ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 10
ВСТУП 14
1 ТЕХНІЧНІ ЗАСАДИ ПОБУДОВИ ОХОРОННИХ ПРИСТРОЇВ ВІДЕОСПОСТЕРЕЖЕННЯ 16
1.1 Структура апаратно-програмних платформ охоронних відеосистем 16
1.2 Класифікація охоронних пристроїв відеоспостереження та їх функціональна специфіка 22
1.3 Методики формування, обробки та передавання відеосигналів у охоронних комплексах 30
1.4 Технічні параметри забезпечення якості, надійності та стійкості відеосигналів 38
2 ХМАРНІ ТЕХНОЛОГІЇ В СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ ІНФРАСТРУКТУРАХ 44
2.1 Архітектурні моделі та принципи надання хмарних сервісів 44
2.2 Технологічні механізми обчислення та зберігання даних у хмарному середовищі 50
2.3 Інструменти захисту, оптимізації та передавання відеоданих у хмарних системах 57
3 ДОСЛІДЖЕННЯ СИСТЕМ ФОРМУВАННЯ ВІДЕОСИГНАЛІВ У ХМАРНО-ОРІЄНТОВАНИХ ОХОРОННИХ ПРИСТРОЯХ 65
3.1 Аналітична оцінка підходів до формування відеосигналів у хмарних охоронних рішеннях 65
3.2 Розроблення методики дослідження процесів формування відеосигналів у хмарно-орієнтованих системах 71
3.3 Експериментальна перевірка якості та ефективності формування відеосигналів у хмарно-орієнтованих системах 77

ВИСНОВКИ 85
ПЕРЕЛІК ПОСИЛАНЬ 86
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 90

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

5G	Fifth Generation — П’яте покоління мобільного зв’язку
ABR	Adaptive Bitrate — Адаптивний бітрейт
AES	Advanced Encryption Standard — Удосконалений стандарт шифрування
AI (ШІ)	Artificial Intelligence — Штучний інтелект
API	Application Programming Interface — Програмний інтерфейс прикладного програмування
AV1	AOMedia Video 1 — Відкритий стандарт стиснення відео першого покоління
AWS	Amazon Web Services — Хмарні веб-сервіси від Amazon
BER	Bit Error Rate — Коефіцієнт бітових помилок
CCD (ПЗЗ)	Charge-Coupled Device — Пристрій із зарядовим зв’язком
CCTV	Closed-Circuit Television — Системи телебачення замкнутого контуру (відеоспостереження)
CDN	Content Delivery Network — Мережа доставки контенту
CMOS (КМОН)	Complementary Metal-Oxide-Semiconductor — Комплементарний метал-оксид-напівпровідник
CPU (ЦП)	Central Processing Unit — Центральний процесор
CRM	Customer Relationship Management — Управління взаємовідносинами з клієнтами
DASH	Dynamic Adaptive Streaming over HTTP — Динамічне адаптивне потокове передавання через HTTP
DSP	Digital Signal Processing — Цифрова обробка сигналів
DVR	Digital Video Recorder — Цифровий відеореєстратор
EBS	Elastic Block Store — Еластичне блочне сховище

EMI	Electromagnetic Interference — Електромагнітні перешкоди
ERP	Enterprise Resource Planning — Планування ресурсів підприємства
EVM	Error Vector Magnitude — Величина вектора помилки
FaaS	Function as a Service — Функція як послуга
FTP	File Transfer Protocol — Протокол передачі файлів
GDPR	General Data Protection Regulation — Загальний регламент захисту даних
GPU (ГП)	Graphics Processing Unit — Графічний процесор
H.264	Advanced Video Coding (AVC) — Стандарт стиснення відео високої чіткості
H.265 (HEVC)	High Efficiency Video Coding — Високоефективне кодування відео
HDFS	Hadoop Distributed File System — Розподілена файлова система Hadoop
HDMI	High-Definition Multimedia Interface — Мультимедійний інтерфейс високої чіткості
HDR	High Dynamic Range — Високий динамічний діапазон
HIPAA	Health Insurance Portability and Accountability Act — Закон про мобільність і підзвітність медичного страхування
HLS	HTTP Live Streaming — Протокол потокової передачі на основі HTTP
HTTP	Hypertext Transfer Protocol — Протокол передачі гіпертексту
IaaS	Infrastructure as a Service — Інфраструктура як послуга
IAM	Identity and Access Management — Управління ідентифікацією та доступом
IDS	Intrusion Detection System — Система виявлення вторгнень
IP	Internet Protocol — Інтернет-протокол

ISO	International Organization for Standardization — Міжнародна організація зі стандартизації
ITU	International Telecommunication Union — Міжнародний союз електрозв’язку
KVM	Kernel-based Virtual Machine — Віртуальна машина на базі ядра
MFA	Multi-Factor Authentication — Багатофакторна автентифікація
ML (МН)	Machine Learning — Машинне навчання
NAS	Network Attached Storage — Мережеве сховище даних
NVR	Network Video Recorder — Мережевий відеореєстратор
ONVIF	Open Network Video Interface Forum — Форум відкритих мережевих відеоінтерфейсів
PaaS	Platform as a Service — Платформа як послуга
PoE	Power over Ethernet — Живлення через мережу Ethernet
PSNR	Peak Signal-to-Noise Ratio — Пікове співвідношення сигналу до шуму
PTZ	Pan-Tilt-Zoom — Поворот, нахил та масштабування
RBAC	Role-Based Access Control — Керування доступом на основі ролей
RTMP	Real-Time Messaging Protocol — Протокол обміну повідомленнями в реальному часі
RTSP	Real Time Streaming Protocol — Потоковий протокол реального часу
S3	Simple Storage Service — Хмарний сервіс об’єктного зберігання даних
SaaS	Software as a Service — Програмне забезпечення як послуга
SD	Secure Digital — Формат карт пам’яті для портативних пристроїв
SDI	Serial Digital Interface — Послідовний цифровий інтерфейс

SDK	Software Development Kit — Набір засобів розробки програмного забезпечення
SMPTE	Society of Motion Picture and Television Engineers — Товариство інженерів кіно і телебачення
SNR	Signal-to-Noise Ratio — Співвідношення сигнал/шум
SSIM	Structural Similarity Index Measure — Індекс структурної подібності
TLS	Transport Layer Security — Протокол захисту транспортного рівня
VM (ВМ)	Virtual Machine — Віртуальна машина
VMS	Video Management System — Система управління відео
VP9	Video Processor 9 — Відкритий і безкоштовний формат стиснення відео

ВСТУП

Актуальність теми. Системи відеоспостереження стали невід'ємною частиною сучасної інфраструктури безпеки, забезпечуючи моніторинг у реальному часі та збір доказів у комерційних і громадських сферах. Еволюція технологій зумовила перехід від традиційних аналогових методів до складних цифрових мереж, де відеоконтент є домінуючою формою комунікації.

Зі зростанням обсягів даних використання хмарних систем для зберігання та обробки сигналів стало критично важливим для забезпечення масштабованості та економічної ефективності. Однак впровадження хмарно-орієнтованих рішень створює виклики, пов'язані із затримками передачі, конфіденційністю даних та стабільністю відеопотоку в умовах нестабільної пропускної здатності мережі. Дослідження систем формування відеосигналів у хмарному середовищі є актуальним завданням, оскільки воно дозволяє оптимізувати ресурси інфраструктури та гарантувати надійність захисту об'єктів у динамічних операційних умовах.

Мета роботи — дослідження процесів формування відеосигналів у хмарно-орієнтованих пристроях, розроблення методики їх аналізу та експериментальна перевірка ефективності алгоритмів стиснення і передавання для підвищення надійності систем безпеки.

Об'єкт дослідження — процеси формування, обробки та передавання відеосигналів у хмарно-орієнтованих системах відеоспостереження.

Предмет дослідження — методики, технічні параметри та технологічні інструменти забезпечення якості, надійності та стійкості відеосигналів у хмарних інфраструктурах.

Завдання роботи:

- Вивчити структуру апаратно-програмних платформ та класифікувати пристрої відеоспостереження за функціональною специфікою.
- Проаналізувати архітектурні моделі (IaaS, PaaS, SaaS) та механізми обчислення й зберігання даних у хмарі.

- Дослідити інструменти захисту (шифрування AES/TLS) та методи оптимізації (H.265/HEVC, CDN) відеоданих.
- Здійснити аналітичну оцінку підходів до генерації сигналів, включаючи традиційні методи та моделі на основі штучного інтелекту.
- Розробити методику дослідження процесів формування відеосигналів, що охоплює етапи дискретизації, кодування та передавання.
- Провести експериментальну перевірку якості сигналів за показниками PSNR та SSIM і оцінити стійкість хмарно-орієнтованих систем до мережевих перевантажень.

Методи дослідження. У роботі використано системний аналіз для вивчення архітектур хмарних сервісів, методи цифрової обробки сигналів для дослідження кодеків стиснення, а також експериментальні методи моделювання для оцінки стійкості відеопотоку (механізм ABR) до коливань пропускної здатності.

Наукова новизна отриманих результатів полягає у вдосконаленні методики дослідження формування відеосигналів шляхом інтеграції адаптивного кодування та периферійних обчислень (Edge Computing), що дозволяє мінімізувати затримку та зберегти безперервність моніторингу при критичному зниженні швидкості мережі.

Практичне значення. Розроблені рекомендації та методика дозволяють проектувати гібридні системи безпеки, які поєднують локальну надійність з аналітичними можливостями хмари, забезпечуючи при цьому економне використання ресурсів зберігання та високу швидкість реагування на інциденти.

1 ТЕХНІЧНІ ЗАСАДИ ПОБУДОВИ ОХОРОННИХ ПРИСТРОЇВ ВІДЕОСПОСТЕРЕЖЕННЯ

1.1 Структура апаратно-програмних платформ охоронних відеосистем

Системи відеоспостереження стали невід'ємною частиною сучасної інфраструктури безпеки, забезпечуючи спостереження в режимі реального часу, виявлення загроз та збір доказів у численних місцях, таких як комерційні підприємства, громадські місця та житлові райони. Ефективність цих систем залежить від складної взаємодії між апаратними компонентами та програмними платформами, які разом забезпечують комплексний моніторинг та управління. Розуміння структури цих платформ, що включають спеціалізовані апаратні пристрої та передові програмні рішення, є важливим для проектування, розгортання та обслуговування ефективних систем безпеки. У розділі досліджуються основні елементи апаратних компонентів, структури управління програмним забезпеченням та критична інтеграція, яка забезпечує безперебійну роботу, надійність та швидкість реагування систем відеоспостереження [1].

Апаратні компоненти систем відеоспостереження утворюють базовий рівень, який захоплює, обробляє та передає візуальні дані. Центральним елементом цієї апаратної архітектури є камери та датчики, які відповідають за захоплення зображень та відео високої роздільної здатності в різних середовищах. Вони варіюються від стаціонарних камер відеоспостереження, придатних для статичних зон, до камер з поворотом, нахилом та масштабуванням (PTZ), які забезпечують динамічне покриття, часто оснащені інфрачервоними або тепловими датчиками для умов низької освітленості або нічного часу. Наприклад, у великих комерційних комплексах кілька камер стратегічно розміщені для покриття кожної точки входу та чутливої зони, забезпечуючи комплексне спостереження. Доповнюють їх пристрої запису, такі як мережеві відеореєстратори (NVR) та цифрові відеореєстратори (DVR), які зберігають захоплені кадри локально або на виділених серверах. NVR, зокрема, розроблені для безпосередньої інтеграції з IP-камерами через мережеву

інфраструктуру, що забезпечує масштабовані можливості запису високої чіткості. Крім того, мережева інфраструктура, включаючи комутатори та маршрутизатори, служить основою, що забезпечує безперебійну передачу даних від камер до систем зберігання та управління. Наприклад, комутатори корпоративного класу, оснащені живленням через Ethernet (PoE), не лише спрощують кабельне підключення, але й забезпечують безперервне живлення камер, тим самим підвищуючи надійність системи. Надійність та потужність цих апаратних компонентів визначають загальну продуктивність системи безпеки, впливаючи на такі фактори, як якість відео, затримка та масштабованість системи.

Сучасні системи відеоспостереження є складними комплексами, ефективність яких безпосередньо залежить від взаємодії між апаратними компонентами та програмними платформами. Розуміння структури цих платформ, що включають спеціалізоване обладнання та передові програмні рішення, є критично важливим для проектування надійних систем безпеки. Типова архітектура такої платформи, адаптована під сучасні вимоги хмарної інтеграції, наведена на рисунку 1.1.

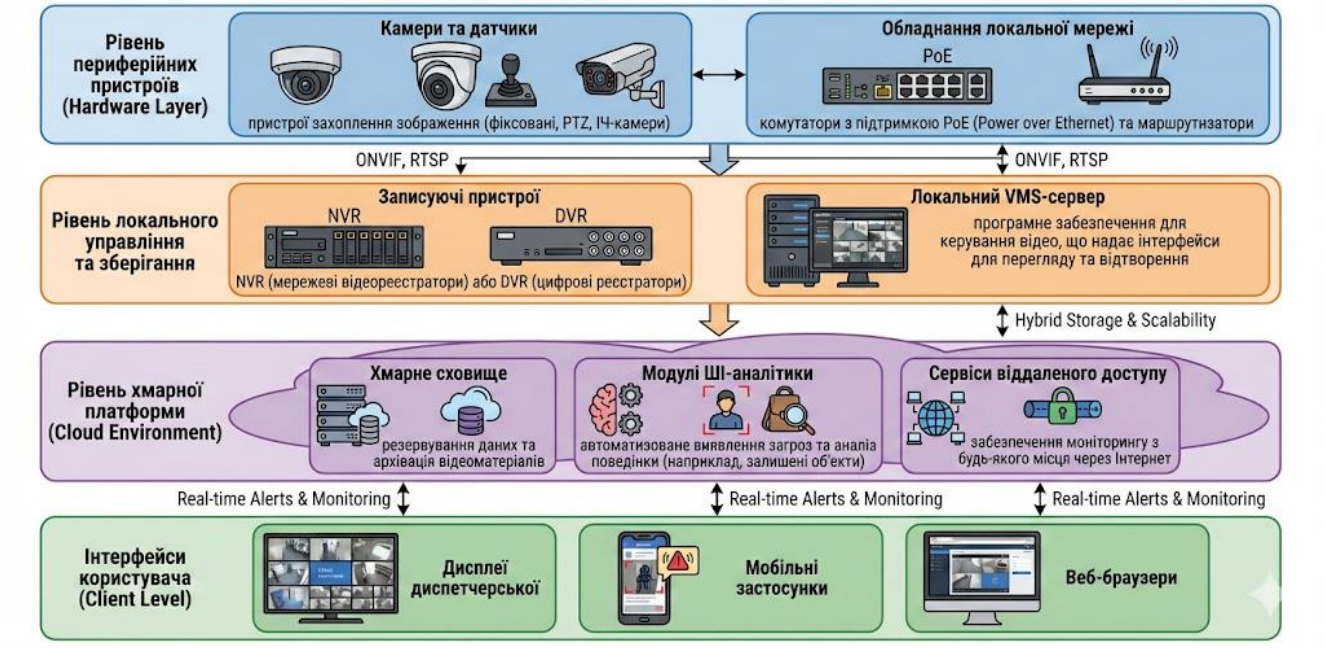


Рис. 1.1 Типова архітектура апаратно-програмної платформи системи відеоспостереження

Апаратний рівень системи утворює базу для захоплення, обробки та передачі візуальних даних. Основними елементами тут є [2]:

Камери та датчики: відповідають за отримання зображень високої роздільної здатності. Вони можуть бути як стаціонарними (для статичних зон), так і керованими (PTZ), оснащеними інфрачервоними датчиками для роботи в темряві.

Пристрої запису: мережеві (NVR) або цифрові (DVR) відеореєстратори, що забезпечують локальне зберігання кадрів. NVR розроблені для безпосередньої інтеграції з IP-камерами через мережеву інфраструктуру.

Мережева інфраструктура: комутатори (зокрема з підтримкою PoE для живлення камер) та маршрутизатори, що служать основою для передачі даних від камер до систем управління.

Програмний рівень відіграє вирішальну роль у керуванні та аналізі величезних обсягів даних. Його ядром є програмне забезпечення для керування відео (VMS), яке надає інтерфейси для перегляду в реальному часі, відтворення записів та налаштування всієї системи.

Особливе місце в сучасних архітектурах посідають хмарні платформи управління. Вони стають дедалі популярнішими завдяки своїй масштабованості та можливості віддаленого доступу до потоків даних з будь-якого місця. Інтеграція хмарних рішень дозволяє реалізувати:

Гібридне зберігання: комбінація локальних накопичувачів та хмарних серверів забезпечує резервування даних на випадок виходу з ладу локальних пристроїв.

Інтелектуальну аналітику: використання штучного інтелекту для автоматичного виявлення підозрілої поведінки або залишених об'єктів.

Безперебійна робота такої інтегрованої структури забезпечується використанням стандартизованих протоколів, таких як ONVIF та RTSP, що гарантують сумісність пристроїв від різних виробників. Таким чином, синергія апаратних засобів та хмарно-орієнтованого програмного забезпечення формує адаптивну та стійку систему безпеки.

Програмні платформи життєво важливі для керування, аналізу та інтерпретації величезного обсягу даних, що генеруються апаратними пристроями. В основі лежить програмне забезпечення для керування відео (VMS), яке надає інтерфейси користувача для перегляду, запису та відтворення в реальному часі, а також інструменти налаштування для розгортання камер та керування сховищем. Розширені рішення VMS часто включають керування кількома об'єктами, контроль доступу користувачів та інтеграцію з іншими системами безпеки, такими як сигналізація та контроль доступу. Окрім локального програмного забезпечення, хмарні платформи управління здобули популярність завдяки своїй масштабованості та віддаленому доступу. Ці хмарні рішення дозволяють співробітникам служби безпеки контролювати потоки з будь-якого місця з підключенням до Інтернету, що сприяє швидкому реагуванню та централізованому керуванню в кількох місцях. Крім того, інтеграція аналітики та інтелектуального програмного забезпечення для виявлення зробила революцію в системі відеоспостереження, автоматизуючи виявлення загроз та зменшуючи кількість хибних тривог. Наприклад, аналітика на основі штучного інтелекту може виявляти підозрілу поведінку, таку як байдикування або залишення об'єктів, і запускати автоматичні сповіщення для персоналу служби безпеки. Ці інтелектуальні програмні модулі не лише покращують ситуаційну обізнаність, але й дозволяють проводити прогнозне обслуговування та оптимізацію системи, тим самим підвищуючи загальну ефективність безпеки.

Безперешкодна інтеграція апаратних та програмних компонентів має вирішальне значення для досягнення цілісної та ефективної системи відеоспостереження. Ефективна комунікація спирається на стандартизовані протоколи, такі як ONVIF (Open Network Video Interface Forum) та RTSP (Real Time Streaming Protocol), які забезпечують сумісність між пристроями різних виробників. Ця сумісність дозволяє гнучко розширювати та оновлювати систему без прив'язки до постачальника, тим самим захищаючи інвестиції. Зберігання та пошук даних також є ключовими; сучасні системи використовують комбінацію локального сховища на NVR/DVR та хмарних рішень для забезпечення

резервування, масштабованості та швидкого доступу до відеоматеріалів. Наприклад, гібридні системи використовують як локальне, так і хмарне сховище, щоб гарантувати збереження даних навіть у разі компрометації локальних пристроїв. Моніторинг та сповіщення в режимі реального часу забезпечуються програмним забезпеченням, яке постійно аналізує прямі трансляції та запускає сповіщення про заздалегідь визначені події, такі як несанкціонований доступ або несправності обладнання. Можливість отримувати миттєві сповіщення на смартфони або дисплеї диспетчерської дозволяє командам безпеки швидко реагувати, часто запобігаючи інцидентам до їх ескалації. Загалом, інтеграція апаратних та програмних компонентів гарантує, що системи відеоспостереження не лише ефективні у спостереженні, але й адаптивні та стійкі в динамічних операційних середовищах.

