис.2.6, 3.12) [12, 13, 32]. До того ж, важливо передбачити застосування резервного живлення, що дозволить підтримувати роботу камер та серверів у разі перебоїв з електропостачанням (див. рис.4.3). Камери відеоспостереження споживають відносно мало електроенергії, а міні-ПК також є енергоефективними, що дозволяє продовжувати їхню роботу навіть під час перебоїв із живленням (див. рис.1.14).

Висока ступінь захисту та конфіденційності. Для забезпечення надійності системи важливо також враховувати безпеку мережевої інфраструктури. Якщо система керується віддалено і використовує загальнодоступні мережі, необхідно забезпечити безпечну передачу даних – це можна зробити шляхом впровадження технологій VPN та SSL сертифікації для захисту переданих даних. Наприклад, використання домену із SSL-сертифікатом є значно безпечнішим рішенням, ніж робота з IP-адресами та відкритими портами, такими як 554, які можуть бути вразливими для атак (див. рис. 3.13) [25, 33, 34, 35, 36].

Якщо система працює на основі локальної обробки даних, без необхідності постійного підключення до Інтернету, ці заходи безпеки можуть бути не такими важливими. Однак, для віддаленого керування і доступу через Інтернет їхнє впровадження є обов'язковим, щоб забезпечити захищеність всієї інфраструктури та запобігти несанкціонованому доступу.

4.4 Економічні та технічні переваги децентралізованих систем

Головною перевагою інтелектуальних децентралізованих систем відеоспостереження є їхні економічні та технічні переваги, які роблять їх все більш популярними. Децентралізовані системи забезпечують значну економію на інфраструктурі порівняно з традиційними централізованими системами:

- відсутність комунікаційних кабелів;
- інтеграція в межах одного пристрою;
- автономність;
- висока енергоефективність;
- інтеграція в сервер без змін для інфраструктури;
- інтеграція різноманітних безпроводних технологій;
- багатогранність у виборі рішень;
- безперервна інтеграція нових можливостей;
- висока степінь надійності та відмовостійкості;
- інтеграція в сервер задля низької затримки;
- сімбіоз локального та хмарного рішень.

Відсутність комунікаційних кабелів. Одна з ключових переваг полягає в суттєвому зниженні витрат на прокладання кабелів. У централізованих системах відеоспостереження необхідно прокладати мережеві та живильні кабелі для кожної камери, що є дорогим і тривалим процесом, особливо в урбанізованих зонах з щільною забудовою. Натомість децентралізовані системи часто використовують безпроводні камери, що усуває необхідність кабельної інфраструктури, значно знижуючи витрати на встановлення та обслуговування (див. рис.1.13).

Інтеграція в межах одного пристрою. Децентралізовані системи можуть функціонувати без необхідності створення великих серверних центрів (див. рис.1.13). Відео можна обробляти локально за допомогою міні-ПК або навіть безпосередньо на самих камерах, якщо вони оснащені інтегрованими мікропроцесорами та пам'яттю, що дозволяє значно зменшити потребу в дорогому

обладнанні для обробки та зберігання даних, що є особливо важливим для невеликих проєктів або розташувань із меншою кількістю камер. Такий підхід також знижує витрати на оренду серверних потужностей або підписки на хмарні сервіси. Наприклад, для невеликих систем із кількома десятками камер можна обійтися локальними міні-ПК для обробки відео, замість того щоб використовувати дорогі хмарні ресурси.

Придбання міні-ПК може вимагати початкових інвестицій, але в довгостроковій перспективі вони окупляться за рахунок зменшення постійних витрат на оренду хмарних сервісів, що особливо актуально для проєктів, де кількість камер невелика і немає потреби в масштабних обчислювальних потужностях.

Для великих систем із понад 100–200 камер, хмарні рішення можуть бути більш доцільними, оскільки вони дозволяють зручно керувати великою кількістю пристроїв. Проте в менш масштабних проєктах використання локальних міні-ПК або невеликих серверів є економічно вигіднішим рішенням (див. рис.3.12) [32].

Автономність. Важливим фактором також є забезпечення безперебійного живлення, для чого може бути встановлено резервне живлення, що дозволить системам працювати навіть у випадку перебоїв з електропостачанням (див. рис.4.3). Наприклад, камери з вбудованими акумуляторами та сонячними панелями можуть працювати повністю незалежно від міської електромережі, що є ідеальним рішенням для місцевостей, де доступ до електроенергії або відсутній, або нестабільний

Висока енергоефективність. Однією з ключових переваг децентралізованих систем відеоспостереження є їхня енергоефективність у порівнянні з традиційними централізованими системами, які потребують численних під'єднань та додаткового обладнання. У централізованих системах необхідно забезпечувати живлення відеореєстраторів та іншого устаткування, що збільшує загальне енергоспоживання і робить систему менш енергоефективною. Натомість децентралізовані рішення дозволяють значно знизити витрати на електроенергію завдяки використанню сучасних енергоефективних протоколів передачі даних [15,16].

Інтеграція в сервер без змін для інфраструктури. Зокрема, застосування міні-ПК, таких як GMKtec NucBox K8 Plus, Intel NUC або Raspberry Pi, у якості серверів для децентралізованих систем дозволяє мінімізувати енергоспоживання (див. рис.3.12) [32]. Ці пристрої споживають значно менше електроенергії, ніж традиційні централізовані сервери, при цьому забезпечуючи виконання всіх необхідних завдань, що особливо важливим у віддалених регіонах або місцевостях з обмеженим доступом до електроенергії, де кожен ват енергії має значення.

Інтеграція різноманітних безпроводних технологій. Ще однією перевагою є можливість використовувати SIM-карти мобільних операторів для підключення камер до мережі, що дозволяє обходитися без складної мережевої інфраструктури, що надає змогу камерам працювати повністю автономно, забезпечуючи зв'язок навіть у віддалених місцях, де немає інтернет-з'єднання або провідної мережі. Такий підхід мінімізує потребу у використанні централізованих серверів для обробки даних, оскільки обробка може здійснюватися локально на самих камерах, що значно скорочує витрати на передачу даних (див. рис.4.5) [43].

Завдяки розподіленій обробці даних і використанню локальних рішень, децентралізовані системи не лише знижують енергоспоживання, але й дозволяють значно зменшити експлуатаційні витрати, роблячи їх економічно вигідними для впровадження в різних умовах. Хоча для деяких сценаріїв може знадобитися більше інвестицій, як-от використання мобільних мереж або додаткових автономних компонентів, загальна ефективність і економія є вагомими перевагами децентралізованих систем відеоспостереження (див. рис.4.5) [43].

Багатогранність у виборі рішень. Децентралізовані інтелектуальні системи відеоспостереження мають значну перевагу завдяки своїй масштабованості та гнучкості – їх можна легко адаптувати до різних умов використання та розширювати без необхідності в значних змінах в інфраструктурі, як це потрібно в централізованих системах. У централізованих рішеннях для збільшення кількості пристроїв необхідно модернізувати сервери, мережі та інші елементи інфраструктури. Натомість у децентралізованих системах достатньо просто додати нові камери або інші пристрої, наприклад міні-ПК, які одразу інтегруються в

існуючу мережу, що дозволить уникнути значних витрат на перебудову мережевої інфраструктури та зменшити складність управління системою.

Децентралізовані системи також підтримують модульність – їх можна налаштувати під конкретні потреби користувача, додаючи або видаляючи компоненти за необхідності, без впливу на загальну працездатність. Наприклад, при встановленні камер у віддалених зонах немає потреби у внесенні глобальних змін в інфраструктуру, що робить процес масштабування ще простішим. Все, що потрібно – це налаштувати нові пристрої через безпроводні мережі, як-от Wi-Fi, і система продовжить працювати без значних зусиль з боку адміністратора.

Безперервна інтеграція нових можливостей. Локальні вузли можуть бути модернізовані для підтримки нових функцій, таких як інтелектуальна обробка даних або машинне навчання, що забезпечує ширші можливості для аналізу відеопотоків на місцевому рівні, що дозволить значно збільшити функціональність системи без необхідності значних змін в архітектурі, оскільки більшість завдань можуть бути виконані за допомогою оновлення існуючих елементів, наприклад, додавання міні-ПК для локальної обробки (див. рис.3.12) [32].

Висока степінь надійності та відмовостійкості. З технічної точки зору, інтелектуальні децентралізовані системи відеоспостереження володіють багатьма перевагами, серед яких – надійність і відмовостійкість. Оскільки кожен елемент системи працює автономно, вихід з ладу одного компонента не впливає на загальну роботу системи. Наприклад, якщо одна камера вийде з ладу, інші продовжуватимуть функціонувати без перебоїв. Така архітектура забезпечує високу надійність у порівнянні з централізованими системами, де відмова одного сервера може спричинити зупинку всієї системи.

Інтеграція в сервер задля низької затримки. Завдяки локальній обробці відеопотоків на міні-ПК або навіть безпосередньо на камерах, дані не потребують надсилання на віддалені сервери, що мінімізує час відгуку, що особливо важливо для систем, що працюють у режимі реального часу, таких як безпекові системи для моніторингу критично важливих об'єктів – впровадження таких рішень дозволяє

підвищити ефективність системи та швидкість реагування на події (див. рис.3.12) [32].

