ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 9
ВСТУП 12
1. ТЕХНОЛОГІЧНІ ОСНОВИ WI-FI СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ НОВОГО ПОКОЛІННЯ 15
1.1. Архітектура та принципи роботи Wi-Fi камер 15
1.2. Формування та передавання відеосигналу у Wi-Fi мережах 21
1.3. Методи забезпечення якості відеопотоку при Wi-Fi підключенні 26
1.4. Переваги технологій на основі Wi-Fi систем відеоспостереження нового покоління 31
2. МОЖЛИВОСТІ ІНТЕГРАЦІЇ IOT ТА МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ П'ЯТОГО ПОКОЛІННЯ В СУЧАСНІ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ... 40
2.1. IoT-підхід до побудови інтелектуальних систем відеонагляду 40
2.2. Роль та технічні можливості 5G для передачі мультимедійних потоків .. 47
2.3. Виклики, обмеження та перспективи поєднання IoT і 5G у відеоспостереженні 54
3. РОЗРОБКА СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ НОВОГО ПОКОЛІННЯ НА БАЗІ WI-FI КАМЕР ІЗ ВИКОРИСТАННЯМ IOT ТА 5G 61
3.1. Концепція інтегрованої системи Wi-Fi–IoT–5G та її функціональна структура 61
3.2. Реалізація прототипу, оптимізація відеопередачі та оцінка ефективності 68
3.3. Порівняльний аналіз системи нового покоління з традиційними рішеннями та формування рекомендацій 77
ВИСНОВКИ 85
ПЕРЕЛІК ПОСИЛАНЬ 87
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 91

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

5G	Fifth Generation	— П'яте покоління мобільного зв'язку
AES	Advanced Encryption Standard	— Удосконалений стандарт шифрування
AI (ШІ)	Artificial Intelligence	— Штучний інтелект
AP	Access Point	— Точка доступу
AR	Augmented Reality	— Доповнена реальність
ARQ	Automatic Repeat ReQuest	— Автоматичний запит на повторну передачу
CCD	Charge-Coupled Device	— Прилад із зарядовим зв'язком (ПЗЗ)
CMOS	Complementary Metal-Oxide-Semiconductor	— Комплементарний метал-оксид-напівпровідник (КМОН)
CoAP	Constrained Application Protocol	— Протокол обмежених додатків
CPU	Central Processing Unit	— Центральний процесор
DASH	Dynamic Adaptive Streaming over HTTP	— Динамічне адаптивне потокове передавання через HTTP
eMBB	Enhanced Mobile Broadband	— Покращений мобільний широкосмуговий доступ
FEC	Forward Error Correction	— Попереджувальна (пряма) корекція помилок
FPS	Frames Per Second	— Кадрів за секунду
GDPR	General Data Protection Regulation	— Загальний регламент захисту даних
HEVC	High Efficiency Video Coding	— Високоефективне кодування відео
HLS	HTTP Live Streaming	— Потокове передавання в реальному часі через HTTP

IEEE	Institute of Electrical and Electronics Engineers	— Інститут інженерів з електротехніки та електроніки
IoT	Internet of Things	— Інтернет речей
ISP	Image Signal Processor	— Процесор обробки сигналів зображення
LTE	Long-Term Evolution	— Довгострокова еволюція (стандарт 4G)
MEC	Mobile Edge Computing	— Мобільні граничні (периферійні) обчислення
ML (MH)	Machine Learning	— Машинне навчання
mMTC	Massive Machine Type Communications	— Масові міжмашинні комунікації
MPEG	Moving Picture Experts Group	— Група експертів з рухомих зображень
MQTT	Message Queuing Telemetry Transport	— Протокол передачі телеметрії черги повідомлень
MU-MIMO	Multi-User Multiple Input Multiple Output	— Багатокористувацька система з багатьма входами і багатьма виходами
OFDM	Orthogonal Frequency-Division Multiplexing	— Ортогональне частотне мультиплексування
OFDMA	Orthogonal Frequency-Division Multiple Access	— Множинний доступ з ортогональним частотним поділом каналів
PoE	Power over Ethernet	— Живлення через Ethernet
PTZ	Pan-Tilt-Zoom	— Панорамування-Нахил-Масштабування
QAM	Quadrature Amplitude Modulation	— Квадратурна амплітудна модуляція
QoS	Quality of Service	— Якість обслуговування
RTP	Real-time Transport Protocol	— Транспортний протокол реального часу
RTSP	Real Time Streaming Protocol	— Протокол потокового передавання в реальному часі

SD	Secure Digital	—	Безпечний цифровий формат (карта пам'яті)
SNR	Signal-to-Noise Ratio	—	Співвідношення сигнал/шум
TLS	Transport Layer Security	—	Безпека транспортного рівня
uRLLC	Ultra-Reliable Low Latency Communications	—	Наднадійний зв'язок з низькою затримкою
VR	Virtual Reality	—	Віртуальна реальність
Wi-Fi	Wireless Fidelity	—	Технологія бездротової локальної мережі
WPA	Wi-Fi Protected Access	—	Захищений доступ до Wi-Fi

ВСТУП

Актуальність теми. Сучасний світ характеризується стрімким зростанням обсягів мультимедійних даних та підвищенням вимог до систем безпеки. Системи відеоспостереження стали невід'ємною частиною інфраструктури «розумних міст», промислових об'єктів та приватного сектору. Традиційні рішення, що базуються виключно на локальному записі або стандартних Wi-Fi мережах попередніх поколінь, все частіше демонструють свою неспроможність перед сучасними викликами: обмеженою пропускною здатністю, високою затримкою передачі даних, нестабільністю сигналу в умовах завад та складністю масштабування.

Інтеграція технологій Інтернету речей (IoT) та мереж п'ятого покоління (5G) відкриває принципово нові можливості для подолання цих бар'єрів. Поєднання гнучкості Wi-Fi, контекстної обізнаності IoT-сенсорів та надвисокої швидкості 5G дозволяє створити гетерогенну систему, здатну передавати відео високої чіткості в реальному часі, забезпечувати автономну аналітику та миттєве реагування на інциденти. Однак практична реалізація такої інтеграції стикається з низкою технічних проблем, зокрема забезпеченням якості обслуговування (QoS), синхронізацією різнорідних даних та адаптацією до динамічних умов бездротового середовища. Тому розробка та дослідження інтегрованої системи відеоспостереження нового покоління є важливим та актуальним науково-технічним завданням.

Мета і завдання дослідження. Метою роботи є підвищення ефективності та надійності систем бездротового відеоспостереження шляхом розробки інтегрованої архітектури на базі технологій Wi-Fi, IoT та 5G, а також створення алгоритмів адаптивного керування передачею відеопотоку.

Для досягнення поставленої мети вирішувалися такі завдання:

1. Проаналізувати технологічні основи сучасних Wi-Fi камер, методи формування відеосигналу та фактори, що впливають на якість передачі даних у бездротових мережах.

2. Дослідити можливості та перспективи інтеграції технологій IoT та 5G у системи відеоспостереження, виявити технічні бар’єри та шляхи їх подолання.

3. Розробити концепцію та трирівневу функціональну структуру інтегрованої системи Wi-Fi–IoT–5G.

4. Створити та обґрунтувати алгоритм адаптивного керування передачею відеоданих, який забезпечує стабільність потоку при зміні параметрів мережі.

5. Реалізувати прототип системи, провести оцінку його ефективності та порівняльний аналіз із традиційними рішеннями.

Об’єкт дослідження — процес передачі мультимедійних даних у гетерогенних бездротових мережах.