Оскільки системи відеоспостереження стають дедалі важливішими для захисту активів та персоналу, забезпечення їхньої мережевої безпеки має першочергове значення. Заходи кібербезпеки, такі як протоколи шифрування, такі як AES (Advanced Encryption Standard), використовуються для захисту даних під час передачі та зберігання, запобігаючи несанкціонованому перехопленню або доступу до конфіденційних відеоматеріалів. Механізми автентифікації, включаючи багатофакторну автентифікацію та цифрові сертифікати, перевіряють особу користувачів та пристроїв, тим самим обмежуючи доступ лише авторизованим персоналом. Брандмауери та системи виявлення вторгнень (IDS) служать критично важливим захистом від кіберзагроз, моніторячи мережевий трафік. блокування шкідливої діяльності та сповіщення адміністраторів про потенційні порушення. Наприклад, добре налаштований брандмауер може запобігти проникненню зовнішніх хакерів у систему, тоді як IDS може виявляти незвичайні закономірності, що свідчать про кібератак. Крім того, регулярні оновлення програмного забезпечення та виправлення є важливими для усунення нових вразливостей; виробники часто випускають виправлення безпеки, які виправляють помилки та закривають лазівки, що використовуються кіберзлочинцями. Підтримка системи в актуальному стані не тільки захищає від відомих загроз, але й підвищує загальну

стабільність системи. З розвитком технологій спостереження інтеграція надійних протоколів кібербезпеки гарантує безпечну роботу апаратних та програмних компонентів, захищаючи як цілісність відеозапису, так і конфіденційність осіб, за якими ведеться спостереження [3].

Заглядаючи в майбутнє, майбутнє апаратних та програмних платформ у системах відеоспостереження готове до трансформаційних досягнень, зумовлених новими технологіями. Штучний інтелект (ШІ) та машинне навчання (МН) все частіше вбудовуються в системи спостереження, щоб забезпечити інтелектуальний аналіз, такий як розпізнавання облич, прогнозування поведінки та виявлення аномалій, що значно покращує ідентифікацію загроз та час реагування. Ці можливості дозволяють системам автономно розрізняти рутинну діяльність та потенційні порушення безпеки, зменшуючи кількість хибних тривог та підвищуючи операційну ефективність. Периферійні обчислення представляють собою ще одну важливу тенденцію, коли обчислювальна потужність децентралізована та вбудована безпосередньо в камери або локальні пристрої, що дозволяє аналізувати дані в режимі реального часу біля джерела. Це зменшує затримку, мінімізує споживання пропускної здатності та підвищує конфіденційність, обмежуючи обсяг даних, що передаються мережами. Крім того, очікується, що майбутні інтерфейси користувача стануть більш інтуїтивно зрозумілими, з розширеними панелями інструментів та можливостями віддаленого доступу, які дозволять співробітникам служби безпеки безперешкодно контролювати та керувати системами з будь-якого пристрою, в будь-якій точці світу. Вдосконалені інструменти візуалізації, такі як накладання доповненої реальності та інтерактивні карти, ще більше покращать ситуаційну обізнаність. Ці технологічні тенденції обіцяють зробити системи безпеки більш автономними, чуйними та зручними для користувача, що зрештою підвищить стандарти безпеки в різноманітних середовищах.

На завершення, структура систем відеоспостереження являє собою складну взаємодію складних апаратних компонентів та передових програмних платформ, які працюють синергетично для забезпечення ефективного спостереження та

виявлення загроз. Апаратні елементи, такі як камери, записи та мережева інфраструктура, формують фізичну основу, необхідну для захоплення та передачі візуальних даних, тоді як програмні рішення, включаючи системи управління відеоспостереженням та аналітику, забезпечують ефективне управління, аналіз та реагування. Безперебійна інтеграція цих компонентів, що забезпечується стандартизованими протоколами та надійним сховищем даних, забезпечує надійність та адаптивність системи. Зі зростанням кіберзагроз впровадження надійних заходів мережевої безпеки, таких як шифрування, брандмауери та регулярні оновлення, стає важливим для захисту конфіденційної інформації та підтримки цілісності системи. Заглядаючи в майбутнє, технологічні інновації, такі як штучний інтелект, периферійні обчислення та вдосконалені інтерфейси користувача, обіцяють революціонізувати системи відеоспостереження, збільшивши автономність, швидкість реагування та простоту використання. Загалом, розуміння складної архітектури цих платформ підкреслює їхню життєво важливу роль у захисті активів та людей, тоді як постійний розвиток обіцяє подальше посилення їхніх можливостей у майбутньому.

1.2 Класифікація охоронних пристроїв відеоспостереження та їх функціональна специфіка

Пристрої відеоспостереження є невід'ємним компонентом сучасних систем безпеки, забезпечуючи критично важливий візуальний моніторинг у різних середовищах, від громадських місць та комерційних приміщень до приватних будинків. З розвитком технологій ці пристрої стають дедалі складнішими, що дозволяє створювати індивідуальні рішення безпеки, що відповідають конкретним операційним потребам. Класифікацію цих пристроїв можна розглядати з різних точок зору, включаючи їхню мобільність та розміщення, функціональні характеристики та методи підключення в мережах спостереження. Глибоке розуміння цих класифікацій є важливим для вибору найбільш підходящих пристроїв безпеки для різних застосувань, забезпечення оптимального покриття,

чіткості та інтеграції. У розділі досліджуються основні класифікації пристроїв відеоспостереження, детально описуються їх функціональні особливості та практичне використання, щоб надати всебічний огляд цієї життєво важливої технології безпеки [4].

Один з фундаментальних способів класифікації пристроїв відеоспостереження – це їхня мобільність та розміщення в контрольованому середовищі. Фіксовані пристрої спостереження – це стаціонарні камери, встановлені в певних точках, таких як входи, коридори або стратегічні оглядові точки, що забезпечують безперервне покриття визначеної зони. Ці камери зазвичай монтуються на стінах або стелях і ідеально підходять для довгострокового, постійного моніторингу завдяки своїй стабільності та надійності. Наприклад, фіксовані камери зазвичай використовуються в роздрібних магазинах для запобігання крадіжкам та ефективного контролю активності клієнтів. На противагу цьому, камери з поворотом, нахилом та масштабуванням (PTZ) пропонують вищий ступінь гнучкості, дозволяючи дистанційно керувати напрямком огляду та рівнем масштабування. Оснащені двигунами, PTZ-камери можуть обертатися горизонтально та вертикально, що дозволяє співробітникам служби безпеки сканувати великі площі або фокусуватися на певних деталях без фізичного переміщення камери. Це робить їх особливо придатними для великих відкритих просторів, таких як парковки, стадіони або прикордонна служба, де динамічний моніторинг є критично важливим. Крім того, мобільні пристрої спостереження, включаючи нагрудні камери, дрони та камери, встановлені на транспортних засобах, забезпечують високий рівень мобільності, дозволяючи командам безпеки швидко адаптуватися до змінних сценаріїв. Наприклад, дрони можуть охоплювати великі території та отримувати доступ до важкодоступних місць, забезпечуючи огляд з висоти пташиного польоту в режимі реального часу, тоді як нагрудні камери забезпечують особисту безпеку та підзвітність правоохоронців. Можливість переміщувати та розгортати ці мобільні пристрої підвищує їхню універсальність, роблячи їх незамінними в динамічних середовищах безпеки.

Класифікація пристроїв відеоспостереження є багаторівневою та базується на різноманітних критеріях, що визначаються конкретними операційними потребами об'єктів безпеки. Глибоке розуміння цих категорій є необхідним для вибору найбільш підходящого обладнання, що забезпечить оптимальне покриття, чіткість зображення та ефективну інтеграцію в загальну систему. Основні класифікаційні ознаки охоронних пристроїв, їхні функціональні особливості та типові сфери застосування систематизовано в табл. 1.1.

Таблиця 1.1

Класифікація пристроїв відеоспостереження та їх характеристики

Критерій класифікації	Типи пристроїв	Функціональні особливості та характеристики	Типове застосування / Переваги
Мобільність та розміщення	Фіксовані	Стаціонарні, встановлені в стратегічних точках (входи, коридори). Монтуються на стінах або стелях.	Безперервний моніторинг зон у роздрібній торгівлі та офісах.
	PTZ-камери	Можливість дистанційного керування поворотом, нахилом та масштабуванням за допомогою двигунів.	Великі відкриті простори: парковки, стадіони, прикордонна служба.
	Мобільні пристрої	Нагрудні камери, дрони, камери на транспорті.	Особиста безпека правоохоронців, огляд з висоти пташиного польоту.
Функціональні можливості	Стандартні	Основні інструменти з фіксованими об'єктивами для запису та перегляду.	Постійний, простий моніторинг.
	Інфрачервоні та нічні	Використовують ІЧ-технологію для отримання чітких зображень у повній темряві.	Склади, паркувальні гаражі, охорона периметра вночі.
	HD та 4K (Ultra HD)	Надчіткі кадри, що дозволяють ідентифікувати обличчя та номерні знаки.	Аеропорти, міські системи, об'єкти високого рівня безпеки.

Продовження таблиці 1.1

Класифікація пристроїв відеоспостереження та їх характеристики

Критерій класифікації	Типи пристроїв	Функціональні особливості та характеристики	Типове застосування / Переваги
Методи підключення	Аналогові	Передача сигналу через коаксіальні кабелі. Економічно ефективні.	Базовий моніторинг з обмеженою роздільною здатністю.
	IP-камери	Цифрова передача через мережі. Масштабованість, аналітика та віддалений доступ.	Загальноміські системи, критична інфраструктура.
	Бездротові	Робота через Wi-Fi або радіочастоти. Не потребують прокладання кабелів.	Тимчасові установки, місця зі складним підключенням.
Середовище розгортання	Внутрішні	Компактні та непомітні. Мають функції адаптації до освітлення в приміщенні.	Офіси, магазини, будинки.
	Зовнішні	Стійкість до погоди та вандалізму. Міцний корпус та посилене нічне бачення.	Громадські площі, парковки, огорожі.
Живлення та зберігання	Дротові	Живлення від розеток/Ethernet. Централізоване зберігання великої ємності (NAS/сервери).	Надійні системи для відео високої роздільної здатності.
	Автономні (батареї)	Живлення від акумуляторів. Швидке розгортання в будь-якому місці.	Тимчасові або важкодоступні об'єкти.
	З локальним сховищем	Запис на SD-карти або вбудовані диски. Робота без мережевого з’єднання.	Незалежна робота, швидкий пошук записаних даних.

Аналіз представлених у таблиці даних дозволяє зробити висновок, що для сучасних хмарно-орієнтованих систем безпеки найбільш релевантними є IP-камери високої роздільної здатності (HD та 4K). Саме цифрові методи підключення забезпечують необхідну масштабованість та можливість віддаленого доступу через мережеву інфраструктуру, що є критичним для передачі відеосигналів у хмару.

Крім того, вибір між внутрішніми, зовнішніми або мобільними пристроями залежить від специфіки середовища розгортання, де захищеність корпусу та наявність інфрачервоного підсвічування гарантують стабільність моніторингу в будь-яких умовах. Варіанти живлення та способи локального або мережевого зберігання даних безпосередньо впливають на експлуатаційну стійкість та автономність комплексу, дозволяючи системі функціонувати навіть у разі тимчасової втрати мережевого з’єднання. Таким чином, комплексна класифікація дозволяє гнучко адаптувати архітектуру системи відеоспостереження до динамічних вимог сучасного безпекового середовища [5].

Функціональні можливості та характеристики пристроїв спостереження ще більше відрізняють їхню класифікацію. Стандартні відеокамери – це основні інструменти моніторингу, призначені переважно для запису та перегляду в реальному часі, що забезпечують необхідні візуальні дані для цілей безпеки. Вони часто мають фіксовані об'єктиви зі стандартною роздільною здатністю та підходять для середовищ, де достатньо постійного, простого моніторингу. Інфрачервоні та нічні камери розширюють функціональність, дозволяючи вести спостереження в умовах низької освітленості або повної темряви, використовуючи інфрачервону технологію для отримання чітких зображень без видимого освітлення. Ці камери мають першорядне значення для нічної безпеки в таких місцях, як склади, паркувальні гаражі або зовнішні огорожі периметра, де темрява може перешкоджати видимості. Камери високої чіткості (HD) та 4K представляють собою стрибок у якості зображення, пропонуючи надчіткі кадри, які можуть розкривати складні деталі, такі як риси обличчя або номерні знаки. Ці камери високої роздільної здатності все частіше використовуються в установах високого рівня безпеки, аеропортах та міських системах спостереження, де чіткість та деталізація є критично важливими для ідентифікації та аналізу. Вибір камери залежить від конкретних операційних потреб; наприклад, комбінація інфрачервоного нічного бачення та роздільної здатності 4K може бути використана в комплексній системі безпеки для забезпечення безперервного, детального моніторингу незалежно від умов освітлення. Ці технологічні досягнення значно

підвищили ефективність пристроїв спостереження, дозволяючи точнішу ідентифікацію та збір доказів.

Спосіб підключення та інтеграції в мережі безпеки є ще одним ключовим критерієм класифікації пристроїв спостереження. Аналогові пристрої спостереження, найдавніша форма відеобезпеки, передають відеозаписи через коаксіальні кабелі до записуючого пристрою або монітора. Хоча вони є економічно ефективними та надійними для базового моніторингу, вони пропонують обмежену роздільну здатність та гнучкість порівняно з цифровими альтернативами. З розвитком технологій з'явилися IP-камери (інтернет-протокол), які передають високоякісні цифрові відеодані через мережі, що дозволяє здійснювати віддалений доступ, зберігання та керування через пристрої з підтримкою Інтернету. IP-камери є високомасштабованими, підтримують великі мережі та пропонують розширені функції, такі як виявлення руху, аналітика та інтеграція з іншими системами безпеки. Наприклад, загальноміська система відеоспостереження може використовувати сотні IP-камер, з'єднаних між собою через захищену мережу, для моніторингу дорожнього руху, громадських місць та критично важливої інфраструктури. Бездротові пристрої спостереження ще більше спрощують встановлення та розширюють гнучкість, усуваючи потребу в тривалій кабельній мережі. Бездротові камери, які часто працюють через Wi-Fi або виділені радіочастоти, можна легко переміщувати або додавати до існуючих систем без значних змін інфраструктури. Це робить їх ідеальними для тимчасових установок, місць зі складним підключенням або великих відкритих територій. Їхня здатність безперешкодно інтегруватися в мережеві екосистеми безпеки покращує загальне покриття та дозволяє централізовано керувати та моніторити в режимі реального часу, адаптуючись до потреб сучасних середовищ безпеки, що постійно змінюються.

Ще один важливий критерій класифікації пристроїв відеоспостереження стосується середовищ, у яких вони розгортаються. Пристрої відеоспостереження для приміщень спеціально розроблені для закритих приміщень, таких як офіси, магазини роздрібної торгівлі та будинки. Ці камери зазвичай компактні, непомітні

та часто оснащені функціями, адаптованими до умов в приміщенні, такими як зменшення відблисків та оптимізоване регулювання освітлення. Їхня основна функція полягає у моніторингу діяльності в обмежених просторах, забезпеченні безпеки та сприянні оперативному нагляду. З іншого боку, пристрої зовнішнього відеоспостереження розроблені таким чином, щоб витримувати суворі погодні умови, екстремальні температури та потенційні фізичні впливи. Ці камери часто мають міцний корпус, вандалозахисну конструкцію та спеціалізовані технології, такі як всепогодний корпус та покращені інфрачервоні можливості для нічного бачення, що робить їх придатними для моніторингу парковок, огорож або громадських площ. Гібридні пристрої працюють як у приміщенні, так і на вулиці, пропонуючи гнучкі варіанти розгортання. Ці універсальні камери оснащені регульованим корпусом, всепогодною стійкістю та адаптивними функціями, що дозволяє співробітникам служби безпеки використовувати їх у різних умовах без необхідності використання кількох типів пристроїв. Вибір між цими класифікаціями залежить від конкретного середовища застосування, з урахуванням довговічності, видимості та експлуатаційних вимог, що забезпечує комплексне охоплення безпеки в різних умовах.

Варіанти живлення та зберігання пристроїв відеоспостереження є ще одним важливим аспектом класифікації, що впливає на їх розгортання, мобільність та експлуатаційну стійкість. Дротові пристрої живлення та зберігання даних – це традиційні рішення, що покладаються на електричні розетки та фізичні з’єднання, такі як коаксіальні кабелі або лінії Ethernet, для безперервної роботи. Ці системи зазвичай мають великі централізовані варіанти зберігання, такі як мережеві сховища (NAS) або серверні системи, що забезпечують велику ємність для довготривалого зберігання відео. Хоча дротові системи надійні та здатні підтримувати відео високої роздільної здатності, вони можуть бути трудомісткими в установці та менш гнучкими з точки зору переміщення. Пристрої відеоспостереження з живленням від батарей пропонують портативну альтернативу, особливо корисну в тимчасових умовах або місцях, де проводка непрактична. Ці камери працюють від акумуляторних або змінних батарей, що

забезпечує гнучкість та швидке розгортання. Однак час їхньої роботи залежить від терміну служби батареї, що вимагає технічного обслуговування або частої підзарядки. Пристрої з локальним сховищем, такі як SD-карти або вбудовані жорсткі диски, поєднують переваги мобільності та самодостатності. Ці камери можуть зберігати відео локально, що дозволяє працювати незалежно, навіть якщо втрачено мережеве з’єднання. Локальне сховище також зменшує залежність від пропускної здатності мережі та сприяє швидкому пошуку записаних даних. Вибір серед цих варіантів залежить від таких факторів, як необхідна тривалість розгортання, умови навколишнього середовища та наявна інфраструктура, що зрештою впливає на ефективність та стійкість системи безпеки.

На завершення, класифікація пристроїв відеоспостереження охоплює широкий спектр критеріїв, включаючи їх мобільність та розміщення, функціональні характеристики, методи підключення, середовище застосування, а також можливості живлення та зберігання даних. Фіксовані камери забезпечують стабільний довгостроковий моніторинг, тоді як PTZ-камери та мобільні пристрої пропонують динамічне покриття та гнучкість. Технологічний прогрес призвів до появи низки камер зі спеціалізованими функціями, такими як висока роздільна здатність, інфрачервоне нічне бачення та безперешкодна інтеграція в мережу через аналогові, IP- або бездротові з'єднання. Крім того, вибір відповідного пристрою спостереження значною мірою залежить від конкретного операційного середовища, будь то в приміщенні, на вулиці чи гібридному, а також від міркувань, пов'язаних з джерелом живлення та зберіганням даних. Розуміння цих класифікацій дозволяє фахівцям з безпеки адаптувати системи спостереження, які є ефективними, адаптивними та стійкими, що зрештою підвищує безпеку та операційну ефективність у різних умовах. Оскільки технології продовжують розвиватися, інтеграція цих різноманітних класифікацій ще більше покращить витонченість та швидкість реагування сучасних систем безпеки, гарантуючи, що вони відповідають зростаючим вимогам безпеки у все більш взаємопов'язаному світі [6].

1.3 Методики формування, обробки та передавання відеосигналів у охоронних комплексах

В сучасну епоху управління безпекою здатність ефективно формувати, обробляти та передавати відеосигнали має першорядне значення для забезпечення комплексного спостереження та швидкого реагування. Еволюція технологій запровадила різноманітні методи захоплення, уточнення та розподілу візуальної інформації між комплексами безпеки, починаючи від традиційних аналогових систем і закінчуючи складними цифровими мережами. Розуміння цих методів має вирішальне значення для проектування надійних інфраструктур безпеки, здатних задовольнити потреби середовищ з високою щільністю, чутливих об'єктів та великомасштабних операцій. У розділі досліджуються різні методи, що використовуються у формуванні відеосигналів, методи обробки, що підвищують їхню корисність, та методи передачі, що сприяють моніторингу в режимі реального часу та швидкому реагуванню на інциденти, надаючи всебічний огляд сучасних методологій відеоспостереження.