Сімбіоз локального та хмарного рішень. Децентралізовані системи можуть поєднувати в собі локальну і хмарну обробку даних, що надає користувачам більше можливостей для гнучкого налаштування систем під свої потреби. Наприклад, можна використовувати локальні міні-ПК для обробки даних та хмарні сервіси для зберігання або проведення додаткової аналітики – дозволяючи зберігати баланс між продуктивністю системи та її ефективністю (див. рис.3.7, 3.8). (Додаток В)

Таблиця 4.1 – Порівняння запропонованого рішення над традиційними

Критерій	Традиційні системи	Запропоноване рішення
Вартість впровадження	Висока, включає сервери, ліцензії, складну інфраструктуру	51,377 грн за всі компоненти, з яких 29000 грн, економічно ефективне рішення
Гнучкість та масштабованість	Обмежена; кожне нове розширення потребує значних витрат	Легко масштабувати за допомогою Proxmox та Home Assistant OS, додавання нових пристроїв доступне
Збереження даних	Здебільшого централізоване, потребує серверів або дорогих хмарних підписок	Локальне (карти пам'яті Kingston) + хмарне (TP-Link Taro Care)
Автономність	Залежність від централізованого енергопостачання, висока вразливість до перебоїв живлення	Низьке споживання – 5.4 Вт (одна камера); ДБЖ забезпечує резервне живлення для ключових компонентів (основна камера: ~ 20 годин; мережеве обладнання: ~ 4 години 10 хвилин)
Автоматизація та аналітика	Додаткові функції доступні лише через дорогі рішення або стороннє ПЗ	Інтеграція з Home Assistant OS та motionEye забезпечує автоматизацію та базову відеоаналітику
Якість обладнання	Висока, але вартість часто завищена через брендову інтеграцію	Камери TP-Link Taro та маршрутизатори Wi-Fi 6 забезпечують високу якість за доступною ціною

ВИСНОВКИ

У підсумку можна стверджувати, що інтелектуальні децентралізовані системи відеоспостереження, або просто камери відеоспостереження, надають значно більше функціональних можливостей у порівнянні з традиційними системами. Навіть при придбанні лише кількох камер від одного виробника, користувачі отримують розширений функціонал, що робить такі системи привабливішими, зокрема для вирішення локальних завдань безпеки. Це може включати захист житла, прибудинкових територій або невеликих роздрібних магазинів, де не потрібна велика кількість камер – вистачить однієї чи двох.

Завдяки децентралізації процесів, такі камери не залежать від централізованого управління чи складної інфраструктури, що включає велику кількість кабелів. Кожна камера є автономною та може працювати незалежно, що робить її мобільною та енергоефективною. Вони можуть бути встановлені в будь-якому місці, як з наявною мережею, так і без неї. У випадку потреби в віддаленому доступі, можна легко налаштувати мережеву інфраструктуру, наприклад, використовуючи Wi-Fi. Такі системи можуть працювати ефективніше за традиційні, які залежать від складної кабельної інфраструктури.

Інтелектуальні децентралізовані камери можуть інтегруватися в сучасні системи управління, такі як «розумні міста» чи «розумні будинки», забезпечуючи взаємодію з іншими датчиками для аналізу даних і прийняття рішень у реальному часі. Завдяки автономності, мобільності та енергоефективності їх можна використовувати в місцях без стабільного електроживлення, зокрема в урбанізованих або важкодоступних районах.

Такі системи мають широкий потенціал для вдосконалення завдяки інтеграції з новітніми технологіями, зокрема платформами для централізованого управління, що сприяє підвищенню зручності та ефективності їх використання в різних сферах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. How Do Security Cameras Get Power: Wireless, PoE Cameras, and More - Reolink Blog. Reolink Official: Security Cameras and Systems for Home & Business. URL: <https://reolink.com/blog/how-do-security-cameras-get-power> (дата звернення: 11.10.2024).
2. 24 Hour Surveillance Monitoring - Twenty First Security. Twenty First Security - Quality Security Systems Melbourne VIC. URL: <https://twentyfirstsecurity.com.au/24-hour-surveillance-monitoring> (дата звернення: 11.10.2024).
3. Everything you need to know about the optimisation and maintenance of your surveillance cameras. Veesion. URL: <https://veesion.io/en/camera-maintenance-the-right-steps-to-optimise-your-video-surveillance-system/> (дата звернення: 11.10.2024).
4. USB key cyber infection: 5 tips to prevent it - TYREX - décontamination USB. TYREX - décontamination USB. URL: <https://tyrex-cyber.com/en/infection-by-usb-5-tips-to-prevent-it/> (дата звернення: 11.10.2024).
5. Johnson J. Common Reasons For Video Loss on Security Cameras: How To Fix Them. Montavue. URL: <https://montavue.com/blogs/news/common-reasons-for-video-loss-on-security-cameras-how-to-fix-them?srltid=AfmBOoq6Xac8IidtOEeG1zTBWxuFNsg22kZHwBbDLdWQ1lSIWTsp9iLE> (дата звернення: 12.10.2024).
6. Cloud Computing and Cloud Computing Architecture. Milestones Education. URL: <https://www.milestones.vic.edu.au/cloud-computing-and-cloud-computing-architecture/> (дата звернення: 12.10.2024).
7. What's the Difference Between AWS vs. Azure vs. Google Cloud?. Coursera. URL: <https://www.coursera.org/articles/aws-vs-azure-vs-google-cloud> (дата звернення: 12.10.2024).
8. RTSP vs RTMP: Which Protocol to Choose?. Reolink Official: Security Cameras and Systems for Home & Business. URL: <https://reolink.com/blog/rtsp-vs-rtmp/> (дата звернення: 13.10.2024).
9. What is the difference between HTTP, RTSP, and RTMP. Huawei. URL: <https://forum.huawei.com/enterprise/en/what-is-the-difference-between-http-rtsp-and-rtmp/thread/667242962666536960-667213859104108544> (дата звернення: 13.10.2024).
10. Cassandra vs MongoDB - Difference Between NoSQL Databases - AWS. Amazon Web Services, Inc. URL: https://aws.amazon.com/compare/the-difference-between-cassandra-and-mongodb/?nc1=h_ls (дата звернення: 13.10.2024).
11. Capture & Record Video Streams - Amazon Kinesis Video Streams - AWS. Amazon Web Services, Inc. URL: <https://aws.amazon.com/kinesis/video-streams/?amazon-kinesis-video-streams-resources-blog.sort-by=item.additionalFields.createdDate&amazon-kinesis-video-streams-resources-blog.sort-order=desc> (дата звернення: 13.10.2024).

12. GeeksforGeeks. Difference Between Edge Computing and Fog Computing - GeeksforGeeks. URL: <https://www.geeksforgeeks.org/difference-between-edge-computing-and-fog-computing/> (дата звернення: 14.10.2024).

13. What Is Fog Computing? definition, Applications, Everything to Know. Cybersecurity Exchange. URL: <https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/fog-computing-everything-to-know/#:~:text=Fog%20computing%20is%20a%20term,on%20top%20of,%20end%20users.> (дата звернення: 14.10.2024).

14. MQTT vs Other IoT Messaging Protocols: Comparison & Use Cases. webbylab. URL: <https://webbylab.com/blog/mqtt-vs-other-iot-messaging-protocols/#:~:text=MQTT%20vs%20CoAP%20Protocol,-Let's%20study%20MQTT&text=When%20comparing%20MQTT%20vs%20CoAP,the%20three%20levels%20of%20QoS.> (дата звернення: 14.10.2024).

15. Rouse M. IPv6 Over Low-Power Wireless Personal Area Networks. Techopedia. URL: <https://www.techopedia.com/definition/29639/ipv6-over-low-power-wireless-personal-area-networks-6lowpan> (дата звернення: 14.10.2024).

16. What is Zigbee? | Soracom. Soracom. URL: <https://www.soracom.io/iot-definitions/what-is-zigbee/> (дата звернення: 15.10.2024).

17. Fog Computing vs. Cloud Computing: Key Differences | SaM Solutions. SaM Solutions. URL: <https://www.sam-solutions.com/blog/fog-computing-vs-cloud-computing-for-iot-projects/#:~:text=Fog%20provides%20low%20latency;%20cloud,due%20to%20its%20distributed%20architecture> (дата звернення: 15.10.2024).

18. IoT platform product architecture on Google Cloud | Cloud Architecture Center. Google Cloud. URL: <https://cloud.google.com/architecture/connected-devices/iot-platform-product-architecture> (дата звернення: 15.10.2024).

19. What is Azure IoT Hub? - Azure IoT Hub. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/uk-ua/azure/iot-hub/iot-concepts-and-iot-hub> (дата звернення: 15.10.2024).

20. IoT, from Cloud to Fog Computing. Cisco Blogs. URL: <https://blogs.cisco.com/perspectives/iot-from-cloud-to-fog-computing> (дата звернення: 16.10.2024).

21. Metropolis | NVIDIA. NVIDIA. URL: <https://www.nvidia.com/en-us/autonomous-machines/intelligent-video-analytics-platform/> (дата звернення: 16.10.2024).

22. Apple Ecosystem vs Google Ecosystem. Tech Journeyman. URL: <https://techjourneyman.com/blog/apple-ecosystem-vs-google-ecosystem/> (дата звернення: 16.10.2024).

23. Documentation. Home Assistant. URL: <https://www.home-assistant.io/docs/> (дата звернення: 16.10.2024).

24. Tapo Care. TP-Link. URL: <https://www.tp-link.com/uk-ua/tapocare/> (дата звернення: 17.10.2024).

25. How to view a Tapo camera on PC/NAS/NVR through the RTSP/ONVIF Protocol | TP-Link. TP-Link Deutschland - Netzwerklösungen für Privat- und

Businessanwender. URL: <https://www.tp-link.com/us/support/faq/2680/> (дата звернення: 17.10.2024).

