ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
Кафедра Мобільних та відеоінформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Методи оптимізації використання систем відеонагляду на основі хмарних технологій»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Телекомунікації та радіотехніка
освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

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

(підпис) Ростислав ЗОСІМОВ
(Ім'я, ПРІЗВИЩЕ)

Виконав: здобувач вищої освіти
групи АРДМ-61
Ростислав ЗОСІМОВ

Керівник: Віталій СТРЕЛЬНІКОВ

Рецензент: К. Лаврінець

Київ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

Кафедра	Мобільних та відеоінформаційних технологій
Ступінь вищої освіти	Магістр
Спеціальність	172 Телекомунікації та радіотехніка
Освітньо-професійна програма	Апаратура радіозв'язку, радіомовлення і телебачення

ЗАТВЕРДЖУЮ
Завідувачка кафедрою МВТ
_____ Наталія РУДЕНКО
« » _____ 2023 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Зосімову Ростиславу Ігоровичу

1. Тема кваліфікаційної роботи: «Методи оптимізації використання систем відеонагляду на основі хмарних технологій»,
керівник кваліфікаційної роботи Віталій СТРЕЛЬНІКОВ, PhD,
затверджені наказом Державного університету інформаційно-комунікаційних технологій від 19.10.2023 р. №145.

2. Строк подання кваліфікаційної роботи 25.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
   1. Відеоспостереження як послуга VSaaS;
   2. Сервіси доступу до хмарного середовища відеоспостереження;
   3. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
   1. 1. Особливості застосування відеонагляду на основі хмарних технологій;
   2. Дослідження архітектури хмарних систем відеоспостереження;
   3. Монтаж систем відеоспостереження та підключення до хмарних сервісів.

5. Перелік ілюстративного матеріалу: презентація.

6. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Підбір науково-технічної літератури	19.10.23	Викон.
2.	Особливості застосування відеонагляду на основі хмарних технологій	31.10.23	Викон.
3.	Дослідження архітектури хмарних систем відеоспостереження	15.11.23	Викон.
4.	Монтаж систем відеоспостереження та підключення до хмарних сервісів	29.11.23	Викон.
5.	Висновки, вступ, реферат	11.12.23	Викон.
6.	Розробка презентації	18.12.23	Викон.

Здобувач вищої освіти _____ Ростислав ЗОСІМОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Віталій СТРЕЛЬНІКОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 80 стор., 15 рис., 2 табл., 23 дж.

Мета роботи – дослідження систем відеонагляду на основі хмарних технологій.

Об'єкт дослідження – процес відеоспостереження, передачі і обробки відеоданих на різних етапах моделі "Відеоспостереження як послуга VSaaS".

Предмет дослідження – архітектура та методи побудови систем відеонагляду, які використовують хмарні технології для зберігання та обробки даних.

Короткий зміст роботи: В першому розділі досліджено особливості застосування відеонагляду на основі хмарних технологій. Розглянуто базові елементи побудови та функціонування хмарних технологій, такі як IaaS, PaaS і SaaS, та розроблена детальна схема "Відеоспостереження як послуга (VSaaS)" яка базується на моделі сервісу "Програмне забезпечення як послуга (SaaS)".

На основі виконаних досліджень розроблена таблиця порівняння традиційних і хмарних систем відеоспостереження, яка вказує на явну перевагу VSaaS над традиційними системами майже у всіх випадках.

У другому розділі досліджено архітектуру розгортання хмарних системи відеоспостереження та розроблено таблицю яка допоможе визначити проблеми і варіантів проектування, пов'язаних із хмарною мультимедійною системою спостереження. Досліджено види камер відеоспостереження за призначенням.

У третьому розділі досліджено особливості монтажу систем відеоспостереження та розглянуто сервіси доступу до хмарного середовища відеоспостереження та контролю. Проведено практичне підключення відеокамери Axis до хмарного сервісу Camcloud.

КЛЮЧОВІ СЛОВА: ВІДЕОСПОСТЕРЕЖЕННЯ ЯК ПОСЛУГА (VSAAS), ХМАРНІ ТЕХНОЛОГІЇ, АРХІТЕКТУРА РОЗГОРТАННЯ, ВИДИ КАМЕР ВІДЕОСПОСТЕРЕЖЕННЯ, ПІДГОТОВКА ДО МОНТАЖУ, СЕРВІСИ ДОСТУПУ ДО ХМАРНОГО СЕРЕДОВИЩА ВІДЕОСПОСТЕРЕЖЕННЯ, HIKVISION, HIK-CONNECT, CAMCLOUD

ABSTRACT

Text part of the master's qualification work: 80 pages, 15 pictures, 2 table, 23 sources.

The purpose of the work - research of video surveillance systems based on cloud technologies.

Object of research – the process of video surveillance, transmission and processing of video data at various stages of the "Video surveillance as a VSaaS service" model.

Subject of research – architecture and construction methods of video surveillance systems that use cloud technologies for data storage and processing.

Summary of the work: The first chapter examines the features of the application of video surveillance based on cloud technologies. The basic elements of the construction and operation of cloud technologies, such as IaaS, PaaS and SaaS, are considered, and a detailed scheme of "Video surveillance as a service (VSaaS)" based on the "Software as a service (SaaS)" service model is developed.

Based on the research, a comparison table of traditional and cloud video surveillance systems has been developed, which indicates a clear advantage of VSaaS over traditional systems in almost all cases.

In the second chapter, the architecture of the deployment of cloud-based video surveillance systems is studied and a table is developed that will help to identify problems and design options related to cloud-based multimedia surveillance systems. The types of video surveillance cameras according to their purpose have been studied.

The third chapter examines the peculiarities of installing video surveillance systems and considers the services of access to the cloud environment of video surveillance and control. A practical connection of the Axis video camera to the Camcloud cloud service was carried out.

KEYWORDS: VIDEO SURVEILLANCE AS A SERVICE (VSAAS), CLOUD TECHNOLOGIES, DEPLOYMENT ARCHITECTURE, TYPES OF VIDEO SURVEILLANCE CAMERAS, PREPARATION FOR INSTALLATION, ACCESS SERVICES TO CLOUD VIDEO SURVEILLANCE ENVIRONMENT, HIKVISION, HIK-CONNECT, CAMCLOUD

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Зосімов Р.І. до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю 172 Телекомунікації та радіотехніка
освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

на тему: Методи оптимізації використання систем відеонагляду на основі хмарних технологій

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Зосімов Ростислав Ігорович показав гарну теоретичну та інженерну підготовку, уміння володіти технологіями нового покоління, вміло працювати з програмно-апаратними засобами мобільного зв'язку, довідковою і науково-технічною літературою. Працюючи над завданнями, які доручались керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу Зосімова Ростислава Ігоровича на оцінку «відмінно» та присвоїти йому кваліфікацію «Магістр з телекомунікацій та радіотехніки».

Керівник кваліфікаційної роботи _____ Віталій СТРЕЛЬНІКОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

" " _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Зосімов Р.І.
(прізвище та ініціали)

допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувачка кафедри
Мобільних та відеоінформаційних технологій _____ Наталія РУДЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

" " _____ 2023 року

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

здобувача вищої освіти Зосімова Ростислава Ігоровича

на тему: «Методи оптимізації використання систем відеонагляду на основі хмарних технологій»

Актуальність:

Системи відеоспостереження на основі хмарних технологій є дуже перспективними рішеннями для багатьох компаній та організацій. Вони дозволяють ефективно використовувати потужність хмарних сервісів та забезпечують більшу безпеку та ефективність в порівнянні з традиційними системами відеоспостереження.

На даний момент проблеми які виникають на шляху побудови систем відеонагляду на базі хмарних технологій не достатньо висвітлені у науково-технічній літературі, що робить актуальною тему магістерської роботи.

Позитивні сторони:

Робота викладена науковою мовою, логічно й послідовно відбиває мету та поставлені в роботі завдання. Пояснювальна записка відповідає стандартам до її оформлення.

Проведені розрахунки свідчать про високий науково-технічний рівень використання інформаційних технологій в даному дослідженні.

Недоліки:

1. Таблиця 1.1 не висвітлює недоліки хмарних методів зберігання та обробки даних, які існують не дивлячись на переваги цих методів, наприклад, потреба в постійному інтернет з'єднанні.

2. Архітектура на рис. 2.1 не достатньо деталізована.

Висновок: кваліфікаційна робота заслуговує оцінку «відмінно», а здобувач Зосімов Ростислав Ігорович заслуговує присвоєння кваліфікації: «Магістр з телекомунікацій та радіотехніки».

Рецензент: КТН, доцент *(науковий ступінь, вчене звання)* *(підпис)* К. Лаврінець *(Ім'я, ПРІЗВИЩЕ)*

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 9
ВСТУП 10
1 ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ВІДЕОНАГЛЯДУ НА ОСНОВІ ХМАРНИХ ТЕХНОЛОГІЙ 12
1.1 Базові елементи побудови та функціонування хмарних технологій 12
1.2 Особливості сервісної моделі "Відеоспостереження як послуга VSaaS" 23
2 РОЗРОБКА АРХІТЕКТУРИ ХМАРНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ 33
2.1 Архітектура розгортання хмарних системи відеоспостереження 33
2.2 Види камер відеоспостереження за призначенням 49
3 МОНТАЖ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ТА ПІДКЛЮЧЕННЯ ДО ХМАРНИХ СЕРВІСІВ 60
3.1 Монтаж систем відеоспостереження 60
3.2 Сервіси доступу до хмарного середовища відеоспостереження та контролю 69
ВИСНОВКИ 82
ПЕРЕЛІК ПОСИЛАНЬ 84
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 87

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DVB (Digital Video Broadcasting) - Цифрове телевізійне мовлення.

EBU (European Broadcasting Union - Європейський Союз Мовлення) - Керівна організація в області радіомовлення в Європі.

HDTV (High - Definition Television. Телебачення високого розділення.

IaaS (Infrastcomcture as a service) - Інфраструктура як послуга.

IEEE (Institute of Electrical and Electronical Engineers) - інститут інженерів по електротехніці і радіоелектроніці.

ITU (International Telecommunication Union) - Міжнародний союз електрозв'язку (МСЕ). Одна з функцій цієї організації - підготовка Рекомендацій, які фактично є міжнародними стандартами.

MPEG (Moving Picture Expert Group) - Група експертів по зображенням, що рухаються. Робоча група ISO, що займається розробкою стандартів кодування і стискування відео- і аудіо- даних. Назва групи є присутньою в назвах стандартів.

OFDM (Orthogonal Frequency Division Multiplex) - Ортогональне частотне мультиплексування. Один з видів модуляції, вживаних в системах цифрового ТБ.

PaaS (Platform as a service) - Платформа як послуга.

SaaS (Software as a service) - Програмне забезпечення як послуга.

ВСТУП

Системи відеоспостереження на основі хмарних технологій - це високотехнологічні рішення, що дозволяють збирати, зберігати та аналізувати великі обсяги відеоданих з використанням потужності хмарних сервісів. Такі системи стають все більш популярними через їх більшу ефективність, безпеку та зниження вартості в порівнянні з традиційними системами відеоспостереження.

Хмарні системи відеоспостереження — це тип цифрової системи відеоспостереження, яка використовує хмарні технології для зберігання та керування відзнятим матеріалом. Ці системи пропонують кілька функцій, включаючи віддалений доступ до відзнятого матеріалу, моніторинг у реальному часі та масштабованість. Компоненти хмарних систем відеоспостереження включають камери, мережеві відеореєстратори, хмарні сховища та програмне забезпечення для керування та аналізу відзнятих матеріалів. Переваги хмарних систем відеоспостереження включають економічну ефективність, гнучкість і простоту використання. Однак деякі обмеження включають занепокоєння щодо конфіденційності та безпеки даних.

Однією з головних переваг систем відеоспостереження на основі хмарних технологій є їх гнучкість. За допомогою таких систем можна здійснювати відеоспостереження з будь-якого місця з Інтернет-підключенням. Також вони дозволяють віддалено керувати камерами відеоспостереження та отримувати детальну інформацію про стан системи в режимі реального часу.

Іншою важливою перевагою систем відеоспостереження на основі хмарних технологій є їх безпека. Завдяки використанню хмарних сервісів, відеодані зберігаються в безпечних місцях, що забезпечує їх конфіденційність та захищеність від несанкціонованого доступу.

Окрім того, системи відеоспостереження на основі хмарних технологій дозволяють ефективно використовувати аналіз даних, що отримані з камер відеоспостереження. Це дозволяє розпізнавати обличчя, автомобілі та інші об'єкти на відео, а також виявляти небажані події, наприклад, крадіжки або вандалізм.

Не зважаючи на переваги, системи відеоспостереження на основі хмарних технологій також мають свої недоліки. Одним з головних недоліків є залежність від Інтернет-підключення, що може стати перешкодою у випадку відсутності мережі. Також віддалене збереження відеоданих може вимагати додаткових витрат на оплату хмарних сервісів, що може збільшувати загальну вартість системи відеоспостереження.

Однак, не зважаючи на недоліки, системи відеоспостереження на основі хмарних технологій є дуже перспективними рішеннями для багатьох компаній та організацій. Вони дозволяють ефективно використовувати потужність хмарних сервісів та забезпечують більшу безпеку та ефективність в порівнянні з традиційними системами відеоспостереження.

У світлі зростаючої кількості інцидентів, пов'язаних з безпекою, дослідження хмарних систем відеонагляду має велике значення для розвитку сучасних підходів до забезпечення безпеки, а також надання широкого спектру послуг та можливостей для різних відомств та користувачів.

Метою роботи є дослідження систем відеонагляду на основі хмарних технологій.

Об'єктом дослідження є процес відеоспостереження, передачі і обробки відеоданих на різних етапах моделі "Відеоспостереження як послуга VSaaS".

Предметом дослідження є архітектура, принципи роботи та методи побудови систем відеонагляду, які використовують хмарні технології для зберігання та обробки даних.

1 ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ВІДЕОНАГЛЯДУ НА ОСНОВІ ХМАРНИХ ТЕХНОЛОГІЙ

1.1 Базові елементи побудови та функціонування хмарних технологій

Термін «хмара», який використовується в цьому офіційному документі, схоже, походить від мережевих схем, які представляють Інтернет або різні його частини у вигляді схематичних хмар. «Хмарні обчислення» були придумані для того, що відбувається, коли програми та служби переміщуються в інтернет-«хмару». Хмарні обчислення – це не щось, що з'явилося раптово за одну ніч; у певній формі це може йти до того часу, коли комп'ютерні системи дистанційно розподіляли обчислювальні ресурси та програми. Однак на даний момент хмарні обчислення стосуються багатьох різних типів послуг і програм, які надаються в Інтернет-хмарі, і того факту, що в багатьох випадках пристрої, які використовуються для доступу до цих послуг і програм, не потребують спеціальних програм [1].

Багато компаній надають послуги з хмари. Ось кілька помітних прикладів:

- Google — має приватну хмару, яку використовує для надання своїм користувачам документів Google та багатьох інших служб, включаючи доступ до електронної пошти, програми для документів, переклад тексту, карти, веб-аналітику та багато іншого.

- Microsoft — має онлайн-сервіс Microsoft Office 365, який дозволяє переміщувати вміст і інструменти бізнес-аналітики в хмару, і Microsoft наразі робить свої офісні програми доступними в хмарі.

- Salesforce.com — запускає свій набір програм для своїх клієнтів у хмарі, а його продукти Force.com і Vmforce.com надають розробникам платформи для створення індивідуальних хмарних сервісів.

Але що таке хмарні обчислення? У наступних розділах описано характеристики хмари та хмарних обчислень, моделі послуг, моделі розгортання, переваги та проблеми.

Хмарні обчислення мають різноманітні характеристики, основні з яких:

- Спільна інфраструктура — використовує віртуалізовану модель програмного забезпечення, уможливлюючи спільне використання фізичних послуг, сховища та мережевих можливостей. Хмарна інфраструктура, незалежно від моделі розгортання, прагне максимально використати доступну інфраструктуру для кількох користувачів.

- Динамічне надання — дозволяє надавати послуги на основі поточних вимог попиту. Це робиться автоматично за допомогою автоматизації програмного забезпечення, що дозволяє розширювати та скорочувати можливості обслуговування за потреби. Таке динамічне масштабування необхідно виконувати, зберігаючи високий рівень надійності та безпеки.

- Доступ до мережі — потрібен доступ через Інтернет із широкого діапазону пристроїв, таких як ПК, ноутбуки та мобільні пристрої, за допомогою API на основі стандартів (наприклад, на основі HTTP). Розгортання служб у хмарі включає все: від використання бізнес-додатків до найновіших програм на найновіших смартфонах.

- Кероване вимірювання — використовує вимірювання для керування та оптимізації послуги, а також для надання звітної та платіжної інформації. Таким чином, споживачам виставляються рахунки за послуги відповідно до того, скільки вони фактично використали протягом розрахункового періоду.

Хмарні технології зробили революцію в тому, як бізнес працює та зберігає дані. Ця технологія стає все більш популярною за останні кілька років, і її переваги незаперечні. Хмарні технології пропонують організаціям масштабований, гнучкий і економічно ефективний спосіб керування даними та програмами.

Хмарні технології стосуються використання віддалених серверів для зберігання, керування та обробки даних і програм. Хмара — це, по суті, мережа серверів, які об'єднані разом і працюють як єдина система. Існує три типи хмарних технологій: публічні, приватні та гібридні. Публічні хмари належать і управляються сторонніми постачальниками та доступні для широкої громадськості. Приватні хмари, з іншого боку, належать і управляються однією

організацією і недоступні для громадськості. Гібридні хмари — це комбінація публічних і приватних хмар. Хмарні технології характеризуються масштабованістю, гнучкістю та економічною ефективністю. Вони дозволяють організаціям легко збільшувати або зменшувати свої обчислювальні ресурси залежно від своїх потреб, і вони економічно ефективніші, ніж традиційні локальні рішення.

Хмарні технології працюють за допомогою віртуалізації та хмарної інфраструктури. Віртуалізація — це процес створення віртуальної версії чогось, наприклад сервера, операційної системи або пристрою зберігання. Хмарна інфраструктура стосується апаратних і програмних компонентів, які використовуються для створення та керування хмарою. Існує три моделі хмарних послуг: програмне забезпечення як послуга (SaaS), платформа як послуга (PaaS) та інфраструктура як послуга (IaaS). SaaS надає програми через Інтернет, PaaS надає платформу для розробки та розгортання програм, а IaaS надає віртуалізовані обчислювальні ресурси через Інтернет. Існує також три моделі розгортання хмари: публічна, приватна та гібридна. Загальнодоступні хмари доступні для широкої громадськості, приватні хмари доступні лише одній організації, а гібридні хмари являють собою комбінацію публічних і приватних хмар.

Хмарні технології пропонують організаціям кілька переваг, зокрема економію коштів, гнучкість, масштабованість, доступність і безпеку. Економія коштів досягається за рахунок усунення потреби у локальному обладнанні та програмному забезпеченні та за допомогою моделі оплати за використання обчислювальних ресурсів. Гнучкість і масштабованість досягаються, дозволяючи організаціям легко збільшувати або зменшувати свої обчислювальні ресурси відповідно до своїх потреб. Доступність досягається завдяки дозволу користувачам отримувати доступ до своїх даних і програм з будь-якого місця, де є підключення до Інтернету. Безпека досягається шляхом забезпечення безпечного доступу до даних і програм, а також наданням послуг резервного копіювання та аварійного відновлення. Однак хмарні технології також створюють ряд проблем, зокрема безпеку даних, прив'язаність до постачальника, відповідність вимогам та

інтеграцію із застарілими системами. Організації повинні ретельно розглянути ці проблеми, перш ніж застосовувати хмарні технології.

Коротше кажучи, хмарні обчислення дозволяють надавати спільний доступ і масштабоване розгортання послуг за потреби майже з будь-якого місця, за які клієнт може виставляти рахунок на основі фактичного використання.

Сервісні моделі. Після створення хмари спосіб розгортання її послуг хмарних обчислень з точки зору бізнес-моделей може відрізнятися залежно від вимог. Основні моделі послуг, які розгортаються (рис. 1.1), зазвичай відомі як [1]:

- Програмне забезпечення як послуга (SaaS) — споживачі купують можливість доступу та використання програми чи послуги, розміщеної в хмарі. Еталонним прикладом цього є Salesforce.com, як обговорювалося раніше, де необхідна інформація для взаємодії між споживачем і службою розміщена як частина послуги в хмарі.

Крім того, корпорація Майкрософт зробила значні інвестиції в цю сферу, і як частина опції хмарних обчислень для Microsoft Office 365, її пакет Office доступний як передплата через її хмарні онлайн-сервіси.

- Платформа як послуга (PaaS) — споживачі купують доступ до платформ, що дозволяє їм розгортати власне програмне забезпечення та програми в хмарі. Споживач не керує операційними системами та доступом до мережі, тому можуть існувати обмеження щодо того, які програми можна розгортати. Приклади включають Amazon Web Services (AWS), Rackspace і Microsoft Azure.

- Інфраструктура як послуга (IaaS) — споживачі контролюють і керують системами з точки зору операційних систем, програм, сховищ і підключення до мережі, але самі не контролюють хмарну інфраструктуру.



Рис. 1.1. Типи моделі сервісу

Також відомі різні підмножини цих моделей, які можуть бути пов'язані з певною галуззю чи ринком. Зв'язок як послуга (CaaS) є однією з таких моделей підмножини, яка використовується для опису розміщених послуг IP-телефонії. Разом із переходом до CaaS відбувається перехід до більш орієнтованого на IP зв'язку та розгортання більшої кількості транкінгів SIP. З IP і SIP розмістити АТС у хмарі так само легко, як і на місці. У цьому контексті CaaS можна розглядати як підмножину SaaS.