Предмет дослідження — методи, моделі та алгоритми оптимізації роботи інтегрованих систем відеоспостереження з використанням технологій Wi-Fi, IoT та 5G.

Методи дослідження. У роботі використано методи системного аналізу для побудови архітектури системи, методи теорії телетрафіку для оцінки пропускної здатності, методи цифрової обробки сигналів для стиснення відео, а також експериментальні методи для тестування прототипу та перевірки запропонованих алгоритмів.

Наукова новизна одержаних результатів полягає в наступному:

1. Удосконалено архітектуру системи відеоспостереження, яка, на відміну від існуючих, базується на трирівневій моделі (Wi-Fi–Edge–Cloud) з використанням 5G для магістральної передачі, що дозволяє знизити затримки та підвищити масштабованість.

2. Набув подальшого розвитку метод передачі відеоданих у бездротових мережах шляхом впровадження авторського алгоритму адаптивної корекції бітрейту та роздільної здатності на основі моніторингу метрик якості каналу (SNR, втрата пакетів) у реальному часі.

3. Запропоновано метод синхронізації відеопотоку з телеметричними даними IoT-сенсорів, що дозволяє підвищити інформативність системи та точність ситуаційної аналітики.

Практичне значення одержаних результатів. Розроблений прототип та алгоритмічні рішення можуть бути використані при проектуванні сучасних систем безпеки для муніципальних об’єктів, транспортних вузлів та промислових підприємств. Запропоновані рекомендації щодо налаштування мережевого обладнання та використання Edge Computing дозволяють оптимізувати витрати ресурсів та підвищити стабільність роботи мереж відеоспостереження.

1. ТЕХНОЛОГІЧНІ ОСНОВИ WI-FI СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ НОВОГО ПОКОЛІННЯ

1.1. Архітектура та принципи роботи Wi-Fi камер

Wi-Fi камери стали невід'ємним компонентом сучасних систем безпеки та моніторингу, пропонуючи зручність бездротового підключення та потокового відео в режимі реального часу. Їхня архітектура та принципи роботи розроблені для забезпечення ефективного захоплення зображень, безпечної передачі даних та надійної роботи в різних середовищах. Розуміння складних компонентів та технологічних структур, що лежать в основі Wi-Fi камер, дає уявлення про їхню функціональність, функції безпеки та апаратні аспекти. У розділі досліджується архітектура Wi-Fi камер, протоколи бездротового зв'язку, які вони використовують, а також їхнє керування живленням та апаратний дизайн, пояснюючи, як ці елементи працюють у гармонії для забезпечення ефективних рішень бездротового спостереження [1].

Архітектура Wi-Fi камери складається з кількох критично важливих компонентів, які дозволяють їй ефективно захоплювати, обробляти та передавати відеодані. В основі лежить датчик зображення, зазвичай CMOS або CCD, який відповідає за перетворення оптичних зображень на електронні сигнали. Ці датчики відрізняються роздільною здатністю, причому датчики з вищою роздільною здатністю забезпечують чіткіші та детальніші зображення, що є життєво важливим для цілей безпеки. Доповнює датчик вбудований процесор, який виконує такі завдання обробки зображень, як стиснення, виявлення руху та покращення зображення. Цей процесор часто включає мікроконтролер або спеціалізовані апаратні прискорювачі для безперешкодного керування цими функціями. Модуль Wi-Fi діє як комунікаційний міст, що дозволяє камері бездротово підключатися до локальної мережі, як через дводіапазонні (2,4 ГГц та 5 ГГц), так і через однодіапазонні частоти. Інтеграція в домашні або охоронні мережі передбачає встановлення камерою безпечного з'єднання через Wi-Fi маршрутизатори, які

можуть одночасно підтримувати кілька пристроїв. Потік даних починається з того, що датчик захоплює зображення, яке потім обробляється та стискається вбудованим процесором для оптимізації використання пропускної здатності. Оброблені дані згодом передаються через модуль Wi-Fi на підключений до мережі пристрій, такий як смартфон або сервер, що дозволяє здійснювати віддалений перегляд та зберігання. Така архітектура забезпечує оптимізований процес від захоплення зображення до бездротової передачі, підкреслюючи ефективність, безпеку та простоту інтеграції (рис. 1.1).

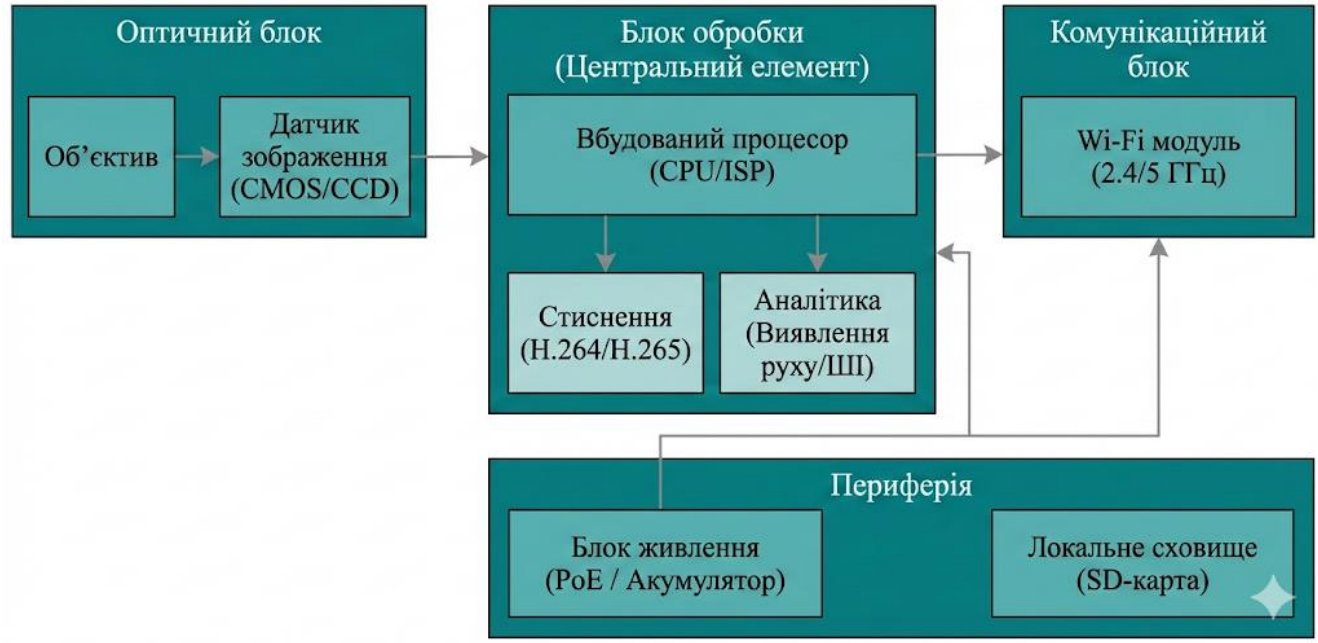


Рис. 1.1. Узагальнена структурна схема архітектури сучасної Wi-Fi камери

Wi-Fi камери використовують усталені протоколи бездротового зв'язку для забезпечення надійної та безпечної передачі даних. Переважно використовуються такі стандарти, як IEEE 802.11n та 802.11ac, які пропонують різні рівні пропускної здатності та діапазону. Наприклад, 802.11ac забезпечує вищу швидкість передачі даних, часто перевищуючи 1 Гбіт/с, що вигідно для передачі потоків відео високої чіткості без затримки або переривання. Для захисту конфіденційних відеоматеріалів впроваджено протоколи шифрування, такі як WPA2 (Wi-Fi Protected Access 2) та новіший WPA3, які забезпечують надійні заходи безпеки від несанкціонованого доступу. Ці функції безпеки шифрують пакети даних,