26. Dashboards. Home Assistant. URL: <https://www.home-assistant.io/dashboards/> (дата звернення: 17.10.2024).

27. GitHub - motioneye-project/motioneye: A web frontend for the motion daemon. GitHub. URL: <https://github.com/motioneye-project/motioneye> (дата звернення: 18.10.2024).

28. How to create Smart Action (Automation or Shortcut) on Tapo app | Tapo. Tapo | Smart Devices for Smart Living. URL: <https://www.tapo.com/en/faq/80/> (дата звернення: 18.10.2024).

29. Installation. Home Assistant. URL: <https://www.home-assistant.io/installation> (дата звернення: 18.10.2024).

30. GitHub - Sandeep9975/Object_Detection_Using_Yolo: Object detection using the YOLO (You Only Look Once). GitHub. URL: https://github.com/Sandeep9975/Object_Detection_Using_Yolo (дата звернення: 19.10.2024).

31. AI-Integrated Video Analytics. i3 International. URL: <https://www.i3international.com/resources/media/yolo-the-best-model-for-ai-integrated-video-analytics> (дата звернення: 19.10.2024).

32. AMD Ryzen 7 8845HS Mini PC--NucBox K8 Plus. GMKtec. URL: https://www.gmktec.com/products/amd-ryzen-7-8845hs-mini-pc-nucbox-k8-plus?srsId=AfmBOoqHyRlNdWAXMRn9f1Bi1f4S8BvhLS_3jK68gksX_BZKdifRe0KG (дата звернення: 19.10.2024).

33. Rouse M. Third-Level Domain. Techopedia. URL: <https://www.techopedia.com/definition/23811/third-level-domain> (дата звернення: 19.10.2024).

34. What is SSL? How do SSL Certificates work?. ComodoSSLstore. URL: <https://comodoSSLstore.com/blog/what-is-ssl-and-how-do-ssl-certificates-work.html> (дата звернення: 19.10.2024).

35. How to set up TP-LINK DDNS on TP-Link Wireless Router (New Logo). TP-Link Deutschland - Netzwerklösungen für Privat- und Businessanwender. URL: <https://www.tp-link.com/us/support/faq/1367/> (дата звернення: 20.10.2024).

36. KeenDNS service. Keenetic. URL: <https://help.keenetic.com/hc/en-us/articles/360000400919-KeenDNS-service> (дата звернення: 20.10.2024).

37. So what is Cloudflare?. Cloudflare. URL: <https://www.cloudflare.com/learning/what-is-cloudflare/#:~:text=Cloudflare%20is%20one%20of%20the,tens%20of%20thousands%20each%20day> (дата звернення: 20.10.2024).

38. Home Assistant App through Cloudflare Tunnel. Home Assistant Community. URL: <https://community.home-assistant.io/t/home-assistant-app-through-cloudflare-tunnel/709951> (дата звернення: 21.10.2024).

39. Google Authenticator now supports Google Account synchronization. Google Online Security Blog. URL: <https://security.googleblog.com/2023/04/google-authenticator-now-supports.html> (дата звернення: 21.10.2024)

40. GitHub - DaniW42/motioneye-telegram: Adding dirty telegram workaround to motioneye. GitHub. URL: <https://github.com/DaniW42/motioneye-telegram> (дата звернення: 03.11.2024). Smart City Surveillance System with AI Video Analytics. Eagle Eye Networks. URL: <https://www.een.com/solutions/cloud-video-surveillance-cities/> (дата звернення 22.10.2024).

41. Solutions - Video Surveillance In An Elevator - Wireless-Tek. Wireless-Tek. URL: <https://wireless-tek.co.za/video-surveillance-in-an-elevator/> (дата звернення: 22.10.2024).

42. Bordelon C. Douglas County wildfire first detected by cameras equipped with AI. Denver 7 Colorado News (KMGH). URL: <https://www.denver7.com/news/wildfire/douglas-county-wildfire-first-detected-by-cameras-equipped-with-ai> (дата звернення: 23.10.2024).

43. Галета В.С., Сімбіоз відеоспостереження та розумного будинку. «Проблеми комп'ютерної інженерії»: Науково-практ. конф., м.Київ, 1 грудня 2023 р. С. 3-4. URL: https://duikt.edu.ua/uploads/p_2626_33497568.pdf.

44. Галета В.С., Антоненко А.В. Чому система відеоспостереження не панацея, а єдине вірне рішення забезпечення безпеки. «Сучасний стан та перспективи розвитку ІОТ»: V Науково-техн. конф., м.Київ, 18 квітня 2024 р. С. 91-94. URL: https://duikt.edu.ua/uploads/p_2661_70423010.pdf.

45. Галета В.С., Антоненко А.В. Реалізація децентралізованих систем відеоспостереження з використанням ІР-камер та інтеграцією з хмарним сховищем. «Застосування програмного забезпечення в ІКТ»: Всеукр. науково-техн. конф., м.Київ, 24 квітня 2024 р. С. 427-430. URL: https://duikt.edu.ua/uploads/p_2661_45497999.pdf.

46. Zaitsev, I., Antonenko, A., Dakova, L., Haleta, V. Implementation of network IP cameras in video surveillance systems with integration with cloud storage for decentralized monitoring. «Sustainability of education and science in conditions of transformation»: International scientific and practical conference, Kyiv, May 21-22, 2024. P. 80-82. URL: https://istu.edu.ua/wp-content/uploads/2024/07/Materialy_II_Mizhnarodnoi_naukovo_praktychnoi_konferentsii_2024_compressed.pdf.

47. Лемешко А.В., Галета В.С. Використання маршрутизатора як точки доступу для розповсюдження мережі WI-FI у важкодоступних місцях. «Інформаційні технології та цифрова економіка»: V Міжн. науково-техн. конф., м.Київ, 9-10 травня 2024 р. С. 104-105. URL: https://files.duit.edu.ua/uploads/%D0%A1%D0%B0%D0%B9%D1%82/3_%D0%9D%D0%90%D0%A3%D0%9A%D0%90/conferences/international-scientific-and-practical-conferences/information-technology-digital-economy.pdf

48. USE OF ARTIFICIAL INTELLIGENCE IN AUTOMATED SYSTEMS / A. ANTONENKO, M. PAKHOMOV, T. KALYTA, V. HALETA, et al. Herald of Khmelnytskyi National University. Technical sciences. 2023. Vol. 323, no. 4. P. 11–20. URL: <https://www.doi.org/10.31891/2307-5732-2023-323-4>

49. OBJECT RECOGNITION SYSTEMS USING INTELLIGENT TECHNOLOGIES IN UAV / A. ANTONENKO, D. SKUDNYI, V. HALETA, M.

YURII, V. HUMINIUK, A. BURACHYNSKYI, S. VOSTRIKOV, A. BALVAK, D. KOROTIN, A. TVERDOKHLIB, G.OLEKSII, S. POPERESHNYAK, O. TKACHENKO, O. GOLUBENKO, D. TUZHILIN. European Science, 2(sge29-02) (2024), P.50–82. URL: <https://doi.org/10.30890/2709-2313.2024-29-00-010>

Технічні характеристики, функціональні можливості ІР камер від TP-Link серії TAPO

Таблиця А.1 – Порівняння технічних характеристик ІР камер від TP-Link серії TAPO

Характеристика	TP-Link TAPO C100	TP-Link TAPO C200	TP-Link TAPO C310
Тип камери	Внутрішня	Внутрішня, PTZ	Зовнішня
Роздільна здатність	1080p (Full HD, 1920x1080)	1080p (Full HD, 1920x1080)	1080p (Full HD, 1920x1080)
Кут огляду	105°	Горизонтальний: 360°, вертикальний: 114°	105°
Поворот і нахил	Немає	Поворот: 360°, нахил: 114°	Немає
Нічне бачення	До 9 м	До 9 м	До 30 м
Підключення	Wi-Fi	Wi-Fi	Wi-Fi + Ethernet
Wi-Fi діапазон	2.4 GHz	2.4 GHz	2.4 GHz
Захист від погоди	Немає	Немає	IP66
Детекція руху	Є	Є	Є
Двосторонній звук	Є	Є	Є
Сховище	MicroSD до 128 ГБ	MicroSD до 128 ГБ	MicroSD до 128 ГБ
Інтеграція	Тапо App, Alexa, Google Assistant	Тапо App, Alexa, Google Assistant	Тапо App, Alexa, Google Assistant
Потужність	5.4 Вт	5.4 Вт	5.4 Вт
Застосування	Дім/офіс	Дім/офіс	Вулиця/дворові зони
Ціна (орієнтовна)	939 грн	1299 грн	1799 грн

Технічні характеристики, функціональні можливості ІР камер від TP-Link серії TAPO

Таблиця А.2 – Функціональні можливості ІР-камер від TP-Link серії TAPO

Функціональна можливість	Опис	Переваги для користувача
Мобільний додаток Таро	Керування камерами через додаток (перегляд відео, налаштування параметрів, отримання сповіщень)	Зручне управління зі смартфона з будь-якої точки світу
Full HD (1080p)	Відео у високій якості з чіткими деталями	Забезпечує розпізнавання осіб та деталей у кадрі
Детекція руху	Виявлення руху в полі зору камери з миттєвими сповіщеннями	Підвищена безпека та своєчасне інформування про потенційні загрози
Двосторонній звук	Вбудований мікрофон і динамік для аудіо-зв'язку	Можливість спілкування з відвідувачами або відлякування непроханих гостей
Нічне бачення	Інфрачервоне підсвічування для зйомки в темряві (дальність до 30 м залежно від моделі)	Забезпечує контроль території навіть у повній темряві
Локальне зберігання	Підтримка microSD-карт до 128 ГБ	Зберігання відеозаписів без необхідності в хмарних сервісах
Зони детекції руху	Можливість налаштування зон, в яких камера виявляє рух	Зменшує кількість хибних сповіщень, фокусуючись на важливих зонах
Режим конфіденційності	Відключення запису або закриття об'єктива	Захист приватності у вибраний час
Шифрування даних	Захист відео та конфіденційності через протоколи шифрування	Гарантія безпеки переданих даних
Розклад роботи	Налаштування часу активності камери	Автоматизація роботи камери для зручності та економії ресурсів
Інтеграція з голосовими помічниками	Підтримка Alexa та Google Assistant для голосового управління	Керування камерою за допомогою голосових команд
Push-сповіщення	Миттєві повідомлення на смартфон у разі виявлення руху	Оперативне реагування на події
Підключення по Wi-Fi	Безпроводове підключення до мережі (2.4 GHz)	Гнучкість у розміщенні камер
Підтримка Ethernet	Додаткове провідне підключення (тільки для Tapo C310)	Стабільне з'єднання для зовнішнього використання