Моделі розгортання. Розгортання хмарних обчислень може відрізнятися залежно від вимог, і було визначено наступні чотири моделі розгортання, кожна з яких має певні характеристики, які відповідають потребам послуг і користувачів хмар певним чином (рис. 1.2).

- Приватна хмара — хмарна інфраструктура була розгорнута, підтримується та експлуатується для певної організації. Операція може здійснюватися на території підприємства або за участю третьої сторони.

- Хмара спільноти — хмарна інфраструктура спільно використовується кількома організаціями зі схожими інтересами та вимогами. Це може допомогти обмежити капітальні витрати на його створення, оскільки витрати розподіляються між організаціями. Операція може здійснюватися на території підприємства або за участю третьої сторони.

- Громадська хмара — хмарна інфраструктура доступна для громадськості на комерційній основі постачальником хмарних послуг. Це дозволяє споживачеві розробляти та розгортати службу в хмарі з дуже невеликими фінансовими витратами порівняно з вимогами капітальних витрат, які зазвичай пов'язані з іншими варіантами розгортання.

- Гібридна хмара — хмарна інфраструктура складається з кількох хмар будь-якого типу, але хмари мають можливість через свої інтерфейси дозволяти переміщувати дані та/або програми з однієї хмари в іншу. Це може бути поєднання приватних і загальнодоступних хмар, які підтримують вимогу зберігати деякі дані в організації, а також потребу пропонувати послуги в хмарі.



Рис. 1.2. Приклад розгортання публічної, приватної та гібридної хмари

Нижче наведено деякі з можливих переваг для тих, хто пропонує послуги та програми на основі хмарних обчислень:

- Економія — Компанії можуть зменшити свої капітальні витрати та використати операційні витрати для збільшення своїх обчислювальних можливостей. Це менший бар'єр для входу, а також вимагає менше внутрішніх IT-ресурсів для забезпечення системної підтримки.

- Масштабованість/гнучкість — компанії можуть розпочати з невеликого розгортання та досить швидко розростатися до великого, а потім, якщо необхідно, зменшувати масштаб. Крім того, гнучкість хмарних обчислень дозволяє компаніям використовувати додаткові ресурси в години пік, дозволяючи їм задовольняти запити споживачів.

- Надійність — служби, що використовують кілька резервних сайтів, можуть підтримувати безперервність роботи та аварійне відновлення.

- Технічне обслуговування — постачальники хмарних послуг здійснюють технічне обслуговування системи, а доступ здійснюється через API, які не вимагають інсталяції програм на ПК, що ще більше зменшує вимоги до обслуговування.

- Мобільна доступність — мобільні працівники підвищили продуктивність завдяки системам, доступним в інфраструктурі, доступній звідусіль.

Нижче наведено деякі з помітних проблем, пов'язаних із хмарними обчисленнями, і хоча деякі з них можуть спричинити уповільнення при наданні додаткових послуг у хмарі, більшість також може надати нові можливості, якщо їх

вирішити з належною увагою та увагою на етапах планування.

- Безпека та конфіденційність. Можливо, дві з найбільш «гарячих» проблем, пов'язаних із хмарними обчисленнями, стосуються зберігання та захисту даних, а також моніторингу використання хмари постачальниками послуг. Зазвичай ці проблеми пов'язані з уповільненням розгортання хмарних служб. Ці проблеми можна вирішити, наприклад, шляхом зберігання внутрішньої інформації організації, але дозволяючи використовувати її в хмарі. Однак, щоб це сталося, механізми безпеки між організацією та хмарою мають бути надійними, і гібридна хмара може підтримувати таке розгортання.

- Відсутність стандартів — Хмари мають задокументовані інтерфейси; однак з ними не пов'язано жодного стандарту, і тому малоймовірно, що більшість хмар будуть сумісні. Open Grid Forum розробляє Open Cloud Computing Interface, щоб вирішити цю проблему, а Open Cloud Consortium працює над стандартами та практиками хмарних обчислень. Висновки цих груп потребуватимуть удосконалення, але невідомо, чи відповідатимуть вони потребам людей, які розгортають послуги, і конкретним інтерфейсам, потрібним цим службам. Однак постійне оновлення останніх стандартів у міру їх розвитку дозволить використовувати їх, якщо це можливо.

- Постійно розвивається — Вимоги користувачів постійно розвиваються, як і вимоги до інтерфейсів, мереж і зберігання. Це означає, що «хмара», особливо публічна, не залишається статичною, а також постійно розвивається.

- Занепокоєння щодо відповідності — Закон Сарбейнса-Оксли (SOX) у США та директиви щодо захисту даних у ЄС є лише двома з багатьох проблем відповідності, які впливають на хмарні обчислення, залежно від типу даних і програм, для яких використовується хмара. ЄС має законодавчу підтримку для захисту даних у всіх державах-членах, але в США захист даних відрізняється і може відрізнятися від штату до штату. Як і у випадку з безпекою та конфіденційністю, згаданими раніше, вони зазвичай призводять до розгортання гібридної хмари, де одна хмара зберігає внутрішні дані організації.

Комунікації в хмарі. Хмарні обчислення, які передбачають надання

обчислювальних послуг через Інтернет, революціонізували спосіб зберігання, доступу та обміну інформацією. Хмарні комунікаційні послуги є природним продовженням цієї тенденції, пропонуючи ряд переваг порівняно з традиційними методами зв'язку.

Хмарні комунікаційні послуги охоплюють широкий спектр інструментів і технологій, включаючи системи голосового зв'язку через Інтернет-протокол (VoIP), платформи відеоконференцій і програми обміну повідомленнями. Ці послуги пропонують низку переваг порівняно з традиційними методами зв'язку, включаючи економію коштів, підвищену гнучкість і покращену співпрацю. Наприклад, системи VoIP дозволяють користувачам здійснювати телефонні дзвінки через Інтернет, усуваючи потребу в дорогому обладнанні та телефонних лініях. Платформи відеоконференцій дозволяють віддаленим командам співпрацювати в режимі реального часу, незалежно від їх фізичного розташування. Програми для обміну повідомленнями дозволяють швидко й легко спілкуватися між членами команди без необхідності електронної пошти чи телефонних дзвінків. Ці інструменти стали важливими для сучасного бізнесу, якому для успіху потрібен швидкий, ефективний і надійний зв'язок.

Однією з ключових переваг хмарного спілкування є його гнучкість. На відміну від традиційних методів зв'язку, які часто прив'язані до певного апаратного чи програмного забезпечення, хмарний зв'язок можна отримати з будь-якого місця, де є підключення до Інтернету. Це робить його ідеальним для віддалених команд, які можуть співпрацювати та спілкуватися так само ефективно, як якщо б вони перебували в одній кімнаті. Крім того, хмарні комунікаційні інструменти часто є економічно ефективнішими, ніж традиційні методи, оскільки вони усувають потребу у дорогому обладнанні та обслуговуванні. Наприклад, компанія, яка використовує хмарну платформу для відеоконференцій, може заощадити тисячі доларів на транспортних витратах, оскільки співробітники можуть відвідувати зустрічі з будь-якої точки світу. Багато компаній успішно впровадили хмарні комунікаційні рішення, зокрема Dropbox, який використовує хмарну програму обміну повідомленнями для покращення співпраці між своїми співробітниками.

Майбутнє хмарних комунікацій яскраве, у ньому постійно з'являються нові технології та тенденції. Однією з найцікавіших подій є використання штучного інтелекту (ШІ) і машинного навчання для покращення спілкування та співпраці. Наприклад, чат-боти на основі штучного інтелекту можна використовувати, щоб відповідати на запити клієнтів і надавати підтримку, звільняючи людей від зосередження на більш складних завданнях. Іншою тенденцією є інтеграція засобів зв'язку з іншими бізнес-додатками, такими як програмне забезпечення для управління проектами та системи управління взаємовідносинами з клієнтами (CRM). Ця інтеграція може підвищити ефективність і оптимізувати робочі процеси, спростивши для компаній спілкування та співпрацю. Однак існують також занепокоєння щодо використання хмарного зв'язку, особливо щодо конфіденційності та безпеки даних. Оскільки все більше конфіденційної інформації зберігається в хмарі, компаніям важливо вживати заходів для захисту своїх даних і гарантувати їх безпеку.

Для розробників послуг доступність послуг у хмарі залежить від типу служби та пристроїв, які використовуються для доступу до них. Процес може бути таким же простим, як користувач, який клацає потрібну веб-сторінку, або може включати програму, яка використовує API, що отримує доступ до служб у хмарі [2].

Телекомунікаційні компанії починають використовувати хмари для випуску власних послуг і послуг, розроблених іншими, але з використанням інфраструктури та даних Telco. Очікується, що комунікаційна інфраструктура Telco забезпечить можливість отримання прибутку.

Перебуваючи в хмарі, комунікаційні служби можуть розширити свої можливості або бути автономними як пропозиції послуг, або надати нові можливості інтерактивності поточним службам.

Хмарні комунікаційні послуги дозволяють компаніям вбудовувати комунікаційні можливості в бізнес-додатки, такі як системи планування ресурсів підприємства (ERP) і системи управління взаємовідносинами з клієнтами (CRM). Для ділових людей, які працюють у русі, доступ до них можна отримати за допомогою смартфона, що підвищує продуктивність поза офісом.

Ці послуги перевищують підтримку розгортання послуг систем VoIP, систем співпраці та систем конференц-зв'язку як для голосу, так і для відео. Доступ до них можна отримати з будь-якого місця та зв'язати з поточними службами, щоб розширити їхні можливості, а також окремими послугами.

З точки зору соціальних мереж, використання комунікацій на основі хмари забезпечує можливість дзвінка з веб-сайтів соціальних мереж, доступ до систем обміну миттєвими повідомленнями та відеозв'язку, розширюючи взаємозв'язки людей у соціальному колі.

Доступ до комунікаційних можливостей у хмарному середовищі досягається за допомогою API, насамперед Web 2.0 RESTful API, що дозволяє розробці додатків поза хмарою використовувати переваги комунікаційної інфраструктури в ньому (рис. 1.3).

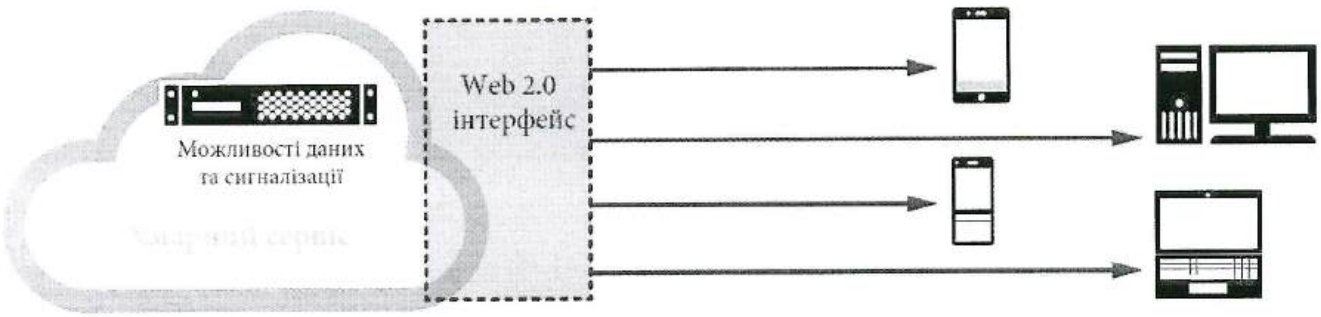


Рис. 1.3. Інтерфейси Web 2.0 для хмари

Ці API відкривають низку можливостей зв'язку для хмарних служб, обмежених лише можливостями медіа та сигналізації в хмарі. Сучасні медіа-сервіси дозволяють здійснювати зв'язок і керувати голосом і відео через складний діапазон кодеків і типів транспорту. Використовуючи веб-інтерфейси API, ці складності можна спростити, а медіа можна легше доставити на віддалений пристрій. Інтерфейси API також забезпечують обмін даними з іншими службами, надаючи нові можливості та сприяючи збільшенню середнього доходу на користувача (ARPU) і рівня підключення, особливо для телекомунікаційних компаній.

Інтерфейси керування медіасервером. Під час створення комунікаційних

можливостей у «ядро хмари», де до них матиме доступ інша служба, можна використовувати API Web 2.0, а також поєднання SIP або VoiceXML і стандартних API керування медіа, таких як MSML, MSCML і JSR309. Комбінації забезпечують різні набори можливостей, але, оскільки MediaCTRL розробляється в Internet Engineering Task Force (IETF), очікується, що MediaCTRL замінить MSML і MSCML і матиме зростання доступності та більше розробок після його ратифікації. JSR309 є чудовим вибором для тих, хто шукає розробки на Java, оскільки він надає інтерфейс Java для керування медіа.

На рис. 1.4 наведено приклад доступу до служб у хмарі через Web 2.0 та API інтерфейсу керування медіа.

Незалежно від того, чи розгортають компанії комунікаційні служби для доступу ззовні чи всередині хмари, середовище є таким, яке підтримує швидкий розвиток і розгортання цих можливостей.

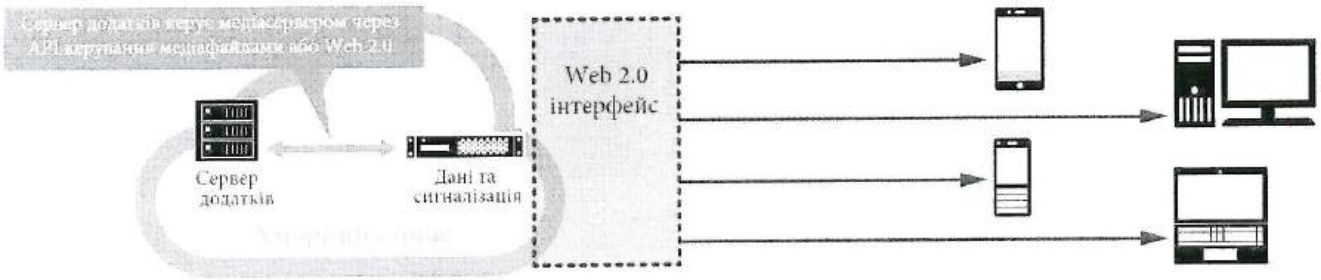


Рис. 1.4. Доступ до комунікаційних можливостей із хмари

Щоб задовольнити вимоги щодо масштабованості для хмарних розгортань, комунікаційне програмне забезпечення має бути здатне працювати у віртуальних середовищах. Це дозволяє легко збільшувати та зменшувати щільність сеансів залежно від поточних потреб, зводячи до мінімуму вимоги до фізичних ресурсів на серверах.

Компанії, які бажають використовувати комунікаційні можливості хмарних служб, отримають вигоду, визначивши правильні інтерфейси.

Dialogic підтримує широкий спектр інтерфейсів, включаючи RESTful API, інтерфейси керування медіафайлами, інтерфейси Java та інтерфейси на основі

XML, що задовольняє широкий спектр розробників програм і сервісів. Ці інтерфейси, доступні через засоби масової інформації та можливості сигналізації, підтримують масштабованість, необхідну в хмарному середовищі, але їх легко розгортати та адмініструвати.

1.2 Особливості сервісної моделі "Відеоспостереження як послуга VSaaS"

Системи відеоспостереження використовуються вже кілька десятиліть з моменту винаходу камер відеоспостереження та магнітофона. Згодом ці системи перейшли до використання комп'ютерної системи та IP-камер для захоплення, зберігання та відтворення записів, які швидко досягли меж у розмірі, вимогах до живлення, обробці, аналізі та особливо зберіганні. Основні перешкоди полягають у тому, що всі вони базуються на рішеннях на основі сайту . Хмарні обчислення представили новий підхід до того, як керувати даними, що також відобразилося на відеоспостереження. Це привело до ідеї, використовуючи величезну мережу хмарних обчислень, можливості зберігання та обробки, створити структуру відеоспостереження як послуги (VSaaS). Можна створити архітектуру VSaaS за допомогою хмарних технологій, таких як програмне забезпечення як послуга (SaaS), платформа як послуга (PaaS) та хмарні сервіси інфраструктури як послуги (IaaS) [3].

Відеоспостереження стало важливим інструментом для забезпечення безпеки в різних місцях, включаючи будинки, підприємства та громадські місця. З розвитком хмарних обчислень та Інтернету речей (IoT) відеоспостереження як послуга (VSaaS) стало економічно ефективною та масштабованою альтернативою традиційним системам відеоспостереження.

Розуміння відеоспостереження як послуги (VSaaS) — це хмарне рішення для відеоспостереження, яке дозволяє користувачам віддалено отримувати доступ, керувати та зберігати відеоматеріали з будь-якого місця, де є підключення до Інтернету. Постачальники VSaaS пропонують ряд послуг, включаючи відеозапис,

пряму трансляцію, виявлення руху та сповіщення про сповіщення. Деякі з ключових переваг VSaaS перед традиційними системами відеоспостереження включають нижчі початкові витрати, простіше встановлення та обслуговування, а також більшу масштабованість. Приклади постачальників VSaaS включають Nest Cam, Ring і Arlo, які пропонують доступні та зручні рішення для домашньої безпеки.

Однією з головних переваг VSaaS є його економічна ефективність. Користувачі можуть уникнути високих початкових витрат на придбання та встановлення апаратного та програмного забезпечення, а також витрат на поточне технічне обслуговування та оновлення. VSaaS також пропонує більшу масштабованість, оскільки користувачі можуть легко додавати або видаляти камери та обсяг пам'яті за потреби. Ще однією перевагою VSaaS є віддалений доступ, який дозволяє користувачам контролювати свої приміщення з будь-якого місця та в будь-який час. Однак VSaaS має деякі обмеження, наприклад залежність від підключення до Інтернету, що може вплинути на якість і надійність відеоканалу. Проблеми безпеки також є потенційною проблемою, оскільки відеозаписи зберігаються на сторонніх серверах. Нарешті, VSaaS може мати обмежені можливості налаштування порівняно з традиційними системами відеоспостереження, які можна адаптувати до конкретних потреб.

Оскільки VSaaS продовжує розвиватися, нові тенденції, такі як штучний інтелект, хмарні обчислення та інтеграція IoT, ймовірно, формуватимуть майбутнє цієї технології. Відеоаналітика на основі штучного інтелекту може допомогти підвищити точність і ефективність відеоспостереження, виявляючи й сповіщаючи користувачів про потенційні загрози. Хмарні обчислення можуть підвищити масштабованість і гнучкість VSaaS, надаючи ресурси та сховище на вимогу. Інтеграція IoT може дозволити VSaaS підключатися до інших інтелектуальних пристроїв і систем, таких як системи контролю доступу та сигналізації, щоб забезпечити комплексне рішення безпеки. Вплив VSaaS на ринок і галузь відеоспостереження є значним, оскільки очікується, що з 2020 по 2027 рік він зростатиме на 16,4% у середньому. Однак такі проблеми, як конфіденційність і

безпека даних, сумісність та інтеграція із застарілими системами, повинні бути вирішені. щоб повністю реалізувати потенціал VSaaS.

Системи відеоспостереження стали важливим інструментом для забезпечення безпеки в різних місцях, включаючи будинки, підприємства та громадські місця. Оскільки технології продовжують розвиватися, хмарні системи відеоспостереження стали популярним варіантом для багатьох організацій.

Системи відеоспостереження – це електронні системи, які фіксують і записують візуальні зображення з метою моніторингу та виявлення будь-якої підозрілої чи злочинної діяльності. Ці системи зазвичай використовуються в будинках, на підприємствах, у громадських місцях і державних установах. Системи відеоспостереження бувають двох видів: аналогові та цифрові. Аналогові системи використовують касети VHS для запису відзнятих матеріалів, тоді як цифрові системи використовують жорсткі диски або хмарні сховища для зберігання відзнятих матеріалів. Переваги систем відеоспостереження включають запобігання злочинам, надання доказів у судових справах і підвищення загальної безпеки. Однак деякі недоліки включають занепокоєння конфіденційністю та можливість зловживань.

Впровадження хмарних систем відеоспостереження включає кілька етапів, включаючи вибір правильного обладнання та програмного забезпечення, налаштування системи та навчання персоналу, як нею користуватися. Однак існують також проблеми, пов'язані з керуванням цими системами, наприклад забезпечення конфіденційності та безпеки даних, вирішення технічних проблем і дотримання правових норм. Щоб подолати ці проблеми, організаціям слід застосовувати найкращі методи підтримки та захисту своїх хмарних систем відеоспостереження, наприклад регулярно оновлювати програмне забезпечення, використовувати надійні паролі та обмежувати доступ до конфіденційних даних.

Служба хмарних обчислень застосовує трирівневий підхід, який є IaaS, PaaS і SaaS, як показано на рис. 1.5.

IaaS забезпечує ресурси мережевих пристроїв, обчислювальні ресурси та ресурси зберігання. PaaS — це програмна платформа для мережевих програм

конфедерації. Користувач може розробити модуль програми для зв'язку з платформою. У своєму дослідженні автори розробили модуль інтеграції Інтернету речей (IoT) за таким підходом. SaaS надає користувачам програмне забезпечення. Існує два основних способи SaaS: вертикальний SaaS (програмне забезпечення, яке відповідає потребам певної галузі) і горизонтальний SaaS (продукти, які зосереджені на категорії програмного забезпечення).