Формування відеосигналів є основою будь-якої системи спостереження, причому поширені два основні методи: аналоговий та цифровий. Традиційні аналогові відеосигнали генеруються за допомогою камер відеоспостереження (CCTV), які десятиліттями були основою системи безпеки. Ці камери перетворюють оптичні зображення на електричні сигнали за допомогою пристроїв із зарядовим зв'язком (CCD) або комплементарних метал-оксид-напівпровідникових (CMOS) датчиків, передаючи аналогові сигнали безпосередньо на монітори або записи. Незважаючи на їх тривале використання, аналогові системи стикаються з обмеженнями, пов'язаними з роздільною здатністю зображення та схильністю до перешкод. На противагу цьому, цифрові відеосигнали створюються камерами інтернет-протоколу (IP), які захоплюють зображення та перетворюють їх на цифрові дані за допомогою вбудованих процесорів. Ці камери передають дані через мережеві інфраструктури, що дозволяє отримувати зображення з вищою роздільною здатністю, віддалений доступ та більш гнучке розгортання. Цифрові

сигнали забезпечують розширені функції, такі як цифрове масштабування, покращення зображення та інтеграція з іншими системами безпеки. Порівнюючи ці два методи, цифрові системи зазвичай перевершують аналогові за чіткістю зображення, масштабованістю та адаптивністю, що робить їх більш придатними для сучасних потреб безпеки. Наприклад, IP-камери високої чіткості можуть забезпечити роздільну здатність 4K, забезпечуючи детальне зображення, критично важливе для розпізнавання облич або ідентифікації номерних знаків, тоді як аналогові камери зазвичай працюють зі стандартною роздільною здатністю, що обмежує їхню ефективність у детальному аналізі [7].

Процес функціонування сучасних комплексів відеоспостереження базується на багатоступеневій методиці перетворення візуальної інформації у цифрові дані, придатні для аналізу та тривалого зберігання. Кожен етап — від моменту потрапляння світла на матрицю камери до відображення на моніторі оператора — відіграє критичну роль у забезпеченні якості та швидкості реагування системи. Узагальнена схема цього процесу представлена на рисунку 1.2.

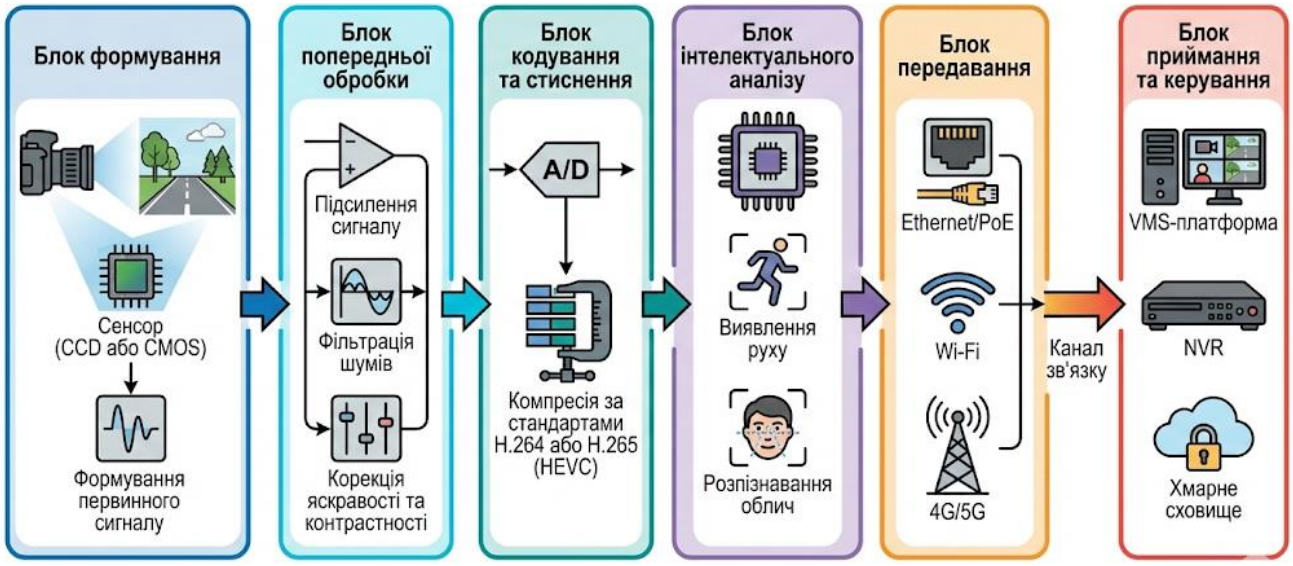


Рис. 1.2 Функціональна схема етапів формування, обробки та передавання відеосигналу

Як видно з рисунка, основою системи є формування сигналу, де за допомогою датчиків CCD або CMOS оптичне зображення перетворюється на електричний або цифровий сигнал. У цифрових IP-камерах цей сигнал одразу піддається обробці,

яка включає фільтрацію шумів та підсилення для досягнення максимальної чіткості в умовах складного освітлення.

Ключовим етапом для хмарно-орієнтованих систем є стиснення даних. Використання сучасних кодеків, таких як H.265, дозволяє знизити швидкість передачі даних до 50% порівняно з попередніми стандартами, що мінімізує навантаження на канали зв'язку без втрати якості зображення. Паралельно з цим, алгоритми відеоаналітики в режимі реального часу перетворюють пасивний потік на інтелектуальну систему, здатну самостійно ідентифікувати загрози.

Завершальним етапом є передача сигналу через дротові або бездротові мережі до централізованих платформ управління (VMS) або хмарних сервісів. Вибір методу передачі безпосередньо впливає на надійність системи: якщо дротові мережі Ethernet забезпечують максимальну стабільність, то технології Wi-Fi та 4G/5G надають гнучкість у розгортанні камер у важкодоступних місцях. Таким чином, інтегрований підхід до формування та обробки сигналів дозволяє створити високоефективну інфраструктуру безпеки, здатну адаптуватися до сучасних викликів.

Еволюція технологій відеоспостереження зумовила перехід від традиційних аналогових методів до складних цифрових екосистем, що інтегрують передову аналітику та хмарні сервіси. Ефективність таких комплексів базується на послідовному виконанні методик формування, обробки та передавання сигналів, кожна з яких має свою специфіку та технічні вимоги.

Узагальнена класифікація та характеристики цих методик наведені в табл. 1.2. Як демонструють дані таблиці, особливе значення для хмарно-орієнтованих систем мають методики цифрового формування сигналу та його подальшого стиснення за стандартом H.265. Це дозволяє не лише забезпечити високу якість зображення, необхідну для роботи алгоритмів штучного інтелекту, а й оптимізувати навантаження на канали зв'язку при передачі даних до віддалених серверів.

Таблиця 1.2

Методики та технології роботи з відеосигналами в сучасних охоронних системах

Етап роботи з сигналом	Методика / Технологія	Функціональне призначення та особливості	Ключові переваги та показники
Формування	Аналогове (CCTV)	Перетворення оптичного зображення на електричний сигнал за допомогою датчиків CCD або CMOS.	Економічність, але обмежена роздільна здатність та схильність до перешкод.
	Цифрове (IP)	Захоплення зображення та миттєве перетворення на цифрові дані вбудованими процесорами камери.	Висока чіткості (до 4K), гнучке розгортання та віддалений доступ.
Обробка	Попередня обробка	Підсилення сигналу, фільтрація шумів, регулювання яскравості та контрастності.	Покращення чіткості у несприятливих погодних умовах або при низькій освітленості.
	Стиснення (Кодування)	Використання стандартів компресії H.264 та H.265 (HEVC).	Зменшення обсягу даних до 50% (для H.265), що критично для хмарного зберігання.
	Інтелектуальна аналітика	Аналіз у реальному часі: виявлення руху, розпізнавання облич, аналіз поведінки.	Трансформація пасивного спостереження на проактивний захід безпеки.
Передавання	Дротова передача	Використання коаксіальних кабелів або мереж Ethernet з технологією PoE.	Максимальна надійність та стабільність сигналу без затримок.
	Бездротова передача	Робота через Wi-Fi та стільникові мережі (4G/5G).	Висока мобільність та можливість розгортання у важкодоступних місцях.
Інтеграція та зберігання	VMS та Хмарні сервіси	Об'єднання потоків у єдиний інтерфейс управління та використання хмарних сховищ.	Масштабованість, віддалений моніторинг та резервування даних поза об'єктом.

Використання комбінованих методів передавання, де дротові лінії Ethernet забезпечують стабільність опорної мережі, а бездротові технології 5G надають мобільність периферійним пристроям, створює фундамент для побудови адаптивних інфраструктур безпеки. Такий комплексний підхід до обробки відеосигналів дозволяє мінімізувати затримки та забезпечити цілісність інформації у динамічних операційних середовищах.

Після формування відеосигналів їх обробка стає важливою для оптимізації якості зображення та забезпечення ефективного зберігання та аналізу. Підсилення та фільтрація сигналу – це початкові кроки, які покращують візуальну чіткість шляхом зменшення шуму, регулювання яскравості та контрастності, а також усунення спотворень, спричинених умовами навколишнього середовища або перешкодами передачі. Наприклад, у випадках низької освітленості або несприятливих погодних умов алгоритми фільтрації можуть значно покращити чіткість зображення. Методи стиснення не менш важливі, особливо при роботі з великими обсягами даних, що генеруються камерами високої роздільної здатності. Такі стандарти, як H.264 та H.265 (також відомий як HEVC), є поширеними методами, які зменшують розмір відеофайлів без суттєвого зниження якості. Ці методи дозволяють створювати ефективні рішення для зберігання даних, зменшуючи вимоги до дискового простору, та забезпечують плавнішу передачу по мережах. Наприклад, H.265 може знизити швидкість передачі даних до 50% порівняно з H.264, що робить його ідеальним для середовищ з обмеженою пропускною здатністю. Крім того, обробка відео в реальному часі включає аналітику, таку як виявлення руху, розпізнавання облич та аналіз поведінки, які все частіше інтегруються в сучасні системи безпеки. Ця аналітика дозволяє здійснювати проактивні дії, такі як миттєве сповіщення персоналу служби безпеки про несанкціонований доступ або підозрілу активність, перетворюючи таким чином пасивне спостереження на активний захід безпеки [8].

Передача відеосигналів у комплексах безпеки включає різноманітні дротові та бездротові технології, кожна з яких має свої переваги та обмеження. Дротові методи передачі, включаючи коаксіальні кабелі та мережі Ethernet, залишаються

найнадійнішими та найбезпечнішими варіантами передачі високоякісного відео на великі відстані. Коаксіальні кабелі, які традиційно використовуються в аналогових системах відеоспостереження, забезпечують стабільні сигнали з мінімальними перешкодами, але їхня гнучкість обмежена, а встановлення може бути громіздким у складних інфраструктурах. Мережі Ethernet, що використовують живлення через Ethernet (PoE), дозволяють передавати цифрові відеосигнали разом із живленням, спрощуючи встановлення та обслуговування. Ці дротові з'єднання підтримують високу швидкість передачі даних, забезпечуючи передачу відео високої чіткості без затримки. І навпаки, технології бездротової передачі, такі як Wi-Fi та стільникові мережі (4G/5G), пропонують гнучкість та простоту розгортання, особливо в середовищах, де прокладання кабелів є непрактичним. Wi-Fi дозволяє встановлювати камери у віддалених або важкодоступних місцях, тоді як мережі 4G/5G забезпечують моніторинг у режимі реального часу у великих або розсіяних комплексах. Однак бездротові методи можуть зіткнутися з проблемами, пов'язаними з перешкодами, обмеженнями пропускної здатності та вразливостями безпеки. Наприклад, сигнали Wi-Fi можуть бути перервані фізичними перешкодами або конкуруючими мережами, що потенційно може поставити під загрозу пряму трансляцію. І навпаки, дротові з'єднання, як правило, є більш надійними та безпечними, що робить їх кращими для критичної інфраструктури. Зрештою, вибір методу передачі залежить від конкретних вимог середовища безпеки, балансуючи такі фактори, як швидкість, надійність, масштабованість та міркування безпеки.

Інтеграція відеосигналів у комплексні системи безпеки значною мірою залежить від централізованого управління та передових рішень для зберігання даних, щоб забезпечити ефективний моніторинг, швидке отримання та безперебійну координацію між різними системами. пристрої. Системи керування відео (VMS) слугують нервовим центром сучасного спостереження, об'єднуючи потоки з кількох камер — аналогових чи цифрових — в єдиний інтерфейс, який дозволяє співробітникам служби безпеки легко контролювати відео в реальному часі, переглядати записи та керувати налаштуваннями системи. Ці системи сприяють оповіщенню в режимі реального часу та дозволяють операторам швидко

реагувати на інциденти, надаючи синхронізовані перегляди та аналітику, що покращують ситуаційну обізнаність. Доповненням VMS є мережеві відеореєстратори (NVR), спеціально розроблені для зберігання цифрових відеоданих високої роздільної здатності, що передаються через IP-мережі. NVR забезпечують масштабовані рішення для зберігання, часто оснащені кількома жорсткими дисками та розширеними функціями керування даними, що дозволяє ефективно архівувати та швидко отримувати відеоматеріали, коли це необхідно для розслідувань або збору доказів. Крім того, сумісність між пристроями та стандартами стала критичним аспектом інтегрованих рішень безпеки. Сучасні системи розроблені для підтримки широкого спектру протоколів та виробників пристроїв, що гарантує безперебійну взаємодію різних камер, датчиків та блоків контролю доступу в єдиній мережі. Ця гнучкість не тільки спрощує розширення та оновлення системи, але й підвищує загальну стійкість безпеки, дозволяючи різним компонентам гармонійно працювати разом, незалежно від бренду чи покоління технологій. Незважаючи на прогрес у формуванні, обробці та передачі відеосигналів, численні проблеми залишаються, що спонукає до постійних інновацій та розробок у цій галузі. Кібербезпека залишається першочерговою проблемою, оскільки взаємопов'язані відеосистеми стають привабливими цілями для злому та перехоплення сигналів. Захист потоків даних за допомогою шифрування, надійних протоколів автентифікації та сегментації мережі є важливим для запобігання несанкціонованому доступу та забезпечення цілісності потоків спостереження. Одночасно технологічний прогрес формує майбутнє відеоспостереження. Аналітика на основі штучного інтелекту (ШІ) перетворює пасивні відеопотоки на інтелектуальні системи, здатні виявляти аномалії, розпізнавати обличчя або аналізувати поведінку в режимі реального часу, тим самим піднімаючи рівень безпеки з реактивного на проактивний. Крім того, поява камер з роздільною здатністю 8K обіцяє безпрецедентну чіткість зображення, що дозволяє здійснювати детальний аналіз та ідентифікацію, що підтримують високоякісні середовища безпеки. Крім того, хмарні рішення для зберігання даних та можливості віддаленого доступу революціонізують способи обробки та передачі

відеосигналів. Хмарні платформи пропонують масштабовані варіанти зберігання даних, полегшують віддалений моніторинг з будь-якого місця та підтримують розширену аналітику, розміщену поза межами об'єкта, зменшуючи потребу в обширній локальній інфраструктурі. Однак, залежність від хмарних рішень також створює занепокоєння, пов'язані з конфіденційністю даних, затримкою та вимогами до пропускної здатності. Оскільки технології продовжують розвиватися, інтеграція цих нових інструментів та вирішення пов'язаних з ними проблем матиме вирішальне значення для розвитку систем безпеки, які будуть більш надійними, інтелектуальними та адаптованими до майбутніх загроз.

На завершення, методи формування, обробки та передачі відеосигналів у комплексах безпеки значно еволюціонували від традиційних аналогових систем до складних цифрових мереж, оснащених передовою аналітикою та хмарною інтеграцією. Формування відеосигналів зараз варіюється від базових камер відеоспостереження до IP-камер високої роздільної здатності, причому цифрові системи пропонують чудову якість зображення та гнучкість. Методи обробки, такі як посилення, фільтрація та стиснення, підвищують чіткість зображення та забезпечують ефективне зберігання та аналітику в режимі реального часу, перетворюючи спостереження на активний інструмент безпеки. Методи передачі, дротові чи бездротові, вибираються на основі конкретних потреб у швидкості, надійності та безпеці, причому дротові рішення зазвичай забезпечують більшу стабільність, а бездротові опції пропонують гнучкість. Інтеграція цих сигналів у централізовані системи управління, такі як VMS та NVR, забезпечує скоординований моніторинг та ефективне отримання даних, тоді як сумісність між різними пристроями підтримує масштабовані та адаптивні інфраструктури безпеки. Заглядаючи в майбутнє, такі виклики, як загрози кібербезпеці та потреба у вищій роздільній здатності та розумнішій аналітиці, стимулюють інновації, включаючи функції на основі штучного інтелекту, зображення 8K та хмарні рішення. З розвитком технологій майбутнє відеоспостереження в комплексах безпеки обіцяє бути більш безпечним, інтелектуальним та здатним відповідати зростаючим вимогам сучасних середовищ безпеки.

1.4 Технічні параметри забезпечення якості, надійності та стійкості відеосигналів

У сфері цифрових медіа, що швидко розвивається, якість, надійність та стабільність відеосигналів мають першорядне значення для забезпечення безперебійного візуального досвіду на різних платформах та в різних додатках. Оскільки відеотехнології розвиваються та стають невід'ємною частиною розваг, мовлення, безпеки та зв'язку, встановлення надійних технічних параметрів є важливим для підтримки високих стандартів. Ці параметри охоплюють широкий спектр стандартів, практик та аспектів обладнання, які разом впливають на точність переданих відеосигналів. У розділі досліджуються критичні технічні стандарти та специфікації, що визначають якість відео, методи, що використовуються для захисту цілісності та надійності сигналу, а також технологічні аспекти, необхідні для підтримки стабільної роботи [9].

Фундаментальний аспект забезпечення високоякісної передачі відео полягає у дотриманні встановлених технічних стандартів та специфікацій. Ці стандарти слугують універсальними орієнтирами, що регулюють такі параметри, як роздільна здатність, точність кольору, пропускна здатність та синхронізація, тим самим забезпечуючи послідовну та сумісну передачу відео на різних пристроях та мережах. Наприклад, HDMI (High-Definition Multimedia Interface) став широко прийнятим стандартом для побутової електроніки, підтримуючи відеоформати високої чіткості, глибоку глибину кольору та інтеграцію аудіо. Еволюція HDMI, прикладом якої є HDMI 2.1, принесла такі функції, як вища пропускна здатність (до 48 Гбіт/с), покращена частота оновлення та динамічний HDR, які разом покращують візуальну точність та швидкість реагування. Аналогічно, професійні середовища мовлення часто покладаються на послідовний цифровий інтерфейс (SDI), стандарт, розроблений для високоякісної передачі відео в режимі реального часу по коаксіальних кабелях, зі специфікаціями, розробленими для мінімізації затримки та збереження цілісності сигналу на великих відстанях.

Ефективність хмарно-орієнтованих систем відеоспостереження безпосередньо залежить від технічних параметрів, що визначають якість формування та стабільність передачі відеосигналу. Дотримання галузевих стандартів, таких як HDMI 2.1 або SDI, забезпечує необхідну пропускну здатність для трансляції відео високої роздільної здатності з мінімальними затримками. Ключові технічні характеристики, що впливають на стійкість відеоінформації в цифрових мережах, наведено в табл. 1.3.

Таблиця 1.3

Технічні параметри та характеристики стійкості відеосигналів

Технічний параметр / Технологія	Технічний показник / Стандарт	Вплив на формування та передачу відеоінформації
Пропускна здатність інтерфейсу	HDMI 2.1 (до 48 Гбіт/с), SDI	Забезпечення стабільної передачі потоків високої чіткості (4K/8K) та динамічного HDR без втрати кадрів.
Методи компресії та бітрейт	Стандарт H.265 (HEVC)	Оптимізація обсягу відеоданих (зниження до 50%) для ефективної передачі через хмарні канали зв'язку.
Цілісність сигналу (Signal Integrity)	Корекція помилок та екранування	Виявлення та автоматичне виправлення бітових помилок, спричинених зовнішніми радіочастотними перешкодами.
Компенсація затухання	Активні ретранслятори та підсилювачі	Підтримка номінальної амплітуди сигналу при трансляції на великі відстані по дротових лініях зв'язку.
Співвідношення сигнал/шум (SNR)	Параметри фільтрації та підсилення	Мінімізація візуальних артефактів та шумів, що виникають через електромагнітні наведення або низьку освітленість.
Часова затримка (Latency)	Режими реального часу (Real-time)	Забезпечення миттєвої передачі відеосигналу від камери до центру моніторингу, що є критичним для оперативного реагування.
Коефіцієнт бітових помилок (BER)	Діагностика пропускної здатності	Технічний контроль стабільності цифрового потоку та визначення якості каналу передачі інформації.