Опис функціональних можливостей додатка від TP-Link – TAPO

Таблиця А.3 – Функціональні можливості додатка від TP-Link – TAPO

Функція	Опис	Переваги
Прямий перегляд (Live View)	Можливість переглядати відео в реальному часі з будь-якої камери	Моніторинг ситуації в режимі онлайн зі смартфона
Віддалене керування	Керування камерами з будь-якої точки світу через інтернет	Гнучкість і контроль навіть поза домом
Детекція руху	Відображення руху на екрані та надсилання push-сповіщень	Оперативне інформування про підозрілі події
Сповіщення у реальному часі	Надсилання повідомлень на смартфон при виявленні руху або звуку (залежить від моделі)	Своєчасне попередження про небезпеку
Поворот і нахил (PTZ)	Керування поворотом та нахилом камери (для моделей із PTZ, наприклад Tapo C200)	Розширення оглядової зони за необхідністю
Аудіо-зв'язок	Двосторонній звук через додаток (розмови з відвідувачами)	Спілкування з відвідувачами або відлякування порушників
Запис відео	Запис відео на microSD-карту або хмарне сховище (за підтримки)	Зберігання важливих подій для подальшого перегляду
Перегляд архіву	Відтворення збережених відеозаписів із локального сховища	Легкий доступ до записів для аналізу ситуацій
Налаштування зон руху	Вибір конкретних зон у полі зору для детекції руху	Зниження кількості хибних сповіщень
Режим конфіденційності	Вимкнення камери або закриття об'єктива	Захист приватності у вибраний час
Планування записів	Налаштування графіка активності камери (часи роботи)	Автоматизація та енергоефективність
Мультиекранний перегляд	Підключення та перегляд кількох камер одночасно на одному екрані	Зручний моніторинг кількох зон в одному додатку
Підтримка голосових помічників	Інтеграція з Alexa та Google Assistant для голосового управління	Голосове керування камерами для зручності
Розпізнавання людей	Вибіркове визначення руху людини (залежить від моделі)	Зменшення кількості хибних сповіщень (наприклад, від тварин)
Інтелектуальні сценарії	Автоматизація роботи камер за умовами (наприклад, увімкнення при виявленні руху)	Підвищення безпеки та зручності
Поділ доступу	Надання доступу до камер іншим користувачам	Спільний доступ до камер для членів сім'ї або колег
Оновлення прошивки	Можливість оновлення програмного забезпечення камер через додаток	Підтримка актуальних функцій і підвищення безпеки

Порівняння технічних характеристик та кошторис локального та хмарного сховища від TP-Link

Таблиця Б.1 – Порівняння технічних характеристик локального та хмарного сховища від TP-Link

Характеристика	Локальне сховище (microSD)	Хмарне сховище TP-Link
Тип зберігання	Запис на microSD-карту, встановлену в камеру	Зберігання відео в хмарному середовищі TP-Link
Обсяг пам'яті	До 128 ГБ (залежно від microSD-карти)	Необмежено
Доступ до відео	Локальний доступ через додаток при підключенні до камери	Віддалений доступ з будь-якої точки світу через інтернет
Надійність	Залежить від якості microSD-карти та фізичного стану камери	Висока, із захистом даних та резервним копіюванням
Захист даних	Шифрування даних на карті (залежно від моделі камери)	Шифрування під час передачі та зберігання даних у хмарі
Автоматизація запису	По руху або в обраний період (коли є потреба у записі)	Автоматичне управління простором і збереження записів
Доступність при збої мережі	Доступне навіть без інтернету (за умови локального підключення)	Не доступне без інтернету
Вартість	Одноразова покупка microSD-карти	Щомісячна або річна підписка (залежно від плану)
Простота налаштування	Просте встановлення microSD-карти	Потребує реєстрації та налаштування облікового запису
Період зберігання відео	До заповнення карти, після чого старі записи видаляються	Регульований період (зазвичай 7, 30 або більше днів)
Безпека від пошкоджень	Вразливе до фізичного пошкодження камери або карти.	Захищене від фізичних загроз
Підтримка багатьох пристроїв	Прив'язане до однієї камери	Можливість доступу з різних пристроїв та швидко змінити підписки між наявними камерами

Порівняння технічних характеристик та кошторис локального та хмарного сховища від TP-Link

Таблиця Б.2 – Кошторис локального та хмарного сховища від TP-Link

Параметр	Локальне сховище (microSD-карта)	Хмарне сховище (Tapo Care)
Приклад об'єму	32 ГБ, 64 ГБ, 128 ГБ	До 1, 2, 3 або 10 пристроїв (залежно від плану)
Вартість microSD-карт	32 ГБ – ≈ 250-350 грн 64 ГБ – ≈ 400-600 грн 128 ГБ – ≈ 700-1000 грн	Надається за підпискою
Щомісячна вартість хмарного сховища	—	1 пристрій – 94,99 грн/місяць 2 пристрої – 184,99 грн/місяць 3 пристрої – 279,99 грн/місяць 10 пристроїв – 309,99 грн/місяць
Річна вартість хмарного сховища	—	1 пристрій – 939,99 грн/рік 2 пристрої – 1849,99 грн/рік 3 пристрої – 2799,99 грн/рік 10 пристроїв – 3099,99 грн/рік (зі знижкою)
Тип оплати	Одноразова покупка	Щомісячна або річна підписка
Можливість віддаленого доступу	При наявності інтернет з'єднання	Доступне з будь-якої точки світу
Обмеження за обсягом записів	До заповнення карти	Обмежується тільки обсягом підписки
Термін зберігання відео	До переповнення microSD-карти	Від 7 днів (залежно від тарифу)
Автоматичне оновлення записів	Ні	Так, автоматичне управління простором
Безпека та резервне копіювання	Обмежена фізичною безпекою пристрою	Захищене шифруванням і резервним копіюванням у хмарі

Порівняння технічних характеристик маршрутизаторів від TP-Link серії Archer

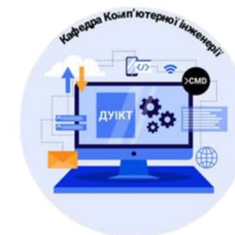
Таблиця В.1 – Порівняння технічних характеристик маршрутизаторів від TP-Link серії Archer AX53, AX73

Характеристика	TP-Link Archer AX53	TP-Link Archer AX73
Стандарт Wi-Fi	Wi-Fi 6 (802.11ax)	Wi-Fi 6 (802.11ax)
Максимальна швидкість Wi-Fi	2402 Мбіт/с (5 ГГц) 574 Мбіт/с (2,4 ГГц)	4804 Мбіт/с (5 ГГц) 574 Мбіт/с (2,4 ГГц)
Загальна пропускна здатність	До 3000 Мбіт/с	До 5400 Мбіт/с
Кількість антен	4 зовнішні антени	6 зовнішніх антен
Порти	4× Gigabit LAN, 1× Gigabit WAN	4× Gigabit LAN, 1× Gigabit WAN, 1× USB 3.0
Процесор	Двоядерний	Чотириядерний
MU-MIMO	Так, 2×2	Так, 4×4
OFDMA (Orthogonal FDMA)	Так	Так
Beamforming	Так	Так
Технологія OneMesh	Підтримується	Підтримується
Технологія EasyMesh	Підтримується	Підтримується
Безпека	WPA3, підтримка TP-Link HomeCare	WPA3, підтримка TP-Link HomeShield
Підтримка VPN	Так (OpenVPN, PPTP VPN)	Так (OpenVPN, PPTP VPN)
Гостьова мережа	Так	Так
Підтримка додатків	TP-Link Tether, TP-Link HomeCare	TP-Link Tether, TP-Link HomeShield
Розміри (Ш×Г×В)	260 × 135 × 41 мм	272 × 147 × 49 мм
Охолодження	Пасивне	Покращене пасивне з вентиляційними отворами
Ціна (орієнтовно)	2499 грн	4999 грн

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ



**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра комп'ютерної інженерії**



КВАЛІФІКАЦІЙНА РОБОТА на здобуття освітнього ступеня магістра

**НА ТЕМУ: «ІНТЕЛЕКТУАЛЬНА СИСТЕМА ВІДЕОСПОСТЕРЕЖЕННЯ НА
ОСНОВІ МАШИННОГО НАВЧАННЯ»**

Виконав студент групи КСДМ-62

Галета Володимир Сергійович

Керівник дипломної роботи:

Антоненко Артем Васильович,

канд.техн.наук, доцент

Київ – 2025

Мета, об'єкт, предмет дослідження

Мета роботи – розробити і впровадити інтелектуальну децентралізовану систему відеоспостереження, яка використовує машинне навчання, хмарні обчислення та платформи Fog Computing для забезпечення надійного спостереження в урбанізованих і важкодоступних регіонах

Об'єкт дослідження – система відеоспостереження з використанням технологій машинного навчання

Предмет дослідження – методи та технології побудови децентралізованих систем відеоспостереження для різних умов середовища, що базуються на інтелектуальних обчисленнях та розподілених обчислювальних платформах

Актуальність роботи

У роботі розглянуто розробку та впровадження інтелектуальних децентралізованих систем відеоспостереження, що поєднують технології машинного навчання, хмарного обчислення та Fog Computing.