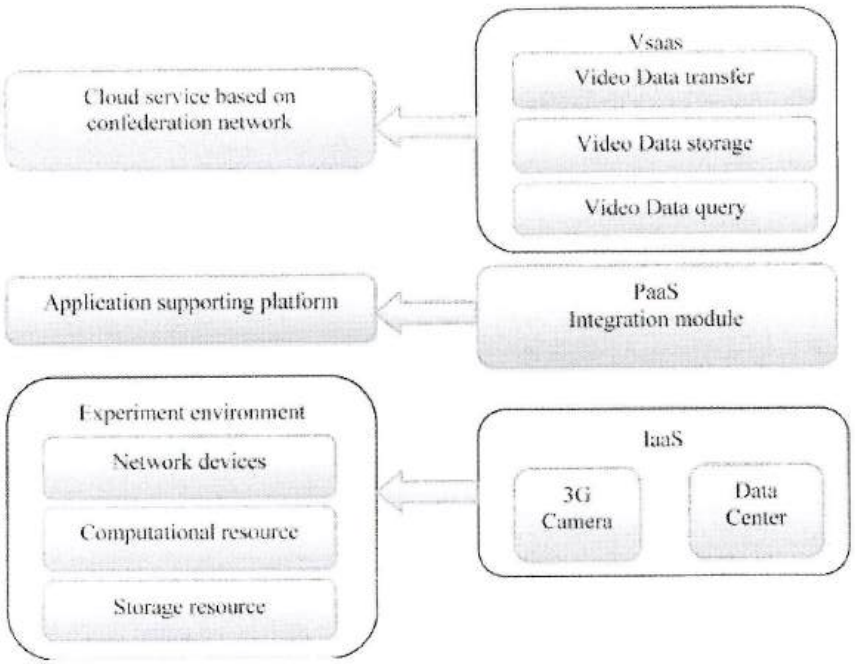


Рис. 1.5. Склад VSaaS з використанням сервісів PaaS, IaaS та SaaS

Відеоспостереження як послуга (VSaaS) призначене для забезпечення повсюдного мережевого доступу на вимогу до спільного пулу записаних мультимедійних ресурсів, які можна швидко отримати та вивільнити з мінімальними зусиллями адміністратора або взаємодії постачальника послуг. Процес хмарного відеоспостереження досить простий для кінцевого користувача: камера на місці записує аудіо/відеоматеріал, надсилає його за допомогою інтернет-з'єднання в хмару, а програмне забезпечення для керування відео (VMS) доставляє відео за вимогою до клієнт. Проте з детальної точки зору процес складається з кількох важливих кроків, як показано на рис. 1.6, який є детальним видом структури VSaaS. Існує кілька похідних послуг, таких як: інтелектуальне

відеоспостереження) як послуга (IVSaaS), кероване відеоспостереження як послуга (MVSaaS або MVaaS), хмарне відеоспостереження (CVS) і онлайн-відеоспостереження як послуга (OVSaaS) [4].

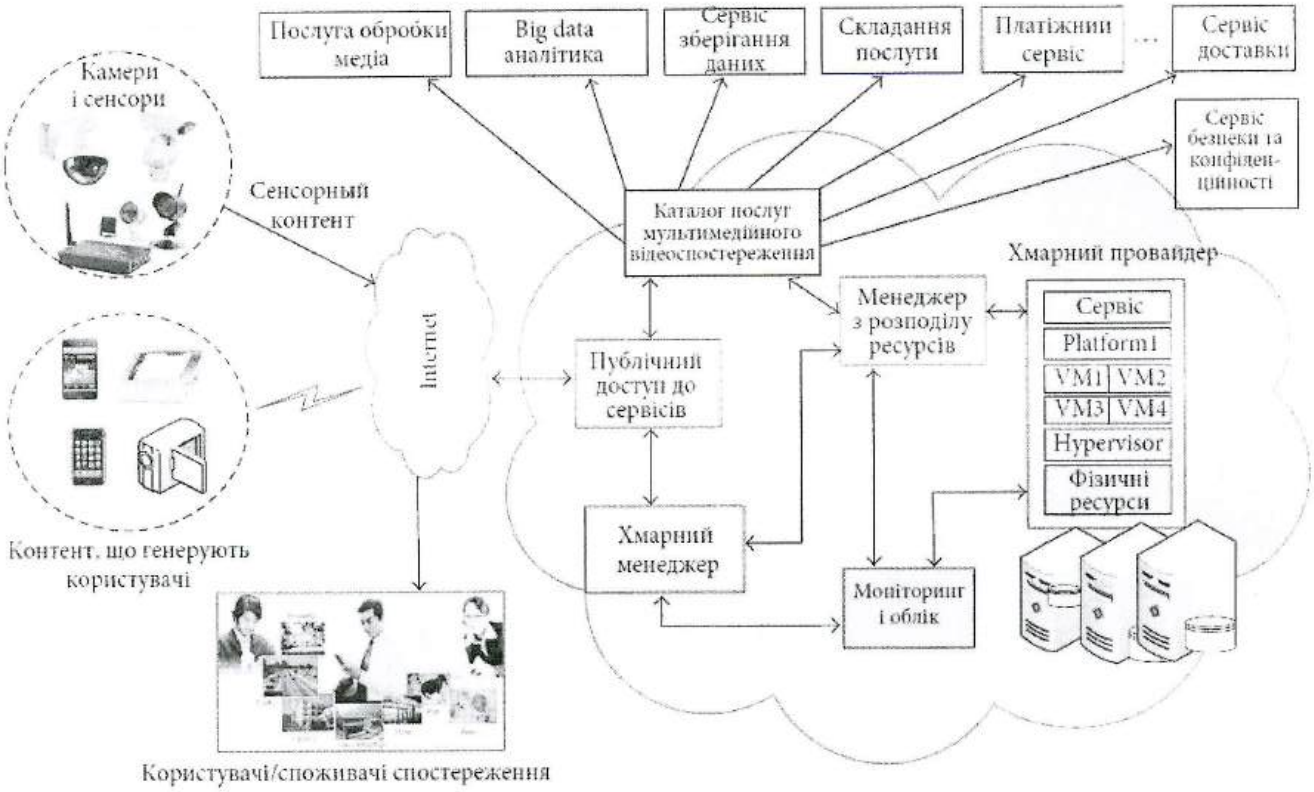


Рис. 1.6. Детальний вигляд архітектури VSaaS

VSaaS може бути загальнодоступною, приватною або гібридною (комбінацією двох). Публічна архітектура передбачає використання постачальника хмарних послуг із уже налаштованою платформою для управління відеоспостереженням. Це найпоширеніший сценарій використання VSaaS. Приватна архітектура відноситься до внутрішньої хмарної служби, розміщеної компанією або підприємством, яке використовувало платформу для цілей відеоспостереження. Це рідко трапляється, оскільки таку систему важче фінансувати та підтримувати.

Методи захоплення сенсорних даних включають: лише надсилання, коли камера постійно надсилає дані до хмари, отримання лише тоді, коли хмарна система отримує дані на вимогу, гібридний (надсилання/отримання) є випадком,

коли система попередньо - налаштований для виконання бажаної дії на основі уподобань клієнта та збору даних, керованих подіями, таких як виявлення руху, звукова активація та активація системи сигналізації.

Наступним кроком є сховище даних, яке можна зберігати локально, Network Attached Storage (NAS) і Storage Area Network (SAN), а потім надсилати в хмару або направляти дані в хмару. Локальне сховище може бути у формі проміжного пристрою, який виконує тимчасове зберігання та конвертацію необробленого відео в певний стиснутий формат, а потім надсилає його в хмару або камеру з вбудованою пам'яттю, яка веде себе як сховище готівки та надсилає дані через визначені проміжки часу. Ці підходи мають вищі значення зручності використання, оскільки вони зменшують споживання пропускної здатності і можуть забезпечити кращу роздільну здатність відео завдяки можливостям стиснення. Недоліком використання цього підходу є неминуча затримка виявлення подій. Пряма потокова передача даних є менш популярним методом через високі вимоги до мережі для надсилання відео та підвищені витрати на хмарне зберігання, однак це можна вирішити за допомогою меншого часу зберігання. Цей метод пропонує перегляд у реальному часі та виявлення небажаних подій.

Коли дані зберігаються, їх потрібно обробити. Очевидна перевага хмарної бази спостереження полягає в тому, що він пропонує незрівнянну обчислювальну потужність у порівнянні з традиційними системами для стиснення відео, інтелектуального аналізу і потокової передачі. Функції обробки включають: виявлення обличчя, розпізнавання обличчя, виявлення руху, відстеження руху людей, оцінку щільності натовпу, розпізнавання шаблонів, підвищення різкості зображення, виявлення втручання, розпізнавання номерних знаків, розумний пошук і великі аналіз даних за допомогою Video Analytics Service (VAS).

Розподіл ресурсів є важливим аспектом проектування VSaaS і визначає загальну продуктивність хмарної системи. Обчислювальна потужність, необхідна для виконання цих операцій, є більшою, ніж будь-яка традиційна система. Перевага VSaaS полягає в тому, що необхідну потужність можна вимагати за потреби. Можливість масштабування служби може значно сприяти підтримці робочого

навантаження відео високої роздільної здатності.

Однією з сучасних функцій середовища VSaaS є можливість інтелектуального сповіщення клієнта про різні події, які вже згадувалися в розділі обробки даних. Сповіщення можна надсилати через електронну пошту, SMS, MMS і мобільні додатки. Мультимедійне сповіщення може містити знімки або навіть відеоряд виявленої події.

У порівнянні з традиційними системами хмарні VMS мають значно менше проблем із уразливістю. Немає необхідності в локальному програмному забезпеченні, брандмауерах і відкритих портах. Крім того, немає ймовірності того, що сховище може бути скомпрометовано через крадіжку, недбалість користувачів, погодні явища тощо. Спостереження доступне в будь-який час з будь-якого пристрою, що забезпечує ще більший рівень безпеки. Постачальники VSaaS мають спеціальні команди з кібербезпеки для моніторингу нових вразливостей і миттєвого застосування патчів безпеки через хмару до локального пристрою.

У таблиці 1.1 наведено порівняння традиційних і хмарних систем відеоспостереження, яке вказує на явну перевагу VSaaS над традиційними системами майже у всіх випадках [3, 4].

Таблиця 1.1

Порівняння традиційних і хмарних систем відеоспостереження

Традиційне підключення до Інтернету DVR/NVR/VMS/IP-VS	Хмарна VMS / VSaaS
1	2
Установка системи	
- Забирає багато часу. - Складна конфігурація.	- Швидке розгортання за вимогою. - Автоматична конфігурація Plug-and-play.
Системна підтримка	
- Інтенсивний процес обслуговування вручну.	- Підтримка здійснюється за межами розміщення обладнання провайдером.

Продовження таблиці 1.1

Порівняння традиційних і хмарних систем відеоспостереження

1	2
Структура оплати	
- Високі авансові капітальні витрати. - Непередбачувані витрати на підтримку. - Дороге масштабування.	- Надзвичайно низькі початкові капітальні витрати. - Передбачувані щомісячні експлуатаційні витрати. - Дешева масштабованість.
Загальна вартість володіння	
- Висока початкова вартість, включаючи високу вартість обладнання/програмного забезпечення та встановлення. - Багато поточних витрат.	- Низька початкова вартість низька, як правило, недорогий мостовий пристрій. - Низька поточна місячна вартість підписки.
Гнучкість зберігання	
- Традиційний DVR, NVR або VMS, зберігайте відео на місці. - Зберігання обмежено. - Дорожче розширення сховища.	- Гнучке поєднання локального та/або хмарного сховища. - Миттєво збільшити термін зберігання. - Низька вартість розширення сховища.
Додавання керуючих камер	
- Підтримка широкого спектру аналогових IP-камер. - Ручне підключення конфігурації нових камер.	- Підтримка широкого спектру аналогових IP-камер. - Ручне підключення автоконфігурації нових камер.
Управління пропускною здатністю	
- Для дистанційного перегляду потрібна пропускна здатність. - Для зберігання відеозапису на місці не потрібна пропускна здатність.	- Для дистанційного перегляду потрібна пропускна здатність. - Більшість сховища є потоковим, що вимагає високої пропускної здатності.

Продовження таблиці 1.1

Порівняння традиційних і хмарних систем відеоспостереження

1	2
Довговічність технології, API	
- Коротший час до морального старіння технології. - Обмежена можливість оновлювати технології. - Оновлення потребують інтенсивної підтримки вручну. - API закриті та зазвичай вимагають підписання NDA. Функціональність API обмежена.	- Швидкий розвиток технологій. - Автоматичне оновлення технологій для локального пристрою. - Постійно розвивається для нових інновацій, має довголіття. - Відкриті API для аналітики, інтеграційних програм. Можна використовувати в інших системах.
Кібербезпека	
- Вищі шанси на вразливість кібербезпеки. - Конфігурація відкритих портів, локальних брандмауерів, локального програмного забезпечення та брандмауера. - Кінцевий користувач стежить за вразливістю атак.	- Надзвичайно низька ймовірність уразливості кібербезпеки. - Ні відкритих портів, ні локальних брандмауерів, ні локального програмного забезпечення, ні встановлення брандмауера. - Спеціалізовані групи кібербезпеки для моніторингу нових вразливостей.
Віддалений доступ	
- Нерідний віддалений доступ до відео, додається лише за запитом. - Непередбачувана, переривчаста якість відео з низькою роздільною здатністю. - Існування рідкісного шифрування. - Несумісність браузера є звичайним явищем.	- Хмарні системи були розроблені для віддаленого доступу. - Плавний доступ до потокового відео високої роздільної здатності. - Вбудоване розширене шифрування. - Підтримка універсальних веб-браузерів і мобільних додатків.

Продовження таблиці 1.1

Порівняння традиційних і хмарних систем відеоспостереження

1	2
Надійність резервування	
- Сильно змінні рівні резервування. - Звільнення, кероване внутрішнім IT- персоналом. - Сервери клонування часто простоюють, що збільшує накладні витрати.	- Хмарні центри обробки даних мають подвійне та потрійне резервування. - Спільна інфраструктура забезпечує повне використання сервера та економію за рахунок масштабу. - Кілька днів локального сховища як резервного копіювання для захисту від збою Інтернету разом із миттєвими сповіщеннями.

VSaaS — це ринок, який постійно зростає, і його майбутнє полягає в розробці нових функцій аналітики від розробки програмного забезпечення та зниженні поточних витрат завдяки вдосконаленню апаратного забезпечення. Відеоспостереження як послуга (VSaaS) пропонує економічно ефективне та масштабоване рішення для забезпечення безпеки та безпеки в різних умовах. Хоча VSaaS має багато переваг, таких як віддалений доступ і легкість встановлення, він також має деякі обмеження, такі як залежність від підключення до Інтернету та потенційні проблеми безпеки.

2 РОЗРОБКА АРХІТЕКТУРИ ХМАРНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

2.1 Архітектура розгортання хмарних системи відеоспостереження

Хмарні системи відеоспостереження останнім часом стають все більш популярними завдяки своїй гнучкості, масштабованості та економічній ефективності. Ці системи використовують технологію хмарних обчислень для забезпечення віддаленого доступу, зберігання та керування даними відеоспостереження.

Хмарні обчислення революціонізували спосіб проектування систем відеоспостереження та керування ними. Він забезпечує віддалений доступ до відеоканалів, моніторинг у реальному часі та централізоване зберігання відеоданих. Компоненти хмарної системи відеоспостереження зазвичай включають камери, мережеву інфраструктуру, хмарне сховище та програмне забезпечення для керування. Існують різні типи хмарних архітектур відеоспостереження, включаючи централізовані, децентралізовані та гібридні. Централізовані архітектури передбачають, що всі відеодані зберігаються в центральному місці, тоді як децентралізовані архітектури розподіляють відеодані в кількох місцях. Гібридні архітектури поєднують елементи централізованої та децентралізованої архітектур.

Розгортання хмарної системи відеоспостереження вимагає ретельного планування та врахування технічних факторів, таких як пропускна здатність, сховище та безпека. Пропускна здатність має вирішальне значення для передачі відеоданих у хмару, а необхідна пропускна здатність залежить від кількості камер, роздільної здатності та частоти кадрів. Зберігання також є важливим моментом, оскільки відеодані можуть швидко накопичуватися і вимагати значного обсягу пам'яті. Безпека є ще одним критичним фактором, оскільки відеодані є конфіденційними та мають бути захищені від несанкціонованого доступу. Інтеграція з існуючими системами та додатками також необхідна для забезпечення безперебійної роботи системи.

Щоб забезпечити ефективність і довговічність хмарної системи відеоспостереження, важливо дотримуватися найкращих практик її проектування. Масштабованість і гнучкість є важливими, оскільки система повинна бути здатна адаптуватися до майбутнього зростання та змін у технологіях. Резервування та відмовостійкість також мають вирішальне значення для забезпечення доступності та надійності системи. Оптимізація витрат і аналіз рентабельності інвестицій також є важливими міркуваннями, оскільки впровадження та обслуговування хмарних систем відеоспостереження може бути дорогим. Дотримуючись цих найкращих практик, організації можуть переконатися, що їх хмарна система відеоспостереження ефективна, ефективна та стійка.

З точки зору системи відеоспостереження, є кілька відмінних питань, які потребують дослідження, особливо коли така система базується на хмарній інфраструктурі. Вони підсумовані таким чином [5].

1. Архітектура розгортання. Хмарна архітектура системи відеоспостереження може бути розроблена для розгортання в публічній хмарі, приватній хмарі або в комбінації обох, що називається гібридною хмарою. Далі йде коротка розмова про них:

- У налаштуваннях публічної хмари хмарна інфраструктура відкрита для звичайного користувача. Крім того, оскільки вони залишаються на території хмарного постачальника, клієнти відеоспостереження часто бояться втратити контроль над своїми даними та стурбовані можливою втратою даних. Однак поточні хмарні постачальники, такі як хмара Amazon, вживають усіх заходів, щоб убезпечити своїх клієнтів від будь-яких подібних нещасних випадків.

- У приватній хмарній мультимедійній системі спостереження хмарна інфраструктура використовується виключно однією організацією, де вона може бути розміщена, і це гарантує підвищену безпеку даних, конфіденційність і право власності.

- Третій варіант проектування – це композиція з двох, де організація може вирішити помістити критично важливі дані спостереження в приватну хмару, одночасно використовуючи публічну хмару для звичайних і неконфіденційних

даних.

Існує три основні варіанти архітектури хмарних систем відеоспостереження: централізована, розподілена та гібридна. У централізованій архітектурі всіма камерами керує єдиний хмарний сервер. Ця архітектура підходить для невеликих систем з обмеженою кількістю камер. У розподіленій архітектурі кілька хмарних серверів використовуються для керування різними групами камер. Ця архітектура підходить для великих систем з великою кількістю камер. У гібридній архітектурі використовується комбінація централізованих і розподілених компонентів. Ця архітектура підходить для систем, які вимагають як масштабованості, так і гнучкості.

При розробці архітектури хмарної системи відеоспостереження необхідно враховувати кілька важливих факторів. Масштабованість і гнучкість мають вирішальне значення для додавання або видалення пристроїв камери за потреби. Надійність і доступність важливі для забезпечення безперервної роботи спостереження. Система повинна бути розроблена таким чином, щоб справлятися зі збоями та мінімізувати час простою. Безпека та конфіденційність також є важливими факторами, які слід враховувати. Відеодані мають бути захищені від несанкціонованого доступу, а система має відповідати відповідним нормам конфіденційності.

Хмарна система відеоспостереження є потужним інструментом для підвищення безпеки та можливостей спостереження. Ретельно враховуючи ці фактори, організації можуть розробити хмарну систему відеоспостереження, яка відповідає їхнім конкретним вимогам і забезпечує надійні, безпечні та масштабовані можливості спостереження.

Зрештою, організація повинна проаналізувати вимоги до систем спостереження, які вони розробляють, і зробити компроміс між можливими варіантами розгортання, які вони мають.

2. Вибір методів передачі відео. Важливо вибрати відповідну стратегію для захоплення потоків даних датчиків і зберігання їх у хмарному сховищі. У цьому випадку існує кілька варіантів проектування, наприклад, лише натискання, лише

натягування, натискання, керування подіями тощо. Нижче наведено їх короткий опис:

- Через push-only підключені датчики можуть постійно надсилати потік даних датчиків у хмару. У цьому підході приймаюча сторона хмарного середовища повинна застосувати спеціальний механізм для обробки безперервного потоку отриманих потоків даних.

- Підхід лише залучення дозволяє хмарній інфраструктурі отримувати потік даних із датчика за запитом. Цей механізм бере на себе тягар двостороннього запиту даних для кожного запиту даних із хмари. Однак, якщо потреби в даних мінімальні та періодичні, цей механізм має потенціал для зменшення споживання енергії та пропускної здатності.

- Механізм Push-Pull — це гібридний підхід до балансування компромісів між механізмами, що тягнуть і тягнуть. Комбінація механізмів push і pull пропонує кілька переваг, таких як зменшення мережевого трафіку, мінімізація витрат на вибірку датчиків і зниження споживання енергії. На рис. 2.1, показано схематичний вигляд механізму push-pull. Це вказує на те, що залежно від ситуації в процесі отримання мультимедійних даних може використовуватися push або pull в одному сеансі.

- Механізм, керований подіями, є популярним підходом, коли потоки даних датчиків надсилаються до хмари лише тоді, коли певна основна подія (тобто виявлення руху) ідентифікується у потоках вхідних даних на стороні клієнта. Цей підхід може значно зменшити споживання енергії та пропускну здатність завдяки мінімальній передачі даних у хмарне середовище порівняно з безперервною передачею.

Таким чином, залежно від вимог програми спостереження, будь-який із вищезазначених підходів до збору даних може бути прийнятий із різним впливом на продуктивність системи спостереження.