гарантуючи, що перехоплені передачі залишаються незрозумілими для сторонніх осіб, тим самим захищаючи конфіденційність користувачів. Управління пропускною здатністю є критично важливим, особливо в середовищах з кількома підключеними пристроями. Wi-Fi-камери часто використовують методи стиснення даних, такі як H.264 або H.265, які значно зменшують розмір відеофайлів без шкоди для якості зображення. Таке стиснення дозволяє ефективно використовувати доступну пропускну здатність, забезпечуючи плавнішу потокову передачу та зменшуючи затримку. Крім того, деякі передові системи включають протоколи якості обслуговування (QoS) для пріоритетності відеоданих над менш критичним мережевим трафіком, забезпечуючи стабільну продуктивність навіть під час перевантаження мережі. Ці протоколи бездротового зв'язку разом лежать в основі здатності камери працювати безпечно та ефективно в складних мережевих середовищах (табл. 1.1) [2].

Таблиця 1.1

Основні компоненти архітектури та функціональні елементи сучасних Wi-Fi камер

Компонент системи	Функціональне призначення та характеристики
Датчик зображення	Перетворює оптичні зображення на електронні сигнали (зазвичай CMOS або CCD). Вища роздільна здатність датчика забезпечує чіткіші зображення для цілей безпеки.
Вбудований процесор	Виконує стиснення даних, виявлення руху та покращення якості зображення. Часто включає мікроконтролери або апаратні прискорювачі.
Комунікаційний модуль	Забезпечує бездротове підключення до локальної мережі на частотах 2,4 ГГц та 5 ГГц. Використовує стандарти IEEE 802.11n/ac та шифрування WPA2/WPA3.
Система живлення	Може бути дротовою (PoE) для безперервної роботи або автономною (акумулятори) для гнучкості розміщення. Включає режими енергозбереження (сон) при відсутності руху.
Підсистема зберігання	Використовує локальні носії (SD-карти) або хмарні сервіси для резервного копіювання та віддаленого доступу. Дані кодуються алгоритмами H.264/H.265.
Користувацький інтерфейс	Реалізується через мобільні додатки для перегляду в реальному часі, керування PTZ та отримання сповіщень.

Керування живленням є життєво важливим аспектом проектування Wi-Fi-камер, особливо враховуючи різноманітні середовища, в яких вони розгортаються. Камери можуть живитися від дротових з'єднань — часто через Power over Ethernet (PoE) — або від акумуляторних чи змінних батарей, кожна з яких має унікальні переваги та проблеми. Дротові джерела живлення забезпечують безперервну роботу та усувають необхідність регулярної заміни батарей, що робить їх придатними для стаціонарних установок, таких як системи безпеки будівель. І навпаки, камери з живленням від батарей забезпечують більшу гнучкість у розміщенні, особливо в місцях, де немає розеток живлення, таких як відкриті або віддалені райони. Для оптимізації споживання енергії сучасні Wi-Fi камери оснащені функціями енергозбереження, такими як режими сну, коли такі компоненти, як датчик зображення та процесор, переходять у режим низького енергоспоживання, коли рух не виявляється. Наприклад, камера може залишатися в режимі очікування та активуватися лише після виявлення руху, що значно подовжує термін служби батареї та знижує експлуатаційні витрати. Довговічність обладнання є ще одним ключовим фактором, особливо для зовнішніх або промислових середовищ, що піддаються впливу погодних умов, пилу або фізичних впливів. Міцні корпуси, всепогодні ущільнення та ударостійкі матеріали гарантують, що Wi-Fi камери залишатимуться працездатними в суворих умовах. Крім того, конструкції обладнання часто включають механізми розсіювання тепла, щоб запобігти перегріву під час тривалого використання або високопродуктивної роботи, тим самим підтримуючи надійність та довговічність. Ці стратегії управління обладнанням та живленням є важливими для забезпечення ефективної роботи Wi-Fi камер у безлічі сценаріїв, балансуючи енергоефективність з довговічністю.

Сучасні Wi-Fi камери оснащені складним інтерфейсом користувача та системами керування, які підвищують зручність використання та доступність для користувачів. Центральним елементом цього є інтеграція з мобільними додатками, які дозволяють користувачам віддалено отримувати доступ до прямих трансляцій, керувати налаштуваннями камери, і отримувати сповіщення незалежно від їхнього

фізичного місцезнаходження. Ці додатки зазвичай мають зручний інтерфейс, що дозволяє користувачам переглядати потокове відео в режимі реального часу, керувати функціями панорамування, нахилу та масштабування (PTZ) та налаштовувати параметри сповіщень. Можливість отримувати миттєві сповіщення про виявлення руху або незвичайну активність підвищує швидкість реагування безпеки. Крім того, багато систем підтримують кількох користувачів з різними рівнями доступу, використовуючи протоколи автентифікації користувачів, такі як паролі, біометрична перевірка або двофакторна автентифікація, для захисту конфіденційності. Контроль конфіденційності є надзвичайно важливим; користувачі можуть налаштовувати зони конфіденційності, вимикати запис або обмежувати доступ до певних функцій, гарантуючи захист персональних даних та відеоматеріалів від несанкціонованого перегляду або втручання. Безперешкодна інтеграція систем керування з мобільними пристроями та хмарними сервісами не лише пропонує зручність, але й посилює безпеку, забезпечуючи зашифровану передачу та безпечні механізми входу. Ці функції разом дозволяють користувачам ефективно контролювати та керувати своїми системами спостереження, зберігаючи контроль над своєю конфіденційністю та безпекою даних [3].

Зберігання та обробка даних є критично важливими компонентами роботи Wi-Fi камер, впливаючи як на безпеку, так і на зручність використання. Камери пропонують різноманітні варіанти зберігання, включаючи хмарні сервіси та локальні рішення для зберігання, такі як SD-карти. Хмарне сховище надає перевагу резервного копіювання даних поза межами об'єкта, забезпечуючи віддалений доступ до відеоматеріалів з будь-якого місця та полегшуючи довгострокове зберігання. І навпаки, локальне зберігання на SD-картах пропонує економічно ефективне та швидке рішення, особливо в ситуаціях, коли підключення до Інтернету обмежене або існують проблеми безпеки щодо сторонніх хмарних постачальників. Відеодані зазвичай кодуються за допомогою передових алгоритмів стиснення, таких як H.264 та H.265, які значно зменшують розміри файлів, зберігаючи при цьому високу якість зображення. Цей баланс є важливим для ефективного використання пропускної здатності та управління сховищем. Крім

того, інтеграція алгоритмів штучного інтелекту (ШІ) розширює можливості обробки даних, забезпечуючи такі функції, як виявлення руху, розпізнавання облич та аналіз активності. Ці функції на основі ШІ дозволяють камерам розрізняти нормальну та підозрілу активність, зменшуючи кількість хибних тривог та покращуючи час реагування. Поєднання надійних варіантів зберігання, ефективних методів кодування та інтеграції ШІ гарантує, що Wi-Fi камери можуть ефективно керувати величезними обсягами даних, надавати змістовну аналітику та підтримувати інтелектуальні рішення безпеки, адаптовані до потреб користувачів.