Проаналізовано сучасні тенденції та обмеження систем відеоспостереження, а також рішення, які підвищують їх продуктивність і надійність. Машинне навчання автоматизує аналіз відеоданих, покращуючи точність виявлення об'єктів і аномалій. Хмарні обчислення забезпечують масштабовану обробку великих обсягів даних, а Fog Computing мінімізує затримки, розташовуючи обчислювальні ресурси ближче до джерел даних. Запропонована архітектура дає змогу ефективно використовувати такі системи в різних умовах.

Проблеми традиційних систем відеоспостереження та необхідність інтелектуальних рішень

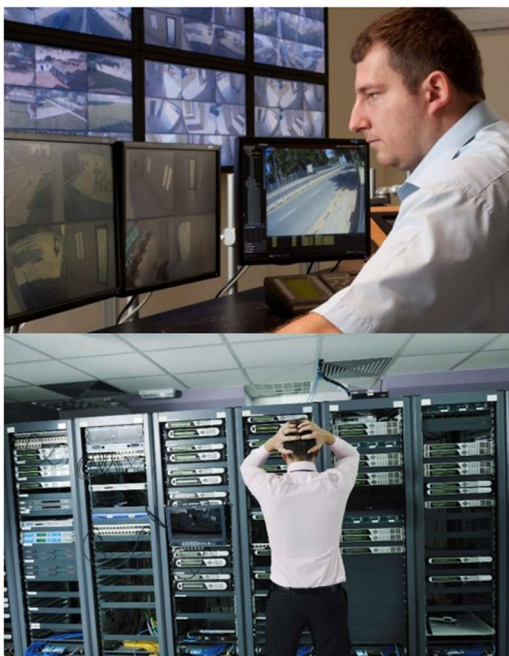


Рис. 1.6 – Складнощі з постійним моніторингом та обслуговуванням традиційних систем відеоспостереження



Рис. 1.5 – Камери відеоспостереження Xiaomi Yi Home 720p з автономним живленням від портативних зарядних пристроїв

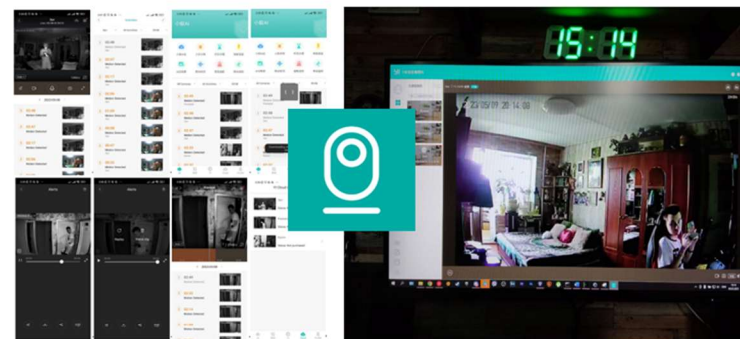


Рис. 1.11 – Інтеграція спрощених інтерфейсів для керування інтелектуальними децентралізованими системами відеоспостереження на різних платформах

Хмарні та туманні обчислення з використанням методів машинного навчання

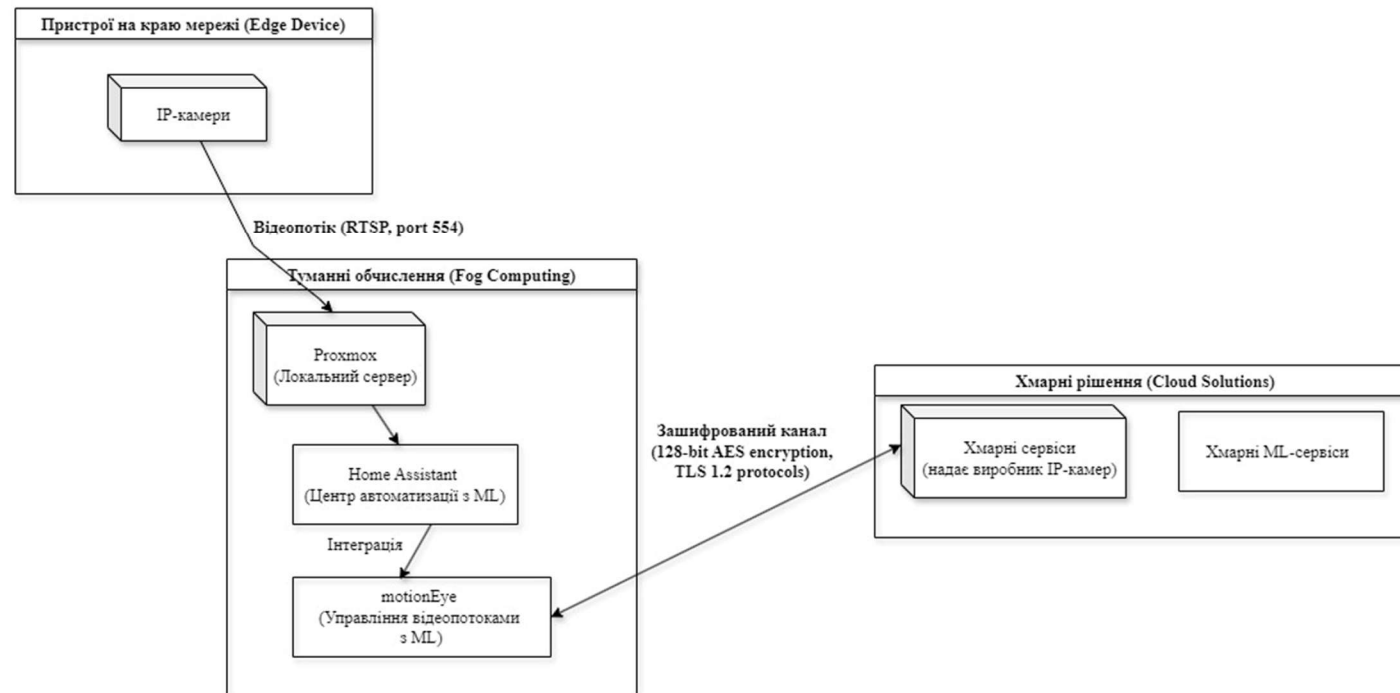


Рис. 2.7 – Fog-Cloud архітектура для інтелектуального відеоспостереження

Архітектура інтелектуальної системи відеоспостереження

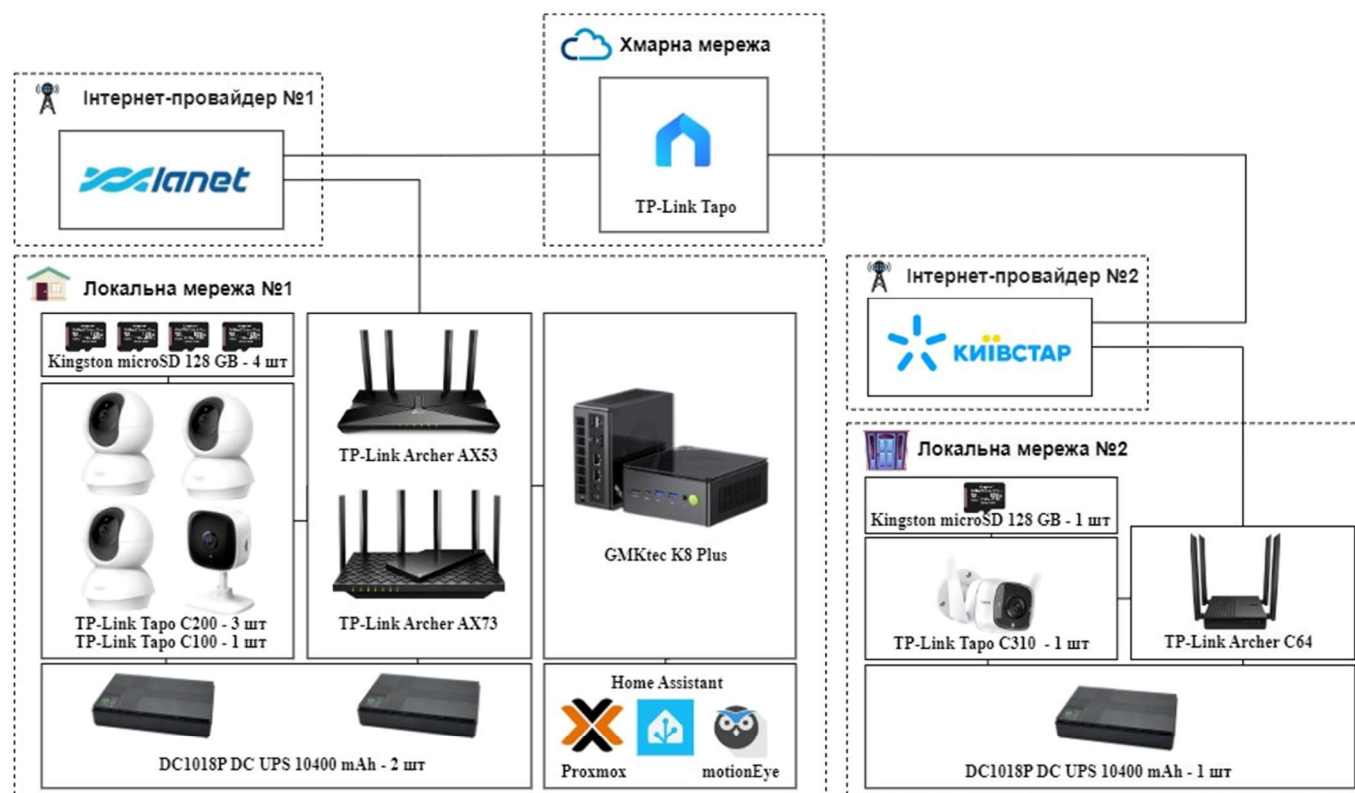


Рис. 3.3 – Схема інтелектуальної системи відеоспостереження з резервуванням, локальним та хмарним сервісами