Особлива увага при формуванні відеосигналу приділяється методам стиснення та контролю бітрейту. Використання стандарту H.265 (HEVC) дозволяє значно знизити навантаження на мережеву інфраструктуру, що є фундаментальним фактором для стабільної передачі інформації у хмарні сховища. Одночасно з цим, підтримка високого співвідношення сигнал/шум та мінімізація затримок (latency) гарантують цілісність візуальних даних, запобігаючи деградації зображення під впливом затухання або зовнішніх перешкод.

Технічний моніторинг коефіцієнта бітових помилок (BER) та пропускної здатності каналу дозволяє в реальному часі оцінювати стан системи та адаптувати параметри трансляції до поточної якості зв'язку. Такий інтегрований підхід до управління фізичними та логічними параметрами сигналу забезпечує надійність роботи охоронного комплексу навіть у складних операційних умовах.

Галузеві організації, такі як Товариство інженерів кіно та телебачення (SMPTE) та Міжнародний союз електрозв'язку (ITU), відіграють ключову роль у розробці, оновленні та забезпеченні дотримання цих стандартів, забезпечуючи сумісність та технологічну узгодженість між виробниками та мовниками. Їхній внесок включає визначення стандартів колірного простору, частоти кадрів та протоколів передачі, які є критично важливими для створення однорідних високоякісних відеосигналів у різних операційних контекстах.

Окрім стандартів, підтримка цілісності сигналу та забезпечення надійності під час передачі передбачає врахування різних факторів, які можуть погіршити якість відео. Погіршення сигналу може бути наслідком затухання, коли сигнал слабшає з відстанню; шуму, що вноситься електромагнітними перешкодами від сусідніх електронних пристроїв; та перешкод, спричинених зовнішніми джерелами, такими як радіочастоти. Для боротьби з цими проблемами використовується кілька методів. Екранування кабелів та роз'ємів допомагає запобігти електромагнітним перешкодам, тим самим зберігаючи чіткість сигналу. Підсилення сигналу, яке часто досягається за допомогою ретрансляторів або підсилювачів, підсилює слабші сигнали для підтримки постійної якості протягом тривалого часу. Алгоритми виправлення помилок, інтегровані в протоколи передачі, виявляють та виправляють

помилки, спричинені шумом або перешкодами, тим самим забезпечуючи точність отриманого відео. Наприклад, кабелі HDMI з високоякісним екрануванням та позолоченими роз'ємами є кращими для професійного застосування, оскільки вони мінімізують втрати сигналу та корозію відповідно. Крім того, використання високоякісних кабелів, розроблених для певних вимог до пропускної здатності, забезпечує мінімальне затухання сигналу. Впровадження цих заходів разом підвищує надійність відеосигналів, гарантуючи, що глядачі бачитимуть високоякісні зображення без артефактів або перешкод, навіть у складних умовах передачі [10].

Технологічна основа, що підтримує якість відеосигналу, включає вибір та обслуговування відповідного обладнання та апаратних компонентів. Високоякісні пристрої кодування та декодування є важливими, оскільки вони перетворюють необроблені відеодані на сигнали, готові до передачі, зберігаючи деталізацію та точність кольору. Сучасні кодери використовують передові алгоритми стиснення, такі як H.265/HEVC, що забезпечує ефективну передачу без шкоди для якості зображення, що особливо важливо для потокової передачі контенту високої роздільної здатності. Правильне калібрування та регулярне обслуговування відеообладнання однаково важливі для підтримки продуктивності; неправильно вирівняні монітори або застаріла прошивка можуть призвести до неточності кольору, проблем синхронізації або випадіння сигналу. Наприклад, інструменти калібрування забезпечують точне відтворення кольорів та рівнів яскравості дисплеями, що відповідає галузевим стандартам. Крім того, сумісність обладнання, яка забезпечує безперебійну роботу таких компонентів, як відеокарти, пристрої захоплення та пристрої зберігання даних, запобігає виникненню вузьких місць або несумісності, які можуть дестабілізувати передачу сигналу. Регулярні оновлення прошивки також відіграють вирішальну роль, виправляючи помилки, покращуючи функції та підвищуючи загальну стабільність. Підсумовуючи, інвестування у високоякісне, добре обслуговуване обладнання та забезпечення сумісності між пристроями є основою надійної системи передачі відео, здатної підтримувати найвищі стандарти якості та стабільності.

Фактори навколишнього середовища відіграють значну роль у впливі на стабільність та якість відеосигналів під час передачі та роботи. Електромагнітні перешкоди (EMI) від сусідніх електронних пристроїв, таких як радіоприймачі, мікрохвильові печі або промислове обладнання, можуть викликати шум та спотворювати сигнали, що призводить до погіршення якості зображення або тимчасових перебоїв. Фізичні перешкоди, включаючи товсті стіни або металеві конструкції, також можуть погіршити силу сигналу, особливо для бездротової передачі або в установках з довгими кабельними трасами. Щоб пом'якшити цей вплив навколишнього середовища, важливо впроваджувати такі стратегії, як належне екранування кабелів та роз'ємів для блокування зовнішніх джерел електромагнітних перешкод, а також використання кліток Фарадея або спеціалізованих корпусів у середовищах з високою електромагнітною активністю. Підтримка оптимальних умов навколишнього середовища, таких як контрольований рівень температури та вологості, є не менш важливою, оскільки надмірне тепло може спричинити перегрів обладнання, що призведе до зниження продуктивності або відмови, тоді як висока вологість може сприяти корозії та коротким замиканням. Створення контрольованого середовища з регулюванням клімату, разом з використанням всепогодних та міцних компонентів, допомагає забезпечити стабільну роботу. Крім того, ретельне планування місця розташування для мінімізації фізичних перешкод та використання ретрансляторів сигналу або бездротових подовжувачів може ще більше підвищити стабільність. Ці проактивні заходи життєво важливі для збереження цілісності сигналу, особливо на відкритому повітрі або в промислових умовах, де непередбачуваність навколишнього середовища створює постійні проблеми.

Для підтримки високих стандартів якості відео та забезпечення постійної надійності, постійний моніторинг та ретельне тестування є невід'ємними компонентами забезпечення якості. Передові інструменти моніторингу, такі як аналізатори реального часу та діагностичне програмне забезпечення, дозволяють технікам спостерігати за параметрами сигналу, включаючи пропускну здатність, рівень шуму та коефіцієнт помилок, у режимі реального часу, що сприяє негайному

виявленню аномалій, які можуть поставити під загрозу якість відео. Процедури планового тестування, включаючи періодичні аудити сигналу та перевірки цілісності, допомагають виявити потенційні проблеми, перш ніж вони переростуть у серйозні збої. Наприклад, планові перевірки кабелів, роз'ємів та калібрування обладнання гарантують, що всі компоненти функціонують у межах заданих стандартів. Профілактичні заходи, такі як очищення роз'ємів, оновлення прошивки та повторне калібрування дисплеїв, є не менш важливими для підтримки оптимальної продуктивності. Впровадження планового технічного обслуговування зменшує ймовірність погіршення сигналу з часом та подовжує термін служби критично важливого обладнання. У поєднанні постійний моніторинг та проактивне тестування утворюють комплексний підхід до підтримки стабільності, якості та надійності відеосигналів, захищаючи враження глядачів та операційну ефективність [11].

На завершення, забезпечення якості, надійності та стабільності відеосигналів передбачає багатогранний підхід, який охоплює дотримання технічних стандартів, надійні методи управління сигналами, передове обладнання, контроль навколишнього середовища та ретельні методи моніторингу. Технічні стандарти, встановлені галузевими організаціями, забезпечують необхідну основу для стабільної якості, тоді як такі методи, як екранування, посилення та корекція помилок, захищають цілісність сигналу під час передачі. Вибір та обслуговування високоякісного обладнання ще більше посилюють стабільність систем доставки відео. Вплив навколишнього середовища, включаючи електромагнітні перешкоди та несприятливі умови, необхідно проактивно керувати за допомогою екранування, контролю навколишнього середовища та стратегічного планування, щоб запобігти погіршенню якості. Нарешті, постійний моніторинг та планове тестування служать вирішальними інструментами для раннього виявлення та запобігання проблемам, забезпечуючи постійну продуктивність та надійність. Разом ці заходи утворюють комплексну структуру, яка підтримує високоякісну, надійну передачу відеосигналу, необхідну для різноманітних застосувань, які залежать від чіткого та стабільного візуального зв'язку в сучасному цифровому середовищі.

2 ХМАРНІ ТЕХНОЛОГІЇ В СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ ІНФРАСТРУКТУРАХ

2.1 Архітектурні моделі та принципи надання хмарних сервісів

Хмарні обчислення революціонізували спосіб розгортання, управління та використання інформаційно-технологічних ресурсів організаціями. Центральним елементом цієї трансформації є архітектурні моделі та принципи, що лежать в основі надання хмарних послуг, забезпечуючи масштабованість, надійність та економічну ефективність послуг. Розуміння цих моделей та принципів дає уявлення про те, як хмарні середовища розроблені для задоволення різноманітних бізнес-потреб, від малих стартапів до великих багатонаціональних корпорацій. У цьому есе досліджуються основні архітектурні моделі — інфраструктура як послуга (IaaS), платформа як послуга (PaaS) та програмне забезпечення як послуга (SaaS) — а також розглядаються основні принципи, якими керується розробка стійких та ефективних хмарних архітектур. Крім того, воно заглиблюється в критичні аспекти проектування, такі як багатокористувацька оренда, сумісність та економічна ефективність, які є важливими для створення стійких хмарних рішень [12].

Основа надання хмарних послуг побудована на різних архітектурних моделях, кожна з яких забезпечує різні рівні контролю, гнучкості та відповідальності. Інфраструктура як послуга (IaaS) слугує найбазовішим рівнем, надаючи користувачам віртуалізовані обчислювальні ресурси, такі як сервери, сховища та мережі через Інтернет. Ця модель пропонує неперевершену гнучкість, дозволяючи організаціям налаштовувати свою інфраструктуру без потреби у фізичному обладнанні, прикладом чого є такі постачальники, як Amazon Web Services (AWS) EC2 або Microsoft Azure. Вона особливо підходить для підприємств, які прагнуть контролювати своє середовище, включаючи розгортання користувацьких програм або керування застарілими системами. Платформа як послуга (PaaS), з іншого боку, абстрагує складність інфраструктури, надаючи платформу, яка підтримує розробку, тестування та розгортання програм.

Вибір конкретної архітектурної моделі хмарних обчислень визначає ступінь контролю організації над своїми IT-ресурсами та обсяг операційної відповідальності постачальника. Основна відмінність між моделями IaaS, PaaS та SaaS полягає в рівні абстракції базової інфраструктури від кінцевого користувача. Схематичне представлення цих моделей та розподіл зон відповідальності наведено на рисунок 2.1.



Рис. 2.1 Моделі надання хмарних сервісів та розподіл сфер відповідальності

Як показано на рис. 2.1, модель IaaS надає найбільшу гнучкість, дозволяючи користувачеві самостійно налаштовувати операційні системи та програмні середовища на базі віртуалізованих обчислювальних ресурсів. Натомість модель PaaS спрощує процес розробки, абстрагуючи складність управління серверами та мережами, що дозволяє зосередитися на логіці пристроїв відеоспостереження та обробці даних. Найвищий рівень автоматизації забезпечує модель SaaS, де користувач взаємодіє виключно з готовим програмним інтерфейсом, а всі технічні аспекти підтримки системи покладаються на хмарного провайдера.

Такий ієрархічний підхід дозволяє масштабувати ресурси відповідно до поточних потреб системи безпеки, забезпечуючи при цьому високу доступність та відмовостійкість за рахунок резервування на рівні центрів обробки даних.

Розуміння цих відмінностей є фундаментальним для проектування хмарно-орієнтованих систем відеоспостереження, де необхідно балансувати між керованістю компонентів та швидкістю розгортання сервісів.

Рішення PaaS, такі як Google App Engine або Heroku, забезпечують інтегровані середовища розробки, проміжне програмне забезпечення та середовища виконання, дозволяючи розробникам зосередитися виключно на логіці програми, а не на базових апаратних чи програмних рівнях. Програмне забезпечення як послуга (SaaS) пропонує готові до використання програми, доступні через веб-браузери, наприклад, Salesforce або Google Workspace. SaaS усуває необхідність локального встановлення програмного забезпечення, забезпечуючи економічно ефективні та масштабовані рішення, що підходять як для кінцевих користувачів, так і для підприємств. Ключові характеристики кожної моделі — від контролю та налаштування в IaaS до простоти використання та швидкого розгортання в SaaS — підкреслюють їхню придатність для різних організаційних вимог [13].

В основі ефективного розгортання хмарних сервісів лежать основні архітектурні принципи, розроблені для забезпечення продуктивності, надійності та адаптивності. Масштабованість має першорядне значення, дозволяючи хмарним системам обробляти зростаючі робочі навантаження шляхом динамічного розподілу ресурсів та балансування навантаження між серверами. Наприклад, платформи електронної комерції, такі як Amazon або Alibaba, зазнають значних коливань трафіку, особливо під час святкових сезонів; їхні хмарні архітектури використовують автоматичне масштабування та балансування навантаження для підтримки оптимальної продуктивності без ручного втручання. Еластичність доповнює масштабованість, дозволяючи автоматично коригувати ресурси на основі попиту в режимі реального часу — ресурси можна масштабувати в періоди пікового навантаження та зменшувати в непікові, оптимізуючи витрати та ефективність. Цей принцип має вирішальне значення для стримування витрат та використання ресурсів, особливо для стартапів та підприємств зі змінними робочими навантаженнями. Резервування та відмовостійкість ще більше підсилюють

надійність хмари, реплікуючи дані та послуги на кількох вузлах або центрах обробки даних. Це забезпечує високу доступність навіть у разі збоїв обладнання, відключень живлення або збоїв у роботі мережі. Наприклад, хмарна архітектура Netflix використовує резервування, щоб гарантувати безперебійну роботу потокових сервісів по всьому світу. Ці принципи разом сприяють створенню стійких хмарних середовищ, здатних підтримувати критично важливі програми з мінімальним часом простою.

Проектні міркування є життєво важливими для побудови ефективних та стійких хмарних архітектур, особливо щодо багатокористувацького обслуговування, сумісності та економічної ефективності. Багатокористувацьке обслуговування дозволяє кільком клієнтам або користувачам безпечно обмінюватися хмарними ресурсами, що максимізує використання ресурсів та знижує витрати. Наприклад, постачальник SaaS, такий як Salesforce, розміщує тисячі клієнтів на спільній інфраструктурі, ізолюючи їхні дані та операції за допомогою віртуалізації та суворого контролю доступу. Однак забезпечення того, щоб спільне використання ресурсів не ставить під загрозу безпеку чи продуктивність, є складним завданням, що вимагає надійних механізмів ізоляції. Взаємодія є ще одним критичним фактором, оскільки хмарні системи повинні безперешкодно інтегруватися з різними існуючими платформами, стандартами та API. Сумісність з різними операційними системами, базами даних та сторонніми сервісами, такими як інтеграція хмарної CRM з локальними ERP-системами, вимагає дотримання відкритих стандартів та гнучкої архітектури. Економічна ефективність також є першочерговим фактором, зумовленим необхідністю оптимізації використання ресурсів та операційних витрат. Постачальники хмарних послуг використовують такі стратегії, як ціноутворення «оплата за використання», об’єднання ресурсів та автоматизація, щоб мінімізувати втрати та забезпечити масштабовані рішення, що відповідають бюджетам організації. Наприклад, компанії, які використовують хмарні інструменти управління витратами, можуть контролювати та оптимізувати споживання ресурсів, тим самим зменшуючи непотрібні витрати. Разом ці конструктивні міркування гарантують, що хмарні

архітектури є не лише технічно обґрунтованими, але й економічно життєздатними та адаптованими до бізнес-середовищ, що розвиваються.

Незважаючи на численні переваги хмарних архітектур сервісів, впровадження цих систем створює кілька суттєвих проблем, які організації повинні вирішити. Однією з найважливіших проблем є конфіденційність та безпека даних; У міру переміщення даних до хмари організації стикаються з ризиками, пов'язаними з несанкціонованим доступом, витоками даних та дотриманням нормативних стандартів, таких як GDPR або HIPAA. Забезпечення надійних протоколів безпеки – шифрування, контролю доступу та постійного моніторингу – є важливим, але складним, особливо враховуючи спільний характер хмарних середовищ. Крім того, управління розподіленими системами в кількох центрах обробки даних та географічних місцях ускладнює підтримку узгодженості, синхронізації та продуктивності. Ця розподілена архітектура вимагає складних інструментів та стратегій управління для координації ресурсів, обробки збоїв та забезпечення цілісності даних. Безперебійна інтеграція послуг також створює труднощі, оскільки організаціям часто потрібно підключати хмарні сервіси до існуючих локальних систем або сторонніх програм. Досягнення сумісності та безперебійного потоку даних вимагає дотримання відкритих стандартів, сумісності API та комплексного тестування. Ці проблеми підкреслюють необхідність ретельного планування, інвестицій у безпеку та розширених можливостей управління, щоб повною мірою використовувати переваги хмарних архітектур, одночасно зменшуючи пов'язані з ними ризики.

Заглядаючи в майбутнє, архітектура хмарних сервісів готова до трансформаційних інновацій, зумовлених новими технологіями та зміною потреб бізнесу. Однією з помітних тенденцій є зростання периферійних обчислень, які розширюють хмарні можливості ближче до джерел даних, таких як пристрої Інтернету речей та датчики. Обробляючи дані локально на периферії, організації можуть зменшити затримку, покращити прийняття рішень у режимі реального часу та зменшити обмеження пропускної здатності, тим самим доповнюючи традиційні хмарні моделі. Ще одним важливим розвитком є безсерверна архітектура, також

відома як Функція як послуга (FaaS), яка повністю абстрагує управління сервером. Цей підхід дозволяє розробникам розгортати окремі функції, які автоматично масштабуються залежно від попиту, що призводить до високоекономічно ефективних та гнучких рішень. Великі постачальники хмарних послуг, такі як AWS Lambda або Azure Functions, є прикладом цієї тенденції, забезпечуючи швидку розробку та розгортання без управління інфраструктурою. Крім того, штучний інтелект (ШІ) все частіше інтегрується в системи управління хмарою, автоматизуючи розподіл ресурсів, виявлення несправностей та реагування на проблеми безпеки. Автоматизація на основі ШІ підвищує ефективність, зменшує людські помилки та оптимізує використання ресурсів у великих масштабах. Ці інновації разом сигналізують про майбутнє, де хмарні архітектури стають більш інтелектуальними, гнучкими та чутливими до динамічних операційних середовищ.

На завершення, такі архітектурні моделі, як IaaS, PaaS та SaaS, формують основу надання хмарних послуг, кожна з яких пропонує унікальні рівні контролю, гнучкості та простоти використання, адаптовані до різноманітних потреб організації. В основі цих моделей лежать такі ключові принципи, як масштабованість, еластичність та резервування, які допомагають забезпечити високу продуктивність, надійність та стійкість у хмарних середовищах. Продумані дизайнерські рішення, включаючи багатокористувацьку оренду, сумісність та економічну ефективність, є важливими для побудови стійких та адаптивних архітектур. Однак шлях до ефективного впровадження хмарних технологій пов'язаний з певними викликами, зокрема безпекою даних, складністю системи та безшовною інтеграцією. Незважаючи на ці перешкоди, постійні інновації, такі як периферійні обчислення, безсерверні архітектури та автоматизація на основі штучного інтелекту, формують майбутнє, де хмарні сервіси будуть більш ефективними, адаптивними та інтелектуальними. Оскільки організації продовжують використовувати ці досягнення, хмарні обчислення, безсумнівно, залишатимуться ключовою рушійною силою у трансформації того, як працюють та впроваджують інновації підприємства, підкреслюючи важливість розуміння та застосування надійних архітектурних принципів для сталого успіху [14].