Wi-Fi камери є прикладом гармонійної інтеграції передового обладнання, безпечних протоколів бездротового зв'язку та інтуїтивно зрозумілих систем керування, які разом забезпечують надійні та гнучкі рішення для спостереження. Їхня архітектура, що включає датчики високої роздільної здатності, процесори та модулі Wi-Fi, забезпечує безперебійне захоплення та передачу зображень, а дотримання таких стандартів, як 802.11ac та протоколи шифрування, такі як WPA3, забезпечує безпечне підключення. Стратегії управління живленням, включаючи дротові та акумуляторні варіанти з функціями енергозбереження, підвищують їхню експлуатаційну довговічність у різних середовищах. Інтерфейс користувача, переважно через мобільні додатки, забезпечує зручний віддалений доступ, сповіщення в режимі реального часу та контроль конфіденційності, надаючи користувачам комплексні можливості управління. Варіанти зберігання даних, від хмари до локальних SD-карт, у поєднанні з ефективним кодуванням відео та покращеною обробкою за допомогою штучного інтелекту, оптимізують обробку даних та забезпечують інтелектуальні функції безпеки. Загалом, ці технологічні принципи лежать в основі ефективності Wi-Fi камер, роблячи їх незамінними інструментами в сучасних інфраструктурах безпеки. З розвитком технологій постійне вдосконалення безпеки, зручності використання та інтеграції штучного інтелекту обіцяє ще більш складні та стійкі бездротові системи спостереження в майбутньому.

1.2. Формування та передавання відеосигналу у Wi-Fi мережах

У сучасну цифрову епоху бездротові мережі стали важливими для передачі високоякісного мультимедійного контенту, особливо відео, що вимагає значної пропускної здатності та надійної передачі. Мережі Wi-Fi, засновані на встановлених стандартах, таких як IEEE 802.11, сприяють бездротовій передачі відеосигналів, дозволяючи користувачам безперешкодно транслювати контент на різні пристрої. Розуміння того, як відеосигнали формуються та передаються в цих мережах, має вирішальне значення для оптимізації продуктивності та вирішення потенційних проблем. У розділі досліджується процес формування відеосигналу, що охоплює перетворення даних, стиснення та модуляцію, а також механізми, що беруть участь у передачі цих сигналів через Wi-Fi, включаючи протоколи, кодування та ролі мережевої інфраструктури. Крім того, в ньому обговорюються поширені проблеми, з якими стикаються під час передачі, такі як обмеження пропускної здатності, перешкоди та втрата даних, що можуть вплинути на якість потокового передавання [4].

Перший крок у передачі відео через Wi-Fi включає перетворення візуальних даних у цифровий формат, який можна ефективно обробляти та передавати. Цей процес починається зі захоплення необробленого відео, часто за допомогою камери або цифрового джерела, яке потім оцифровується — перетворюючи аналогові сигнали на двійкові дані, що складаються з нулів та одиниць. Після перетворення в цифрову форму дані піддаються стисненню, щоб зменшити свій розмір, що робить їх придатними для бездротової передачі без надмірного зниження якості. Популярні стандарти стиснення, такі як MPEG, H.264 та їхні наступники, використовують передові алгоритми для усунення надлишкової інформації, тим самим зменшуючи споживання пропускної здатності, зберігаючи при цьому чіткість. Наприклад, H.264 широко використовується на потокових платформах завдяки своїм ефективним можливостям стиснення, що дозволяє плавно передавати відео високої чіткості через обмежену пропускну здатність. Після стиснення цифровий відеосигнал необхідно модулювати для бездротової передачі. Це включає

перетворення цифрових даних на радіочастотні (РЧ) сигнали за допомогою схем модуляції, таких як квадратурна амплітудна модуляція (QAM) або ортогональне частотне мультиплексування (OFDM). Ці методи кодують двійкові дані на несучі хвилі, готуючи їх до передачі через бездротове середовище. Процес модуляції забезпечує бездротову передачу цифрового сигналу, долаючи фізичні обмеження радіоспектру та дозволяючи сигналу ефективно проходити ефірні хвилі (рис. 1.2).

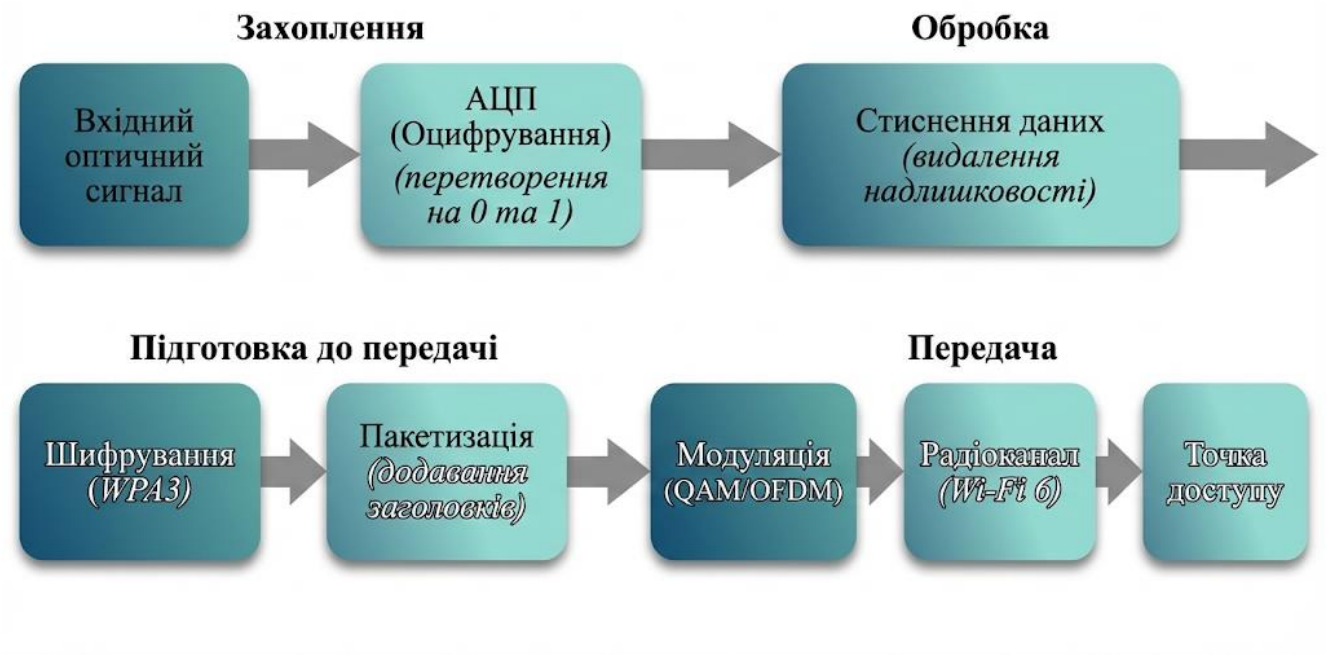


Рис. 1.2. Етапи обробки та передачі відеопотоку у бездротовій мережі

Після модуляції відеосигналу він передається через мережу Wi-Fi з використанням специфічних бездротових протоколів та стандартів, що регулюються в основному специфікаціями IEEE 802.11. Ці стандарти визначають методи бездротового зв'язку, включаючи діапазони частот, швидкість передачі даних та методи передачі, забезпечуючи сумісність між пристроями. Наприклад, Wi-Fi 5 (802.11ac) та Wi-Fi 6 (802.11ax) пропонують підвищену швидкість передачі даних та ефективність, що життєво важливо для високоякісного потокового відео. Під час передачі цифрові дані кодуються в пакети — процес, який називається пакетизацією — де дані розбиваються на менші, керовані блоки, кожен з яких містить заголовки, що містять інформацію про адресацію, послідовність та

перевірку помилок. Пакетизація сприяє виявленню помилок та повторній передачі, допомагаючи підтримувати цілісність даних під час бездротової передачі. Точки доступу (AP) та маршрутизатори слугують життєво важливими компонентами інфраструктури в цьому процесі; Вони координують бездротовий зв'язок, отримуючи закодовані пакети від вихідного пристрою та пересилаючи їх до пункту призначення. Вони також обробляють модуляцію сигналу, керують мережевим трафіком та реалізують протоколи безпеки. У сценаріях потокової передачі точки доступу забезпечують пріоритетність та ефективну передачу відеопакетів, зменшуючи затримку та буферизацію, що є критично важливим для забезпечення плавного відтворення. Поєднання стандартів протоколів, управління пакетами та інфраструктурних ролей разом гарантує, що цифровий відеосигнал надійно досягає пристроїв кінцевих користувачів через Wi-Fi [5].