Розміщення камер відеоспостереження у різних локаціях

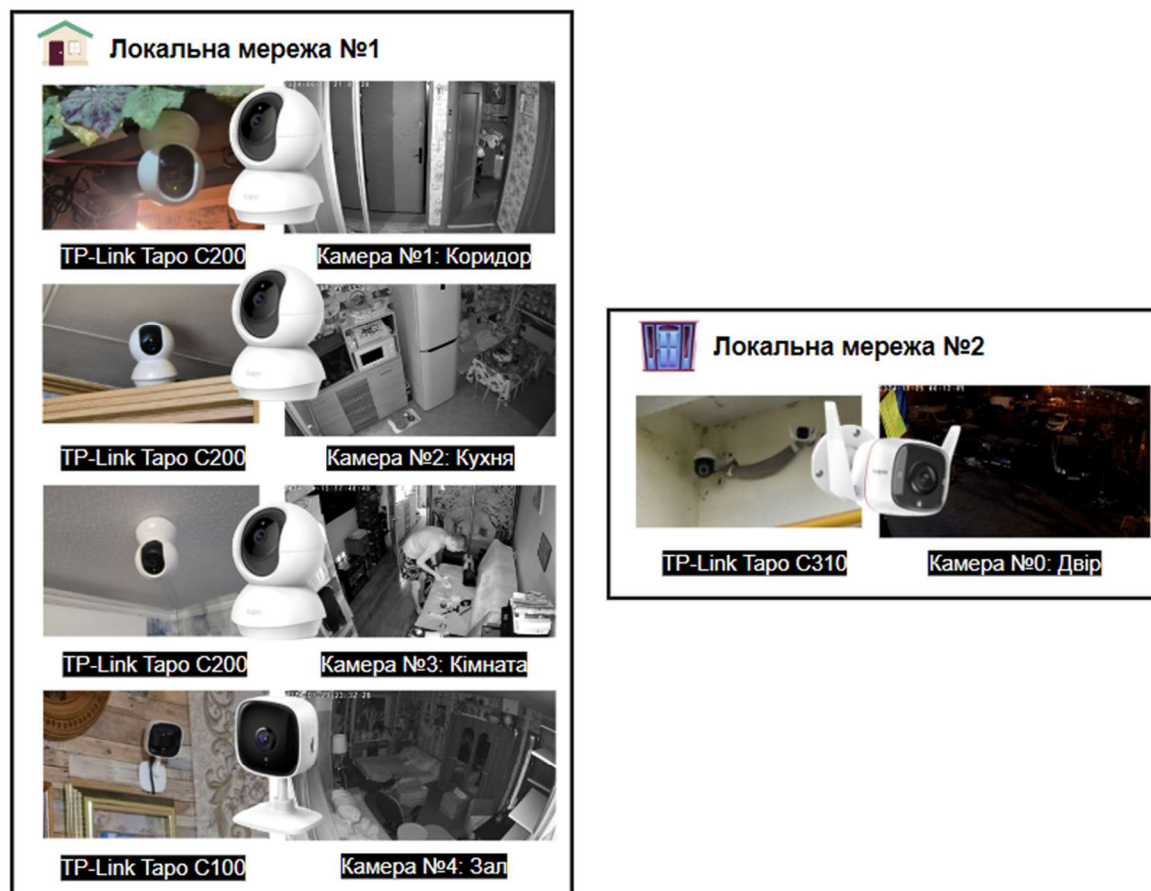


Рис. 3.5 – Розташування системи відеоспостереження

Мережева інфраструктура та резервування

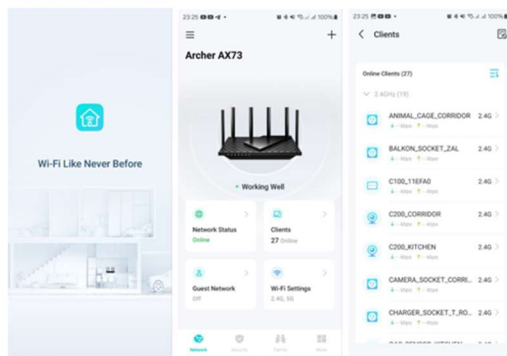


Рис. 3.19 – Додаток Tether для маршрутизаторів TP-Link



Рис. 3.17 – Маршрутизатори TP-Link Archer AX73 та AX53 (з'єднані у EasyMesh – провідним бекхолом)

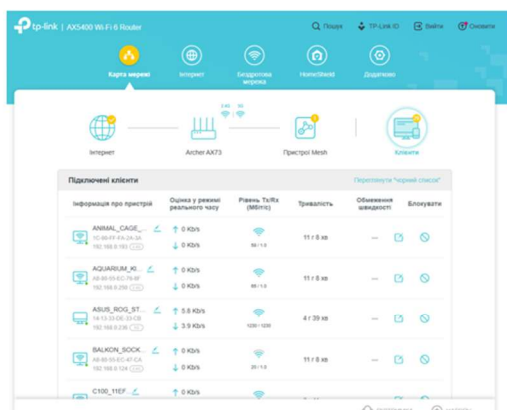


Рис. 3.20 – Веб-сервіс TP-Link для маршрутизаторів TP-Link

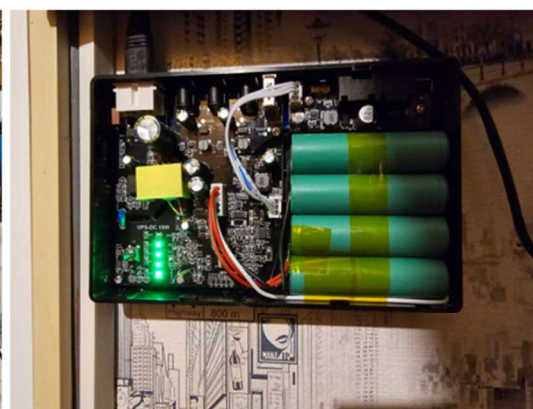
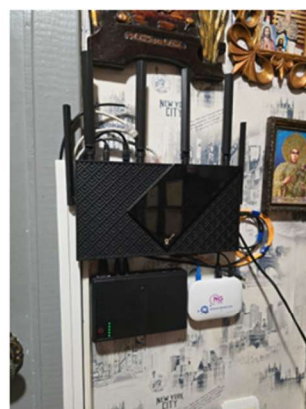


Рис. 3.18 – Резервування мережевої інфраструктури завдяки DC1018P DC UPS 10400 mAh (~4 години 10 хвилин)

Забезпечення резервуванням основної камери відеоспостереження



Рис. 4.3 – Забезпечення автономності інтелектуальній камері відеоспостереження у якості ДБЖ (максимальне споживання 5.4 Вт, ~20 годин автономності зі ДБЖ)

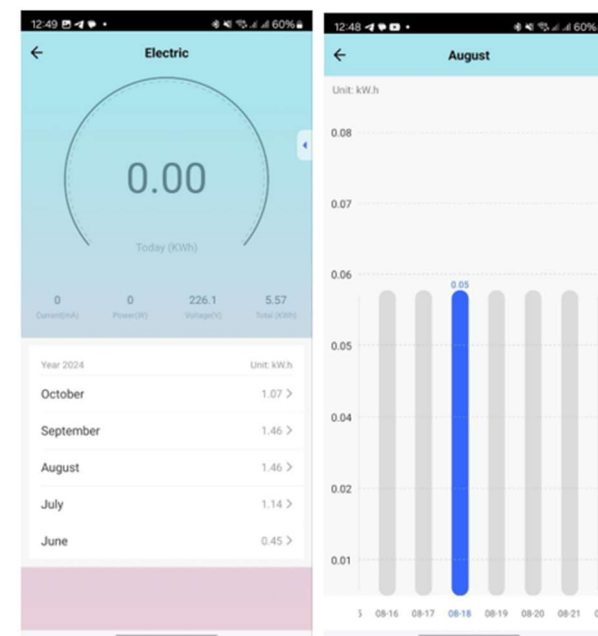


Рис. 4.4 – Рівень споживання електроенергії однієї інтелектуальної камери відеоспостереження (за допомогою додатка Smart Life та розумної розетки)