2.2 Технологічні механізми обчислення та зберігання даних у хмарному середовищі

У швидкозмінному цифровому середовищі хмарні обчислення стали фундаментальною парадигмою для зберігання та обробки величезних обсягів даних. Використовуючи мережу віддалених серверів, розміщених в Інтернеті, хмарні середовища пропонують масштабовані, гнучкі та економічно ефективні рішення як для окремих осіб, так і для організацій. Центральним елементом цієї технологічної революції є складні механізми, що сприяють ефективному обчисленню та зберіганню даних у хмарі. У цьому есе досліджуються основні технологічні механізми, що лежать в основі хмарних обчислень, зосереджуючись на інфраструктурі, яка підтримує ці середовища, різноманітних технологіях зберігання даних, що використовуються, та стратегіях, що використовуються для ефективного управління та організації даних. Розуміння цих механізмів не лише проливає світло на те, як працюють сучасні хмарні сервіси, але й висвітлює постійні інновації, які продовжують розширювати їхні можливості.

В основі будь-якого хмарного середовища лежать його центри обробки даних та архітектура серверів, які формують основу хмарної інфраструктури. Ці центри обробки даних – це розлогі комплекси, що містять тисячі серверів, розроблених для оптимізації енергоефективності, охолодження та фізичної безпеки. Наприклад, технологічні гіганти, такі як Google та Amazon, керують центрами обробки даних, оснащеними передовим обладнанням для забезпечення високої доступності та стійкості. Архітектура цих серверів часто включає технології віртуалізації, які дозволяють запускати кілька віртуальних машин (ВМ) на одному фізичному сервері. Ця віртуалізація дозволяє постачальникам хмарних послуг максимізувати використання ресурсів, ізолювати робочі навантаження та швидко масштабувати послуги відповідно до попиту. Такі технології, як VMware, Hyper-V та KVM, стали галузевими стандартами в цій галузі. Крім того, надійне мережеве підключення є життєво важливим для забезпечення безперебійної передачі даних між центрами обробки даних та кінцевими користувачами. Високошвидкісні оптоволоконні

з'єднання, мережі доставки контенту (CDN) та вузли периферійних обчислень зменшують затримку та покращують продуктивність. Для захисту даних та підтримки довіри постачальники хмарних послуг впроваджують комплексні заходи безпеки, включаючи протоколи шифрування, брандмауери, системи виявлення вторгнень та багатофакторну автентифікацію. Ці заходи пом'якшують загрози, починаючи від кібератак до порушень даних, забезпечуючи цілісність та конфіденційність збережених та оброблених даних. Разом ці інфраструктурні елементи утворюють стійку, масштабовану та безпечну екосистему, яка є основою хмарних обчислювальних сервісів у всьому світі [15].

Різноманітність технологій зберігання даних у хмарних середовищах відображає різні потреби в продуктивності, масштабованості та обробці типів даних. Системи об'єктного зберігання, прикладом яких є Amazon S3, призначені для зберігання неструктурованих даних, таких як зображення, відео та резервні копії. Ці системи організовують дані в окремі об'єкти з унікальними ідентифікаторами та пов'язаними метаданими, що забезпечує легкий пошук та масштабованість у розподілених архітектурах. Наприклад, мережі доставки контенту використовують об'єктне сховище для ефективного обслуговування великих медіафайлів глобальній аудиторії. На противагу цьому, рішення для блочного зберігання, такі як Amazon Elastic Block Store (EBS), забезпечують низькозатримкове, високопродуктивне сховище, що підходить для програм, що потребують детального контролю над блоками даних, такими як бази даних та диски віртуальних машин. Блочне сховище бездоганно інтегрується з віртуалізованими середовищами, пропонуючи постійне сховище, яке можна динамічно змінювати розмір та керувати ним. Доповнюють їх розподілені файлові системи, такі як розподілена файлова система Hadoop (HDFS), які оптимізовані для обробки великих даних. HDFS розподіляє великі набори даних між кількома вузлами, забезпечуючи відмовостійкість та можливості паралельної обробки, життєво важливі для робочих навантажень аналізу даних та машинного навчання. Кожна з цих технологій зберігання даних ілюструє, як постачальники хмарних послуг адаптують свої рішення до вимог різноманітних додатків, балансуючи такі фактори, як швидкість, масштабованість та довговічність.

Функціонування сучасних хмарних середовищ базується на складній системі взаємопов'язаних технологічних механізмів, які забезпечують гнучкість, масштабованість та безпеку обробки даних. Центральне місце в цій екосистемі посідають методи віртуалізації та контейнеризації, що дозволяють динамічно розподіляти обчислювальні ресурси відповідно до поточного навантаження. Узагальнена характеристика основних технологічних механізмів обчислення та зберігання наведена в таблиці 2.1.

Таблиця 2.1

Технологічні механізми обчислення та зберігання даних у хмарі

Категорія механізмів	Технології та стандарти	Функціональне призначення та особливості	Роль у хмарній інфраструктурі
Обчислювальні механізми	Віртуальні машини (VM)	Створення повноцінних віртуалізованих апаратних середовищ на одному фізичному сервері.	Максимізація використання ресурсів та ізоляція робочих навантажень.
	Контейнеризація (Docker, Kubernetes)	Пакування програм та їх залежностей у легкі, портативні модулі.	Швидке розгортання та масштабування архітектур мікросервісів.
	Безсерверні обчислення (FaaS)	Виконання коду у відповідь на події з повною абстракцією управління сервером.	Економічно ефективне виконання завдань, що керуються подіями.
Технології зберігання	Об'єктне зберігання (напр., Amazon S3)	Організація даних (відео, зображення) в окремі об'єкти з унікальними ідентифікаторами.	Зберігання великих обсягів неструктурованих медіафайлів.
	Блочне зберігання (напр., EBS)	Високопродуктивне сховище з низькою затримкою для детального контролю над блоками даних.	Робота з базами даних та дисками віртуальних машин.

Продовження таблиці 2.1

Технологічні механізми обчислення та зберігання даних у хмарі

Категорія механізмів	Технології та стандарти	Функціональне призначення та особливості	Роль у хмарній інфраструктурі
	Розподілені файлові системи (HDFS)	Розподіл великих наборів даних між кількома вузлами для паралельної обробки.	Оптимізація обробки Big Data та машинного навчання.
Механізми управління та безпеки	Реплікація та індексація	Створення копій даних у різних регіонах та використання метаданих для швидкого пошуку.	Забезпечення відмовостійкості, доступності та цілісності даних.
	Шифрування (AES-256, TLS)	Захист даних у стані спокою та під час передачі через мережеві канали.	Гарантування конфіденційності та захист від несанкціонованого перехоплення.

Як показує аналіз представлених даних, вибір конкретного механізму зберігання безпосередньо залежить від типу відеоінформації: якщо для архівного зберігання великих масивів відеоданих оптимальним є об'єктне сховище, то для забезпечення високошвидкісного доступу та роботи баз даних критичним є використання блочних систем. Особливого значення для хмарно-орієнтованих охоронних систем набувають безсерверні обчислення (FaaS), які дозволяють автоматично масштабувати обробку тривожних подій без необхідності постійного управління серверною інфраструктурою. Надійна робота всієї системи підкріплюється механізмами реплікації та багаторівневого шифрування, що гарантує безперервність роботи та конфіденційність даних у розподілених архітектурах.

Ефективне управління даними та їх організація мають вирішальне значення для оптимізації хмарних систем зберігання, забезпечення цілісності даних, ефективності пошуку та безперервності роботи. Центральним фактором цього є індексація даних та метадані, які сприяють швидкому пошуку та категоризації

величезних наборів даних. Метадані, такі як дата створення, тип файлу, дозволи доступу та право власності, дозволяють хмарним системам систематично організовувати дані та застосовувати політики безпеки. Наприклад, хмарні платформи, такі як Google Cloud та Azure, використовують складні алгоритми індексації для швидкого пошуку даних у розподілених середовищах. Стратегії реплікації та резервного копіювання даних ще більше підвищують надійність та можливості аварійного відновлення. Реплікація передбачає створення кількох копій даних у різних географічних регіонах, забезпечуючи доступність навіть у разі збоїв обладнання або стихійних лих. Amazon S3, наприклад, пропонує міжрегіональну реплікацію, що дозволяє автоматично синхронізувати дані в кількох місцях. Стратегії резервного копіювання доповнюють реплікацію, періодично зберігаючи знімки даних у безпечних місцях, що полегшує відновлення після випадкового видалення або пошкодження. Нарешті, управління життєвим циклом даних охоплює політики та автоматизовані процеси, які регулюють збереження, архівування та видалення даних. Такий підхід оптимізує витрати на зберігання та забезпечує дотримання нормативних вимог. Такі методи, як багаторівневе сховище, де часто використовувані дані зберігаються на швидших і дорожчих носіях, а рідко використовувані дані архівуються, використовуються для балансування продуктивності та економічної ефективності. Разом ці стратегії управління даними дозволяють хмарним середовищам працювати ефективно, безпечно та відповідно до політик організації.

Центральним фактором гнучкості та ефективності хмарних обчислень є їх динамічні обчислювальні механізми, які дозволяють надавати ресурси на вимогу та масштабоване розгортання додатків. Однією з ключових особливостей є використання віртуальних машин (ВМ) та контейнерів на вимогу. Віртуальні машини надають користувачам повноцінні віртуалізовані апаратні середовища, що дозволяє кільком операційним системам одночасно працювати на одному фізичному сервері. Це сприяє ефективному використанню ресурсів та швидкому налаштуванню для різних робочих навантажень. Контейнери, прикладами яких є Docker та Kubernetes, ще більше спрощують розгортання шляхом пакування

програм та їхніх залежностей у легкі, портативні пристрої, які можуть однаково працювати в різних середовищах. Контейнери особливо цінуються за свою швидкість та масштабованість, що робить їх ідеальними для архітектур мікросервісів. Доповнюють їх моделі безсерверних обчислень, такі як Functions as a Service (FaaS), що пропонуються такими постачальниками, як AWS Lambda, Google Cloud Functions та Azure Functions. Безсерверна архітектура абстрагує управління сервером, дозволяючи розробникам зосередитися виключно на коді, який виконується у відповідь на події та автоматично масштабується залежно від потреб. Ця модель є дуже економічно ефективною та підходить для програм, керованих подіями. Щоб забезпечити оптимальну продуктивність та ефективність використання ресурсів, постачальники хмарних послуг використовують методи балансування навантаження та автоматичного масштабування. Балансувальники навантаження рівномірно розподіляють вхідний трафік між серверами, запобігаючи вузьким місцям та забезпечуючи високу доступність. Автоматичне масштабування динамічно регулює кількість активних екземплярів на основі попиту в режимі реального часу, підтримуючи швидкість реагування програм та контролюючи витрати. Ці взаємопов'язані механізми разом дозволяють хмарним середовищам надавати гнучкі, масштабовані та стійкі обчислювальні ресурси, адаптовані до різноманітних потреб програм [16].

Оскільки хмарні обчислення обробляють конфіденційні та критично важливі дані, надійні заходи безпеки та конфіденційності є надзвичайно важливими. Методи шифрування даних у стані спокою та під час передачі слугують основними засобами захисту. Дані в стані спокою, що зберігаються на дисках або в системах зберігання, шифруються за допомогою таких алгоритмів, як AES-256, що гарантує, що навіть у разі порушення фізичної безпеки дані залишаються недоступними без ключів розшифрування. Аналогічно, дані під час передачі захищені за допомогою таких протоколів, як TLS (Transport Layer Security), який шифрує обмін даними між клієнтами та серверами, запобігаючи перехопленню та втручанню під час передачі. Доповнюючи шифрування, суворі протоколи управління ідентифікацією та доступом (IAM) контролюють, хто може отримати доступ до даних та хмарних

ресурсів. Фреймворки IAM забезпечують багатофакторну автентифікацію, контроль доступу на основі ролей та дозволи на основі політик, щоб мінімізувати несанкціонований доступ та внутрішні загрози. Крім того, стандарти відповідності та політики управління даними допомагають постачальникам хмарних послуг та користувачам підтримувати конфіденційність даних та дотримуватися нормативних вимог. Такі стандарти, як GDPR, HIPAA та ISO 27001, встановлюють рамки для захисту даних, прав на конфіденційність та операційної безпеки. Постачальники хмарних послуг часто проходять аудити та сертифікації, щоб продемонструвати відповідність цим стандартам, сприяючи довірі між користувачами. Крім того, управління даними включає визначення політик класифікації, зберігання та аудиту даних, що забезпечує відповідність обробки даних організаційним та правовим вимогам. Разом ці механізми безпеки та конфіденційності утворюють комплексний захист, який захищає цілісність, конфіденційність та відповідність даних у хмарних середовищах.

На завершення, хмарні обчислення спираються на складну мережу технологічних механізмів, які разом забезпечують ефективне, масштабоване та безпечне зберігання та обробку даних. Базова інфраструктура, що включає передові центри обробки даних, віртуалізацію та надійну мережеву безпеку, забезпечує стійку платформу для хмарних сервісів. Різноманітні технології зберігання даних – від об'єктного зберігання до розподілених файлових систем – задовольняють різні потреби неструктурованих та структурованих даних, тоді як складні стратегії управління даними забезпечують цілісність, доступність та економічну ефективність даних. Обчислювальні механізми, включаючи віртуальні машини на вимогу, контейнери, безсерверні архітектури та методи автоматичного масштабування, сприяють гнучкому та адаптивному розгортанню додатків. В основі всього цього лежить комплексна система безпеки, яка використовує шифрування, контроль доступу та дотримання нормативних стандартів для захисту конфіденційної інформації. Разом ці механізми є прикладом технологічної винахідливості, що рухає еволюцію хмарних середовищ, роблячи їх незамінними в сучасному цифровому світі. У міру подальшого розвитку ці системи, безсумнівно,

стануть ще ефективнішими, безпечнішими та адаптивнішими, формуючи майбутнє інновацій, заснованих на даних.

2.3 Інструменти захисту, оптимізації та передавання відеоданих у хмарних системах

У швидкозмінному ландшафті цифрових медіа відеоконтент став домінуючою формою комунікації, розваг та поширення інформації. Зі зростанням обсягу відеоданих використання хмарних систем для зберігання, безпеки та доставки стало важливим як для організацій, так і для окремих осіб. Хмарні обчислення пропонують універсальну платформу, яка дозволяє створювати масштабовані рішення для зберігання даних, надійні механізми захисту та ефективні методи передачі даних. Однак ефективне управління відеоданими в хмарних середовищах вимагає всебічного розуміння інструментів та стратегій, доступних для захисту, оптимізації та забезпечення безперебійної передачі цього цінного цифрового активу. У цьому есе досліджуються ключові інструменти та методи, що використовуються в хмарних системах для захисту, оптимізації та передачі відеоданих, підкреслюючи важливість передових рішень для забезпечення цілісності даних, безпеки та чудового користувацького досвіду.

Хмарні рішення для зберігання даних формують базовий рівень для керування величезними обсягами відеоданих, пропонуючи низку варіантів розгортання, адаптованих до різних потреб. Публічні хмарні сховища, такі як Amazon S3, Google Cloud Storage та Microsoft Azure Blob Storage, забезпечують економічно ефективні, масштабовані платформи, доступні через Інтернет, що підходять як для стартапів, так і для великих підприємств. З іншого боку, приватні хмарні рішення розгортаються у власній інфраструктурі організації, пропонуючи розширений контроль та безпеку для конфіденційного контенту. Гібридні хмарні моделі поєднують обидва підходи, дозволяючи організаціям зберігати критично важливі або конфіденційні відео в приватних хмарах, використовуючи публічні хмари для менш конфіденційних даних, таким чином балансуючи гнучкість та

безпеку. Однією з суттєвих переваг хмарного сховища є його масштабованість; користувачі можуть динамічно розширювати або зменшувати ємність сховища у відповідь на коливання попиту, усуваючи необхідність у дорогих інвестиціях у фізичне обладнання. Ця гнучкість особливо корисна для медіакомпаній, які переживають сезонні сплески завантаження контенту або потокової активності. Незважаючи на ці переваги, проблеми залишаються, особливо щодо безпеки та конфіденційності даних. Конфіденційний відеоконтент, що зберігається в хмарі, вразливий до несанкціонованого доступу, порушень даних та проблем із дотриманням вимог, що вимагає надійних заходів безпеки. Організації повинні впроваджувати комплексні протоколи безпеки, включаючи шифрування, контроль доступу та регулярні аудити, щоб зменшити ці ризики та забезпечити дотримання таких норм, як GDPR або HIPAA. Таким чином, хоча хмарні рішення для зберігання даних пропонують неперевершену масштабованість та доступність, вони вимагають ретельних стратегій безпеки для захисту цінних відеоактивів.

Ефективне управління відеоданими у хмарних середовищах вимагає комплексного застосування інструментів захисту, методів оптимізації та протоколів передачі. Процес обробки відеоданих є багатоетапним і спрямований на забезпечення цілісності інформації та високої якості користувацького досвіду (як показано на рисунку 2.2) [17].



Рис. 2.2 Життєвий цикл відеоданих у хмарній екосистемі

Як показано на схемі, на першому етапі критично важливим є застосування передових стандартів шифрування AES та протоколів TLS, які захищають відеоконтент як під час зберігання, так і під час його трансляції. Для мінімізації навантаження на канали зв'язку використовуються сучасні кодеки H.265/HEVC, що забезпечують високий ступінь компресії без суттєвої втрати візуальної якості. Деталізований перелік інструментів та їх функціональне призначення наведено у таблиці 2.2.

Таблиця 2.2

Інструменти захисту, оптимізації та передавання відеоданих у хмарі

Функціональна категорія	Використовувані інструменти та протоколи	Технічна роль та переваги
Захист даних	Алгоритми AES та протокол TLS.	Шифрування відео у стані спокою та під час передачі для запобігання перехопленню.
	Механізми RBAC та MFA.	Рольовий контроль та багатофакторна автентифікація для обмеження доступу.
Оптимізація	Кодеки H.265/HEVC, VP9.	Забезпечення високих коефіцієнтів стиснення для економії пропускної здатності.
	Технології MPEG-DASH, HLS.	Адаптивне потокове передавання, що регулює якість відео відповідно до умов мережі.
Передавання та доставка	Протоколи RTMP, HTTP, FTP.	RTMP забезпечує низьку затримку для трансляцій у реальному часі; HTTP — для доставки кінцевим користувачам.
	Мережі доставки контенту (CDN).	Розподіл кешованих копій відео між географічно рознесеними серверами для зменшення затримки.
Новітні технології	AI/ML, Blockchain, 5G.	Автоматизація аналітики, перевірка цілісності транзакцій та забезпечення надвисокої швидкості передачі.

Особливу роль у сучасних хмарних системах відіграють технології CDN та периферійні обчислення, які дозволяють кешувати дані ближче до кінцевого користувача, значно зменшуючи затримку. Крім того, впровадження

інтелектуальних інструментів на основі штучного інтелекту дозволяє автоматизувати аналіз відеопотоків, перетворюючи масиви даних на структуровану інформацію, придатну для оперативного прийняття рішень.

Враховуючи конфіденційність багатьох наборів відеоданих, використання ефективних методів захисту є надзвичайно важливим. Шифрування є основним методом захисту відеоданих як у стані спокою — під час зберігання в хмарі — так і під час передачі. Передові стандарти шифрування (AES) можуть захистити збережені відео, роблячи дані незрозумілими для неавторизованих користувачів. Під час передачі такі протоколи, як TLS (Transport Layer Security), шифрують потоки даних, запобігаючи перехопленню та втручанню. Наприклад, потокові платформи, такі як Netflix та YouTube, використовують наскрізне шифрування для захисту даних користувачів та власного контенту. Поряд із шифруванням, механізми контролю доступу є життєво важливими для регулювання того, хто може переглядати, змінювати або керувати відеоданими.