Незважаючи на технологічний прогрес, передача високоякісного відео через мережі Wi-Fi стикається з численними проблемами, які можуть погіршити враження від перегляду. Обмеження пропускної здатності є одними з найсуттєвіших перешкод, особливо в перевантажених мережах, де кілька пристроїв конкурують за один і той самий спектр, що призводить до перевантаження мережі та зниження швидкості передачі даних. Наприклад, потокова передача відео 4K у перевантаженій мережі Wi-Fi може призвести до буферизації або зниження роздільної здатності через недостатню пропускну здатність. Перешкоди сигналу та шум від інших електронних пристроїв, таких як мікрохвильові печі та Bluetooth-гаджети, ще більше ускладнюють передачу, порушуючи радіочастотні сигнали, спричиняючи коливання якості сигналу та потенційне пошкодження даних. Крім того, фізичні перешкоди, такі як стіни та меблі, можуть послаблювати сигнали Wi-Fi, що призводить до поганого прийому та збільшення втрати пакетів. Втрата даних, у свою чергу, призводить до випадання пакетів, що особливо негативно впливає на потокове відео в реальному часі, спричиняючи артефакти, заїкання або повне переривання відеопотоку (табл. 1.2).

Таблиця 1.2

Етапи формування відеосигналу та фактори впливу на передачу даних у бездротовому середовищі

Етап / Фактор	Опис процесу та особливості
Оцифрування та стиснення	Перетворення аналогових сигналів у двійковий формат. Використання стандартів (MPEG, H.264) для зменшення розміру даних та економії пропускної здатності.
Модуляція сигналу	Кодування цифрових даних у радіочастотні сигнали за допомогою схем QAM або OFDM для проходження через ефір.
Пакетизація даних	Розбиття даних на пакети із заголовками для адресації та перевірки помилок, що сприяє цілісності передачі.
Протоколи передачі	Використання стандартів Wi-Fi 5 (802.11ac) та Wi-Fi 6 (802.11ax) для забезпечення високої швидкості та ефективності.
Проблеми передачі	Обмеження пропускної здатності та перевантаження мережі, що веде до буферизації. Інтерференція від інших пристроїв (Bluetooth, мікрохвильові печі) та фізичні перешкоди (стіни).
Технології корекції	Використання ARQ та FEC для виявлення та виправлення помилок у пакетах. Адаптивні методи (DASH, HLS) регулюють якість відео в реальному часі.

Щоб зменшити ці проблеми, мережеві адміністратори часто використовують такі стратегії, як управління пропускною здатністю, вибір каналу та розгортання кількох точок доступу для покращення покриття та зменшення перешкод. Передові методи виправлення помилок та адаптивні протоколи потокового передавання також допомагають компенсувати втрату пакетів, динамічно регулюючи якість відео для підтримки безперервного перегляду. Загалом, ці проблеми підкреслюють важливість надійного проектування та управління мережею для забезпечення високоякісної передачі відео через мережі Wi-Fi.

Для вирішення проблем передачі високоякісних відео через Wi-Fi було розроблено кілька передових технологій та протоколів для підвищення надійності та підтримки оптимальної якості відео. Одним із критичних аспектів є протоколи виправлення помилок та повторної передачі, такі як Automatic Repeat ReQuest (ARQ) та Forward Error Correction (FEC).Ці механізми виявляють помилки в переданих пакетах даних і спонукають до повторної передачі або застосовують

алгоритми виправлення для відновлення втрачених або пошкоджених даних, тим самим зменшуючи візуальні артефакти та переривання. Крім того, адаптивні методи потокової передачі, такі як Dynamic Adaptive Streaming over HTTP (DASH) та HTTP Live Streaming (HLS) від Apple, революціонізували доставку відео, динамічно регулюючи якість відео на основі мережевих умов у режимі реального часу. Ці протоколи сегментують відео на кілька рівнів якості та плавно перемикаються між ними, щоб запобігти буферизації, пропонуючи глядачам плавний перегляд навіть у коливальних мережевих середовищах. Крім того, механізми якості обслуговування (QoS) відіграють життєво важливу роль, надаючи пріоритет пакетам відеоданих над менш чутливим до часу трафіком, забезпечуючи ефективний розподіл пропускної здатності для мінімізації затримки та буферизації. Мережеві пристрої використовують політики QoS для розпізнавання та визначення пріоритетів потокового трафіку, що особливо важливо в години пікового навантаження, коли перевантаження мережі високе. Разом ці технологічні інновації працюють синергетично для підтримки високоякісної передачі відео, роблячи потокову передачу більш стійкою та зручною для користувача в різних середовищах Wi-Fi. Забігаючи вперед, постійний розвиток технології Wi-Fi та суміжних галузей обіцяє змінити те, як відеосигнали формуються та передаються бездротовими мережами. Еволюція від Wi-Fi 5 (802.11ac) до Wi-Fi 6 (802.11ax) і далі, таких як Wi-Fi 7, забезпечує вищі швидкості передачі даних, покращену ефективність використання спектру та розширену можливість одночасної підтримки кількох пристроїв з високою пропускною здатністю. Ці вдосконалення значно зменшать буферизацію та дозволять безперешкодно передавати ще вищі роздільні здатності, такі як потокове передавання 8K. Паралельно інтеграція штучного інтелекту (ШІ) у мережеві системи готова динамічно оптимізувати передачу сигналу. Алгоритми ШІ можуть аналізувати стан мережі в режимі реального часу, прогнозувати перешкоди та коригувати такі параметри, як схеми модуляції та розподіл каналів, для максимізації продуктивності та стабільності. Крім того, розробка більш складних алгоритмів стиснення дозволить отримувати відео вищої якості з нижчими бітрейтами, зменшуючи вимоги до пропускної здатності без шкоди для візуальної

точності. Такі методи, як стиснення на основі нейронних мереж, можуть революціонізувати кодування відео, забезпечуючи більш ефективні та адаптивні методи, адаптовані до складності контенту та стану мережі. Оскільки ці інновації поєднуються, майбутнє передачі відео на основі Wi-Fi обіцяє бути швидшим, надійнішим та здатним підтримувати дедалі захопливіший мультимедійний досвід.