Демонстрація функціональних можливостей додатка від виробника

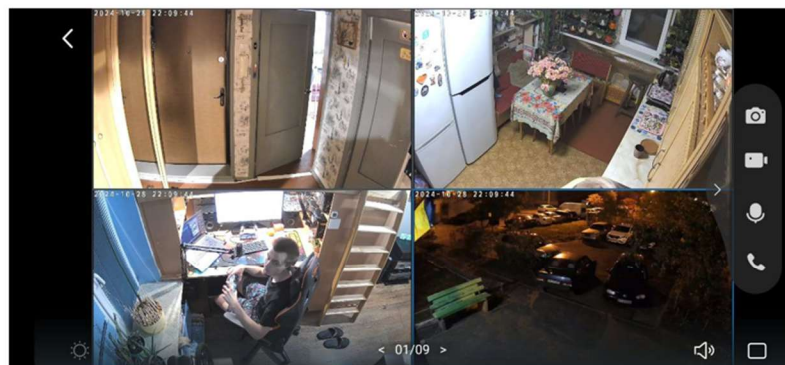


Рис. 3.6 – Одночасний перегляд зі 4 камер відеоспостереження TP-Link серії Таро в різних локаціях (9 зон – 32 камери максимум)

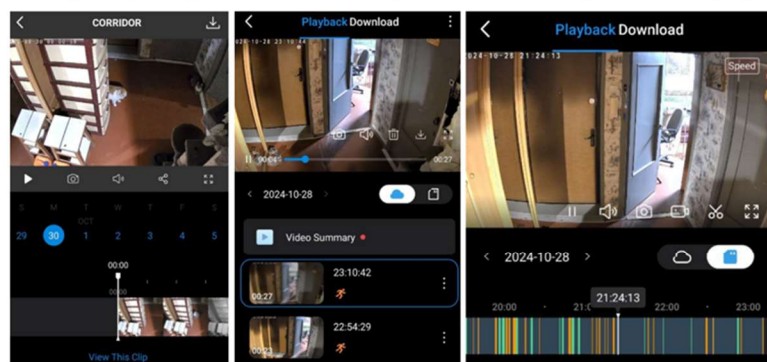


Рис. 3.11 – Порівняння хмарного та локального сховища (підсумковий ролик у хмарному, зручна часова шкала у локальному)

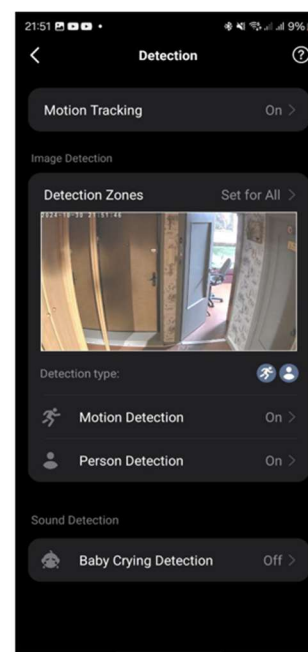


Рис. 3.21 – Функції на основі машинного навчання (трекінг по зонах, детекція по руху, виявлення людини та плачу дитини)

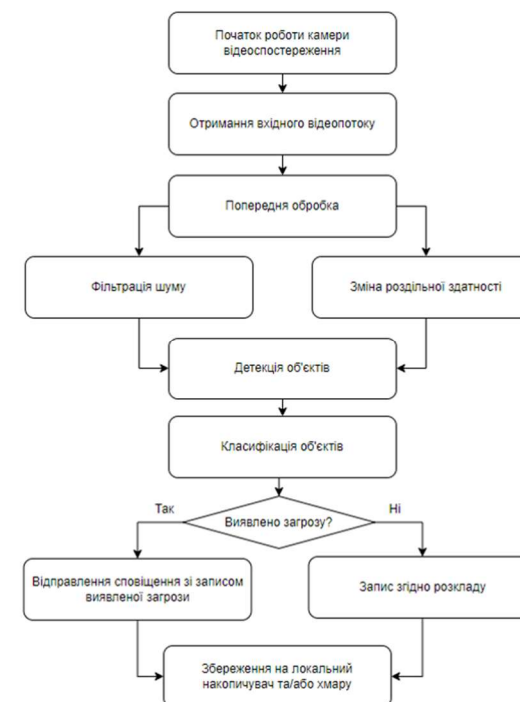


Рис. 3.22 – Схема роботи машинного навчання на предмет шаблонної детекції та класифікації об'єктів

Власний сервер для реалізації закритого локального спостереження

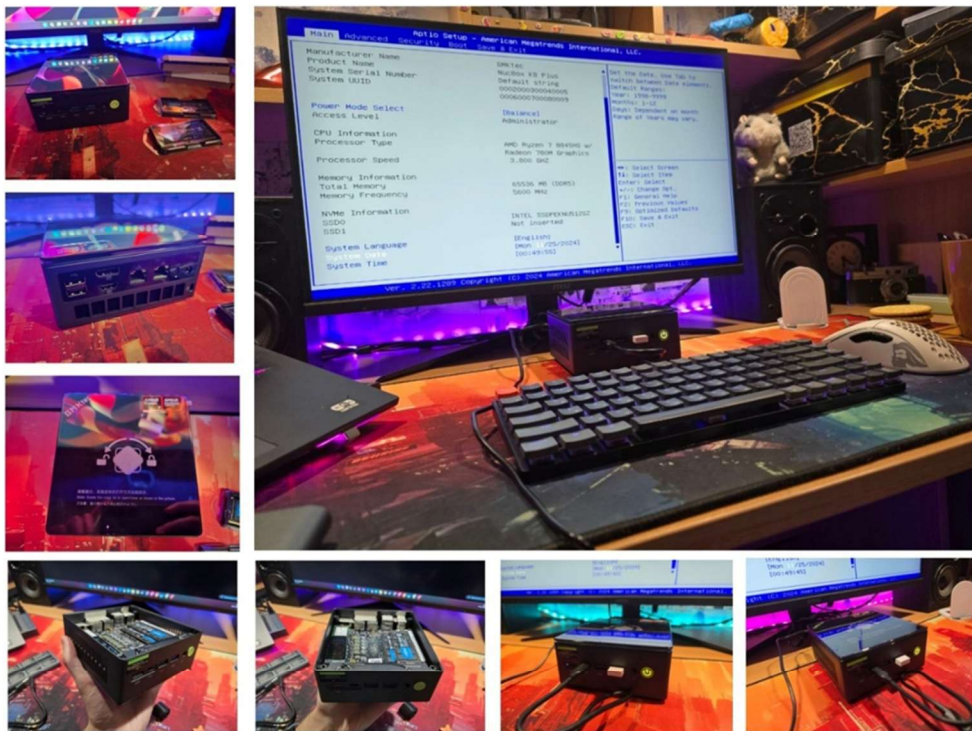


Рис. 3.12 – Сервер на базі міні-ПК GMKtec NucBox K8 Plus та його інтерфейс

Характеристика	GMKtec K8 Plus
Процесор	AMD Ryzen 7 8845HS (8 ядер, 16 потоків)
Оперативна пам'ять	До 96 ГБ DDR5, частота до 5600 МГц (2 слоти)
Накопичувачі	Підтримка до 2x M.2 2280 PCIe 4.0 SSD (до 8 ТБ)
Графіка	Вбудована графіка Radeon 780M, можливість підключення eGPU через OCuLink
Порти	2x USB 4.0, HDMI, DisplayPort, 2x Ethernet (2.5 Гбіт/с), Wi-Fi, Bluetooth 5.2
Підтримка дисплеїв	До 4 дисплеїв одночасно
Розміри	135 x 125 x 58 мм
Операційна система	Підтримка Windows 11 Pro (опціонально)
Ціна	Від \$389.99

Табл. 3.1 – Технічні характеристики міні-ПК GMKtec K8 Plus

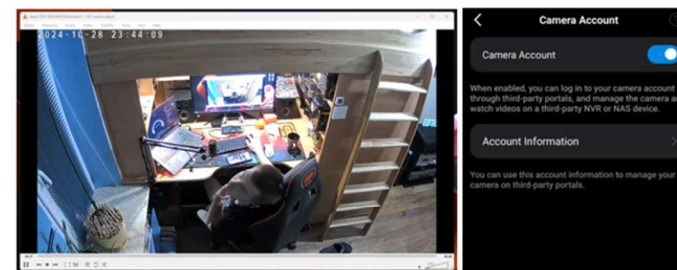


Рис. 3.14 – Обхід хмарних сервісів TP-Link через протокол RTSP (порт 554) (попередньо має бути створено акаунт у додатку TP-Link Таро для отримання доступу до RTSP потоку)

Proxmox та Home Assistant: інтеграція motionEye для моніторингу

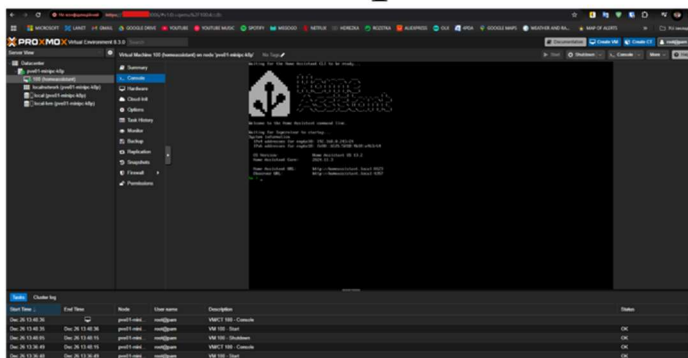


Рис. 3.31 – Ініційований сервіс Home Assistant на міні-ПК для роботи 24/7

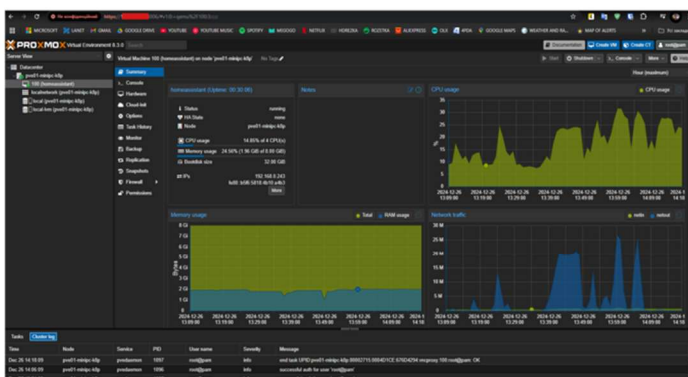


Рис. 3.32 – Гнучкий контроль над запущеними вузлами завдяки гіпервізору 1-го типу Proxmox