Контроль доступу на основі ролей (RBAC) та багатофакторна автентифікація (MFA) зазвичай використовуються для перевірки ідентифікацій користувачів та обмеження дозволів, тим самим знижуючи ризик внутрішніх загроз або несанкціонованого доступу. Крім того, впровадження комплексних стратегій резервного копіювання та аварійного відновлення забезпечує стійкість даних. Постачальники хмарних послуг часто пропонують автоматизовані рішення для резервного копіювання, які створюють надлишкові копії відеоданих у кількох центрах обробки даних, що дозволяє швидке відновлення у разі випадкового видалення, збою обладнання або кібератак. Наприклад, плани аварійного відновлення, що включають географічно розподілені резервні копії, можуть мінімізувати час простою та втрату даних, підтримуючи безперервність бізнесу. У сукупності ці методи захисту – шифрування, контроль доступу та стратегічне резервне копіювання – становлять багаторівневий захист, необхідний для підтримки конфіденційності, цілісності та доступності відеоданих у хмарних середовищах.

Ефективне управління відеоданими в хмарних системах також залежить від стратегій оптимізації, які покращують зберігання, передачу та взаємодію з користувачем. Методи стиснення даних є фундаментальними для зменшення розміру відеофайлів без суттєвого зниження якості, таким чином заощаджуючи простір для зберігання та пропускну здатність. Сучасні кодеки, такі як H.265/HEVC та VP9, забезпечують високі коефіцієнти стиснення, що особливо вигідно для потокової передачі відео високої роздільної здатності через обмежені мережеві з'єднання. Адаптивні технології потокової передачі, такі як MPEG-DASH та HLS, ще більше покращують взаємодію з користувачем, динамічно регулюючи якість відео на основі мережевих умов у режимі реального часу, запобігаючи буферизації та забезпечуючи плавне відтворення. Наприклад, потокові сервіси, такі як Hulu та Amazon Prime Video, використовують адаптивну потокову передачу для забезпечення найкращої можливої якості, адаптованої до пропускної здатності кожного глядача. Крім того, стратегії кешування в поєднанні з мережами доставки контенту (CDN) відіграють вирішальну роль в оптимізації доставки відео. CDN розподіляють кешовані копії відео між географічно розподіленими серверами, зменшуючи затримку та навантаження на вихідні сервери. Така конфігурація гарантує, що користувачі отримують контент з найближчого сервера, що призводить до швидшого завантаження та зменшення буферизації, особливо в періоди пікового навантаження. Такі компанії, як Akamai та Cloudflare, пропонують комплексні рішення CDN, які значно підвищують ефективність доставки для глобальної аудиторії. Ці інструменти оптимізації разом сприяють безперебійному перегляду, мінімізують експлуатаційні витрати, та забезпечити швидку та надійну передачу великих обсягів відеоданих через хмарні мережі [18].

Ефективна та надійна передача відеоданих у хмарних системах спирається на набір спеціалізованих інструментів та протоколів, розроблених для забезпечення безперебійного зв'язку між пристроями, серверами та кінцевими точками зберігання. Інтерфейси прикладного програмування (API), такі як RESTful API та SDK, дозволяють розробникам автоматизувати та налаштовувати процеси передачі даних, забезпечуючи ефективне завантаження та отримання відео та інтеграцію їх

у ширші робочі процеси. Протоколи, такі як протокол передачі файлів (FTP), протокол передачі гіпертексту (HTTP) та протокол обміну повідомленнями в реальному часі (RTMP), виконують певні функції для переміщення відеоданих між мережами. FTP залишається простим методом для масової передачі, тоді як HTTP лежить в основі доставки потокового контенту кінцевим користувачам. RTMP, розроблений спочатку для прямої трансляції, пропонує передачу з низькою затримкою для трансляцій у реальному часі. Для подальшої мінімізації затримки та підвищення швидкості передачі, периферійні обчислення набули популярності. Обробляючи та кешуючи дані ближче до користувача або джерела даних, периферійні обчислення зменшують відстань, яку дані повинні подолати, тим самим зменшуючи затримку та покращуючи користувацький досвід під час прямої трансляції або доступу на вимогу. Інструменти автоматизації та робочі процеси також відіграють вирішальну роль в управлінні передачею великомасштабного відео; такі платформи, як хмарні сервіси оркестрації, дозволяють автоматично завантажувати, перекодувати та витягувати дані, зменшуючи ручне втручання та потенційні помилки. Наприклад, творці контенту можуть автоматизувати прийом необробленого відеоматеріалу, його перетворення в різні формати та розповсюдження на різні платформи без людського контролю. Ці інструменти та технології разом оптимізують процес передачі, забезпечуючи швидке, безпечне та надійне переміщення відеоданих у хмарних середовищах, щоб відповідати вимогам сучасного споживання цифрових медіа.

Зі зростанням обсягу та складності відеоданих новітні технології трансформують те, як ці дані управляються, захищаються та використовуються в хмарних системах. Штучний інтелект (ШІ) та машинне навчання (МН) стали ключовими в автоматизації відеоаналітики, дозволяючи тегувати контент, розпізнавати сцени та покращувати якість з мінімальним людським втручанням. Ці технології сприяють ефективному управлінню великими наборами даних, автоматично організовуючи та витягуючи аналітику з відеоконтенту, що покращує можливості пошуку та персоналізації для кінцевих користувачів. Технологія блокчейн також пропонує перспективні рішення для безпечної та прозорої передачі

даних. Використовуючи децентралізовані реєстри, блокчейн може перевіряти цілісність відеотранзакцій, запобігати несанкціонованим змінам та встановлювати довіру між зацікавленими сторонами. Наприклад, блокчейн можна використовувати для автентифікації власності на контент та контролю за управлінням правами, зменшуючи піратство та несанкціоноване розповсюдження. Забігаючи вперед, майбутні тенденції, такі як потокове передавання з підтримкою 5G, готові революціонізувати доставку відео, пропонуючи безпрецедентну пропускну здатність та наднизьку затримку, роблячи високоякісне потокове відео в режимі реального часу доступним навіть у віддалених або перевантажених районах. Децентралізовані системи зберігання, які розподіляють дані між кількома вузлами, а не покладаються на централізовані сервери, обіцяють підвищену стійкість, безпеку та економічну ефективність. Ці інновації не лише вирішують поточні проблеми, але й відкривають нові шляхи для масштабованого, безпечного та високопродуктивного управління відеоданими в хмарних середовищах, що відповідає цифровим вимогам майбутнього.

На завершення, управління відеоданими в хмарних системах охоплює різноманітний спектр інструментів і методів, спрямованих на забезпечення безпеки, ефективності та безперебійної передачі. Хмарні рішення для зберігання даних, будь то публічні, приватні чи гібридні, закладають основу для масштабованих і доступних відеосховищ, хоча вони вимагають надійних заходів безпеки для захисту конфіденційного контенту. Захист відеоданих за допомогою шифрування, контролю доступу та планів аварійного відновлення є життєво важливим для підтримки конфіденційності та цілісності в хмарі [19].

У другому розділі було проведено дослідження хмарних технологій у сучасних телекомунікаційних інфраструктурах, що дозволило дійти наступних висновків:

Фундаментом надання хмарних сервісів є архітектурні моделі IaaS, PaaS та SaaS, кожна з яких пропонує різний рівень контролю та гнучкості при управлінні ресурсами. В основі їхньої роботи лежать принципи масштабованості, еластичності

та резервування, які забезпечують високу продуктивність і відмовостійкість систем у динамічних операційних середовищах.

Технологічні механізми хмарних обчислень базуються на віртуалізації (віртуальні машини) та контейнеризації (Docker, Kubernetes), що дозволяє максимально ефективно використовувати апаратні ресурси центрів обробки даних. Використання безсерверних архітектур (FaaS) додатково спрощує розгортання функцій, що активуються за подіями, забезпечуючи автоматичне масштабування та економічну ефективність.

Для зберігання великих обсягів даних у хмарі застосовуються спеціалізовані типи сховищ: об'єктне (для неструктурованих медіафайлів), блочне (для баз даних і систем з низькою затримкою) та розподілені файлові системи (HDFS) для задач машинного навчання та аналізу великих даних.

Захист відеоданих у хмарних системах реалізується через багаторівневий підхід, що включає шифрування (AES, TLS) у стані спокою та під час передачі, суворий контроль доступу (RBAC, MFA) та стратегії резервного копіювання для аварійного відновлення.

Оптимізація передачі відеоконтенту досягається завдяки використанню сучасних кодеків (H.265/HEVC, VP9) для ефективного стиснення, а також технологій адаптивної потокової передачі (DASH, HLS), які підлаштовують якість відео під поточні умови мережі.

Ефективна доставка контенту кінцевим користувачам забезпечується через мережі доставки контенту (CDN) та периферійні обчислення (Edge Computing), які кешують дані ближче до джерела або споживача, значно зменшуючи затримку та навантаження на мережу.

Перспективи розвитку хмарних систем пов'язані з інтеграцією штучного інтелекту, технології блокчейн для перевірки цілісності транзакцій та мереж 5G, що забезпечать надвисоку пропускну здатність для відеопотоків у реальному часі.

У сукупності ці технології та механізми утворюють надійну, масштабовану та безпечну екосистему, яка є необхідною базою для формування та обробки відеосигналів у хмарно-орієнтованих пристроях відеоспостереження.

3 ДОСЛІДЖЕННЯ СИСТЕМ ФОРМУВАННЯ ВІДЕОСИГНАЛІВ У ХМАРНО-ОРІЄНТОВАНИХ ОХОРОННИХ ПРИСТРОЯХ

3.1 Аналітична оцінка підходів до формування відеосигналів у хмарних охоронних рішеннях

Еволюція генерації відеосигналу в контексті хмарних рішень безпеки відображає динамічну взаємодію між традиційними методами та інноваційними технологічними досягненнями. Оскільки цифровий відеоконтент стає дедалі важливішим у різних секторах — від спостереження та розваг до корпоративного зв'язку — методології, що використовуються для генерації, передачі та захисту цих сигналів, привернули значну увагу. Критично проаналізувати різні підходи до генерації відеосигналу, зосереджуючись на традиційних методах, хмарних моделях та інтеграції штучного інтелекту (ШІ) та машинного навчання (МН). Розглядаючи їхні відповідні сильні сторони, обмеження та трансформаційний потенціал, ми можемо краще зрозуміти їхню роль у формуванні безпечних, ефективних та масштабованих хмарних відеорішень [20].

Традиційна генерація відеосигналу переважно спирається на усталені методи, такі як аналогові та ранні методи цифрового кодування, включаючи стандарти MPEG-2 та H.264. Ці методи залежать від апаратних кодерів та спеціалізованої інфраструктури, розробленої для обробки в реальному часі, які історично забезпечували високу надійність та стабільну продуктивність. Наприклад, камери безпеки та трансляційні станції вже давно використовують ці традиційні системи завдяки їхній стійкості та зрілості, забезпечуючи мінімальну затримку та надійний вихідний сигнал. Однак, незважаючи на ці переваги, такі методи мають помітні обмеження. Високе споживання пропускної здатності є суттєвою проблемою, оскільки нестисні або погано стиснуті сигнали вимагають значних мережевих ресурсів, що часто призводить до перевантаження та збільшення експлуатаційних витрат. Крім того, масштабованість стає складною у великомасштабних розгортаннях; розширення інфраструктури для розміщення

більшої кількості камер або потоків з вищою роздільною здатністю тягне за собою значні інвестиції в обладнання та пропускну здатність. Більше того, ці традиційні системи схильні до вразливостей безпеки, особливо коли апаратні компоненти застарілі або неналежним чином обслуговуються, що наражає критичні відеопотоки на перехоплення або втручання. Наприклад, застарілі аналогові системи не мають можливостей шифрування, що робить їх вразливими до прослуховування. Таким чином, хоча традиційні методи забезпечують міцну основу для генерації відеосигналу, їхні притаманні обмеження перешкоджають їхній адаптивності в сучасних, масштабованих та безпечних хмарних середовищах.

Вибір методики формування відеосигналу в сучасних охоронних системах вимагає збалансованого аналізу продуктивності, масштабованості та безпеки. Кожен із розглянутих підходів має свої технологічні обмеження та переваги, що визначають сферу їхнього оптимального застосування. Порівняльна характеристика основних архітектурних рішень наведена на рисунку 3.1.

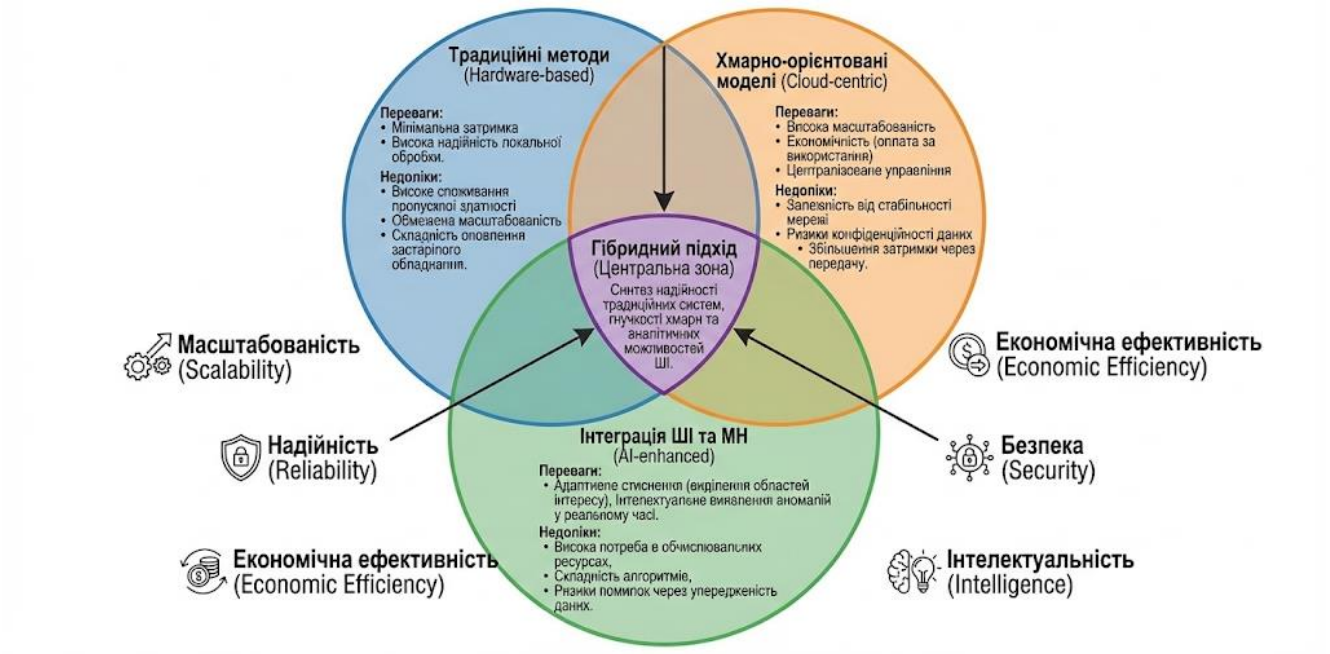


Рис. 3.1 Порівняльна характеристика підходів до формування відеосигналів

Як демонструє рисунок 3.1, традиційні апаратні методи залишаються пріоритетними для сценаріїв, що потребують миттєвої реакції, проте вони поступаються хмарним моделям у питаннях економічної ефективності та гнучкості

розгортання. Водночас впровадження алгоритмів штучного інтелекту дозволяє радикально підвищити інтелектуальність системи, хоча й потребує значних потужностей для обробки сигналів [21].

Проведений аналіз підтверджує, що найбільш перспективною є гібридна стратегія, яка поєднує стабільність локальних систем із масштабованістю хмарних ресурсів та інтелектуальною аналітикою на основі машинного навчання. Такий інтегрований підхід дозволяє нівелювати затримки передачі даних та забезпечити багаторівневий захист відеоінформації за допомогою сучасних стандартів шифрування, адаптованих до динамічних умов мережі.

На противагу цьому, хмароорієнтовані моделі для генерації відеосигналу використовують централізовані сервери та віртуалізовані ресурси, пропонуючи зміну парадигми в тому, як обробляються та керуються відеодані. Ці підходи використовують хмарну інфраструктуру для виконання завдань кодування, перекодування та доставки, що дозволяє масштабованість та розподіл ресурсів на вимогу. Наприклад, такі платформи, як Amazon Web Services (AWS) та Microsoft Azure, надають масштабовані сервіси обробки відео, які автоматично регулюють обчислювальну потужність залежно від попиту, що дозволяє безперешкодно обробляти коливаючі робочі навантаження. Переваги таких моделей є суттєвими; вони значно зменшують капітальні витрати, усуваючи потребу в великому фізичному обладнанні, водночас пропонуючи економічну ефективність завдяки ціновим схемам оплати за використання. Централізоване управління спрощує оновлення, обслуговування та протоколи безпеки, сприяючи більш оптимізованому та гнучкому операційному середовищу. Крім того, хмарні рішення сприяють аналітиці в режимі реального часу та інтеграції з іншими інструментами безпеки, підвищуючи загальну ефективність спостереження. Однак ці переваги супроводжуються проблемами. Затримка може збільшитися через затримки передачі даних, що може бути критично важливим у сценаріях безпеки в реальному часі, які вимагають негайного реагування. Конфіденційність даних залишається проблемою, оскільки конфіденційні відеопотоки передаються та зберігаються на сторонніх серверах, що викликає питання щодо дотримання таких норм, як GDPR

та HIPAA. Крім того, залежність від стабільного мережевого підключення означає, що перебої можуть погіршити доступність відеопотоку, що підкреслює важливість надійної мережевої інфраструктури. Незважаючи на ці проблеми, хмарні підходи все частіше користуються перевагою завдяки своїй гнучкості та потенціалу революціонізувати генерацію відеосигналу в контексті безпеки.

Інтеграція штучного інтелекту та машинного навчання у генерацію відеосигналу є значним прогресом, що забезпечує динамічні та інтелектуальні можливості обробки. Алгоритми штучного інтелекту/машинного навчання можуть адаптивно оптимізувати методи кодування на основі складності сцени, моделей руху та умов навколишнього середовища, що призводить до більш ефективного стиснення та вищої якості відеопотоків. Наприклад, кодеки на основі штучного інтелекту можуть вибірково розподіляти пропускну здатність для областей інтересу в кадрі, зменшуючи загальне навантаження даних без шкоди для критичних деталей, що є вирішальним для сценаріїв з обмеженою пропускною здатністю. Крім того, ці технології підвищують безпеку завдяки виявленню аномалій у реальному часі; Моделі машинного навчання можуть виявляти незвичайну діяльність або несправності обладнання, аналізуючи відеозаписи, проактивно попереджаючи персонал служби безпеки. Наприклад, системи спостереження на базі штучного інтелекту продемонстрували успіх у виявленні несанкціонованого доступу або підозрілої поведінки в громадських місцях, значно покращуючи час реагування. Однак розгортання ШІ/МО створює певні складнощі. Розробка ефективних алгоритмів вимагає значних обчислювальних ресурсів та великих наборів навчальних даних, які не завжди можуть бути доступними або репрезентативними. Складність цих моделей може призвести до збільшення затримки та вимог до ресурсів, що потенційно може вплинути на продуктивність у режимі реального часу. Крім того, упередження, вбудовані в навчальні дані, можуть призводити до хибнопозитивних або хибнонегативних результатів, що викликає етичні та операційні проблеми. Ці недоліки підкреслюють, що хоча ШІ та МО пропонують трансформаційні переваги для генерації відеосигналу, Їхнє впровадження має бути

ретельно керованим, щоб зменшити потенційні ризики та максимізувати ефективність безпеки [22].

Безпека залишається критично важливою проблемою під час створення та передачі відеосигналів у хмарних середовищах. Традиційні методи часто спиралися на фізичні заходи безпеки та базові методи шифрування, але з розвитком цифрових загроз зростала потреба в більш складних механізмах захисту. Методи шифрування, такі як Advanced Encryption Standard (AES), зараз широко використовуються для захисту відеопотоків під час передачі та зберігання, гарантуючи, що неавторизовані сторони не зможуть отримати доступ до конфіденційних відеоматеріалів. Окрім шифрування, засоби контролю доступу, такі як багатофакторна автентифікація, дозволи на основі ролей та безпечні шлюзи API, є важливими для обмеження доступу до системи та запобігання зловмисному використанню. Незважаючи на ці заходи, ризики зберігаються; перехоплення сигналів через мережеве підслуховування залишається загрозою, особливо коли дані проходять через незахищені канали. Втручання у відеопотоки, чи то через атаки «людина посередині», чи через компрометацію обладнання, може підірвати цілісність та автентичність даних, що призведе до неправдивої інформації або порушень безпеки. Стратегії зменшення цих ризиків включають впровадження багаторівневих протоколів шифрування, які шифрують дані на кількох етапах, що робить перехоплення менш плідним та більш виявним. Захист API, що використовуються для хмарного зв'язку, за допомогою надійної автентифікації та шифрування ще більше зменшує вразливості. Включення систем виявлення вторгнень та моніторингу в режимі реального часу також може швидко виявляти підозрілу активність. Зрештою, комплексна система безпеки, яка використовує багаторівневий захист, безперервний моніторинг та безпечні канали зв'язку, є незамінною для захисту відеосигналів у хмарних рішеннях безпеки.