3. Хмарне сховище. Типові системи відеоспостереження потребують великого обсягу пам'яті для зберігання великої кількості даних, що надходять від кількох датчиків. Ці дані обробляються в режимі реального часу і часто в

автономному режимі для виявлення подій безпеки. Однак типові системи спостереження не можуть впоратися з постійним попитом на масивне зберігання. Хмарне сховище приходить як порятунок, яке може підключати різні типи мережевих пристроїв зберігання даних для задоволення конкретних вимог систем спостереження, наприклад (а) запис медіа-потоків із вищою частотою кадрів без втрати кадрів, (б) економічне сховище для більш тривалого зберігання медіа-даних і (в) можливість еластичного зберігання для змінного попиту та майбутнього зростання. Крім того, хмарне сховище вважається високодоступним, завжди ввімкненим і надійнішим, ніж локальне сховище. Як наслідок, він не може лише задовольнити потреби у великих системах відеоспостереження, але й надавати інтелектуальну відеоаналітику як послугу на вимогу для кількох клієнтів. Однак є кілька ключових проблем, які потребують конструктивних рішень при використанні хмарного сховища [6].

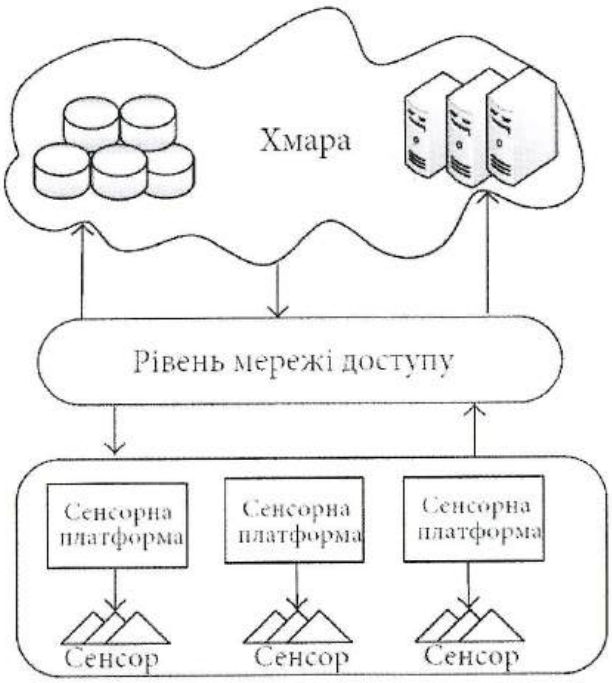


Рис. 2.1. Механізм Push-pull між датчиками, середнім шаром (краєм) і хмарою

Деякі з цих проблем такі:

- Блокування постачальника є важливою проблемою, яка стосується клієнтів відеоспостереження. Через те, що служби хмарного зберігання даних відрізняються

продуктивністю, ціною та часто географічним розподілом сховищ даних, клієнтам може бути складно та дорого змінити постачальника. Це критично для клієнтів, оскільки йдеться про конфіденційні дані спостереження.

- Можливість аварійного відновлення є важливим фактором, який слід враховувати при виборі хмарного сховища через конфіденційні та часто приватні дані, які обробляє система спостереження. Постачальник хмарних сховищ, який пропонує надійний механізм аварійного відновлення, матиме менше простоїв і, отже, забезпечуватиме безперервну громадську безпеку.

- Еластичність хмарного сховища є важливим фактором для клієнта відеоспостереження, який гарантує, що хмарний постачальник має можливість динамічно пом'якшувати мінливість попиту на сховище. На продуктивність системи відеоспостереження можна значно вплинути, якщо хмарний постачальник не забезпечує гнучку еластичність зберігання.

- Для хмарного сховища має бути відповідна політика безпеки та конфіденційності. Існують різні варіанти, наприклад, проведення публічного аудиту для забезпечення конфіденційності та цілісності даних.

- Структура оплати та ціноутворення визначає вибір хмарного провайдера. Система відеоспостереження, яка потребує великої підтримки пам'яті, повинна узгодити модель ціноутворення, перш ніж вона зможе вибрати конкретного хмарного постачальника.

При проектуванні та розгортанні системи відеоспостереження важливо розглянути вищезазначені проблеми та прийняти відповідний механізм хмарного зберігання, який може служити цій меті.

4. Обробка медіа. Різні датчики в мультимедійній системі відеоспостереження генерують величезну кількість медіаданих, які часто потрібно обробляти в режимі реального часу, щоб вчасно виявити події. Традиційні системи відеоспостереження, які включають обмежений набір процесорів і серверів, можуть бути легко перевантажені інтенсивною обробкою мультимедійних даних залежно від кількості завдань спостереження. Таким чином, хмарна обробка даних спостереження виглядає багатообіцяючою завдяки величезним можливостям

обробки, які можна використовувати. Однак обробка медіа в хмарному середовищі приносить багато проблем. У контексті системи спостереження це можна коротко викласти так:

- Обробка мультимедійних даних для систем відеоспостереження зазвичай виконується для підтримки різноманітних завдань мультимедійного аналізу, таких як виявлення облич, розпізнавання облич, виявлення руху, відстеження людей і оцінка щільності натовпу. Система відеоспостереження, отримуючи різні сенсорні медіа-потоки в хмарі, виконує ці завдання, щоб ідентифікувати небезпечні події безпеки та генерує сигнали тривоги, коли це необхідно. Загальний вигляд архітектури обробки медіа спостереження наведено на рис. 2.2. Проблеми в цій конфігурації полягають у тому, що сенсорні носії мають різний тип, і, отже, різні завдання аналізу медіа споживають різну кількість часу та ресурсів. Подібно до різних типів носіїв, проблеми також залишаються пов'язаними з неоднорідністю QoS, мережі та пристроїв, щоб вміст спостереження можна було доставити на різні клієнтські пристрої через різні типи мережевих з'єднань і підтримувати гарантію QoS.



Рис. 2.2. Обробка мультимедійних даних для виявлення подій у хмарі

- Важливо вирішити, чи варто розробляти систему спостереження в реальному часі, щоб усі медіа-потоки миттєво оброблялися в хмарі. Небагато у цьому відношенні варто згадати фактори, такі як необхідна частота кадрів, із якою

захоплюється медіа, кількість пікселів, швидкість алгоритму обробки медіа та динамічне забезпечення ресурсів, необхідних для підтримки обробки. Крім обробки в реальному часі, основні обчислення в хмарі відбуваються для автономної обробки відеоканалів спостереження. Багато речових доказів, які використовуються для кримінального розслідування, виявляються під час офлайн-обробки ЗМІ. Хоча час не має критичного значення для автономної обробки мультимедійних даних, важливо зарезервувати достатні ресурси для різних автономних завдань.

- Особливі міркування повинні бути зроблені, коли обробка мультимедійних даних зустрічається з мобільними хмарними обчисленнями, які є дуже динамічним середовищем, яке отримує величезний обсяг мобільного медіаконтенту.

Загалом обробка медіа є центральною для хмарної мультимедійної системи спостереження. Система може обробляти медіафайли в режимі реального часу та/або офлайн; однак це також залежить від можливостей системи відеоспостереження, алгоритмів, кількості кадрів, що обробляються за секунду, і вимог високого рівня до системи. Розробка системи відеоспостереження повинна зосереджуватися на цих аспектах для підтримки великомасштабної обробки медіа в хмарі.

5. Розподіл ресурсів. Через величезні вимоги до ресурсів зберігання та обробки для додатків відеоспостереження, традиційні системи відеоспостереження стикаються з обмеженням кількості таких ресурсів, які доступні та використовуються. Тому, коли такі ресурси переходять у хмарне середовище, можливості систем відеоспостереження швидко зростають. Хмарні ресурси — це обчислювальні ресурси у формі віртуальних машин (ВМ), які використовуються на вимогу та розгортаються в центрі обробки даних хмарного провайдера. Хмарні ресурси не тільки надаються на вимогу, але й можуть використовуватися на основі оплати за використання. Ця опція особливо цікава для мультимедійної системи відеоспостереження, яка потребує ресурсів увімкнення та вимкнення залежно від поточних завдань виявлення подій. У контексті хмарного мультимедійного спостереження запити на ресурси для виконання різних завдань спостереження

транслюються у форму запитів на ресурси віртуальної машини, які потім відображаються на розподіл ресурсів віртуальної машини для резервування фізичних ресурсів сервера, на якому розміщені віртуальні машини. Масове зберігання та обробка потоків даних спостереження вимагає ефективного механізму розподілу ресурсів з урахуванням QoS, який повинен справлятися з динамічними змінами умов мережі, підключення до ресурсів або пов'язаних з цим витрат, онлайн або офлайн змінами вимог користувача, і інші фактори. При розробці відповідної моделі розподілу ресурсів необхідно врахувати декілька міркувань. Це такі [6, 7]:

- Механізм розподілу ресурсів — це в основному завдання оптимізації вибору ресурсів у хмарі, яке спрямоване на досягнення мети оптимізації, наприклад, максимізація використання ресурсів при мінімізації часу відповіді та вартості, знаходження балансу між використанням ресурсів, часом відповіді, або вартість, встановлюючи компроміс між середнім часом очікування обслуговування та довгостроковою вартістю обслуговування, максимізуючи індивідуальний прибуток або мінімізуючи збитки, рівномірно збалансовуючи розподіл навантаження між усіма вузлами, що володіють ресурсами, і так далі:

- Існує багато різних стратегій розподілу ресурсів для хмарних ресурсів для задоволення цілей оптимізації, таких як теоретико-ігровий підхід, модель динамічного програмування і генетичний алгоритм.

- Конкретна модель розподілу ресурсів також залежить від різних варіантів механізму отримання, зберігання, обробки та спільного використання медіа.

- У зв'язку з виникненням динамічних подій у контексті спостереження системі спостереження потрібно визначити відповідну модель динамічного розподілу ресурсів, а не залежати від попередньо визначеного рішення хмарного постачальника.

Таким чином, хмарні мультимедійні системи відеоспостереження повинні досліджувати вищезазначені проблеми та відповідно розробляти модель розподілу ресурсів, яка підходить для застосування в контексті.

6. Сповіщення та обмін. Основними проблемами, що керують

мультимедійними системами відеоспостереження, є своєчасне сповіщення про події та повсюдний обмін записами відеоспостереження з будь-якого місця та в будь-який час авторизованими користувачами спостереження. Очікується, що менеджер служби безпеки у випадку екстреного інциденту зможе поділитися відеозаписом у прямому ефірі з поліцією чи іншими правоохоронними органами, щоб отримати негайну відповідь. Один із способів полегшити це — розробити механізм публікації-підписки, за допомогою якого клієнти системи спостереження можуть публікувати інформацію про події, а користувачі можуть отримувати опублікований вміст на основі певної підписки. У хмарній мультимедійній системі спостереження механізм публікації та підписки також розгортається на хмарній платформі, що дозволяє використовувати хмарні ресурси за вимогою. Нижче наведено кілька проблем проектування, про які варто згадати:

- Як і типова система публікації-підписки, хмарна система публікації-підписки має вказувати, як передплатник виражає свою зацікавленість (наприклад, на основі теми, на основі вмісту, на основі типу та параметризовано) і як виконується відповідність система сповіщень.

- Важливо визначити, як інформація розповсюджується або поширюється від видавців до передплатників. Зазвичай він використовує багатоадресний підхід для підключення та доставки медіа-потоків спостереження різним користувачам системи спостереження. Крім того, можна використовувати мережеву архітектуру на рівні брокера та P2P:

- Використовуваний алгоритм обробки/відповідності подій є важливим фактором розробки.

- Також викликає занепокоєння те, скільки інформації потрібно поширювати та ділитися, наприклад, у мультимедійній системі відеоспостереження є відеодокази, якими часто потрібно ділитися з кількома зацікавленими сторонами.

Усі щойно згадані варіанти вплинуть на продуктивність і корисність певного механізму публікації та підписки в хмарному середовищі.

7. Спостереження на основі натовпу та аналіз великих даних. Спостереження на основі натовпу та аналіз великих даних Cloud CCTV

пропонують кілька переваг перед традиційними методами спостереження. По-перше, вони забезпечують підвищену точність і ефективність виявлення та запобігання злочинній діяльності. Аналізуючи великі обсяги даних у режимі реального часу, ці методи можуть виявляти підозрілу поведінку та швидко сповіщати правоохоронні органи. Це може призвести до швидшого часу реагування та вищих шансів спіймати злочинців. По-друге, спостереження за натовпом і аналіз великих даних Cloud CCTV дозволяють здійснювати моніторинг і аналіз великих обсягів даних у реальному часі. Це означає, що правоохоронні органи можуть швидко виявляти моделі та тенденції злочинної діяльності та вживати профілактичних заходів для запобігання майбутнім інцидентам. Крім того, ці методи є економічно ефективними порівняно з традиційними методами спостереження. Використовуючи хмарні технології, правоохоронні органи можуть заощадити гроші на апаратному забезпеченні, обслуговуванні та витратах на персонал.

Незважаючи на переваги, існує кілька проблем із запровадженням спостереження за натовпом і аналізу великих даних хмарного відеоспостереження. По-перше, серйозними проблемами є питання конфіденційності та потенційне зловживання даними. Збір та аналіз великих обсягів даних може призвести до порушення конфіденційності та можливого зловживання особистою інформацією. Крім того, технічні проблеми, такі як обробка та зберігання даних, можуть бути складними. Сам обсяг зібраних даних може бути величезним, а потужність обробки, необхідна для аналізу цих даних, може бути дорогою. Нарешті, юридичні та етичні питання, пов'язані з володінням даними, доступом і спільним використанням, також є важливими міркуваннями. Є питання щодо того, кому належать зібрані дані, хто має до них доступ і як ними можна поділитися. Без чітких інструкцій і правил існує ризик неправильного використання даних або зловживання ними.

Є кілька захоплюючих розробок у сфері спостереження за натовпом і аналізу великих даних хмарного відеоспостереження. По-перше, існує потенціал для інтеграції з іншими технологіями, такими як штучний інтелект і машинне навчання. Це може призвести до ще більш точного та ефективного виявлення та запобігання

злочинній діяльності. По-друге, зростає увага до підвищення безпеки даних і захисту конфіденційності. Це включає розробку методів шифрування та безпечних методів зберігання даних. Нарешті, існує потреба у співпраці між правоохоронними органами, технологічними компаніями та громадськістю для забезпечення успішної реалізації. Працюючи разом, ці групи можуть вирішити проблеми та максимізувати потенційні переваги спостереження за натовпом і аналізу великих даних хмарного відеоспостереження.

Поява смартфонів, камер і соціальних мереж принесла нові можливості для мультимедійного спостереження. На відміну від традиційної системи відеоспостереження, де дані збираються лише з розгорнутих датчиків, сучасні можливості спостереження поширюються на включення звітів про інциденти, засновані на натовпі, які є потенційними підказками для розслідування злочинів. Вже зараз записи з камер спостереження є найбільшим джерелом великих даних, а новий підхід стеження за допомогою натовпу робить речі ще більшими. Тому, коли хмара стає хостом для всіх цих даних, хмарна система спостереження може отримати переваги колективного розуму. Проте з цими новими явищами пов'язано декілька міркувань, а саме:

- Великі дані створюють проблеми аналізу та маніпулювання даними в хмарі для цілей спостереження. Велике питання полягає в тому, чи це корисно, чи покращує це точність інформації, чи покращує своєчасність відповіді.

- Великі дані пов'язані з проблемами, пов'язаними з безпекою та конфіденційністю даних. Отже, вибір правильних механізмів для захисту даних і конфіденційності є важливим вибором, який має більший вплив на стеження.

Оскільки спостереження за натовпом і великі дані відкривають нові можливості, щойно згадані виклики необхідно вирішити, щоб отримати від них переваги.

8. Безпека та конфіденційність. Безпека та конфіденційність є важливим питанням для управління інформацією датчиків у хмарному середовищі. Однією з основних проблем безпеки в хмарних системах відеоспостереження є загроза конфіденційності та конфіденційності даних. Ці системи збирають і зберігають конфіденційні дані, такі як відеоматеріали та інформацію про користувачів, які

можуть бути вразливими до кібератак і витоку даних. Неавторизований доступ і злом також становлять значний ризик, оскільки вони можуть поставити під загрозу цілісність і доступність даних. Крім того, забезпечення цілісності та доступності даних може бути складним завданням, оскільки системи потребують постійного моніторингу та обслуговування, щоб запобігти втраті або пошкодженню даних.

Занепокоєння щодо конфіденційності також виникають у хмарних системах відеоспостереження, оскільки існує ризик зловживання та неправильного використання спостереження. Збір і зберігання персональних даних може викликати правові та етичні проблеми, зокрема щодо згоди та прозорості для користувачів. Отримати згоду може бути складно, оскільки користувачі можуть не повністю розуміти наслідки збирання та зберігання їхніх даних. Крім того, може бути складно забезпечити прозорість для користувачів щодо того, як використовуються їхні дані, оскільки системи можуть бути складними та важкозрозумілими.

Щоб зменшити ризики безпеки та конфіденційності, пов'язані з хмарними системами відеоспостереження, можна застосувати декілька рішень. Можуть бути реалізовані сувора автентифікація та контроль доступу, щоб забезпечити доступ до даних лише авторизованим користувачам. Методи шифрування та маскування даних також можуть бути використані для захисту даних від кібератак і порушень даних. Нарешті, прийняття принципів конфіденційності при проектуванні та проведення оцінки впливу на конфіденційність може допомогти переконатися, що системи розроблені з урахуванням конфіденційності та що потенційні ризики для конфіденційності виявлені й усунені.

Хмарні системи відеоспостереження пропонують багато переваг, але вони також несуть значні ризики для безпеки та конфіденційності. Щоб пом'якшити ці ризики, важливо впровадити потужні заходи безпеки та конфіденційності, а також прийняти принципи конфіденційності за проектом і провести оцінку впливу на конфіденційність. Таким чином ми можемо гарантувати, що ці системи є безпечними, захищають конфіденційність користувачів і використовуються етично та відповідально.

За відсутності належної політики безпеки та конфіденційності розгортання

хмарної мультимедійної системи спостереження буде ускладнено. Це стосується кількох проблем, які потребують уваги, наприклад наступних:

- Відео з камер спостереження має бути захищеним і протистояти різним загрозам безпеки. Для забезпечення безпеки на різних рівнях застосовуються різні підходи, наприклад криптографічний підхід для безпеки хмарних сховищ, щоб переконатися, що клієнти впевнені в послугах, що надаються постачальником хмарних технологій.

- Існують різні підходи до автентифікації та керування ідентифікацією, які можуть забезпечити різний рівень безпеки для доступу до хмари.

- Механізм забезпечення конфіденційності може вплинути на те, чи будуть клієнти обирати хмару для мультимедійної інфраструктури спостереження чи ні. Існує кілька політик керування доступом, які мають різний рівень прийнятності, наприклад контроль доступу на основі ролі (RBAC), контроль доступу на основі порогових значень (TBAC) і контроль доступу на основі діяльності (ABAC). Хмарна система спостереження може використовувати відповідну політику контролю доступу серед різноманітних варіантів.

- Вибрана архітектура хмарного розгортання, наприклад приватна чи публічна, впливатиме на безпеку та конфіденційність хмарних систем спостереження.

Тому важливо визначити канали витоку безпеки та конфіденційності в хмарних мультимедійних системах спостереження та вжити рішучих заходів для пом'якшення будь-яких відповідних загроз.

9. Проблеми з продуктивністю. Хмарна мультимедійна система відеоспостереження може використовувати величезні ресурси зберігання та обчислювальні ресурси в обмін на певні витрати. Таким чином, важливо вимірювати наслідки ефективності різних завдань, пов'язаних зі спостереженням. Нижче наведено кілька факторів, пов'язаних із продуктивністю:

- Важливо визначити параметри якості, які необхідно виміряти, наприклад, точність виявлення подій, час відгуку, використання процесора та пам'яті, робоче навантаження, співвідношення вартості, середній час очікування завдання тощо.

- Іншим важливим аспектом є визначення того, чи забезпечують хмарні процеси та служби гарантію QoS. Вимірювання якості інформації (QoI) і якості досвіду (QoE) також є необхідним через важливість виявлення подій та обміну діями, які здійснюються системами спостереження.

Продуктивність апаратного забезпечення хмарної системи відеоспостереження має вирішальне значення для визначення її ефективності та ефективності. Апаратні можливості та обмеження камери відіграють значну роль у якості знятого відеоматеріалу. Роздільна здатність камери, поле зору та можливості роботи в умовах слабкого освітлення є важливими факторами, які слід враховувати при оцінці апаратних можливостей камери. Крім того, потужність і масштабованість серверного обладнання є критично важливими для того, щоб система могла обробляти великий обсяг даних. Інфраструктура мережі та вимоги до пропускної здатності також мають вирішальне значення для визначення продуктивності системи. Повільне мережеве з'єднання може призвести до затримок у передачі відеозапису, що призведе до низької продуктивності системи.

Продуктивність програмного забезпечення хмарної системи відеоспостереження також важлива для забезпечення її оптимальної роботи. Функції та функції програмного забезпечення визначають такі можливості системи, як виявлення руху, розпізнавання обличчя та відстеження об'єктів. Сумісність програмного забезпечення з різними моделями та брендами камер також має вирішальне значення для забезпечення того, що система може працювати з різними камерами, надаючи користувачам гнучкість. Функції безпеки програмного забезпечення та механізми захисту даних є важливими для забезпечення безпеки системи та захисту даних від несанкціонованого доступу.

Залежно від вибору кількох факторів, що стосуються хмарного сховища, обробки мультимедійних даних, розподілу ресурсів тощо, буде визначатися продуктивність загальної системи спостереження. Можливо, варто розробити структуру якості для вимірювання загальної продуктивності хмарних систем спостереження.

Короткий перелік різних проблем і варіантів проектування представлено в

табл. 2.1 [7, 8].