Формування та передача відеосигналів через мережі Wi-Fi включає складну послідовність процесів, від перетворення візуальних даних у цифрові формати та використання методів стиснення та модуляції до використання бездротових протоколів та інфраструктури для доставки. Хоча ці системи забезпечують зручний доступ до високоякісного відеоконтенту, вони не позбавлені проблем; такі проблеми, як обмеження пропускної здатності, перешкоди та втрата даних, можуть погіршити враження від перегляду. Однак технологічні рішення, такі як корекція помилок, адаптивна потокова передача та механізми QoS, відіграли важливу роль у підвищенні надійності та якості. Забігаючи вперед, досягнення у стандартах Wi-Fi, інтеграція штучного інтелекту та більш ефективні алгоритми стиснення мають на меті ще більше покращити надійність та точність бездротової передачі відео. У міру розвитку цих розробок вони продовжуватимуть формувати все більш пов'язаний та захопливий мультимедійний ландшафт, підкреслюючи важливість постійних інновацій у технологіях бездротового зв'язку [6].

1.3. Методи забезпечення якості відеопотоку при Wi-Fi підключенні

В епоху, коли цифровий зв'язок та віддалені розваги є невід'ємною частиною повсякденного життя, якість потокового відео через мережі Wi-Fi стала критично важливою. Безперебійний перегляд залежить від безлічі факторів, від надійності мережевої інфраструктури до інтелектуального управління трафіком даних. Оскільки попит на контент високої чіткості та 4K продовжує зростати, забезпечення стабільних та високоякісних відеопотоків через бездротові з'єднання створює як технічні труднощі, так і можливості. У розділі досліджуються три фундаментальні методи оптимізації мереж Wi-Fi для забезпечення вищої якості потокового відео:

вдосконалення мережевої інфраструктури, впровадження протоколів якості обслуговування (QoS) та впровадження технологій виправлення помилок та стиснення. Кожен підхід відіграє життєво важливу роль у пом'якшенні поширених проблем, таких як буферизація, затримка та втрата пакетів, що зрештою дозволяє користувачам насолоджуватися безперебійним відеоконтентом високої якості.

Основа надійного потокового відео через Wi-Fi починається з надійної мережевої інфраструктури. Модернізація маршрутизаторів для підтримки стандартів з вищою пропускною здатністю, таких як Wi-Fi 6 (802.11ax), є вирішальним кроком у цьому процесі. Wi-Fi 6 пропонує значні покращення порівняно з попередніми стандартами, включаючи збільшення швидкості передачі даних, краще керування кількома пристроями одночасно та зменшення затримки, що безпосередньо сприяє плавнішому відтворенню відео. Наприклад, домогосподарства з кількома потоковими пристроями можуть зіткнутися з меншою кількістю перебоїв під час використання маршрутизаторів з підтримкою Wi-Fi 6. Крім того, стратегічне розташування маршрутизаторів є важливим; розміщення їх у центральних місцях подалі від фізичних перешкод або електронних перешкод забезпечує оптимальне покриття сигналу. Розширення покриття за допомогою mesh-мереж або додаткових точок доступу може усунути мертві зони у великих будинках або офісах. Мінімізація перешкод від інших електронних пристроїв, таких як бездротові телефони, мікрохвильові печі або сусідні мережі Wi-Fi, також підвищує стабільність сигналу. Такі методи, як зміна каналів Wi-Fi або використання дводіапазонних маршрутизаторів, можуть допомогти зменшити ці джерела перешкод. У сукупності ці покращення інфраструктури створюють більш стійке мережеве середовище, здатне підтримувати високоякісні відеопотоки з мінімальними перебоями. Окрім оновлення обладнання, керування розподілом мережевих ресурсів є життєво важливим для підтримки якості відеопотоку. Протоколи якості обслуговування (QoS) розроблені для пріоритетності критичного трафіку, такого як потокове відео, над менш чутливими діями, такими як завантаження файлів або фонові оновлення. Налаштовуючи параметри QoS на маршрутизаторах, користувачі можуть призначати потоковим програмам вищі рівні

пріоритету, гарантуючи, що вони отримують достатню пропускну здатність навіть у періоди високого навантаження мережі. Наприклад, потокові платформи, такі як Netflix або YouTube, можна позначити як трафік з високим пріоритетом, що зменшує ймовірність буферизації в години пікового використання. Параметри розподілу пропускної здатності можна точно налаштувати, щоб гарантувати мінімальну швидкість передачі даних для відеопотоків, що особливо важливо для контенту високої чіткості або 4K. Крім того, постійний моніторинг продуктивності мережі дозволяє динамічно регулювати параметри QoS. Якщо виявлено перевантаження мережі, адміністратори або користувачі можуть змінювати налаштування в режимі реального часу, щоб оптимізувати стабільність потокової передачі. Впровадження QoS не тільки покращує взаємодію з користувачем, але й забезпечує справедливий розподіл мережевих ресурсів, що робить його практичним рішенням для домівок та організацій з кількома підключеними пристроями [7].

Останній рівень забезпечення високоякісного потокового відео включає передові технології, які вирішують такі проблеми, як втрата даних та обмеження пропускної здатності. Адаптивне потокове передавання з бітрейтом – це техніка, яка динамічно регулює якість відео на основі стабільності з’єднання в режимі реального часу. Коли стан мережі погіршується, потоковий сервіс зменшує роздільну здатність відео, щоб запобігти буферизації, а потім відновлює вищу якість, коли умови покращуються. Наприклад, багато потокових платформ автоматично знижують роздільну здатність під час перевантаження мережі, забезпечуючи безперервний перегляд. Алгоритми виправлення помилок, такі як пряма корекція помилок (FEC), допомагають зменшити втрату пакетів – поширену причину погіршення якості відео – додаючи надлишкові дані, що дозволяють приймачу відновлювати втрачені пакети без повторної передачі. Крім того, методи стиснення відео, такі як H.264 або HEVC, ефективно кодують відеодані, щоб зменшити необхідну пропускну здатність, зберігаючи при цьому якість зображення. Ці методи особливо корисні в середовищах з обмеженою пропускною здатністю, дозволяючи плавно передавати потоки високої чіткості через неідеальні з’єднання. Поєднання технологій адаптивного потокового передавання, виправлення помилок

та стиснення створює складну систему, яка адаптується до коливань стану мережі, забезпечуючи стабільну якість відео навіть за складних обставин (табл. 1.3) [8].

Таблиця 1.3

Методи та технології оптимізації якості відеопотоку в системах відеоспостереження

Метод забезпечення якості	Механізм дії та переваги
Модернізація інфраструктури	Перехід на Wi-Fi 6 (802.11ax) для кращого керування багатьма пристроями та зменшення затримки. Використання Mesh-мереж для усунення «мертвих зон».
Якість обслуговування (QoS)	Надання пріоритету відеоданим над менш важливим трафіком (завантаження файлів) для запобігання буферизації.
Адаптивний бітрейт	Динамічна зміна роздільної здатності відео залежно від стабільності з'єднання (зниження якості при перевантаженні).
Ефективне кодування	Застосування кодеків H.264 або HEVC для зменшення бітрейту без втрати візуальної якості.
Оптимізація клієнтських пристроїв	Оновлення прошивки для підтримки нових стандартів. Мінімізація фонових процесів та використання дротових з'єднань (Ethernet) для критичних вузлів.
Безпека та моніторинг	Регулярна діагностика мережі, оновлення протоколів безпеки та керування кількістю підключених пристроїв для запобігання перенасиченню каналу.