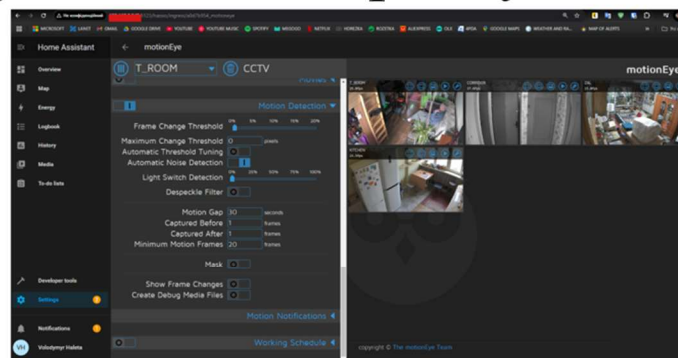


Рис. 3.15 – Налаштування детекції на рух у сервісі Home Assistant через доповнення motionEye

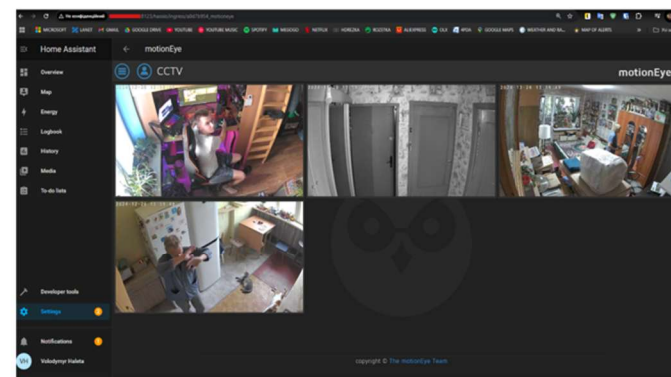


Рис. 3.30 – Камери відеоспостереження підключенні до сервісу Home Assistant через доповнення motionEye

Кошторис реалізації інтелектуальної системи відеоспостереження

№	Найменування обладнання/сервіси	К-сть	Орієнтовна ціна за одиницю (грн)	Загальна вартість (грн)
1	Маршрутизатор TP-Link Archer AX73	1	4 999	4 999
2	Маршрутизатор TP-Link Archer AX53	1	2 799	2 799
3	Маршрутизатор TP-Link Archer C64	1	1 399	1 399
4	Камера відеоспостереження TP-Link Tapo C100	1	1 099	1 099
5	Камера відеоспостереження TP-Link Tapo C200	3	1 499	4 497
6	Камера відеоспостереження TP-Link Tapo C310	1	1 999	1 999
7	Карта пам'яті Kingston 128GB microSDXC Class 10 Canvas Select Plus	5	419	2 095
8	TP-Link Tapo Care (підписка на хмарний сервіс)	2	95 (на міс.)	190 (на міс.)
9	Джерело безперебійного живлення DC1018P DC UPS 10400 mAh	3	1 100	3 300
10	Міні-ПК GMKtec K8 Plus	1	15 200 (без комплектації) 29 000 (3)	29 000
11	Гіпервізор 1-го типу Proxmox	1	безкоштовно	безкоштовно
12	Home Assistant OS + доповнення motionEye	1	безкоштовно	безкоштовно
Разом:				51 377 грн

Табл. 3.2 – Специфікація обладнання із зазначенням кількості та вартості

Порівняльний аналіз традиційних систем відеоспостереження та запропонованого рішення

Критерій	Традиційні системи	Запропоноване рішення
Вартість впровадження	Висока, включає сервери, ліцензії, складну інфраструктуру	51,377 грн за всі компоненти, з яких 29000 грн, економічно ефективне рішення
Гнучкість та масштабованість	Обмежена; кожне нове розширення потребує значних витрат	Легко масштабувати за допомогою Proxmox та Home Assistant OS, додавання нових пристроїв доступне
Збереження даних	Здебільшого централізоване, потребує серверів або дорогих хмарних підписок	Локальне (карти пам'яті Kingston) + хмарне (TP-Link Tapo Care)
Автономність	Залежність від централізованого енергопостачання, висока вразливість до перебоїв живлення	Низьке споживання – 5.4 Вт (одна камера); ДБЖ забезпечує резервне живлення для ключових компонентів (основна камера: ~ 20 годин; мережеве обладнання: ~ 4 години 10 хвилин)
Автоматизація та аналітика	Додаткові функції доступні лише через дорогі рішення або стороннє ПЗ	Інтеграція з Home Assistant OS та motionEye забезпечує автоматизацію та базову відеоаналітику
Якість обладнання	Висока, але вартість часто завищена через брендову інтеграцію	Камери TP-Link Tapo та маршрутизатори Wi-Fi 6 забезпечують високу якість за доступною ціною

Табл. 4.1 – Порівняння запропонованого рішення над традиційними

Висновки

Інтелектуальні децентралізовані системи відеоспостереження надають значно більше можливостей порівняно з традиційними. Навіть кілька камер одного виробника забезпечують розширений функціонал, що робить їх привабливими для вирішення локальних завдань безпеки, таких як захист житла чи невеликих об'єктів, де достатньо однієї-двох камер.

Завдяки автономності, такі камери не залежать від централізованого управління чи складної інфраструктури. Вони енергоефективні, мобільні та можуть працювати як із мережею, так і без неї, з можливістю налаштування віддаленого доступу через Wi-Fi, що робить їх зручнішою та ефективнішою альтернативою традиційним системам.

Інтелектуальні децентралізовані камери можуть інтегруватися в сучасні системи управління, такі як «розумні міста» чи «розумні будинки», забезпечуючи взаємодію з іншими датчиками для аналізу даних і прийняття рішень у реальному часі. Завдяки автономності, мобільності та енергоефективності їх можна використовувати в місцях без стабільного електроживлення, зокрема в урбанізованих або важкодоступних районах.

Такі системи мають широкий потенціал для вдосконалення завдяки інтеграції з новітніми технологіями, зокрема платформами для централізованого управління, що сприяє підвищенню зручності та ефективності їх використання в різних сферах.

Публікації та апробація роботи

1. Галета В.С., Сімбіоз відеоспостереження та розумного будинку. «Проблеми комп'ютерної інженерії» : Науково-практ. конф., м.Київ, 1 грудня 2023 р. С. 3-4. URL: https://duikt.edu.ua/uploads/p_2626_33497568.pdf
2. Галета В.С., Антоненко А.В. Чому система відеоспостереження не панацея, а єдине вірне рішення забезпечення безпеки. «Сучасний стан та перспективи розвитку ІОТ» : V Науково-техн. конф., м.Київ, 18 квітня 2024 р. С. 91-94. URL: https://duikt.edu.ua/uploads/p_2661_70423010.pdf
3. Галета В.С., Антоненко А.В. Реалізація децентралізованих систем відеоспостереження з використанням ІР-камер та інтеграцією з хмарним сховищем. «Застосування програмного забезпечення в ІКТ» : Всеукр. науково-техн. конф., м.Київ, 24 квітня 2024 р. С. 427-430. URL: https://duikt.edu.ua/uploads/p_2661_45497999.pdf
4. Zaitsev, I., Antonenko, A., Dakova, L., Haleta, V. Implementation of network IP cameras in video surveillance systems with integration with cloud storage for decentralized monitoring. «Sustainability of education and science in conditions of transformation» : International scientific and practical conference, Kyiv, May 21-22, 2024. P. 80-82. URL: https://istu.edu.ua/wp-content/uploads/2024/07/Materialy_II_Mizhnarodnoi_naukovo_praktychnoi_konferentsii_2024_compressed.pdf
5. Лемешко А.В., Галета В.С. Використання маршрутизатора як точки доступу для розповсюдження мережі WI-FI у важкодоступних місцях. «Інформаційні технології та цифрова економіка» : V Міжн. науково-техн. конф., м.Київ, 9-10 травня 2024 р. С. 104-105. URL: https://files.duit.edu.ua/uploads/%D0%A1%D0%B0%D0%B9%D1%82/3_%D0%9D%D0%90%D0%A3%D0%9A%D0%90/conferences/international-scientific-and-practical-conferences/information-technology-digital-economy.pdf
6. USE OF ARTIFICIAL INTELLIGENCE IN AUTOMATED SYSTEMS / A. ANTONENKO, M. PAKHOMOV, T. KALYTA, V. HALETA, et al. Herald of Khmelnytskyi National University. Technical sciences. 2023. Vol. 323, no. 4. P. 11–20. URL: <https://www.doi.org/10.31891/2307-5732-2023-323-4> (date of access: 03.11.2024).
7. OBJECT RECOGNITION SYSTEMS USING INTELLIGENT TECHNOLOGIES IN UAV / A. ANTONENKO, D. SKUDNYI, V. HALETA, M. YURII, V. HUMINIUK, A. BURACHYNSKYI, S. VOSTRIKOV, A. BALVAK, D. KOROTIN, A. TVERDOKHLIB, G.OLEKSII, S. POPERESHNYAK, O. TKACHENKO, O. GOLUBENKO, D. TUZHILIN. European Science, 2(sge29-02) (2024), P.50–82. URL: <https://doi.org/10.30890/2709-2313.2024-29-00-010> (date of access: 03.11.2024).