Таблиця 2.1

Короткий опис проблем і варіантів проектування, пов'язаних із хмарною мультимедійною системою спостереження

Відмінні питання	Вибір проектування
1	2
Архітектура розгортання	Громадські, приватні та гібридні
Вибір методів передачі відео	Push-only, pull-only, push-pull, and event-driven
Хмарне сховище	Блокування постачальника, аварійне відновлення, еластичність, безпека та конфіденційність, а також оплата та ціноутворення
Обробка медіа	Різні завдання обробки мультимедійних даних, різнорідність QoS, мережі та пристроїв, а також міркування щодо мобільної хмари
Розподіл ресурсів	Інша ціль оптимізації (максимальне використання ресурсів проти мінімізації часу відгуку та вартості, компроміс між середнім часом очікування обслуговування та довгостроковою вартістю обслуговування, максимальний прибуток проти мінімізації збитків і рівномірний розподіл навантаження)
Сповіщення та обмін	Механізми публікації-підписки (на основі теми, на основі контенту, на основі типу, параметризовані), режим розповсюдження інформації, алгоритми зіставлення подій та обсяг інформації

Продовження таблиці 2.1

Короткий опис проблем і варіантів проектування, пов'язаних із хмарною мультимедійною системою спостереження

1	2
Спостереження на основі натовпу та аналітика великих даних	Корисність великих даних, точність інформації, своєчасність реагування, безпека та конфіденційність даних
Безпека та конфіденційність	Криптографічний підхід, різні підходи до автентифікації та керування ідентифікацією, різні політики контролю доступу (RBAC, TBAC і ABAC) і вплив безпеки на вибір хмарного розгортання
Проблеми з продуктивністю	Кілька показників продуктивності (точність виявлення подій, час відгуку, використання ЦП і сховища, робоче навантаження, компроміс вартості, середній час очікування завдання, QoS, QoI та QoE)

Хмарні системи відеоспостереження пропонують багато переваг порівняно з традиційними системами відеоспостереження, включаючи гнучкість, масштабованість і економічну ефективність. Щоб забезпечити успіх хмарної системи відеоспостереження, важливо ретельно розглянути її архітектуру, розгортання та найкращі практики. Дотримуючись цих вказівок, організації можуть запровадити ефективну, результативну та безпечну хмарну систему відеоспостереження.

2.2 Види камер відеоспостереження за призначенням

Камери відеоспостереження стали невід'ємною частиною систем безпеки в

різних місцях, включаючи житлові, комерційні та громадські приміщення. Ці камери є засобом моніторингу та запису дій, що допомагає стримувати злочинну діяльність і надавати докази у випадку кримінального розслідування.

Система відеоспостереження складається з трьох основних компонентів: камер, записуючих пристроїв і програмного забезпечення для перегляду. Камери знімають відеозйомку території, що контролюється, і передають її на записуючий пристрій. Записуючий пристрій зберігає відзнятий матеріал і дозволяє відтворювати та переглядати. Програмне забезпечення для перегляду надає доступ до відзнятого матеріалу та дозволяє здійснювати віддалений моніторинг. Деякі системи також мають додаткові функції, такі як виявлення руху, розпізнавання обличчя та розпізнавання номерних знаків.

Переваги використання камер відеоспостереження в системах безпеки численні. По-перше, наявність камер є стримуючим фактором для злочинної діяльності. Злочинці рідше скоюють злочини в тих місцях, де вони знають, що за ними стежать. По-друге, відеозапис є цінним доказом у кримінальних розслідуваннях. Зйомки можуть бути використані для встановлення осіб підозрюваних та надання доказів у суді. Нарешті, камери відеоспостереження можна використовувати для моніторингу громадських місць, таких як парки та вулиці, забезпечуючи безпеку громадян і знижуючи рівень злочинності.

Камери відеоспостереження є важливою складовою будь-якої системи відеонагляду. Їх використовують для запису відео зображення та аудіо даних з метою забезпечення безпеки, контролю доступу, а також для збору різноманітної інформації. Камери відеоспостереження можна розподілити за різними ознаками, такими як [9]:

- за формою і розміром: круглі, кутові, прямокутні, циліндричні, дискові тощо.

- за методом передачі сигналу: провідні, бездротові, аналогові, цифрові.

- за технологією передачі зображення: IP-камери, HD-TVI камери, AHD камери, CVI камери.

- за рівнем захисту: вуличні, внутрішні, з підсвічуванням, з захистом від

вандалізму.

- за типом матриці: CCD, CMOS.

- за об'єктивом: фіксований, змінний фокус, зум.

- за кутом огляду: ширококутний, стандартний, телескопічний.

Кожен з цих типів камер має свої переваги і недоліки, а також відповідний спектр застосування. Наприклад, IP-камери є більш ефективними та можливостями-завантаженими, але вони також дорожчі та вимагають більш складної настройки. Аналогові камери, з іншого боку, є більш доступними, але не мають тієї самої якості зображення.

Оскільки кожна ситуація є унікальною, вибір камери відеоспостереження залежить від різних факторів, таких як бюджет, місцезнаходження, тип об'єкта тощо. Отже, важливо зробити дослідження, перш ніж вибирати камеру відеоспостереження, і враховувати різноманітні параметри, щоб забезпечити ефективну та надійну систему відеонагляду, яка відповідає вимогам конкретного об'єкту та завданням, що перед ним стоять.

Також важливим фактором при виборі камери відеоспостереження є її можливості зберігати велику кількість даних та мати відповідну роздільну здатність. Це дозволяє забезпечити більш детальну інформацію про події, що відбуваються на об'єкті. Крім того, на вибір камер впливає також відстань, на якій потрібно зафіксувати об'єкт, а також освітлення в місці встановлення.

У своїй роботі камери відеоспостереження можуть бути використані для вирішення різних завдань, наприклад [10]:

- контроль доступу до території або об'єкту;

- відслідковування руху транспорту або пішоходів на вулицях;

- моніторинг роботи промислового обладнання;

- контроль за поведінкою співробітників в офісі або на виробництві;

- виявлення порушень на території, наприклад, викрадення чи вандалізм.

Таким чином, камери відеоспостереження є важливою технічною складовою для забезпечення безпеки та контролю різних процесів. При їх виборі потрібно враховувати різноманітні фактори, щоб забезпечити ефективну та надійну систему

відеонагляду, яка відповідає вимогам конкретного об'єкту та завданням, що перед ним стоять.

Сьогодні сучасні системи відеоспостереження є важливою складовою для забезпечення безпеки та контролю різних процесів. Технологічний прогрес останніх років значно змінив обличчя відеоспостереження, зробивши його більш ефективним, надійним і доступним. Сучасні системи відеоспостереження забезпечують високу якість зображення, аудіо та відеозапис, а також здатність до розпізнавання обличчя та інших важливих параметрів.

Однією з головних переваг сучасних систем відеоспостереження є їх мобільність. Сьогодні більшість камер має можливість передавати зображення в режимі реального часу на мобільні пристрої. Це дозволяє оперативно реагувати на події та забезпечувати швидкий доступ до відеоінформації. Крім того, розвиток мережевих технологій дозволяє створювати великі мережі відеоспостереження, що об'єднують багато камер і дозволяють проводити ефективний моніторинг за об'єктами на великій відстані.

Окрім цього, сучасні системи відеоспостереження використовують інтелектуальні алгоритми обробки даних. Завдяки цьому можливо автоматизувати роботу системи відеоспостереження та підвищити її ефективність. Наприклад, система може автоматично відслідковувати рух транспорту на вулиці або виявляти небажані предмети на території.

Отже, сучасні системи відеоспостереження мають великий потенціал для забезпечення безпеки та контролю різних процесів. Вони забезпечують високу якість зображення, мобільність та інтелектуальну обробку даних. Проте, є проблема збереження та обробки великої кількості відеоінформації. Тому, для ефективного використання сучасних систем відеоспостереження необхідно вирішувати проблему збереження та обробки даних.

Для забезпечення ефективної роботи системи відеоспостереження необхідно забезпечити її якісне проектування та установку. Важливо вибрати правильний тип камери, щоб забезпечити високу якість зображення та максимальну покриття. Також, необхідно правильно вибрати місце установки камер, щоб забезпечити

максимальну ефективність відеоспостереження.

У майбутньому сучасні системи відеоспостереження можуть бути ще більш ефективними та інноваційними, завдяки постійному розвитку технологій. За допомогою розумних алгоритмів та штучного інтелекту, можливо розробити системи, які зможуть прогнозувати події та вчасно реагувати на них. Таким чином, сучасні системи відеоспостереження мають великий потенціал для захисту нашої безпеки та контролю різних процесів, але їх ефективне використання потребує комплексного підходу та постійного вдосконалення технологій.

Системи відеоспостереження - це технологія, яка використовує відеокамери для захоплення та запису відеоінформації в реальному часі з метою безпеки та контролю. В залежності від їх призначення та масштабу використання, існують різні види систем відеоспостереження. Розглянемо найпоширеніші з них.

Системи відеоспостереження в приміщеннях - це системи, які використовуються для спостереження в приміщеннях, таких як офіси, магазини, банки, готелі та інші. Вони зазвичай складаються з однієї або декількох відеокамер, які встановлюються в певних місцях приміщення, щоб захоплювати відеоінформацію з усіх кутів.

Системи відеоспостереження на вулиці - це системи, які використовуються для спостереження на відкритому повітрі, наприклад, на вулицях, в парках, на стадіонах та інших місцях загального користування. Вони зазвичай складаються з великої кількості відеокамер, які встановлюються на різних висотах для захоплення відеоінформації з різних кутів.

Мобільні системи відеоспостереження - це системи, які використовуються для спостереження в рухомих об'єктах, таких як автомобілі, поїзди, літаки та інші. Вони зазвичай складаються з відеокамер, які встановлюються в рухомих об'єктах та передають відеоінформацію на центральний сервер для обробки та аналізу.

Інтелектуальні системи відеоспостереження - це системи, які використовуються для автоматичного аналізу відеоінформації з метою виявлення певних подій або поведінки. Вони зазвичай включають в себе програмне забезпечення, яке дозволяє використовувати різні алгоритми для виявлення певних

об'єктів, руху або подій, таких як вибух, пожежа, крадіжка тощо. Інтелектуальні системи відеоспостереження є дуже ефективними засобами забезпечення безпеки та контролю в різних сферах, включаючи бізнес, громадську безпеку та військові цілі.

Камери відеоспостереження є важливою складовою сучасних систем безпеки. Вони забезпечують засоби моніторингу та запису діяльності, що допомагає стримувати злочинну діяльність і надавати докази у разі кримінального розслідування. Різні типи камер і компонентів системи відеоспостереження пропонують широкий вибір варіантів для різних налаштувань. Переваги використання камер відеоспостереження в системах безпеки неможливо переоцінити, що робить їх цінною інвестицією для будь-якої організації чи окремої особи, яка займається безпекою.

У світі використовуються різні види систем відеоспостереження залежно від їх призначення та масштабу використання. Важливо вибрати правильний тип системи відеоспостереження для вашої потреби та забезпечити її належну настройку та ефективну роботу.

Аналогові системи відеоспостереження. Нещодавно установка відеоспостереження була побудована на аналогових камерах, мікшерах і моніторах, сучасне охоронне відеоспостереження витісняє старі системи і в багатьох комплексах практично не використовує аналогові системи, майже повністю переключившись на цифровий формат. Схема роботи аналогових систем відеоспостереження представлена рис. 2.3 [11].



Рис. 2.3. Аналогові системи відеоспостереження

Тенденція розвитку цифрових технологій ніколи не зможе повністю витіснити аналогову апаратуру, так само як цифрова фотографія не замінить фотодрук. Звичайно, передача аналогових сигналів неефективна, низька завадостійкість, втрата сигналу, складність у записі та обробці цифрових сигналів. Проте, відеоспостереження не виключає можливості використання аналогових камер.

Установка відеоспостереження на основі аналогових відеокамер не втрачає своєї популярності. Серед безлічі недоліків аналогового відеоспостереження є істотні позитивні сторони.

Встановлення відеоспостереження та його налаштування набагато простіше, ніж встановлення відеоспостереження цифрового формату. Це пов'язано з виключенням цифрової синхронізації між камерами та обладнанням для запису сигналу:

– аналогове охоронне спостереження на порядок дешевше, ніж рівносильне цифрове обладнання, тому встановлення відеоспостереження на аналогових відеокамерах у невеликих магазинах або офісах є прийнятним за бюджетом і є досить ефективним;

– цифрове охоронне відеоспостереження відрізняється від аналогового зручністю зберігання та обробки даних. Відео сервери мають можливість

оцифровувати сигнал, таким чином, на аналогових відео системах можна організувати якісне охоронне відеоспостереження. За допомогою відео серверів аналогові камери можна підключати до мереж;

– незважаючи на складність підвищення дозволів зображення та швидкості, встановлення відеоспостереження на основі аналогових камер має попит. Якість кольору для кольорових аналогових камер значно вища, крім того, в порівнянні з цифровим відеоспостереженням аналогові системи краще працюють у темряві, чутливість матриці досить висока, щоб можна було розрізнити не тільки силует, але і обличчя злочинця.

Аналог краще працює в темряві, тому встановлення відеоспостереження базується не на сучасності того чи іншого обладнання, а на конкретних завданнях, позначених для складання проекту. Багато фахівців, які працюють з професійним обладнанням, ведуть охоронне відеоспостереження, та використовують аналогові відеокамери.

Цифрові системи відеоспостереження. Для людей, хто ніколи не стикався з установкою системи відеоспостереження, фраза цифрове відеоспостереження є просто поєднання двох сучасних слів. Цифрове телебачення, відеокамери та цифрові фотоапарати знайомі всім, але чим цифрова техніка краща і чому встановлення систем відеоспостереження з цифровою якістю є такою популярною.

За кілька десятків років наш світ якісно змінився. Багато хто пам'ятає вінілові пластинки з характерним потріскуванням при відтворенні, а зараз у нас є лазерні диски. Різниця між цими двома носіями інформації в тому, що вініл – це аналоговий формат, а компакт-диск – цифровий.

Відповідно різні розміри і колосальна різниця в обсязі інформації, що зберігається, крім того цифровий носій стійкий до впливу часу і зчитування з нього інформації. Ось у принципі й загальна відповідь.

Якщо провести паралель та взяти за основу цифрове відеоспостереження, то вийде приблизно така картина. Аналоговий потік обмежений реальним часом, таким чином, по одному дроту можна передати лише один сигнал однієї відеокамери, що виходить. Установка системи відеоспостереження аналогового

типу має на увазі індивідуальне підключення для кожної камери.

Цифрові системи як і аналогові ведуть послідовну передачу даних, але швидкість передачі незрівнянно вище. Завдяки існуючим протоколам. Таким чином, цифрове відеоспостереження дозволяє підключати велику кількість камер, керувати ними, швидко зберігати інформацію та паралельно працювати з нею.

Установка системи відеоспостереження цифрового формату дозволяє уникнути втрат під час передачі даних, це пов'язано з тим, що цифровий сигнал складається з послідовності одиниць і нулів, а аналоговий на амплітуді коливань.

Цифрове відеоспостереження відрізняється високою роздільною здатністю картинки, так можна збільшувати зображення, розглядати окремі деталі, такий ефект досягається за рахунок зменшення розміру осередків матриці, і відтак їх кількості, яка вимірюється в мега пікселях.

Застосування цифрових камер має бути обґрунтованим для економічної доцільності проекту відеоспостереження.

IP-системи відеоспостереження. IP – це протокол (Internet Protocol) між мережевої взаємодії. Він дозволяє пристроям підключатися до мережі та взаємодіяти за допомогою програм із комп'ютером.

Саме IP-відеоспостереження використовується в сучасних системах, нових системах виявлення та аналізу предметів, для автоматичного розпізнавання номерних знаків автомобілів. Монтаж відеоспостереження на основі IP дозволяє об'єднати відеокамери за допомогою існуючої мережі, звернення до камери можливо безпосередньо з комп'ютера, досить просто ввести IP-адресу камери.

Монтаж відеоспостереження займає мінімум часу, камери швидко встановлюються. IP-відеоспостереження підходить як для роботи всередині приміщень, так і зовні. Для вуличного спостереження використовується спеціальний кожух та об'єктив.

Камери для IP-відеоспостереження мають функцію пре і пост запису (за сигналом тривоги), для цього використовується карта пам'яті.

Відеокамери бувають декількох типів, високочутливі, панорамні, купольні, з високою роздільною здатністю 1280x1024 пікс. та швидкістю до 30 к/с. Усі вони

розроблені в організацію систем спостереження. Для IP-відеоспостереження випускаються спеціальні кожухи до камер, для роботи в умовах підвищеної вологості, низьких температур та навіть антивандальний кожух для міського відеоспостереження.

Монтаж відеоспостереження з використанням IP зазвичай здійснюється спільно з організацією локальних мереж. Можна оцінити надійність і простоту забезпечення безпеки і спостереження.

Монтаж системи відеоспостереження стандартного провідного підключення обтяжений деякими технологічними складнощами, зокрема, з монтажем кабелю для підключення.

Бездротові системи відеоспостереження. Думка професіоналів щодо бездротового відеоспостереження - однозначно, фахівці вважають за краще проводити монтаж системи відеоспостереження, заснованої на кабельному з'єднанні. Давайте визначимо переваги та недоліки бездротового відеоспостереження [11].

Недоліки бездротового відеоспостереження:

– монтаж системи відеоспостереження стандартного, кабельного типу, дозволяє отримати: якісне зображення з високою роздільною здатністю та швидкістю 25 к/с., звуковий супровід, можливість керувати відеокамерою, та можливістю її підключення безпосередньо до локальної мережі LAN.

Бездротове відеоспостереження позбавлене або частину без цих переваг;

– бездротове відеоспостереження потребує джерела живлення. Це можуть бути акумулятори, в такому випадку необхідна постійна заміна або заряджання, або виносні мережеві блоки живлення. Системи бездротового відеоспостереження позбавлені захисту від перепадів напруги.

До переваг бездротового відеоспостереження можна віднести дві основні переваги. По-перше, монтаж системи відеоспостереження не вимагає свердління стін для прокладання ліній. По-друге, бездротове спостереження - це мобільна система, за бажанням Ви можете змінювати розташування відеокамери. Крім того сучасні системи можуть бути мініатюрні і працювати зі спеціальним приймачем, з

дисплеєм. Здебільшого це побутове застосування.

Хоча існує і вулична система бездротового відеоспостереження. Відеокамери оснащені спеціальним кожухом та інфрачервоними світлодіодами для зйомки у нічний час, вони автоматично перемикаються в режим нічної зйомки за умови недостатньої видимості. Монтаж системи відеоспостереження виправдано, якщо з різних причин виникають складності з прокладкою кабелю.

3 МОНТАЖ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ТА ПІДКЛЮЧЕННЯ ДО ХМАРНИХ СЕРВІСІВ

3.1 Монтаж систем відеоспостереження

Відеоспостереження є практичним і перевіреним способом запобігання багатьом злочинам. Компактні розміри сучасних камер спостереження дозволяють встановлювати їх не тільки на великих промислових, фінансових та складських об'єктах, а й у житлових та підвальних приміщеннях, коморах, невеликих торгових та виробничих майданчиках. І це спричиняє культуру монтажу відеокамер в громадських місцях, що обумовлює зовнішній вигляд точок установки, а на виробничих територіях ще й безпеку їх знаходження в технологічному оточенні.

Системи відеоспостереження останнім часом стають все більш популярним засобом безпеки. Ці системи призначені для моніторингу та запису дій у певній зоні, забезпечуючи цінний інструмент для підвищення безпеки та безпеки.

Системи відеоспостереження призначені для захоплення та запису візуальних зображень певної області, які потім можна контролювати та аналізувати з метою безпеки. Ці системи можна класифікувати на два основних типи: аналогові та цифрові. Аналогові системи використовують традиційні камери та реєстратори відеоспостереження, тоді як цифрові системи використовують IP-камери та мережеві реєстратори. Компоненти типової системи відеоспостереження включають камери, реєстратори та монітори. Камери є найважливішим компонентом системи, оскільки вони фіксують зображення, які будуть записані та проаналізовані. Записи зберігаються на реєстраторі, яким може бути цифровий відеорекордер (DVR) або мережевий відеорекордер (NVR). Монітори використовуються для перегляду прямого або записаного відео.

Однією з головних переваг встановлення систем відеоспостереження є стримуючий ефект від злочинів та крадіжок. Наявність камер може перешкодити злочинцям націлюватися на певну територію, оскільки вони знають, що їхні дії будуть зафіксовані та можуть бути використані як доказ проти них. Крім

стримування злочинної діяльності, системи відеоспостереження також підвищують безпеку приміщень і мешканців. Ці системи можна використовувати для моніторингу зон високого ризику, таких як входи, виїзди та стоянки, і можуть попереджати персонал служби безпеки про будь-які підозрілі дії. Вони також можуть бути використані для моніторингу поведінки співробітників і запобігання крадіжці або неправомірній поведінці. Нарешті, системи відеоспостереження полегшують розслідування та збір доказів. У разі злочину чи інциденту кадри з системи можуть бути використані для ідентифікації підозрюваних, надання доказів у суді та допомоги в процесі розслідування.

Встановлюючи системи відеоспостереження, важливо враховувати правові та етичні наслідки їх використання. Необхідно враховувати закони та правила щодо конфіденційності та розміщувати знаки, які інформуватимуть людей про те, що за ними стежать. Вартість – ще один важливий фактор при встановленні систем відеоспостереження. Вартість системи залежатиме від кількості необхідних камер, реєстраторів і моніторів, а також від складності монтажу. Також слід брати до уваги бюджет поточного обслуговування та модернізації. Нарешті, важливо розглянути, як система відеоспостереження буде інтегруватися з існуючими системами безпеки. Інтеграція з системами контролю доступу, системами сигналізації та іншими засобами безпеки може підвищити загальну ефективність системи.

Процес монтажу є основою побудови будь-якої системи, що визначає її подальшу ефективність та функціональність. Початкове його опрацювання та постановка завдань, рівень використаних матеріалів та засобів, грамотність та кваліфікація установника – визначають те, що прийнято називати культурою монтажу [12, 13].