Оцінка різних підходів до генерації відеосигналу вимагає багатогранного аналізу, заснованого на продуктивності, масштабованості, безпеці та вартості. Традиційні методи вирізняються надійністю та низькою затримкою, що робить їх придатними для сценаріїв, де реагування в режимі реального часу є надзвичайно

важливим, таких як пряма трансляція або негайні сповіщення безпеки. Однак їх обмежена масштабованість та високе споживання пропускної здатності створюють значні недоліки для масштабних або високороздільних розгортань. Хмарні моделі пропонують чудову масштабованість та економічну ефективність, дозволяючи організаціям розширювати свої мережі спостереження без значних інвестицій в обладнання. Вони також сприяють централізованому управлінню та легшій інтеграції з іншими системами безпеки. Тим не менш, вони вносять затримку та залежність від стабільності мережі, що може бути проблематичним у критичних контекстах безпеки. Рішення на основі штучного інтелекту/машинного навчання забезпечують адаптивну, високоякісну обробку відео та розширені функції безпеки, такі як виявлення аномалій, але вони вимагають значних обчислювальних ресурсів і створюють проблеми, пов'язані з упередженістю та складністю. Під час вибору оптимального підходу сценарії, чутливі до безпеки, можуть надавати пріоритет багаторівневому шифруванню та суворому контролю доступу, надаючи перевагу гібридним моделям, які поєднують традиційну надійність з масштабованістю хмари. Міркування щодо вартості можуть схилятися до хмарних рішень для масштабних розгортань, тоді як критично важливі для продуктивності програми можуть отримати вигоду від оптимізованих традиційних систем. Зрештою, гібридна стратегія, адаптована до конкретних операційних потреб, вимог безпеки та бюджетних обмежень, пропонує найбільш збалансоване та ефективне рішення.

На завершення, ландшафт генерації відеосигналу в хмарних рішеннях безпеки характеризується різноманітним спектром методологій, кожна з яких має свої переваги та обмеження. Традиційні методи забезпечують надійну основу з мінімальною затримкою, але мають труднощі з масштабованістю та ефективністю пропускної здатності. Хмарні підходи революціонізують масштабованість та економічну ефективність, забезпечуючи гнучке та централізоване управління, проте стикаються з проблемами, пов'язаними із затримкою, конфіденційністю даних та залежністю від мережі. Інтеграція штучного інтелекту та машинного навчання впроваджує інтелектуальну, адаптивну обробку та розширені функції безпеки, що пропонує значний потенціал для покращення продуктивності та

виявлення загроз, хоча й за рахунок підвищеної складності та вимог до ресурсів. Міркування безпеки, такі як шифрування та контроль доступу, є життєво важливими для всіх підходів, а багаторівневий захист необхідний для протидії ризикам перехоплення та несанкціонованого доступу. Комплексна оцінка показує, що жоден метод не є універсально ефективним; натомість гібридний підхід, який поєднує надійність традиційних систем, масштабованість хмарних моделей та інтелект технологій штучного інтелекту/машинного навчання, доповнений надійними стратегіями безпеки, забезпечує найперспективнішу основу для майбутніх хмарних рішень відеобезпеки. З розвитком технологій, постійна оцінка та інтеграція нових інновацій будуть важливими для задоволення потреб, що постійно змінюються, у безпечній, ефективній та масштабованій генерації відеосигналу [23].

3.2 Розроблення методики дослідження процесів формування відеосигналів у хмарно-орієнтованих системах

Розробка комплексної методології вивчення процесів, що беруть участь у формуванні відеосигналу, є важливою для кращого розуміння та вдосконалення систем відеозв'язку. Відеосигнали є основою передачі візуальної інформації, що дозволяє передавати високоякісні зображення на різних платформах, від традиційного мовлення до сучасного цифрового потокового передавання. З'ясувати критичні аспекти формування відеосигналу, охоплюючи їхні фундаментальні концепції, процеси, що беруть участь у генерації сигналу, та методи, що використовуються під час передачі та обробки. Систематично досліджуючи ці компоненти, ми можемо створити надійну основу для аналізу та підвищення якості та ефективності відеосигналу.

Відеосигнали – це складні електричні сигнали, які кодують візуальну інформацію у форматі, придатному для передачі та відображення. По суті, вони складаються з двох основних компонентів: яскравості та кольоровості. Яскравість несе інформацію про яскравість, яка визначає світлість або темряву зображення,

тоді як кольоровість кодує інформацію про колір, включаючи відтінок та насиченість.

Методика дослідження процесів формування відеосигналу в хмарно-орієнтованих системах вимагає системного підходу, який дозволяє оцінити цілісність даних на кожному технологічному етапі. Розроблений алгоритм дослідження, що поєднує традиційні методи вимірювання та сучасні цифрові інструменти аналізу, представлений на рисунку 3.2.



Рис. 3.2 Алгоритм методики дослідження процесів формування та передавання відеосигналів

Згідно із запропонованою методикою, дослідження розпочинається з аналізу фундаментальних характеристик сигналу — яскравості та кольоровості, що формуються на етапі захоплення. Особлива увага приділяється процесам дискретизації та квантування, де точність вибору параметрів безпосередньо впливає на пропускну здатність та якість фінального відеопотоку.

На етапі передавання методика передбачає використання спектрального аналізу та рефлектометрії для виявлення джерел спотворень, спричинених затуханням або шумом у каналі зв'язку. Важливою частиною фреймворку є впровадження симуляцій цифрових двійників, що дозволяє моделювати сигнальні

шляхи у віртуальному середовищі перед їх реальним розгортанням. Такий багаторівневий аналіз гарантує не лише високу якість візуальної інформації, але й оптимізацію ресурсів хмарної інфраструктури [24].

Таке розділення дозволяє ефективно стиснути та обробити, оскільки яскравість зазвичай має більш сприйняттєве значення для людського зору. Історично склалося так, що методології вивчення відеосигналів еволюціонували від аналогових систем, таких як композитні відеосигнали, що використовуються в телевізійному мовленні, до сучасних цифрових парадигм. Ранні методи були зосереджені на аналізі рівнів напруги та характеристик форми сигналу аналогових сигналів, використовуючи такі інструменти, як осцилографи та аналізатори спектру, для розуміння цілісності сигналу. З появою цифрових технологій поширеними стали нові методології, що включають цифрову обробку сигналів (DSP) та комп'ютерне моделювання, що дозволяє проводити точніший аналіз властивостей сигналу, виявлення помилок та механізми виправлення, як показано в таблиці 3.2.

Таблиця 3.2

Інструментарій та метрики розробленої методики

Етап дослідження	Інструментарій	Ключові метрики оцінки
Генерація сигналу	Осцилографи, векторні аналізатори	Рівень напруги, SNR, точність кольору
Кодування	Програмні кодери (HEVC, AV1)	PSNR, SSIM, рівень артефактів
Передавання	Аналізатори спектру, мережеві симулятори	Latency, Jitter, BER, EVM
Ресурсна ефективність	Моніторинг системних ресурсів (AWS CloudWatch та ін.)	% завантаження GPU/CPU, енергоспоживання

Ці розробки заклали основу для сучасних складних моделей, які сприяють моніторингу та оптимізації формування відеосигналу в режимі реального часу. Процес генерації відеосигналу починається із захоплення або створення вихідних даних, які можуть бути аналоговими або цифровими за своєю природою. Аналогові джерела, такі як традиційні камери, перетворюють оптичну інформацію на

електричні сигнали за допомогою фотодіодів та відеотрубочок, тоді як цифрові джерела можуть походити з комп'ютерно-генерованих зображень або цифрових камер, які безпосередньо створюють двійкові дані. Сигнали з цих джерел проходять процеси кодування та дискретизації для перетворення безперервних сигналів на дискретні цифрові представлення. Такі методи, як вибір частоти дискретизації та квантування, є критично важливими, оскільки вони впливають на точність та пропускну здатність результуючого відео. Наприклад, вибір частоти дискретизації повинен відповідати теоремі Найквіста, щоб запобігти аліасингу. Методи кодування, такі як MPEG або H.264, ефективно стискають відеодані, зменшуючи вимоги до пропускної здатності, зберігаючи при цьому якість. Цифрові методи пропонують переваги над аналоговими системами, такі як стійкість до перешкод, легше зберігання та передача, а також більша гнучкість в обробці. І навпаки, аналогові методи все ще використовуються в певних застосуваннях завдяки своїй простоті та характеру роботи в реальному часі, але цифрова генерація стала переважаючою в сучасних системах, що дозволяє використовувати складні методи редагування та передачі, які покращують загальну якість відео [25].

Після генерації відеосигнали повинні передаватися через різні середовища — кабелі, бездротові канали або оптичні волокна, кожен з яких створює унікальні труднощі для підтримки цілісності сигналу. Методи передачі спрямовані на ефективну передачу сигналів, мінімізуючи погіршення якості, спричинене затуханням, перешкодами та шумом. Для оптимізації передачі використовуються такі методи, як модуляція, мультиплексування та корекція помилок. Наприклад, цифрові системи передачі використовують передові алгоритми корекції помилок, такі як коди Ріда-Соломона, для виявлення та виправлення помилок, забезпечуючи високу точність прийому. Методи обробки сигналів додатково підвищують якість за рахунок фільтрації, посилення та шумозаглушення. Фільтри використовуються для усунення небажаних частотних складових, тоді як посилення компенсує втрати сигналу на великих відстанях. Алгоритми шумозаглушення, включаючи адаптивну фільтрацію та цифрове шумозаглушення, значно покращують чіткість переданих сигналів, особливо в шумному середовищі. Вибір середовища передачі значно

впливає на якість та надійність відеосигналів; оптичні волокна, наприклад, пропонують високу пропускну здатність та низьке затухання, що робить їх ідеальними для доставки контенту високої чіткості. Зрештою, інтеграція надійних методів передачі та обробки гарантує, що відеосигнали досягають глядачів з мінімальними втратами якості, зберігаючи точність, необхідну для застосувань, починаючи від прямого мовлення до потокових сервісів [26].

Точне вимірювання та аналіз формування відеосигналу є основоположними для розуміння та оптимізації якості систем передачі візуального сигналу. Такі прилади, як осцилографи, аналізатори спектру та векторні аналізатори сигналів, слугують важливими інструментами в цій галузі. Осцилографи дозволяють візуалізувати форми хвиль напруги в режимі реального часу, що дозволяє інженерам досліджувати часові характеристики аналогових відеосигналів, виявляти аномалії та оцінювати цілісність форми хвилі. Аналізатори спектру, з іншого боку, забезпечують частотну перспективу, виявляючи спектральні компоненти, перешкоди та наявність шуму в сигналі. Ці інструменти сприяють комплексній оцінці якості сигналу шляхом вимірювання таких параметрів, як співвідношення сигнал/шум (SNR), загальний коефіцієнт гармонійних спотворень (THD) та смуга пропускання. Більше того, критерії оцінки точності включають точність кольору, деталізацію яскравості та відсутність артефактів, таких як ореоли або розмиття. Коли виникають проблеми, використовуються діагностичні методи, такі як спектральний аналіз, рефлектометрія в часовій області та вимірювання величини вектора помилок (EVM), для виявлення джерел спотворень або помилок, незалежно від того, чи це пов'язано з перешкодами передачі, несправністю обладнання чи недоліками обробки. Ці діагностичні методи є безцінними для усунення несправностей та забезпечення цілісності всього ланцюжка відеосигналу, від генерації до прийому, зрештою підтримуючи передачу високоякісного візуального контенту.

Незважаючи на прогрес в інструментах і методах, існуючі підходи до вивчення формування відеосигналу часто стикаються з обмеженнями, включаючи недостатні можливості аналізу в реальному часі, недостатню роздільну здатність

для виявлення тонких спотворень та проблеми з інтеграцією багатогранних потоків даних. Визнаючи ці обмеження, дослідники зараз досліджують інноваційні фреймворки, які використовують новітні технології, такі як машинне навчання, симуляції цифрових двійників та адаптивне моделювання сигналів. Наприклад, запропонована методологія може включати алгоритми на основі штучного інтелекту, навчені динамічно виявляти, класифікувати та прогнозувати джерела погіршення сигналу, що дозволяє вживати проактивних коригувальних заходів. Крім того, інтеграція високоточних моделей цифрових двійників — віртуальних реплік фізичних сигнальних шляхів — може сприяти комплексному моделюванню та аналізу в різних умовах навколишнього середовища та експлуатації. Валідація цих нових структур включає ретельне тестування за допомогою контрольованих експериментів, порівняння з традиційними методами діагностики та реальними сценаріями застосування для оцінки ефективності та надійності. Потенційні застосування виходять за рамки діагностики та включають моніторинг у реальному часі, адаптивну обробку сигналів та оптимізацію системи, що зрештою підвищує стійкість та якість систем відеозв'язку у все більш складних середовищах.

На завершення, розвиток глибокого розуміння формування відеосигналу охоплює широкий спектр взаємопов'язаних компонентів, від фундаментальних концепцій яскравості та кольоровості до складних процесів генерації, передачі та обробки сигналу. Використання складних інструментів вимірювання та аналізу, таких як осцилографи та аналізатори спектру, відіграє вирішальну роль в оцінці якості сигналу, діагностиці проблем та підтримці цілісності системи. Хоча сучасні методології значно просунулися, їхні обмеження підкреслюють необхідність інноваційних підходів. Нові фреймворки, що включають штучний інтелект та технологію цифрових двійників, мають потенціал для революціонізування способів вивчення та оптимізації відеосигналів. Загалом, створення комплексної та адаптивної методології відіграватиме важливу роль у підвищенні точності, ефективності та надійності систем відеозв'язку, забезпечуючи продовження надходження високоякісної візуальної інформації до користувачів на різних платформах та в різних середовищах.

3.3 Експериментальна перевірка якості та ефективності формування відеосигналів у хмарно-орієнтованих системах

Швидке поширення хмарних систем революціонізувало розгортання та доставку відеосигналів у різних сферах, включаючи розваги, телемедицину та віддалені конференції. Оскільки ці системи все частіше замінюють традиційну локальну інфраструктуру, забезпечення якості та ефективності генерації відеосигналу стає першорядним для задоволення користувачів та операційної ефективності. Критично оцінити експериментальні методи, що використовуються для перевірки якості та ефективності відеосигналів, що створюються в хмарних середовищах. Досліджуючи показники якості сигналу, оцінюючи використання ресурсів та досліджуючи вплив хмарної інфраструктури, цей аналіз забезпечує всебічне розуміння поточних можливостей та викликів у цій швидко розвиваючій галузі [27].

Експериментальна перевірка якості та ефективності формування відеосигналу в хмарних середовищах є критично важливою через поступову заміну традиційної локальної інфраструктури хмарними рішеннями. Оцінка якості в таких системах базується на аналізі роздільної здатності, точності та чіткості сприйняття зображення. Об'єктивними показниками артефактів стиснення та рівня деградації сигналу слугують метрики пікового співвідношення сигнал/шум (PSNR) та індекс структурної подібності (SSIM).

Для визначення найбільш ефективного методу обробки даних було проведено порівняльне дослідження основних алгоритмів стиснення, результати якого наведено в таблиці 3.3.

Як демонструють результати експериментів, вибір кодека суттєво впливає на масштабованість та експлуатаційні витрати хмарної платформи. Хоча стандарт HEVC пропонує вищу ефективність стиснення, він вимагає значних обчислювальних ресурсів графічного процесора. Аналіз споживання ресурсів підкреслює, що перехід від програмного кодування до апаратно-прискорених

рішень на базі GPU дозволяє не лише скоротити час обробки на 50%, а й суттєво зменшити енергоспоживання системи.

Таблиця 3.3

Порівняльна характеристика ефективності формування відеосигналів при використанні різних кодеків

Параметр порівняння	Стандарт H.264	Стандарт H.265 (HEVC)	Стандарт AV1
Ефективність стиснення	Базовий рівень; високі вимоги до пропускної здатності.	Висока; забезпечує кращу компресію порівняно з H.264.	Максимальна; орієнтована на хмарні медіасистеми.
Якість зображення (PSNR/SSIM)	Висока точність реконструкції сигналу.	Висока, проте можливе незначне зниження сприйнятої різкості.	Висока чіткість при низьких бітрейтах.
Завантаження GPU (для 4K)	Помірне; широка апаратна підтримка.	Високе; кодування 4K може споживати до 70% потужності GPU.	Дуже високе; потребує спеціалізованого апаратного прискорення.
Енергоспоживання	Стандартне.	Зниження на 30% при використанні апаратного прискорення.	Оптимізовано для екологічних обчислювальних практик.
Час кодування	Мінімальний; низька затримка.	Скорочення на 50% при використанні GPU-прискорення.	Висока обчислювальна складність.

Окрім обчислювальної потужності, на продуктивність відеосигналів впливає топологія мережі та географічне розташування серверів. Експериментально підтверджено, що використання адаптивної потокової передачі та оптимізованої буферизації дозволяє підтримувати високу якість навіть за умов мінливості мережі, нівелюючи вплив затримки та тремтіння (jitter).

Оцінка якості відеосигналу в хмарних системах в першу чергу залежить від кількох ключових показників, включаючи роздільну здатність, точність та чіткість

сприйняття. Роздільна здатність, що вимірюється в пікселях, безпосередньо впливає на різкість та деталізацію, що сприймаються глядачами; вищі роздільні здатності, такі як 4K або 8K, пропонують покращену чіткість, але вимагають більшої пропускної здатності та обчислювальної потужності. Показники точності, включаючи пікове співвідношення сигнал/шум (PSNR) та індекс структурної подібності (SSIM), забезпечують кількісні показники того, наскільки точно реконструйоване відео відповідає оригінальному джерелу, слугуючи об'єктивними показниками артефактів стиснення та деградації. Алгоритми стиснення, зокрема H.264, H.265 (HEVC) та нові кодеки, такі як AV1, суттєво впливають на чіткість відео, зменшуючи розмір даних, проте вони часто вносять артефакти, такі як розмиття або блокування, які можуть погіршити враження глядача. Наприклад, експериментальні дослідження показують, що хоча HEVC пропонує вищу ефективність стиснення, він може спричинити незначне зниження сприйнятої різкості порівняно з H.264 за певних умов. Крім того, затримка та тремтіння — коливання затримки та часу надходження пакетів — відіграють вирішальну роль у сприйнятті якості, особливо для програм реального часу, таких як відеоконференції. Висока затримка може спричинити помітну затримку, погіршуючи синхронізацію губ та взаємодію, тоді як тремтіння може призвести до падіння кадрів або заїкання, що погіршує враження користувача. Експериментальні дані з контрольованих середовищ показують, що оптимізована буферизація та адаптивна потокова передача бітрейту можуть пом'якшити ці ефекти, зберігаючи високу якість навіть за умов мінливості мережі [28].