Окрім зміцнення мережевої інфраструктури та управління трафіком даних, важливо забезпечити оптимізацію підключених пристроїв для високоякісного потокового передавання. Пристрої із застарілою прошивкою можуть не повністю підтримувати найновіші стандарти Wi-Fi, такі як Wi-Fi 6, що може знижувати продуктивність, незважаючи на надійну мережу. Регулярне оновлення прошивки пристрою забезпечує сумісність із розширеними функціями Wi-Fi, що призводить до кращого підключення та зменшення затримки або буферизації. Крім того, мінімізація фонових програм, які споживають пропускну здатність, таких як автоматичні оновлення, резервне копіювання в хмару або інші потокові сервіси, може значно покращити стабільність потокової передачі. Користувачам слід

закривати непотрібні програми під час сеансів перегляду, щоб звільнити пропускну здатність для відеопотоків. Крім того, коли це можливо, використання дротових Ethernet-з'єднань для критично важливих пристроїв, таких як смарт-телевізори, ігрові консолі або комп'ютери, може забезпечити стабільніше та швидше з'єднання, ніж бездротові. Дротові з'єднання усувають проблеми, спричинені перешкодами сигналу або слабким сигналом Wi-Fi, забезпечуючи стабільну високу якість потокового передавання. Заохочення оптимізації та сумісності пристроїв не лише покращує враження від перегляду, але й сприяє загальній ефективності мережі, роблячи потокове передавання високої чіткості надійнішим та менш схильним до перебоїв.

Підтримка безпечної та добре обслуговуваної мережі не менш важлива для забезпечення стабільної якості потокового відео. Регулярні оновлення прошивки та протоколів безпеки необхідні для виправлення вразливостей, які можуть спричинити перебої в роботі мережі або уповільнення. Незахищена мережа може бути вразливою до несанкціонованого доступу або шкідливого програмного забезпечення, які можуть споживати пропускну здатність або призводити до збоїв пристроїв, негативно впливаючи на продуктивність потокового передавання. Регулярна діагностика мережі, така як перевірка сили сигналу, використання пропускної здатності та підключення пристроїв, допомагає виявити потенційні проблеми, перш ніж вони переростуть у серйозні. Проактивне вирішення цих проблем гарантує стабільність та ефективність мережі. Крім того, керування перевантаженням мережі шляхом обмеження кількості пристроїв, підключених під час сеансів потокового передавання, може запобігти перенасиченню пропускної здатності. Наприклад, призупинення або відключення непотрібних пристроїв під час критичного часу перегляду дозволяє важливим пристроям працювати з оптимальною швидкістю. Впровадження цих методів безпеки та обслуговування створює стійке мережеве середовище, яке підтримує безперебійне потокове відео високої якості, захищаючи як користувацький досвід, так і цілісність мережі.

Досягнення високоякісного потокового відео через Wi-Fi вимагає комплексного підходу, який враховує різні аспекти продуктивності мережі.

Модернізація та стратегічне розташування маршрутизаторів покращує основну інфраструктуру, забезпечуючи міцну основу для передачі даних. Впровадження протоколів якості обслуговування (QoS) гарантує, що потоковий трафік отримає пріоритет, зменшуючи проблеми з буферизацією та затримкою. Передові технології виправлення помилок та стиснення додатково оптимізують передачу даних, адаптуючись до мережевих умов та зменшуючи вимоги до пропускної здатності. Не менш важливими є зусилля щодо сумісності та оптимізації пристроїв, які включають оновлення пристроїв, мінімізацію фонового використання пропускної здатності та використання дротових з'єднань, коли це можливо. Нарешті, ретельні методи забезпечення безпеки та обслуговування мережі відіграють життєво важливу роль у збереженні стабільності мережі та запобіганні перебоям. Разом ці методи утворюють надійну основу для забезпечення плавних потокових відео високої якості через Wi-Fi, що дозволяє користувачам насолоджуватися безперебійними цифровими розвагами у все більш пов'язаному світі.

1.4. Переваги технологій на основі Wi-Fi систем відеоспостереження нового покоління

В епоху швидкого технологічного прогресу системи відеоспостереження нового покоління з технологією Wi-Fi стали життєво важливими інструментами для підвищення безпеки, операційної ефективності та масштабованості в різних умовах. Ці системи використовують бездротове з'єднання для забезпечення безперебійного моніторингу, сповіщень у режимі реального часу та інтеграції зі складною аналітикою, пропонуючи численні переваги порівняно з традиційними заходами безпеки. Оскільки організації шукають більш ефективні та адаптивні рішення для захисту активів та оптимізації операцій, розуміння переваг цих передових систем стає дедалі важливішим. Досліджуються три основні переваги технології відеоспостереження на основі Wi-Fi: покращені можливості безпеки та спостереження, економічна ефективність у поєднанні з операційною ефективністю,

а також чудова масштабованість і гнучкість, які ці системи пропонують різним типам організацій (табл. 1.4) [9].

Таблиця 1.4

Переваги технологій на основі Wi-Fi систем відеоспостереження нового покоління

Технологія / Інновація	Ключові характеристики	Переваги для системи відеоспостереження
Wi-Fi 6 (IEEE 802.11ax)	Підтримка технологій OFDMA та MU-MIMO, вища пропускна здатність.	Забезпечує стабільну передачу відео з кількох камер одночасно, зменшує затримки та буферизацію у перевантажених мережах.
Інтелектуальна аналітика (AI)	Вбудовані алгоритми машинного навчання для розпізнавання об'єктів та поведінки.	Автоматичне виявлення загроз, зменшення кількості хибних спрацьовувань та можливість превентивного реагування без участі оператора.
Ефективне кодування (H.265/HEVC)	Удосконалені алгоритми стиснення відеоданих без втрати візуальної якості.	Зменшення навантаження на канал зв'язку та економія дискового простору для зберігання архівів.
Протоколи безпеки (WPA3)	Посилене шифрування даних та захист від несанкціонованого доступу.	Гарантує конфіденційність відеопотоків та захист від перехоплення даних зловмисниками.
Периферійні обчислення (Edge Computing)	Обробка даних безпосередньо на камері або локальному шлюзі.	Зниження затримок передачі (Latency), розвантаження центральних серверів та підвищення швидкості реакції системи.
Інтеграція з 5G	Наднизька затримка (<1 мс) та швидкість до 20 Гбіт/с.	Можливість передачі відео 4K/8K у реальному часі та керування PTZ-камерами без відчутних затримок.

Системи відеоспостереження Wi-Fi значно підвищують безпеку, забезпечуючи моніторинг у режимі реального часу в поєднанні з механізмами миттєвого сповіщення, що значно покращує час реагування в надзвичайних ситуаціях. Наприклад, співробітники служби безпеки можуть отримувати негайні сповіщення про виявлення підозрілої активності, що дозволяє їм швидко втрутитися, тим самим запобігаючи потенційним крадіжкам, вандалізму чи іншим