Чимало прикладів установок, змонтованих на об'єктах, де стикаються з проблемами недостатньої ефективності систем, частковими або повними їх відмовами, що виникають в основному через допущені при монтажі помилки, або через здешевлення за рахунок відмови від компонентів, що визначаються культурою монтажу. Найчастіше спостерігається зневага до цього процесу, що є головною помилкою. Основні проблеми замовника у цьому, що у більшості

випадків або монтаж сприймається як простий механічний процес, і тоді, покладаючись на професіоналізм та відповідальність виконавця, йому не приділяється особливої уваги, або навпаки надмірного втручання замовника у цей технологічний процес та регулювання матеріалів та дій самостійно, повністю знижуючи надійність та можливості системи через недостатнє знання.

Найважливішою частиною, що впливає на якість монтажних робіт, що проводяться, є етап початкового проектування, але їм багато хто нехтує. Побудова будь-якої системи обов'язково має виконуватися після детального опрацювання проекту, будь то система відеоспостереження, система контролю доступу (СКУД), система сигналізації тощо. Перед виконанням слід з'ясувати:

– для яких саме завдань буде використовуватися система, що будується, та її ресурси;

– які завдання потенційно можуть виникнути додатково в період її експлуатації;

– чи планується розширення системи і якщо так, то планувати ресурс місткість необхідно з розрахунком на це;

– чи планується система як єдиний інструмент, чи скрадатиметься з кількох самостійних компонентів.

Якісне складання проекту без з'ясування цих питань у принципі неможливе.

Системи відеоспостереження є цінним інструментом для підвищення безпеки та захисту в різних ситуаціях. Вони забезпечують стримуючий вплив на злочинну діяльність, підвищують безпеку та спрощують розслідування та збір доказів. Однак під час встановлення цих систем необхідно ретельно розглянути правові та етичні наслідки, вартість і бюджет, а також інтеграцію з існуючими системами безпеки

Види камер відеоспостереження. Подумаєш, встановити відеокамеру, що може бути простішим. Взяти та прикрутити до чого не будь, повернути у бік перегляду та готово. Але на практиці встановлення камер спостереження - це набір різноманітних дій, що вимагають, крім монтажного вміння, ще й розуміння їх роботи та експлуатації.

Установка відеокамери всередині приміщення вимагає попередньо врахувати

дизайн відеокамери та загальний вигляд інтер'єру та властивості поверхні кріплення, чи не буде вона занадто помітна чи невидна, чи поєднується з оточенням, а потім, чи надійно закріплена, яким способом підійде до неї кабель, чи виглядатиме і т.п. Так само важливі технічні та технологічні аспекти установки та самої відеокамери.

Крім того, важливо направити камеру так, щоб світло від освітлювальних ламп не падало в її об'єктив, інакше в кадрі буде сильне засвічення, що робить марною частиною зображення з відеокамери.

Установка камери зовнішнього спостереження складніша. Для вуличної відеокамери важливі: кут огляду, висота установки, а ще більше джерела освітлення, включаючи Сонце. Вуличне спостереження має вестися і вночі, а якщо вночі джерело світла потрапляє в огляд відеокамери, то відображається просто біла пляма. Тому камеру потрібно встановити, якнайдалі від протипоставлених і перетинають огляд джерел світла. Також важливо встановлювати вуличну відеокамеру під карнизом так, щоб край даху не був прямо над відеокамерою, оскільки бурульки, що звисають теплою зимою, можуть її істотно пошкодити.

Правила встановлення камер відеоспостереження. Ці правила можуть залежати від системи та дещо відрізнятися за умовами експлуатації. Наприклад, вимоги щодо встановлення для вуличних камер будуть жорсткішими, ніж для внутрішніх. У загальному випадку, установка камер в офісі, будинку, квартирі або іншому об'єкті, що охороняється, не має значних відмінностей. Тому, попри індивідуальні особливості кожного об'єкта спостереження, є єдині вимоги, викладені нижче (рис. 3.1) [14].

Фокусна відстань	2,8мм	3,6мм	6мм	8мм	12мм	16мм
Кут огляду	86°	72°	48°	30°	25°	17°
Відстань до об'єкта	0- 5м	0- 6м	5- 10м	10- 20м	25- 35м	35- 50м

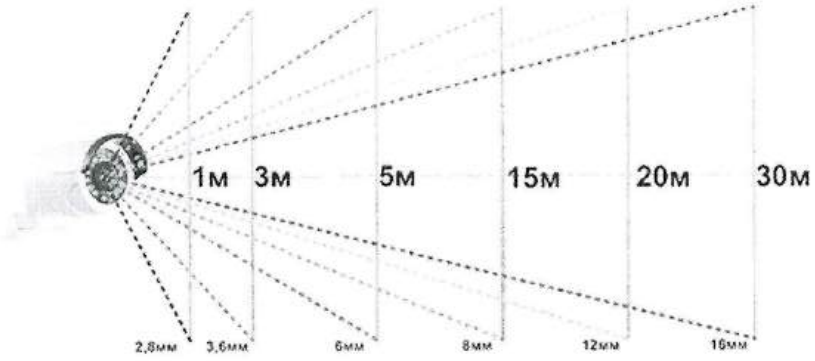


Рис. 3.1. Відстань зміни обзору камер

Під час встановлення відеоспостереження слід керуватися такими правилами та рекомендаціями:

За форм-фактором у будинку краще підходять купольні камери, а для охорони та спостереження на вулиці – циліндричні. Але циліндричні легше зламати та вкрасти.

Перед монтажем кронштейнів та прокладанням проводів для камери, слід спочатку визначити місцевість охоплення, яку вона повинна показати, визначити дальність огляду, висоту та нахил установки, перевірити її справність, перевірити режим денного та нічного бачення. Для цього слід побачити зображення, яке вона передає у всіх режимах експлуатації.

На захищених об'єктах краще проводити приховане відеоспостереження, але використовувати його в комбінації зі звичайним, щоб не порушувати закон.

Перевірте, щоб у місцевості, що спостерігається, освітлення було розподіллено рівномірно. Якщо встановити камеру в затемненому місці, направивши її на яскраво освітлену територію, якість зображення буде низькою. Швидше за все це можна буде відкоригувати функціями WDR, BLC, HLC, доступними в більшості IP камер і не дешевих HD-TV, але постарайтеся досягти однакової освітленості в місцях встановлення та огляду камери.

Камери можуть вийти з ладу, якщо вони спрямовані у бік яскравого світла чи сонця. При проектуванні відеоспостереження обов'язково зважайте на добовий рух сонця.

Як правило, камера має «хвіст» проводів, що закінчуються сполучними роз'ємами, якими вона підключається. Для їх приховування та захисту необхідно використовувати сполучні коробки, що виконують функцію тримача камери.

Вибираючи місця встановлення, передбачте максимальний захист камер та сполучних коробок від можливого потрапляння прямого сонячного світла, утворення льоду, випадання снігу та дощу.

Щоб уникнути поломки або крадіжки обладнання зловмисниками, рекомендується встановлювати камери якомога вище.

При установці камер переконайтеся, що ви зможете дістатися до них. Це необхідно для того, щоб можна було протерти пил і вологу, видалити павутиння і т.д. Регламентні роботи забезпечать якісну та тривалу роботу системи відеоспостереження.

При проектуванні прокладки ліній передачі відеосигналу та живлення відеокамер виключіть можливий вплив будь-яких електромагнітних наведень на відеосигнал, що вносять спотворення зображення на моніторі.

При установці камер спостереження зовні з використанням індивідуальних блоків живлення їх необхідно помістити в герметичну коробку, так як вони не розраховані для вуличного застосування. При цьому не забудьте встановити ущільнювачі отворів введення дротів у цю коробку. Для перевірки якості рівня відеосигналу в різних точках лінії даних використовуйте осцилограф, а для знаходження обривів та коротких замикань у них та лініях живлення – тестер (авометр).

Для нічного відеоспостереження слід домогтися достатнього освітлення на ділянці. При нестачі можна встановити додатково до камер світлодіодне підсвічування.

У будинку, магазині, складі чи офісі обов'язково передбачте камеру перед кожним входом (виходом). Це дозволить виявити, хто і коли заходив і виходив з

приміщення.

Забезпечте захист відео реєстратора, він повинен бути в добре провітрюваному місці, недоступному для сторонніх. Зловмисники обов'язково захочуть спеціально пошкодити чи вилучити його.

Попередня підготовка до монтажу. Щоб досягти максимуму інформації одержуваних відеоданих від вибраних камер, необхідно їх правильне розміщення при монтажі. Оптимальне охоплення зон спостереження дозволяє зменшити потрібну кількість відеокамер, а, як наслідок, заощадити на обладнанні системи відео контролю загалом (рис. 3.2) [14, 15].

Основними параметрами розташування відеокамери спостереження, незалежно від того, вулична вона чи внутрішня, будуть:

– висота встановлення;

– розташування щодо охоронюваної спостереженням зони;

– кут огляду або фокусна відстань.

В обов'язковому порядку максимально знизити можливі можливості несанкціонованого впливу на роботу системи, особливо при розміщенні камер поза приміщеннями. Найбільш поширеним впливом є пошкодження відеокамери механічного. Це призводить до повного виходу з ладу, або у разі - частковій втраті архіву чи відображення кадру. Як правило, це результат вандалізму, але часто і завдання пошкоджень навмисне з метою тимчасової зупинки спостереження на конкретній території об'єкта, що сприяє вчиненню протиправних дій.

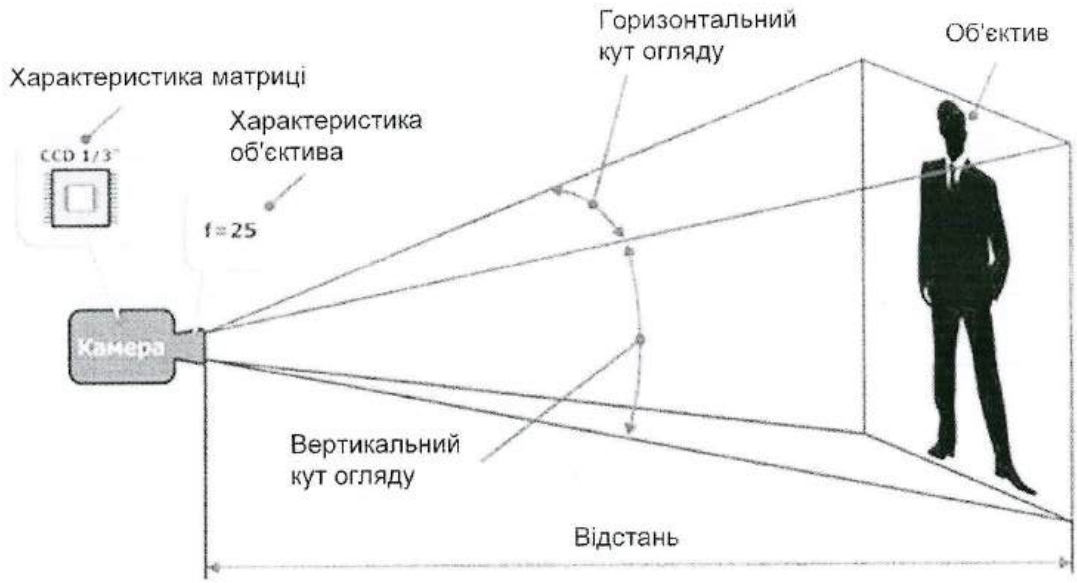


Рис. 3.2. Розташування відеокамери

Сучасні системи відеоспостереження здатні зафіксувати тряску, удар та втрату чи раптову зміну картинки, сформувавши відповідний сигнал тривоги. Однак це ефективно за наявності посту охорони з постійним перебуванням людей та розміщення реєстратора у захищеному приміщенні.

Розміщення відеокамер на недоступній для прямого доступу висоті є одним з найбільш ефективних способів її захисту, але має дуже серйозний недолік. У міру підйому місця встановлення камери, збільшуватиметься кут її нахилу до необхідної зони огляду, що призводить до спотворення зображення, а відповідно знижує ідентифікацію об'єкта або дію.

Зона огляду визначається кутами огляду по горизонталі та вертикалі обернено пропорційними фокусній відстані відеокамер. Вони визначають відстань ефективного спостереження та впливають на ступінь ідентифікації.

При розміщенні камер спостереження слід враховувати унікальні конструктивні особливості кожного об'єкта відеоспостереження. Місцями установки можуть бути карнизи, виступи, балкони, пілястри, колони, інші елементи та будівельні конструкції.

При розміщенні камери слід враховувати можливу наявність «сліпих зон»,

тобто ділянок певної зони контролю, що не переглядаються. Умовно їх можна поділити на два типи:

– статичні - їх формують дерева, виступи стін, меблі, споруди чи їх елементи тощо;

– динамічні - їх створюють об'єкти, що рухаються, на передньому плані, в основному це люди і транспортні засоби, що періодично потрапляють у зону перегляду відеокамери.

Визначити та обійти статичні проблемні місця праці не складе. Передбачити ж час і місце появи об'єкта, що рухається, практично неможливо. У цьому випадку рішенням може бути встановлення декількох камер відеоспостереження, що контролюють ту саму зону з різних ракурсів.

Якщо відеозапис ведеться по оптичному детектору руху, то будь-які об'єкти, що рухаються, можуть викликати його спрацьовування, а як наслідок буде проводитися запис польоту мух і шелесту листя з марною витратою дискового простору. Почасти це можна мінімізувати ретельним вибором зон детекції та налаштуванням чутливості обладнання, але краще, якщо таких помилкових спрацьовувань багато, використовувати камери з PIR-датчиком.

Контроль входу до будівлі. Спостереження за входом до будівлі є найчастіше вирішуваною системою відеоспостереження завдань. Розміщення відеокамери в цьому випадку, як правило, має забезпечувати ідентифікацію вхідних. Крім візуального пізнання по обличчю, яке можна якимось способом прикрити, слід зафіксувати:

– загальний зовнішній вигляд людини;

– зростання, комплекція, хода.

Для цього найкращими будуть висота розміщення камери 1,5-2 метри та спосіб установки – прихований.

Контроль периметра території. В цьому випадку, як правило, розміщення камер проводиться на зовнішній огорожі, кутах будівель або спеціально встановлених опорах. При цьому слід досягти:

– перетину зон спостереження та відсутності «мертвих» зон;

– взаємного візуального контролю несанкціонованого доступу до кожної відеокамери.

Внутрішнє розташування камер. У цьому випадку, як правило, основними є такі моменти:

– забезпечення необхідних зон огляду та ступенів деталізації;

– не створює незручності розміщення та максимальне збереження дизайну приміщень;

– меншою мірою, але може бути у громадських місцях, питання захисту від актів вандалізму.

Найчастіше для внутрішньої установки застосовуються купольні камери, оскільки для переважної більшості приміщень їх дизайн є оптимальним.

3.2 Сервіси доступу до хмарного середовища відеоспостереження та контролю

Хмарні системи відеоспостереження та контролю стають все більш популярними в останні роки. Ці системи пропонують ряд переваг, включаючи масштабованість, доступність і економічну ефективність.

Хмарне відеоспостереження означає використання хмарних технологій для зберігання та керування записами відеоспостереження. Ця технологія дозволяє користувачам отримувати доступ до своїх відеоканалів з будь-якого місця, де є підключення до Інтернету, що робить її ідеальним рішенням для компаній із кількома локаціями або віддалених працівників. Хмарне відеоспостереження також пропонує масштабованість, оскільки компанії можуть легко додавати або видаляти камери за потреби без необхідності інвестувати в нове обладнання.

Хмарне відеоспостереження часто є економічно ефективнішим, ніж традиційні локальні рішення, оскільки усуває потребу у дорогому апаратному та програмному забезпеченні. У порівнянні з традиційними локальними рішеннями хмарне відеоспостереження пропонує кілька переваг. Наприклад, з локальними

рішеннями компанії повинні інвестувати в дороге обладнання та програмне забезпечення, а також наймати IT-спеціаліст для керування та обслуговування системи. Навпаки, хмарне відеоспостереження не потребує попередніх інвестицій у апаратне чи програмне забезпечення, і системою керує постачальник. Крім того, хмарне відеоспостереження часто є більш надійним, ніж локальні рішення, оскільки воно розміщується на резервних серверах, які забезпечують безперебійну роботу та мінімізують ризик втрати даних.

Хмарні системи керування стосуються використання хмарних технологій для керування та моніторингу різних систем, таких як ОВК, освітлення та безпеки. Ці системи пропонують низку переваг, включаючи віддалений доступ, моніторинг у реальному часі та автоматизацію. За допомогою хмарних систем керування компанії можуть дистанційно контролювати та контролювати свої системи з будь-якого місця, де є підключення до Інтернету, що дозволяє їм швидко реагувати на будь-які проблеми, що виникають.

Крім того, хмарні системи керування пропонують моніторинг у режимі реального часу, що дозволяє підприємствам виявляти та вирішувати проблеми до їх загострення. Порівняно з традиційними локальними рішеннями, хмарні системи керування мають кілька переваг. Наприклад, з локальними рішеннями компанії повинні інвестувати в дороге обладнання та програмне забезпечення, а також наймати IT-спеціаліст для керування та обслуговування системи. Навпаки, хмарні системи керування не потребують попередніх інвестицій у апаратне чи програмне забезпечення, і системою керує постачальник. Крім того, хмарні системи керування часто є більш надійними, ніж локальні рішення, оскільки вони розміщені на резервних серверах, що забезпечує безперебійну роботу та мінімізує ризик втрати даних.

Інтеграція хмарних систем відеоспостереження та контролю може запропонувати низку переваг, включаючи підвищення ефективності, покращену безпеку та покращену обізнаність про ситуацію. Наприклад, завдяки інтеграції систем відеоспостереження та контролю підприємства можуть автоматизувати певні завдання, такі як вимикання світла, коли кімната порожня, що може

заощадити час і зменшити витрати на електроенергію. Крім того, інтеграція цих систем може покращити безпеку, оскільки підприємства можуть використовувати відеоматеріали для моніторингу та реагування на потенційні загрози в режимі реального часу.

Хмарна технологія спостереження стосується використання віддалених серверів для зберігання відеозаписів, знятих камерами, встановленими на території. Ця технологія дозволяє користувачам отримувати доступ до своїх відеозаписів з будь-якого місця, де є підключення до Інтернету, і отримувати сповіщення про виявлення руху. Одна з головних переваг хмарного відеоспостереження перед традиційними системами спостереження полягає в тому, що воно усуває потребу у локальному сховищі, обслуговування якого може бути дорогим і трудомістким. Крім того, хмарні системи часто більш надійні та безпечні, ніж традиційні системи. Деякі з компаній, які пропонують послуги хмарного відеоспостереження, включають Nest, Ring і Arlo.

Порівнюючи найкращі компанії, які надають послуги хмарного відеоспостереження, важливо враховувати такі фактори, як функції, ціни та відгуки клієнтів. Наприклад, Nest пропонує ряд розширених функцій, таких як розпізнавання обличчя та інтелектуальні сповіщення, але відносно дорогий порівняно з іншими варіантами. З іншого боку, Ring пропонує більш доступну послугу з базовим набором функцій, але її критикують за політику конфіденційності. Arlo відомий своїми високоякісними камерами та гнучкими ціновими планами, але деякі користувачі повідомили про проблеми з підключенням. Зрештою, вибір компанії залежатиме від конкретних потреб і вподобань користувача.

Оскільки технологія спостереження на основі хмарних технологій продовжує розвиватися, ми можемо очікувати появи ряду нових тенденцій на ринку. Наприклад, прогрес у штучному інтелекті та машинному навчанні, ймовірно, призведе до більш складних систем оповіщення, які зможуть розрізняти різні типи руху та виявляти незвичну поведінку. Крім того, ми можемо побачити збільшення використання хмарного відеоспостереження в таких галузях, як охорона здоров'я

та освіта, де безпека є головним пріоритетом. Загалом очікується, що ринок послуг хмарного відеоспостереження зростатиме в найближчі роки, оскільки все більше компаній і окремих осіб визнають переваги цієї технології.

Ось короткий опис кількох компаній, які надають послуги з хмарного відеоспостереження [16]:

Amazon Web Services (AWS): AWS пропонує рішення з хмарного відеоспостереження Amazon Kinesis Video Streams, що дозволяє реалізувати відеоспостереження в режимі реального часу на основі AWS.

Google Cloud: Google Cloud пропонує послугу Video Intelligence API, яка надає засоби машинного навчання для розпізнавання об'єктів, осіб та дій на відео.

Microsoft Azure: Microsoft Azure надає послуги зі зберігання та обробки відео, такі як Media Services та Video Indexer. Ці послуги дозволяють завантажувати, зберігати, стрімувати та обробляти відео в хмарі.

Hikvision: Hikvision є провідним світовим постачальником відеоспостереження та контролю доступу. Компанія надає рішення з хмарним відеоспостереженням, які дозволяють клієнтам зберігати та здійснювати доступ до відео з будь-якого місця з використанням веб-браузера або мобільного додатку.

Dahua Technology: Dahua Technology є одним з провідних виробників обладнання відеоспостереження. Компанія надає послуги з хмарного відеоспостереження, які дозволяють користувачам зберігати відео в хмарі та отримувати доступ до нього з будь-якого місця.

Camcloud: Camcloud є провідним постачальником послуг з хмарного відеоспостереження для домашнього та бізнес-використання. Компанія надає клієнтам зручні інструменти для зберігання, перегляду та керування відеоспостереженням з будь-якого місця з використанням веб-браузера або мобільного додатку.

Hikvision, як один з провідних світових виробників обладнання для відеоспостереження, пропонує сервіс хмарного відеоспостереження, який забезпечує зручне зберігання, доступ та управління відеоданими. Цей сервіс називається Hik-Connect Cloud.