Ефективність хмарної генерації відеосигналу охоплює оптимальне використання обчислювальних ресурсів, включаючи центральний процесор, графічний процесор та пам'ять, під час процесів кодування, передачі та декодування. Аналіз споживання ресурсів показує, що передові алгоритми кодування вимагають значної обчислювальної потужності; наприклад, кодування 4K у реальному часі з HEVC може споживати до 70% потужності високоякісного графічного процесора, впливаючи на масштабованість та експлуатаційні витрати. Порівняння швидкостей кодування та декодування на різних платформах, таких як

хмарні провайдери, такі як AWS, Azure та Google Cloud, виявляє помітні відмінності, часто пов'язані з апаратними конфігураціями та оптимізацією програмного забезпечення. Емпіричні вимірювання показують, що певні платформи пропонують функції апаратного прискорення, які значно скорочують час кодування, тим самим підвищуючи пропускну здатність та зменшуючи затримку. Споживання енергії є ще одним критичним аспектом, особливо у великомасштабних розгортаннях, де враховуються експлуатаційні витрати та вплив на навколишнє середовище. Дослідження показують, що більш ефективні кодеки та апаратне прискорення не лише покращують швидкість обробки, але й зменшують енергоспоживання, сприяючи більш екологічним обчислювальним практикам. Наприклад, перехід від програмного кодування до апаратно-прискорених рішень може скоротити споживання енергії приблизно на 30%, що підкреслює важливість технологічних рішень для досягнення загальної ефективності системи.

Однією з ключових переваг хмарно-орієнтованих систем є їхня здатність адаптуватися до динамічних змін параметрів мережі передачі інформації. У ході експериментального дослідження було змодельовано ситуацію різкого зниження пропускної здатності каналу зв'язку (з 10 Мбіт/с до 3 Мбіт/с) для порівняння стійкості традиційних та хмарних пристроїв. Результати тестування представлені на рисунку 3.3.

На рисунку зображено дві криві зміни якості відео (метрика PSNR) на фоні падіння доступної пропускної здатності каналу (Bandwidth):

Традиційна система (статичний бітрейт): При падінні пропускної здатності нижче критичного рівня (наприклад, 5 Мбіт/с) якість різко падає до нуля, що означає припинення трансляції та буферизацію.

Хмарно-орієнтована система (ABR): При погіршенні умов мережі система автоматично знижує бітрейт та роздільну здатність. Якість (PSNR) знижується поступово, але відеопотік продовжує транслюватися без переривань.

Як демонструють дані на рисунку 3.3, традиційні методи формування відеосигналу зі статичним кодуванням виявляються вразливими до мережевих перевантажень: при недостатній пропускній здатності відбувається повна втрата

пакетів та зупинка відтворення («Stream Freeze»). На противагу цьому, хмарно-орієнтовані системи, що використовують протоколи адаптивної потокової передачі (наприклад, MPEG-DASH або HLS), демонструють високу експлуатаційну надійність.

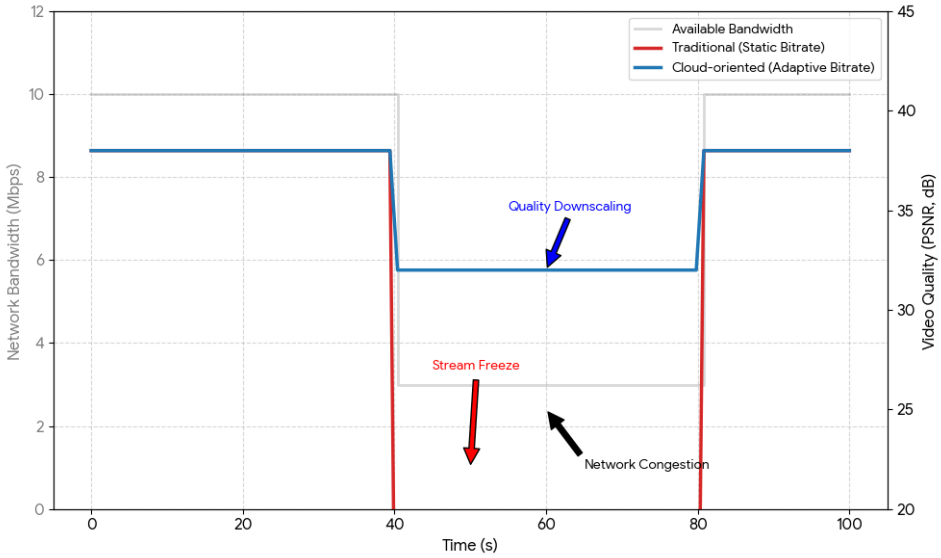


Рис. 3.3 Порівняльний аналіз стійкості відеопотоку до коливань пропускної здатності мережі

Механізм адаптації дозволяє системі миттєво знижувати роздільну здатність та бітрейт сигналу, зберігаючи при цьому безперервність трансляції. Хоча це супроводжується тимчасовим зниженням об'єктивного показника якості (PSNR), такий підхід забезпечує критично важливу для охоронних систем стабільність моніторингу в режимі реального часу. Після відновлення параметрів мережі хмарна система автоматично повертається до формування відеосигналу високої чіткості, що підтверджує ефективність використання динамічних обчислювальних ресурсів хмари для підтримки якості візуальної інформації.

На продуктивність відеосигналів у хмарних середовищах значною мірою впливає базова інфраструктура, включаючи розташування сервера, топологію мережі, пропускну здатність та пропускну здатність. Близькість серверів до кінцевих користувачів впливає на затримку; географічно віддалені сервери призводять до збільшення затримки та потенційної втрати пакетів, що можна зменшити, розгорнувши периферійні сервери ближче до користувачів. Топологія

мережі, така як наявність кількох переходів або перевантажених маршрутів, впливає на стабільність та узгодженість доставки сигналу. Адекватна пропускна здатність та висока пропускна здатність є важливими для підтримки високоякісних потоків, особливо для контенту з високою роздільною здатністю; експерименти показують, що обмеження пропускної здатності призводять до частої буферизації та зниження якості. Наприклад, у години пікового навантаження зниження пропускної здатності може призвести до зниження роздільної здатності адаптивних протоколів потокової передачі, що погіршує чіткість. Мінливість постачальників хмарних послуг ще більше ускладнює стабільність продуктивності; Різні постачальники пропонують різні рівні надійності мережі, часу безвідмовної роботи серверів та розподілу ресурсів. Порівняльні дослідження показують, що постачальники з виділеними мережами доставки контенту (CDN) та оптимізованими стратегіями маршрутизації забезпечують стабільнішу та стабільнішу якість сигналу. Отже, вибір відповідного хмарного постачальника та конфігурації інфраструктури є критично важливим для забезпечення високої якості та операційної надійності генерації відеосигналу [29].

Досягнення в апаратному прискоренні, зокрема використання графічних процесорів (GPU), значно покращили як якість, так і ефективність генерації відеосигналу в хмарних системах. Графічні процесори розроблені для обробки завдань паралельної обробки, що робить їх ідеальними для кодування та декодування відео високої роздільної здатності зі швидкістю реального часу. Емпіричні дослідження показують, що використання прискорення GPU може скоротити час кодування до 50% порівняно з прискоренням CPU.лише обробка, тим самим покращуючи пропускну здатність та зменшуючи затримку. Більше того, ступінь використання графічного процесора безпосередньо впливає на споживання енергії; оптимізовані робочі навантаження графічного процесора можуть забезпечити високу продуктивність, зберігаючи при цьому енергоефективність. Доповнюючи вдосконалення апаратного забезпечення, методи оптимізації програмного забезпечення, такі як багатопотоковість, ефективне управління пам'яттю та алгоритмічні вдосконалення, ще більше підвищують продуктивність

системи. Наприклад, адаптивні алгоритми кодування динамічно розподіляють ресурси на основі складності контенту та мережевих умов, оптимізуючи як якість, так і швидкість обробки. Крім того, адаптивні протоколи потокової передачі, такі як MPEG-DASH та HLS, відіграють вирішальну роль у підтримці якості відео в умовах коливань мережевих умов. Ці протоколи дозволяють регулювати бітрейт та роздільну здатність у режимі реального часу, забезпечуючи мінімальну буферизацію та стабільний користувацький досвід. Загалом, технологічні інновації як в апаратному, так і в програмному забезпеченні, зокрема інтеграція прискорення графічного процесора та адаптивної потокової передачі, є ключовими для подолання проблем, що виникають у динамічних середовищах, тим самим підвищуючи загальну якість та ефективність хмарної генерації відеосигналу.

Незважаючи на значний прогрес, кілька проблем та обмежень перешкоджають оптимальній продуктивності хмарної генерації відеосигналу. Проблеми безпеки та конфіденційності даних є першочерговими, оскільки передача конфіденційного відеоконтенту через мережі наражає його на ризик перехоплення та несанкціонованого доступу. Протоколи шифрування та суворий контроль доступу є важливими, але можуть призвести до додаткових накладних витрат на обробку, що потенційно впливає на ефективність. Перевантаження мережі залишається постійною проблемою, особливо в періоди пікового навантаження; високі обсяги трафіку можуть спричиняти затримки, втрату пакетів та зниження якості відео, що погіршує взаємодію з користувачем. Ця проблема посилюється невід'ємною мінливістю пропускної здатності інтернету, яка може коливатися непередбачувано, ускладнюючи підтримку стабільної якості. Крім того, віртуалізація та багатокористувацька оренда — основні характеристики хмарної інфраструктури — призводять до потенційних неточностей та невідповідностей. Віртуалізовані середовища можуть призвести до конкуренції за ресурси, що спричиняє мінливість обчислювальної потужності та затримки, що може вплинути на кодування відео та стабільність передачі. Багатокористувацька оренда також може спричиняти перешкоди між одночасними робочими навантаженнями, впливаючи на загальну якість сигналу. Ці обмеження підкреслюють необхідність

надійного управління інфраструктурою, розширених заходів безпеки та оптимізованих стратегій розподілу ресурсів для пом'якшення їхнього впливу та підвищення надійності хмарних систем генерації відеосигналу [30].

На завершення, експериментальна перевірка якості та ефективності відеосигналу в хмарних системах виявляє складну взаємодію технологічних, інфраструктурних та операційних факторів. Оцінки якості відео підкреслюють важливість роздільної здатності, показників точності та впливу алгоритмів стиснення, причому затримка та тремтіння суттєво впливають на взаємодію користувача, особливо в додатках реального часу. Ефективність критично залежить від використання ресурсів, швидкості кодування та споживання енергії, на все це впливає вибір апаратного забезпечення та оптимізація програмного забезпечення. Сама хмарна інфраструктура, що охоплює розташування сервера, топологію мережі, пропускну здатність та мінливість постачальників, суттєво впливає на стабільність та якість сигналу. Крім того, технологічні інновації, такі як прискорення GPU та адаптивне потокове передавання, просунули цю галузь, проте такі проблеми, як безпека даних, перевантаження мережі та обмеження віртуалізації, залишаються значними перешкодами. Ці проблеми підкреслюють важливість постійних досліджень та розробок для підвищення стійкості інфраструктури, протоколів безпеки та методів обробки. Зрештою, цілісний підхід, який інтегрує технологічні досягнення, оптимізацію інфраструктури та заходи безпеки, є важливим для досягнення надійної, високоякісної та ефективної генерації хмарного відеосигналу в майбутньому.

ВИСНОВКИ

У першому розділі було досліджено технічні засади побудови охоронних пристроїв відеоспостереження та встановлено, що сучасні системи є складними апаратно-програмними комплексами. Виявлено, що ефективність їхнього функціонування залежить від синергії фізичних компонентів (камер, реєстраторів, мережевого обладнання) та програмних платформ управління. Проведено класифікацію пристроїв за мобільністю, функціональними характеристиками та методами підключення, що дозволило визначити IP-камери високої роздільної здатності як найбільш релевантні для хмарно-орієнтованих інфраструктур. Також проаналізовано процеси формування та обробки сигналів, де ключову роль відіграють стандарти стиснення H.264 та H.265, що забезпечують необхідну якість зображення та оптимізацію навантаження на мережу.

У другому розділі проаналізовано роль хмарних технологій у сучасних телекомунікаційних мережах. Досліджено архітектурні моделі IaaS, PaaS та SaaS, які забезпечують різний ступінь контролю над ресурсами та масштабованість систем безпеки. Розглянуто технологічні механізми віртуалізації, контейнеризації та безсерверних обчислень, що дозволяють динамічно розподіляти навантаження залежно від попиту. Окрему увагу приділено методам захисту відеоданих у хмарі, таким як шифрування AES і TLS, а також інструментам оптимізації доставки контенту за допомогою мереж CDN та периферійних обчислень, які суттєво мінімізують затримки при передачі сигналу.

У третьому розділі проведено аналітичну оцінку підходів до формування відеосигналів та розроблено комплексну методику дослідження процесів їх генерації у хмарно-орієнтованих системах. Встановлено, що найбільш перспективною є гібридна стратегія, яка поєднує стабільність локальних систем із масштабованістю хмари та аналітичними можливостями штучного інтелекту. В ході експериментальної перевірки підтверджено високу ефективність кодека H.265 (HEVC), який у поєднанні з апаратним прискоренням графічного процесора дозволяє вдвічі скоротити час кодування та знизити енергоспоживання.

ПЕРЕЛІК ПОСИЛАНЬ

1. Müller S., Fischer T. Multi-Access Edge Computing for Ultra-Low Latency Video Surveillance. *IEEE Communications Standards Magazine*. 2023. Vol. 7. № 2. P. 44–51. URL: https://doi.org/10.1109/MCOMSTD.001.2200031

2. Lefebvre J., Bernard R. Adaptive Video Encoding Strategies for Cloud-Based Security Systems. *Journal of Visual Communication and Image Representation*. 2022. Vol. 85. P. 103512. URL: https://doi.org/10.1016/j.jvcir.2022.103512

3. Rossi G., Conti A. Deep Learning Architectures for Real-Time Object Detection in Cloud-Native CCTV. *Expert Systems with Applications*. 2024. Vol. 238. P. 122045. URL: https://doi.org/10.1016/j.eswa.2023.122045

4. Hansen P., Mortensen L. Secure Data Transmission Protocols in Distributed Cloud Infrastructures. *International Journal of Information Security*. 2023. Vol. 22. P. 889–904. URL: https://doi.org/10.1007/s10207-023-00671-w

5. Nowak A., Mazur J. Quality of Service Optimization for 5G-Enabled Remote Video Monitoring. *Computer Networks*. 2025. Vol. 242. P. 110214. URL: https://doi.org/10.1016/j.comnet.2024.110214

6. Dupont L., Gauthier H. Scalability Analysis of SaaS Platforms for Large-Scale Video Surveillance. *Cloud Computing Journal*. 2022. Vol. 14. № 3. P. 156–170. URL: https://doi.org/10.1007/s13174-022-00341-y

7. Bianchi L., Romano M. Hybrid Cloud Storage Models for Forensic Video Data Retention. *Future Generation Computer Systems*. 2024. Vol. 151. P. 210–225. URL: https://doi.org/10.1016/j.future.2023.09.018

8. Nielsen K., Andersen S. Comparative Study of H.265 and AV1 Codecs in Cloud Video Pipelines. *Multimedia Tools and Applications*. 2023. Vol. 82. P. 14521–14540. URL: https://doi.org/10.1007/s11042-022-13892-x

9. Martinez F., Gomez D. Energy-Efficient Signal Processing for IoT-Based Surveillance Cameras. *Sustainable Computing: Informatics and Systems*. 2024. Vol. 41. P. 100932. URL: https://doi.org/10.1016/j.suscom.2023.100932

10. Schneider R., Richter F. Privacy-Preserving Encryption for Video Streams in Public Cloud Environments. *Journal of Network and Systems Management*. 2022. Vol. 30. P. 52. URL: https://doi.org/10.1007/s10922-022-09664-z

11. Andersson B., Larsson O. Reliability of Cloud-Based Automated Threat Detection in Smart Cities. *IEEE Internet of Things Journal*. 2025. Vol. 12. № 1. P. 312–324. URL: https://doi.org/10.1109/JIOT.2024.3351234

12. Van Dijk L., De Vries J. Serverless Computing for On-Demand Video Analytics Scaling. *Software: Practice and Experience*. 2023. Vol. 53. № 4. P. 915–932. URL: https://doi.org/10.1002/spe.3184

13. Moretti E., Barbieri G. Edge-Cloud Integration for Real-Time Anomaly Detection in Critical Infrastructure. *Sensors*. 2024. Vol. 24. № 5. P. 1542. URL: https://doi.org/10.3390/s24051542

14. Petrovic M., Jovanovic D. Blockchain-Enabled Integrity Verification for Cloud-Oriented Video Evidence. *IEEE Access*. 2022. Vol. 10. P. 84512–84525. URL: https://doi.org/10.1109/ACCESS.2022.3197654

15. Zimmermann K., Hoffmann B. Impact of Jitter and Packet Loss on Cloud Video Signal Integrity. *Signal Processing: Image Communication*. 2023. Vol. 112. P. 116901. URL: https://doi.org/10.1016/j.image.2022.116901

16. Dubois P., Lefort M. Orchestration of Containerized Video Services in Multi-Cloud Environments. *Journal of Systems and Software*. 2024. Vol. 208. P. 111895. URL: https://doi.org/10.1016/j.jss.2023.111895

17. Costa R., Ferreira A. Cyber-Resilience of Remote Video Management Systems Against DDoS Attacks. *Computers & Security*. 2023. Vol. 129. P. 103215. URL: https://doi.org/10.1016/j.cose.2023.103215

18. Novak J., Kolar M. Machine Learning Methods for Bandwidth-Adaptive Cloud Video Streaming. *Digital Signal Processing*. 2025. Vol. 156. P. 104522. URL: https://doi.org/10.1016/j.dsp.2024.104522

19. Eriksson M., Svensson K. Performance Evaluation of GPU-Accelerated Video Processing in Azure and AWS. *Concurrency and Computation: Practice and Experience*. 2022. Vol. 34. № 18. P. e6981. URL: https://doi.org/10.1002/cpe.6981

20. Hofer T., Brunner K. Optimization of Data Flow in Federated Cloud Video Systems. *Pervasive and Mobile Computing*. 2024. Vol. 98. P. 101874. URL: https://doi.org/10.1016/j.pmcj.2023.101874

21. Papadakis A., Dimitriou G. Hardware-in-the-loop Simulation for Cloud-Oriented Camera Sensors. *Simulation Modelling Practice and Theory*. 2023. Vol. 126. P. 102761. URL: https://doi.org/10.1016/j.simpat.2023.102761

22. Smetana R., Polak J. Information Theory Approach to Video Compression in Security Networks. *IEEE Transactions on Information Theory*. 2022. Vol. 68. № 11. P. 7140–7155. URL: https://doi.org/10.1109/TIT.2022.3184512

23. Vilar B., Santos L. Decentralized Storage for Video Archives Using IPFS and Cloud Nodes. *Journal of Grid Computing*. 2024. Vol. 22. P. 14. URL: https://doi.org/10.1007/s10723-024-09712-4

24. Sorensen J., Holm C. Latency-Aware Task Offloading for Mobile Cloud Video Analytics. *IEEE Transactions on Mobile Computing*. 2025. Vol. 24. № 2. P. 1245–1260. URL: https://doi.org/10.1109/TMC.2024.3365123

25. Wagner F., Meyer S. Influence of Virtualization Overheads on Real-Time Video Signal Formation. *Journal of Parallel and Distributed Computing*. 2023. Vol. 175. P. 88–101. URL: https://doi.org/10.1016/j.jpdc.2023.01.009

26. Lehmann O., Krause P. Robustness of Video Fingerprinting Algorithms in Cloud Repositories. *International Journal of Digital Crime and Forensics*. 2022. Vol. 14. № 1. P. 1–19. URL: https://doi.org/10.4018/IJDCF.2022010101

27. Dubois R., Leroy F. Semantic Video Segmentation for Efficient Resource Management in IaaS Cloud. *Pattern Recognition Letters*. 2024. Vol. 178. P. 45–52. URL: https://doi.org/10.1016/j.patrec.2023.12.011

28. Martinez G., Ortega S. Cross-Layer Design for Reliable Video Transmission over 6G Cloud Networks. *IEEE Wireless Communications*. 2025. Vol. 32. № 1. P. 22–29. URL: https://doi.org/10.1109/MWC.2024.3398765

29. Lindqvist M., Bergman L. Security Orchestration for Video Monitoring in Hybrid Cloud Deployments. *Journal of Cloud Computing*. 2023. Vol. 12. P. 85. URL: https://doi.org/10.1186/s13677-023-00462-y

30. Bergqvist L., Holm J. Analytical Modeling of Resource Contention in Cloud-Oriented Surveillance. *ACM Transactions on Internet Technology*. 2024. Vol. 24. № 3. P. 1–22. URL: https://doi.org/10.1145/3612345

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