Особливості та переваги сервісу Hik-Connect Cloud включають:

1. Легкість налаштування: Завдяки Hik-Connect Cloud, користувачам не потрібно знати складні деталі мережевих налаштувань або мати статичну IP-адресу. Просто зареєструйте свій обліковий запис Hik-Connect, додайте відеокамери, і вони будуть автоматично підключені до хмари.

2. Віддалений доступ: Користувачі можуть легко отримати доступ до відеоданих зі своїх мобільних пристроїв або комп'ютерів, використовуючи додаток Hik-Connect або веб-інтерфейс. Ви можете переглядати відео в реальному часі, проглядати архівні записи та керувати налаштуваннями камери з будь-якого місця, де є доступ до Інтернету.

3. Зберігання в хмарі: Відеодані зберігаються в безпечних хмарних серверах, що забезпечує надійне зберігання та захист від втрати даних через відмову обладнання або інші проблеми.

4. Гнучкість зберігання: Hik-Connect Cloud пропонує різні плани зберігання, від безкоштовних до платних, в залежності від потреб користувача. Ви можете вибрати план, який найкраще підходить для вас, залежно від обсягу відеоданих та тривалості зберігання.

5. Керування пристроями: З додатком Hik-Connect, користувачі можуть керувати різ ними пристроями, підключеними до системи відеоспостереження, такими як камери, реєстратори, датчики руху та інше. Це забезпечує централізоване управління всіма компонентами системи, що спрощує процес моніторингу та контролю.

6. Сповіщення та тривоги: Hik-Connect Cloud дозволяє налаштувати сповіщення та тривоги на основі різних подій, таких як рух, проникнення в зону, зникнення об'єктів тощо. Користувачі можуть отримувати миттєві сповіщення на свої мобільні пристрої або електронну пошту, що дозволяє швидко реагувати на події, що відбуваються [22].

7. Інтеграція з іншими системами: Hik-Connect Cloud може інтегруватися з іншими системами безпеки, такими як системи контролю доступу та системи сповіщення про пожежу. Це забезпечує комплексний підхід до безпеки та контролю

на об'єкті.

У підсумку, сервіс хмарного відеоспостереження Hikvision, Hik-Connect Cloud, пропонує потужні та гнучкі можливості для зберігання, доступу та управління відеоданими в корпоративних мережах. Завдяки цьому сервісу, користувачі можуть сконцентруватися на забезпеченні безпеки та контролю на своїх об'єктах, знаючи, що їх відеодані захищені та доступні з будь-якого місця з Інтернетом. Хмарні послуги відеоспостереження пропонують ряд переваг порівняно з традиційними системами спостереження, включаючи економічну ефективність, надійність і доступність. Вибираючи постачальника, важливо враховувати такі фактори, як характеристики, ціни та відгуки клієнтів. Оскільки ця технологія продовжує розвиватися, ми можемо очікувати появи нових тенденцій на ринку, а попит на хмарні послуги відеоспостереження продовжуватиме зростати.

3.3 Додатки мобільних телефонів для хмарного відеоспостереження та контролю

Хмарні системи відеоспостереження можна розділити на два основних типи: розміщені та гібридні системи. Розміщені системи — це ті, у яких відеозаписи зберігаються на віддалених серверах, якими керує сторонній постачальник, тоді як гібридні системи поєднують як локальні, так і віддалені параметри зберігання. Програми для мобільних телефонів для хмарного відеоспостереження зазвичай складаються з кількох компонентів, включаючи камеру, мобільний пристрій і хмарний сервер. Ці програми пропонують низку функцій, таких як прямі трансляції, виявлення руху та віддалений доступ, що дозволяє користувачам контролювати свої приміщення з будь-якого місця та в будь-який час.

Однією з головних переваг використання програм для мобільних телефонів для хмарного відеоспостереження є підвищена гнучкість і зручність, яку вони пропонують. Користувачі можуть отримати доступ до своїх відеоканалів з будь-

якого місця, де є підключення до Інтернету, що полегшує віддалений моніторинг своїх приміщень. Крім того, хмарні додатки для відеоспостереження можуть підвищити безпеку, надаючи сповіщення про будь-які підозрілі дії або несанкціонований доступ. Ще однією перевагою є зниження витрат порівняно з традиційними системами відеоспостереження, оскільки хмарні рішення усувають потребу у дорогому обладнанні та обслуговуванні.

Хоча мобільні телефонні програми для хмарного відеоспостереження пропонують багато переваг, вони також мають деякі проблеми та обмеження. Однією з головних проблем є залежність від підключення до Інтернету та надійності мережі, оскільки перебої в обслуговуванні можуть вплинути на якість і доступність відеоканалів. Крім того, існує занепокоєння щодо конфіденційності та безпеки даних, оскільки відеозаписи зберігаються на віддалених серверах, якими керують сторонні постачальники. Проблеми сумісності з різними мобільними пристроями та операційними системами також можуть становити проблему, оскільки деякі програми можуть не працювати на певних пристроях або платформах.

Отже, ось список додатків для мобільних телефонів для хмарного відеоспостереження [16, 17]:

1. Google Nest: Це додаток від Google, який працює з розумними камерами Nest і дозволяє користувачам віддалено спостерігати за своїм будинком чи офісом.

2. Camcloud: Сумісний з різними пристроями, цей додаток дозволяє користувачам переглядати відео в режимі реального часу, отримувати сповіщення про рух та зберігати записи в хмарі.

3. Ring: Додаток для смартфонів, який дозволяє користувачам віддалено керувати камерами Ring та переглядати відео в режимі реального часу.

4. Wansview Cloud: Цей додаток пропонує віддалене відеоспостереження для камер Wansview та забезпечує зберігання відео в хмарі.

5. Hik-Connect: Створений компанією Hikvision, цей додаток дозволяє користувачам віддалено керувати камерами Hikvision, переглядати відео в режимі реального часу та зберігати записи в хмарі.

6. Reolink: Додаток для смартфонів, який дозволяє користувачам віддалено керувати камерами Reolink та переглядати відео в режимі реального часу.

7. Foscam: Цей додаток дозволяє користувачам віддалено керувати камерами Foscam, переглядати відео в режимі реального часу та зберігати записи в хмарі.

8. Wyze: Додаток пропонує віддалене відеоспостереження для камер Wyze та забезпечує зберігання відео в хмарі.

Ці додатки допоможуть користувачам відстежувати та керувати своїми камерами відеоспостереження в режимі реального часу та зберігати записи в хмарі для безпечного та надійного зберігання. Вибір конкретного додатка залежить від потреб користувача та сумісності з використовуваним обладнанням. Використання хмарного відеоспостереження не тільки спрощує процес моніторингу та керування камерами, але також забезпечує додатковий рівень безпеки, оскільки дані зберігаються віддалено та можуть бути легко доступні в разі необхідності.

Hik-Connect - це мобільний додаток, розроблений компанією Hikvision, лідером у виробництві відеоспостереження та обладнання для безпеки. Додаток Hik-Connect дозволяє користувачам з легкістю керувати відеоспостереженням та іншим обладнанням Hikvision через смартфон або планшет.

Основні можливості Hik-Connect включають [17]:

1. Відеоспостереження в режимі реального часу: Додаток надає доступ до живого відео з камер спостереження та дозволяє перемикатись між різними камерами або місцями.

2. Зберігання відео в хмарі: Hik-Connect пропонує хмарне зберігання відео для збереження записів з камер спостереження. Користувачі можуть налаштувати розклад запису та вибрати тривалість зберігання відео. Завдяки хмарному зберіганню, користувачі можуть легко переглядати та завантажувати записи зі своїх пристроїв, незалежно від місця перебування.

3. Отримання сповіщень: Додаток Hik-Connect дозволяє користувачам отримувати сповіщення на своїх пристроях про рух або інші події, виявлені камерами спостереження.

4. Управління пристроями: Крім керування камерами спостереження, Hik-

Connect також дозволяє керувати іншим обладнанням Hikvision, таким як системи доступу, відеодомофони, автоматичні ворота та інше.

5. Поділитися доступом: Додаток Hik-Connect дозволяє користувачам надавати доступ до своїх камер спостереження іншим користувачам, що може бути корисним у сімейному або корпоративному середовищі.

6. Багатоплатформний доступ: Hik-Connect доступний для Android та iOS, що дозволяє користувачам використовувати додаток на різних пристроях, включаючи смартфони, планшети та інші мобільні пристрої. Це забезпечує гнучкість та зручність при керуванні відеоспостереженням і іншим обладнанням Hikvision [23].

У цілому, Hik-Connect є потужним інструментом для керування відеоспостереженням та іншим обладнанням Hikvision через мобільні пристрої. Завдяки хмарному зберіганню відео та широкому спектру функцій, додаток значно спрощує процес моніторингу та управління безпекою для користувачів.

Camcloud є хмарним сервісом відеоспостереження, який надає простий і доступний спосіб моніторингу та зберігання відео з IP-камер і веб-камер. Цей додаток дозволяє користувачам підключати свої камери до хмарного сервісу, отримувати сповіщення про рух та переглядати відео в режимі реального часу з будь-якого місця з доступом до інтернету. Ось деякі ключові можливості та функції Camcloud:

1. Легка налаштування: Camcloud підтримує широкий спектр IP-камер і веб-камер, що спрощує процес налаштування. Користувачам потрібно лише створити обліковий запис, підключити камеру і налаштувати параметри зберігання відео.

2. Зберігання відео в хмарі: Відео з камер зберігається в хмарі, що забезпечує безпечне зберігання даних та можливість доступу до них з будь-якого місця за допомогою інтернету. Користувачі можуть налаштувати параметри зберігання, такі як тривалість зберігання записів та якість відео.

3. Сповіщення про рух: Camcloud має вбудовану функцію виявлення руху, яка автоматично відправляє сповіщення користувачам, коли камера виявляє активність. Користувачі можуть налаштувати параметри виявлення руху, такі як чутливість та зони відстеження.

4. Перегляд відео в режимі реального часу: Користувачі можуть переглядати відео з камер в режимі реального часу з будь-якого пристрою з доступом до інтернету. Додаток Camcloud доступний для смартфонів, планшетів та комп'ютерів.

5. Мультикамерний моніторинг: Camcloud дозволяє користувачам підключати та керувати декількома камерами одночасно, що полегшує моніторинг різних місць та зон. Користувачі можуть створювати спеціальні групи камер для більш ефективного керування та перегляду відео.

6. Історія записів: Camcloud зберігає історію записів відео, що дозволяє користувачам легко знайти та переглянути потрібні події за конкретний період часу. Ця функція може бути корисною для аналізу подій або відстеження дій персоналу чи відвідувачів.

7. Багатоплатформний додаток: Camcloud доступний для різних платформ, таких як iOS, Android та веб-версія, що дозволяє користувачам стежити за відеоспостереженням з різних пристроїв та операційних систем.

8. Технічна підтримка та оновлення: Camcloud надає технічну підтримку своїм користувачам та регулярно оновлює свій додаток, щоб поліпшити функціональність та забезпечити найкращий досвід користувача.

Загалом, додаток Camcloud - це потужний інструмент для хмарного відеоспостереження, який надає користувачам широкий спектр можливостей для моніторингу та зберігання відео в режимі реального часу.

Підключення IP-камери до хмарного середовища Camcloud:

1. Додайте свою камеру до Camcloud за допомогою нашого Майстра додавання камери (рис. 3.3). У нашому випадку це передбачає реєстрацію безкоштовного облікового запису на www.camcloud.com. Звідси вам потрібно повідомити хмарній службі IP-адресу камери, а також облікові дані камери для входу. Спочатку увійдіть на сайт Camcloud.com і натисніть вкладку «камери» [18-21].

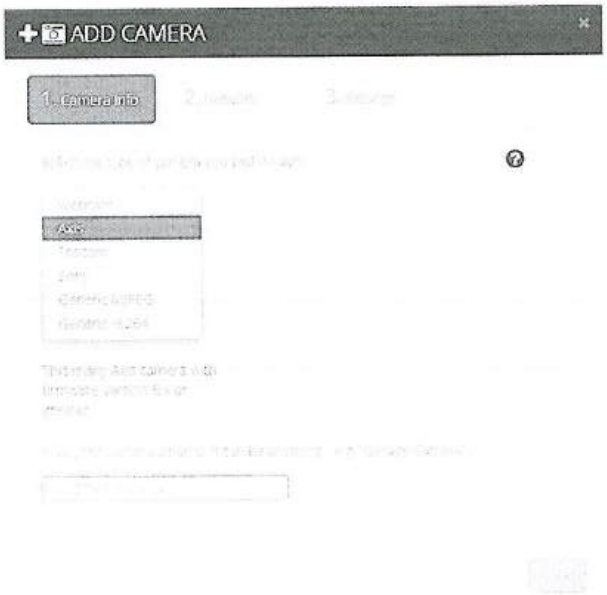


Рис. 3.3. Додавання камери

Натисніть «Додати камеру». Ви можете назвати камеру як завгодно. Коли ви натиснете «Далі», вам потрібно буде додати ім'я користувача, пароль, IP-адресу, порти HTTPS і RTSP камери. Вам потрібно перенаправити маршрутизатор на IP-камеру, щоб хмарна служба мала дозвіл на доступ до камери (рис. 3.4.). Це означає, що ваші порти RTSP і HTTPS повинні перенаправлятися на вашому маршрутизаторі (рис. 3.5).



Рис. 3.4. Налаштування



Рис. 3.5. Камера підключена

2. Налаштуйте функцію виявлення руху та повороту/нахилу.

Оскільки налаштування завершено, її буде додано до вашого списку камер. Перейдіть на вкладку Live view і перевірте, чи працює вона.

Ви можете подивитися на те, що відбувається прямо зараз, на вкладці «Live View». Ви також можете змінити положення камери за допомогою функції повороту/нахилу тут, якщо ваша камера це підтримує.



Рис. 3.6. Налаштування функції виявлення руху

Налаштуйте функцію виявлення руху камери, натиснувши кнопку виявлення руху. Щоб змінити зону виявлення руху камери, перемістіть червоне поле, збільште або зменште його розмір, а потім натисніть «Зберегти область».

3. Переконайтеся, що ваша сторінка часової шкали заповнюється.

Додатки для мобільних телефонів для хмарного відеоспостереження

пропонують низку переваг, включаючи підвищену гнучкість, покращений захист і безпеку, а також зниження витрат. Однак вони також мають певні проблеми та обмеження, такі як залежність від підключення до Інтернету, занепокоєння щодо конфіденційності та безпеки даних і проблеми сумісності. Оскільки технології продовжують розвиватися, цілком імовірно, що програми мобільного телефону для хмарного відеоспостереження стануть ще більш досконалими та поширеними, пропонуючи ще більше переваг і можливостей для користувачів.

ВИСНОВКИ

В роботі досліджено особливості застосування відеонагляду на основі хмарних технологій. Розглянуто базові елементи побудови та функціонування хмарних технологій, такі як IaaS, PaaS і SaaS, та розроблена детальна схема "Відеоспостереження як послуга (VSaaS)" яка базується на моделі сервісу "Програмне забезпечення як послуга (SaaS)".

На основі виконаних досліджень розроблена таблиця порівняння традиційних і хмарних систем відеоспостереження, яка вказує на явну перевагу VSaaS над традиційними системами майже у всіх випадках.

У другому розділі досліджено архітектуру розгортання хмарних системи відеоспостереження та розроблено таблицю яка допоможе визначити проблеми і варіантів проектування, пов'язаних із хмарною мультимедійною системою спостереження.

Досліджено види камер відеоспостереження за призначенням.

У третьому розділі досліджено особливості монтажу систем відеоспостереження та розглянуто сервіси доступу до хмарного середовища відеоспостереження та контролю. Проведено практичне підключення відеокамери Axis до хмарного сервісу Camcloud.

Застосування VSaaS має широкий спектр застосувань, від безпеки та спостереження в громадських місцях до моніторингу критичної інфраструктури. У громадських місцях, таких як аеропорти, вокзали та торгові центри, VSaaS може допомогти виявити та запобігти злочинній діяльності, стежити за поведінкою натовпу та забезпечити громадську безпеку. У критичній інфраструктурі, такій як електростанції та водоочисні споруди, VSaaS може допомогти виявити та запобігти несправності обладнання, контролювати умови навколишнього середовища та забезпечити дотримання правил безпеки. VSaaS також корисний у роздрібних і комерційних установах, де він може допомогти запобігти крадіжкам, контролювати поведінку співробітників і покращити обслуговування клієнтів. Наприклад, роздрібний магазин може використовувати VSaaS для моніторингу процесу

оформлення замовлення та переконатися, що працівники дотримуються належних процедур. Крім того, VSaaS може допомогти роздрібним торговцям проаналізувати поведінку клієнтів і вдосконалити свої маркетингові стратегії.

Вибираючи постачальника послуг VSaaS, слід враховувати кілька факторів, як-от моделі вартості та ціноутворення, якість відео та аудіо, параметри зберігання даних і заходи безпеки. Вартість VSaaS залежить від кількості камер і необхідної ємності зберігання. Деякі постачальники пропонують модель ціноутворення на основі передплати, тоді як інші стягують плату за камеру або за місяць. Якість відео та аудіо є ще одним важливим фактором, який слід враховувати. Користувачам слід шукати постачальника, який пропонує відео високої роздільної здатності та чіткий звук, щоб переконатися, що вони можуть захопити важливі деталі. Крім того, параметри зберігання даних і заходи безпеки мають вирішальне значення для забезпечення безпеки та конфіденційності записів відеоспостереження. Користувачам слід шукати постачальника, який пропонує безпечне зберігання даних і шифрування для захисту від несанкціонованого доступу.

Таким чином, VSaaS — це хмарне рішення для відеоспостереження, яке пропонує ряд переваг перед традиційними системами спостереження. Його широкий спектр застосувань і легка масштабованість роблять його популярним вибором для підприємств і організацій будь-якого розміру. Вибираючи постачальника VSaaS, користувачі повинні враховувати такі фактори, як вартість, якість відео та аудіо, а також варіанти зберігання даних і заходи безпеки, щоб гарантувати, що вони отримують найкраще можливе обслуговування.

ПЕРЕЛІК ПОСИЛАНЬ

1. Smith J. R., Anderson M. K. Cloud-based video surveillance: Benefits and challenges // International Journal of Security and Privacy. – 2017. – Vol. 3, No. 2. – P. 45-58.

2. Brown L. A., Harris P. D. The role of cloud computing in video surveillance systems: A comparative study // Journal of Information Technology and Telecommunication Systems. – 2018. – Vol. 10, No. 4. – P. 99-110.

3. Wilson N. G., Adams R. J. Implementing cloud-based video surveillance for smart cities: A case study // Journal of Urban Technology and Infrastructure. – 2019. – Vol. 5, No. 3. – P. 67-81.

4. Turner S. L., Thompson D. E. Evaluating security and privacy concerns in cloud-based video surveillance systems // Journal of Cloud Computing and Security. – 2020. – Vol. 8, No. 1. – P. 25-37.

5. Patel V. K., Gupta A. S. Integration of IoT and cloud computing for enhanced video surveillance in smart cities // Journal of Internet of Things and Smart Environments. – 2021. – Vol. 3, No. 1. – P. 12-24.

6. Хмарне відеоспостереження: переваги і недоліки [Електронний ресурс] / TechRadar. — Режим доступу: https://www.techradar.com/news/cloud-video-surveillance-pros-and-cons. (дата звернення 02.10.23)

7. Огляд сучасних хмарних систем відеоспостереження [Електронний ресурс] / CloudWedge. — Режим доступу: https://www.cloudwedge.com/security/best-cloud-video-surveillance-systems/. (дата звернення 02.10.23)

8. Інтеграція хмарного відеоспостереження з Інтернетом речей [Електронний ресурс] / IoT For All. — Режим доступу: https://www.iotforall.com/cloud-video-surveillance-iot-integration. (дата звернення 15.10.23)

9. Питання безпеки в хмарних системах відеоспостереження [Електронний ресурс] / Security Magazine. — Режим доступу: https://www.securitymagazine.com/articles/95825-security-considerations-for-cloud-video-surveillance. (дата звернення 22.10.23)

10. Хмарне відеоспостереження як сервіс: можливості та виклики [Електронний ресурс] / SourceSecurity. — Режим доступу: https://www.sourcesecurity.com/insights/video-surveillance-as-a-service-vsaaS-cloud-security-co-289-ga.19077.html. (дата звернення 04.11.23)

11. Hu W., Xu G. Cloud-based video surveillance: architecture, challenges, and solutions // Journal of Cloud Computing and Security. – 2016. – Vol. 4, No. 3. – P. 12-24.

12. Kim H., Park J. Performance analysis of cloud video surveillance systems using edge computing // International Journal of Network Management. – 2017. – Vol. 10, No. 1. – P. 45-59.

13. Liu X., Zhang Y. Integrating Internet of Things and cloud video surveillance for smart city applications // Journal of Information Technology and Urban Development. – 2018. – Vol. 5, No. 2. – P. 33-47.

14. Sharma P., Kumar A. Security considerations for cloud-based video surveillance systems // Journal of Cyber Security and Networking. – 2019. – Vol. 7, No. 3. – P. 81-95.

15. L. Cao, "A New Age of AI: Features and Futures", IEEE Intelligent Systems, vol. 37, no. 1, pp. 25-37, Jan.-Feb. 2022.

16. P M Grulich and F. Nawab, "Collaborative edge and cloud neural networks for real-time video processing[J]", Proceedings of the VLDB Endowment, vol. 11, no. 12, pp. 2046-2049, 2018.

17. Brown S., Smith T. Video Surveillance as a Service (VSaaS): opportunities and challenges in the era of cloud computing // Journal of Cloud Services and Applications. – 2020. – Vol. 8, No. 4. – P. 112-126.

18. Sui Xin, "New H3C 5G MEC smart video cloud empowers digital transformation of water conservancy industry", Communication World, vol. 803, no. 11, pp. 40-41, 2019.

19. Top 12 apps to turn old phone into security camera 2023. AirDroid | Delight Your Multi-Screen Life. URL: https://www.airdroid.com/remote-control/best-free-app-to-turn-old-phone-into-security-camera/ (дата звернення 21.11.23)

20. Hik-Connect для iPhone і Android. Nadzor.Ua. URL: https://nadzor.ua/product/hik-connect/ (дата звернення 21.11.23)

21. Lv Huazhang, Chen Dan and Wang Youxiang, "Focus on MEC edge cloud and empower 5G industry applications", Information and Communication Technology, vol. 12, no. 05, pp. 22-30, 2018.

22. A blog that covers the latest in IP cameras, home automation and video monitoring. | setup a cloud IP camera in 3 easy steps!. A Blog that Covers the Latest in IP Cameras, Home Automation and Video Monitoring. | IP Camera Reviews, Tutorials, and More. URL: https://blog.camcloud.com/setup-a-cloud-ip-camera-in-3-easy-steps/ (дата звернення 21.11.23)

23. Liu Qiuyan, Lv Huazhang, Li Mingxuan et al., "Edge-cloud collaboration strategy for 5G video services for user experience", Automation Expo, vol. 000, no. 004, pp. 48-51, 2020.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Презентація по магістерській роботі на тему:

“МЕТОДИ ОПТИМІЗАЦІЇ ВИКОРИСТАННЯ СИСТЕМ ВІДЕОНАГЛЯДУ НА ОСНОВІ ХМАРНИХ ТЕХНОЛОГІЙ”

Виконав: студент
Зосімов Ростислав Ігорович

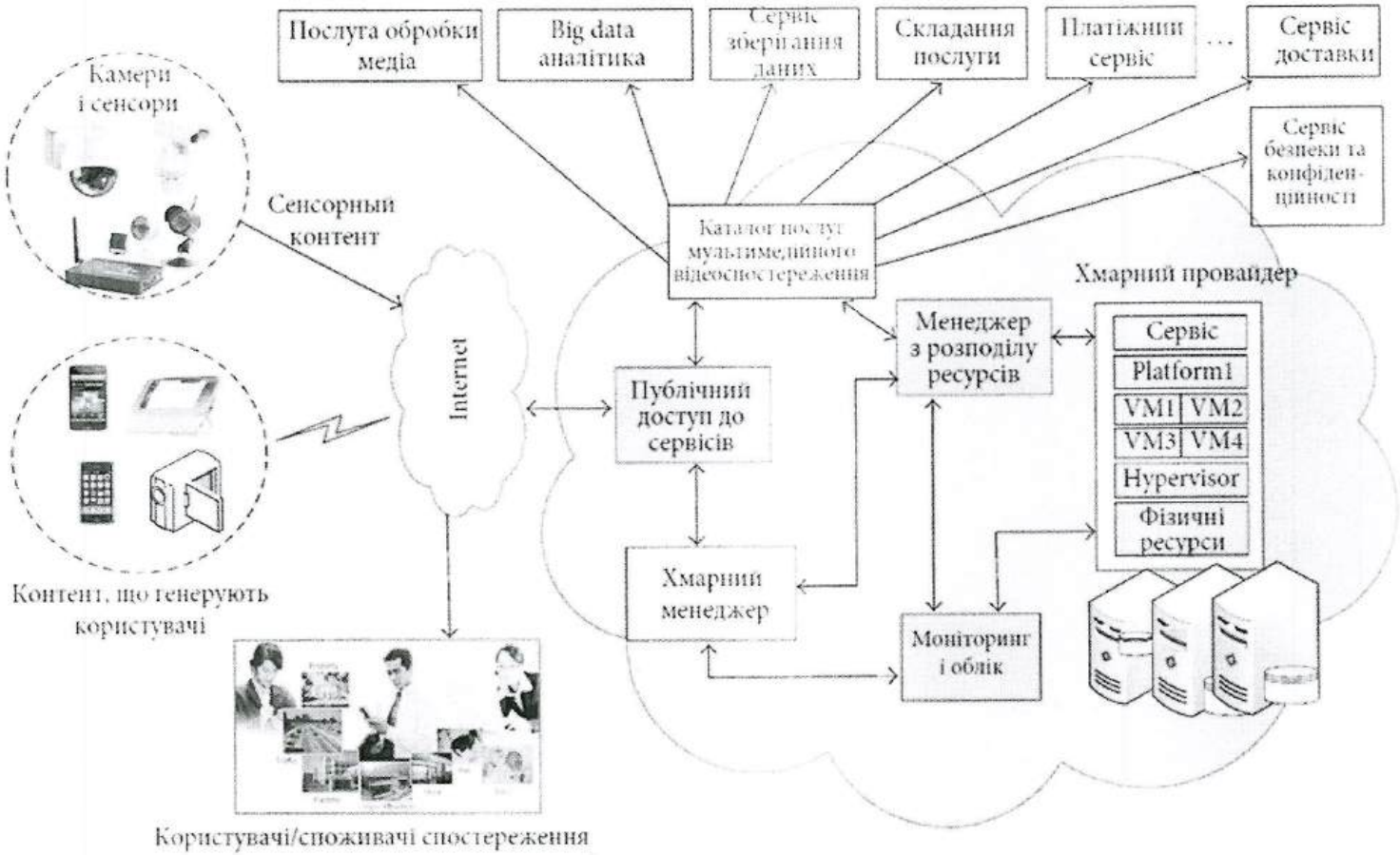
МЕТА РОБОТИ

- **Метою роботи** є дослідження систем відеонагляду на базі хмарних технологій.
- **Об'єктом дослідження** є процес відеоспостереження, передачі і обробки відеоданих на різних етапах моделі "Відеоспостереження як послуга VSaaS".
- **Предметом дослідження** є архітектура та методи побудови систем відеонагляду, які використовують хмарні технології для зберігання та обробки даних.

АКТУАЛЬНІСТЬ ДОСЛІДЖЕННЯ

- Системи відеоспостереження на основі хмарних технологій - це високотехнологічні рішення, що дозволяють збирати, зберігати та аналізувати великі обсяги відеоданих з використанням потужності хмарних сервісів. Такі системи стають все більш популярними через їх більшу ефективність, безпеку та зниження вартості в порівнянні з традиційними системами відеоспостереження.
- Однією з ключових переваг хмарних систем відеонагляду є масштабованість та гнучкість, яка дозволяє швидко адаптуватися до змінюваних вимог та створювати індивідуальні рішення для конкретних потреб. Крім того, хмарні технології забезпечують високий рівень захисту даних, адже інформація зберігається у захищеному віртуальному середовищі з регулярними резервними копіями.
- У світлі зростаючої кількості випадків, пов'язаних з безпекою, дослідження хмарних систем відеонагляду має велике значення для розвитку сучасних підходів до забезпечення безпеки, а також надання широкого спектру послуг та можливостей для різних відомств та користувачів.

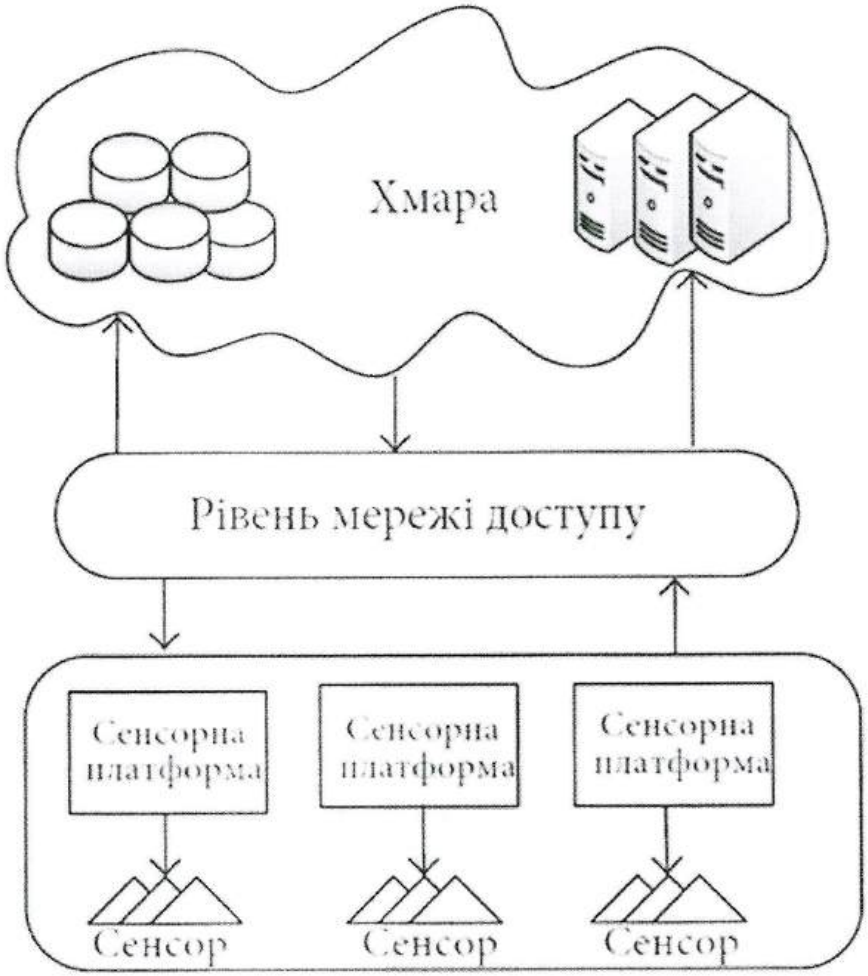
ВІДЕОСПОСТЕРЕЖЕННЯ ЯК ПОСЛУГА (VSaaS)



ПОРІВНЯННЯ ТРАДИЦІЙНИХ І ХМАРНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Традиційне підключення до Інтернету	Хмарна VSaaS
Установка системи	
- Забирає багато часу. - Складна конфігурація.	- Швидке розгортання за вимогою - Автоматична конфігурація Plug-and-play.
Системна підтримка	
- Інтенсивний процес обслуговування вручну.	- Підтримка здійснюється за межами розміщення обладнання провайдером.
Структура оплати	
- Високі авансові капітальні витрати. - Непередбачувані витрати на підтримку. - Дороге масштабування.	- Надзвичайно низькі початкові капітальні витрати. - Передбачувані щомісячні експлуатаційні витрати. - Дешева масштабованість.
Загальна вартість володіння	
- Висока початкова вартість, включаючи високу вартість обладнання програмного забезпечення та встановлення. - Багато поточних витрат.	- Низька початкова вартість низька, як правило, недорогий мостовий пристрій. - Низька поточна місячна вартість підписки.
Гнучкість зберігання	
- Традиційний DVR, NVR або VMS, зберігайте відео на місці. - Зберігання обмежено. - Дорожче розширення сховища.	- Гнучке поєднання локального та або хмарного сховища. - Миттєво збільшити термін зберігання - Низька вартість розширення сховища.
Додавання керуючих камер	
- Підтримка широкого спектру аналогових IP-камер. - Ручне підключення конфігурації нових камер.	- Підтримка широкого спектру аналогових IP-камер. - Ручне підключення автоконфігурації нових камер.
Управління пропускною здатністю	
- Для дистанційного перегляду потрібна пропускна здатність. - Для зберігання відеозапису на місці не потрібна пропускна здатність.	- Для дистанційного перегляду потрібна пропускна здатність. - Більшість сховища є потоковим, що вимагає високої пропускної здатності.
Довговічність технології, API	
- Коротший час до морального старіння технології. - Обмежена можливість оновлювати технології. - Оновлення потребують інтенсивної підтримки вручну. - API закриті та зазвичай вимагають підписання NDA. Функціональність API обмежена.	- Швидкий розвиток технології. - Автоматичне оновлення технології для локального пристрою. - Постійно розвивається для нових інновацій, має довголіття. - Відкриті API для аналітики, інтеграційних програм. Можна використовувати в інших системах.
Кібербезпека	
- Вищі шанси на вразливість кібербезпеки. - Конфігурація відкритих портів, локальних брандмауерів, локального програмного забезпечення та брандмауера. - Кінцевий користувач стежить за вразливістю атак.	- Надзвичайно низька ймовірність уразливості кібербезпеки. - Ні відкритих портів, ні локальних брандмауерів, ні локального програмного забезпечення, ні встановлення брандмауера. - Спеціалізовані групи кібербезпеки для моніторингу нових вразливостей.
Віддалений доступ	
- Нерідний віддалений доступ до відео, додається лише за запитом. - Непередбачувана, переривчаста якість відео з низькою роздільною здатністю. - Існування рідкісного шифрування. - Несумісність браузера є звичайним явищем.	Хмарні системи були розроблені для віддаленого доступу. - Плавний доступ до потокового відео високої роздільної здатності. - Вбудоване розширене шифрування - Підтримка універсальних веб-браузерів і мобільних додатків.
Надійність резервування	
- Сильно змінні рівні резервування. - Звільнення, кероване внутрішнім IT- персоналом. - Сервери клонування часто простоюють, що збільшує накладні витрати.	- Хмарні центри обробки даних мають подвійне та потрійне резервування. - Спільна інфраструктура забезпечує повне використання сервера та економію за рахунок масштабу. - Кілька днів локального сховища як резервного копіювання для захисту від збою Інтернету разом із миттєвими сповіщеннями.

АРХІТЕКТУРА РОЗГОРТАННЯ ХМАРНИХ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ



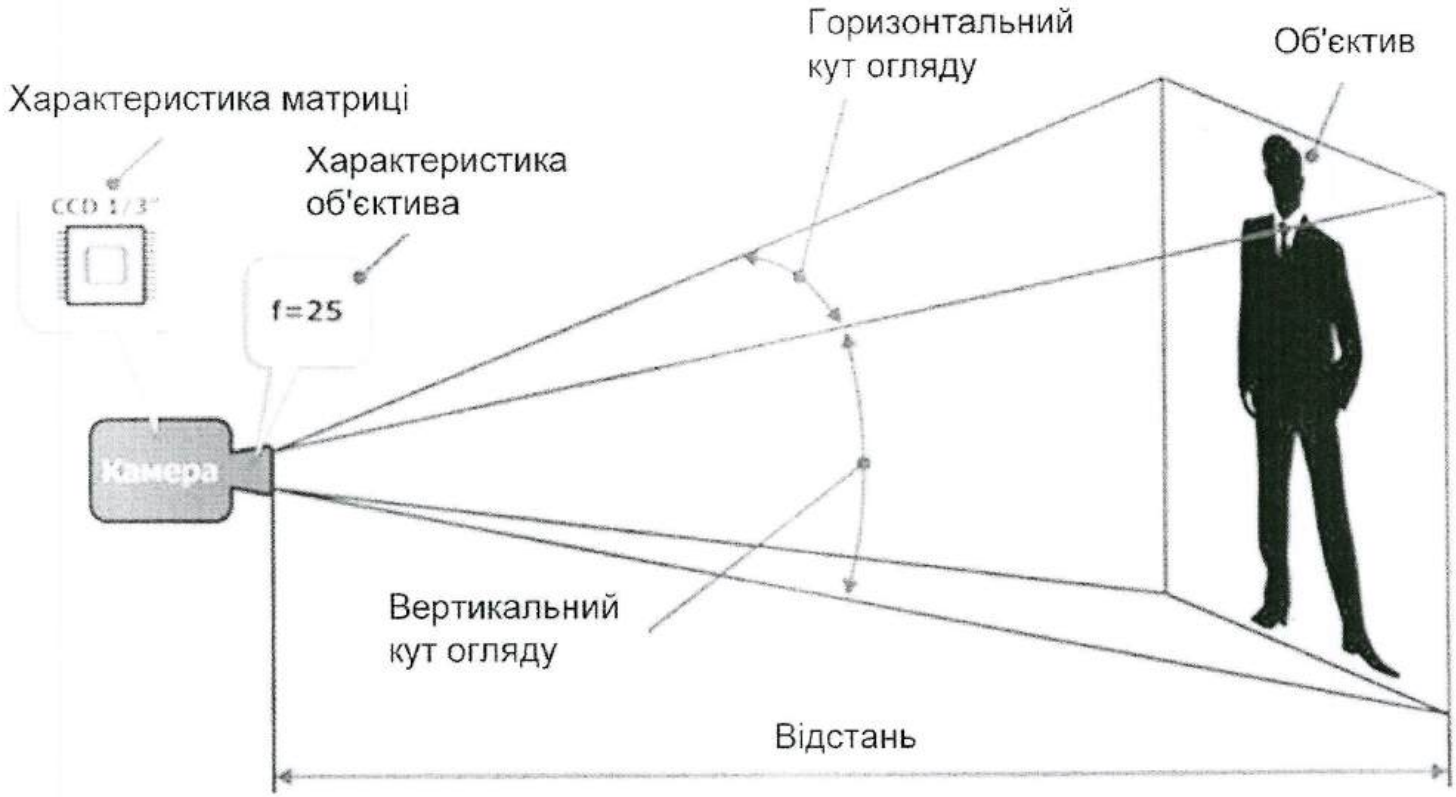
ОПИС ПРОБЛЕМ І ВАРІАНТІВ ПРОЕКТУВАННЯ, ПОВ'ЯЗАНИХ ІЗ ХМАРНОЮ МУЛЬТИМЕДІЙНОЮ СИСТЕМОЮ СПОСТЕРЕЖЕННЯ

Відмінні питання	Вибір проектування
Архітектура розгортання	Громадські, приватні та гібридні
Хмарне сховище	Блокування постачальника, аварійне відновлення, еластичність, безпека та конфіденційність, а також оплата та ціноутворення
Обробка медіа	Різні завдання обробки мультимедійних даних, різнорідність QoS, мережі та пристроїв, а також міркування щодо мобільної хмари
Розподіл ресурсів	Інша ціль оптимізації (максимальне використання ресурсів проти мінімізації часу відгуку та вартості, компроміс між середнім часом очікування обслуговування та довгостроковою вартістю обслуговування, максимальний прибуток проти мінімізації збитків і рівномірний розподіл навантаження)
Сповіщення та обмін	Механізми публікації-підписки (на основі теми, на основі контенту, на основі типу, параметризовані), режим розповсюдження інформації, алгоритми зіставлення подій та обсяг інформації
Спостереження на основі натовпу та аналітика великих даних	Корисність великих даних, точність інформації, своєчасність реагування, безпека та конфіденційність даних
Безпека та конфіденційність	Криптографічний підхід, різні підходи до автентифікації та керування ідентифікацією, різні політики контролю доступу і вплив безпеки на вибір хмарного розгортання
Проблеми з продуктивністю	Кілька показників продуктивності (точність виявлення подій, час відгуку, використання ЦП і сховища, робоче навантаження, компроміс вартості, середній час очікування завдання)

ВИДИ КАМЕР ВІДЕОСПОСТЕРЕЖЕННЯ ЗА ПРИЗНАЧЕННЯМ



ОСОБЛИВОСТІ МОНТАЖУ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ



СЕРВІСИ ДОСТУПУ ДО ХМАРНОГО СЕРЕДОВИЩА ВІДЕОСПОСТЕРЕЖЕННЯ ТА КОНТРОЛЮ

Amazon Web Services	Google Cloud
Microsoft Azure	Hikvision
Dahua Technology	Camcloud

ПІДКЛЮЧЕННЯ ВІДЕОКАМЕРИ AXIS ДО ХМАРНОГО СЕРВІСУ CAMCLOUD



ВИСНОВКИ

В першому розділі досліджено особливості застосування відеонагляду на основі хмарних технологій. Розглянуто базові елементи побудови та функціонування хмарних технологій, такі як IaaS, PaaS і SaaS, та розроблена детальна схема "Відеоспостереження як послуга (VSaaS)" яка базується на моделі сервісу "Програмне забезпечення як послуга (SaaS)".

На основі виконаних досліджень розроблена таблиця порівняння традиційних і хмарних систем відеоспостереження, яка вказує на явну перевагу VSaaS над традиційними системами майже у всіх випадках.

У другому розділі досліджено архітектуру розгортання хмарних системи відеоспостереження та розроблено таблицю яка допоможе визначити проблеми і варіантів проектування, пов'язаних із хмарною мультимедійною системою спостереження.

Досліджено види камер відеоспостереження за призначенням.

У третьому розділі досліджено особливості монтажу систем відеоспостереження та розглянуто сервіси доступу до хмарного середовища відеоспостереження та контролю. Проведено практичне підключення відеокамери Axis до хмарного сервісу Camcloud.

АПРОБАЦІЯ РЕЗУЛЬТАТІВ МАГІСТЕРСЬКОЇ РОБОТИ

Основні результати магістерської роботи доповідалися на Всеукраїнській науково-практичній конференції «Telecommunication: problems and innovation», Київ: ДУІКТ, 20 грудня 2023 р.

Основні наукові результати магістерської роботи опубліковано в науковому журналі "Наукові записки ДУІКТ, – 2023, – №2".

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Ростислав ЗОСІМОВ

Назва: Методи оптимізації використання систем відеонагляду на основі хмарних технологій

Координатор: Віталій СТРЕЛЬНІКОВ

Підрозділ: ННІТ

Коефіцієнт подібності 1 :12.0

Коефіцієнт подібності 2 :7.6

Тривога: 5

Після аналізу Звіту подібності констатую наступне:

☑ виявлені в роботі запозичення є сумлінними і не мають ознак плагіату. Тому робота визнається самостійною і допускається до захисту;

☐ виявлені в роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і самостійності її автора. Роботу направити на доопрацювання;

☐ виявлені в роботі запозичення є недобросовісними і мають ознаки плагіату або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. У зв'язку з чим, робота не допускається до захисту.

....

Дата *Підпис Наукового керівника*