загрозам. Висока чіткість відео, що забезпечується сучасними камерами спостереження, гарантує чітке фіксування таких деталей, як риси обличчя, номерні знаки чи підозрілі об'єкти, що сприяє точній ідентифікації та збору доказів. Крім того, інтеграція аналітики штучного інтелекту (ШІ) перетворює ці системи з простих камер на інтелектуальні рішення безпеки. Функції на базі ШІ, такі як виявлення руху, розпізнавання облич та аналіз поведінки, можуть автоматично виявляти незвичайну активність або несанкціонований доступ, зменшуючи залежність від людського нагляду та мінімізуючи хибні тривоги. Наприклад, алгоритми ШІ можуть розрізняти звичайний рух та потенційні загрози, попереджаючи служби безпеки лише тоді, коли виникають справжні занепокоєння. Таке поєднання даних у режимі реального часу, зображень високої роздільної здатності та інтелектуальної аналітики призводить до створення комплексної системи безпеки, здатної адаптуватися до складних та мінливих загроз, що робить системи відеоспостереження Wi-Fi незамінним активом для сучасного управління безпекою. Однією з найпереконливіших переваг систем відеоспостереження на основі Wi-Fi є їхня економічна ефективність, яка випливає з кількох факторів, що разом зменшують витрати та оптимізують операції з безпеки. Традиційні системи відеоспостереження часто вимагають розгалуженої проводки, спеціалізованої інфраструктури та значної кількості співробітників служби безпеки для моніторингу кількох об'єктів. На противагу цьому, бездротові системи усувають необхідність у дротових з'єднаннях, тим самим знижуючи витрати на встановлення та мінімізуючи перебої під час розгортання. Можливості автоматизованого моніторингу ще більше зменшують залежність від людського контролю; інтелектуальні системи можуть постійно спостерігати за камерами та позначати аномалії, дозволяючи співробітникам служби безпеки зосередитися на перевірених загрозах, а не на звичайному спостереженні. Крім того, витрати на обслуговування нижчі, оскільки бездротові камери зазвичай мають менше механічних компонентів, схильних до зносу, а оновлення програмного забезпечення можна проводити

дистанційно без значного технічного втручання. Можливість дистанційного доступу до каналів спостереження ще більше підвищує операційну ефективність; менеджери з безпеки можуть одночасно контролювати кілька місць розташування з централізованих диспетчерських або навіть через мобільні пристрої, що дозволяє швидко приймати рішення та скорочувати час реагування. Наприклад, роздрібна мережа може контролювати всі свої торгові точки з одного пристрою, оперативно вирішуючи порушення безпеки або операційні проблеми без необхідності присутності на місці. Ці фактори разом сприяють більш економічній та ефективній інфраструктурі безпеки, яка добре адаптується до бюджетних обмежень та динамічних операційних потреб [10].

Завдяки притаманній масштабованості та гнучкості систем відеоспостереження Wi-Fi вони дуже підходять для організацій різного розміру та складності. На відміну від традиційних систем, які часто потребують значних інфраструктурних модифікацій для розширення, рішення на основі Wi-Fi дозволяють легко додавати камери та датчики без значних фізичних змін. Такий модульний підхід означає, що підприємства можуть почати з базової конфігурації та поступово розширюватися в міру зростання своїх потреб у безпеці чи експлуатації. Сумісність з існуючими мережами Wi-Fi ще більше прискорює розгортання, що робить можливим встановлення комплексного охоплення спостереженням за лічені години, а не дні чи тижні. Наприклад, малий бізнес може спочатку впровадити кілька камер та масштабуватися в міру розширення, не турбуючись про складну проводку чи реконфігурацію мережі. Великі підприємства або кампуси отримують вигоду від можливості керувати сотнями камер у кількох місцях через централізовані платформи, забезпечуючи узгоджені стандарти безпеки. Крім того, ці системи адаптуються до різних середовищ, від роздрібних магазинів та офісів до відкритих приміщень та промислових об'єктів. Їхня універсальність дозволяє організаціям налаштовувати конфігурації спостереження відповідно до конкретних потреб, будь то зони високого рівня безпеки чи загальний

моніторинг, що робить Wi-Fi відеоспостереження перспективним рішенням, здатним розвиватися разом з технологічним прогресом та зростанням організації.

Істотною перевагою сучасних систем Wi-Fi відеоспостереження є їхня здатність до передових рішень для управління даними та зберігання, що значно підвищує операційну ефективність та безпеку. Хмарні варіанти зберігання даних революціонізували спосіб зберігання та доступу до записів спостереження, пропонуючи організаціям можливість безпечно зберігати великі обсяги відеоданих поза межами об'єкта. Це не лише захищає критично важливі відеоматеріали від фізичного пошкодження або крадіжки, але й гарантує доступ до даних з будь-якого місця з підключенням до Інтернету, що полегшує віддалений моніторинг та швидке їх отримання. Крім того, використання передових технологій стиснення відіграє життєво важливу роль в оптимізації ємності сховища. Сучасні камери використовують складні алгоритми стиснення, такі як H.264 та H.265, які значно зменшують розміри файлів без шкоди для якості відео, дозволяючи організаціям зберігати більше відеоматеріалів в обмежених ресурсах сховища. Це особливо корисно для середовищ з високими вимогами до моніторингу, де великі матеріали необхідно зберігати протягом тривалого часу. Ці технології ще більше покращують спрощений доступ та обмін відеоматеріалами спостереження; уповноважений персонал може легко отримувати певні кліпи для розслідувань або подання доказів, а обмін ними з правоохоронними органами або зацікавленими сторонами стає простим через безпечні онлайн-портали. Загалом, покращені можливості управління даними та зберігання гарантують, що організації ведуть комплексні, безпечні та легкодоступні записи спостереження, які мають вирішальне значення для поточних аудитів безпеки та експлуатації.

Інтеграційні можливості систем спостереження на основі Wi-Fi виходять за рамки автономного відеомоніторингу, дозволяючи цілісний підхід до управління безпекою завдяки безперебійному з'єднанню з іншими системами будівлі. Ці системи можна інтегрувати з механізмами контролю доступу, що дозволяє

перевіряти особу в режимі реального часу перед наданням дозволу на вхід, а також автоматично вмикати сигналізацію або блокувати двері у разі виявлення підозрілої активності. Така інтеграція покращує загальну екосистему безпеки, створюючи взаємопов'язані рівні захисту, які динамічно реагують на загрози. Крім того, системи Wi-Fi-спостереження підтримують інтеграцію елементів керування освітленням та датчиків навколишнього середовища, що сприяє розумнішій автоматизації будівель. Наприклад, зовнішні камери можуть працювати разом з освітленням, що активується рухом, освітлюючи зони лише тоді, коли виявляється рух, таким чином заощаджуючи енергію та підтримуючи безпеку. Інтернет речей (IoT) ще більше розширює ці можливості, підключаючи камери спостереження до інших інтелектуальних пристроїв, таких як датчики температури або пожежна сигналізація, утворюючи комплексну автоматизовану мережу безпеки. Централізовані платформи управління дозволяють співробітникам служби безпеки контролювати всі ці компоненти з єдиного інтерфейсу, спрощуючи операції, скорочуючи час реагування та забезпечуючи комплексну ситуаційну обізнаність. Ця взаємопов'язана екосистема не тільки зміцнює безпеку, але й підвищує операційну ефективність, управління енергоспоживанням та безпеку мешканців, що робить системи Wi-Fi-відеоспостереження невід'ємною частиною сучасних інтелектуальних будівель [11].

Незважаючи на свої численні переваги, системи Wi-Fi-відеоспостереження стикаються зі значними проблемами, пов'язаними з надійністю мережі та ризиками кібербезпеки. Ефективність цих систем значною мірою залежить від стабільного та надійного Wi-Fi-з’єднання; будь-які перебої або перешкоди можуть призвести до перебоїв у спостереженні, залишаючи прогалини в безпеці. Наприклад, перевантаження мережі або збої, спричинені високим трафіком або технічними несправностями, можуть призвести до затримки або втрати відеопотоків, підриваючи здатність системи забезпечувати безперервний моніторинг. Більше того, оскільки ці системи підключені до Інтернету, вони вразливі до кібератак та

витоків даних, якщо їх належним чином не захистити. Хакери можуть намагатися отримати доступ до прямих трансляцій, маніпулювати відеозаписами або скомпрометувати збережені дані, що може мати серйозні правові та безпекові наслідки. Впровадження надійних протоколів шифрування, брандмауерів та регулярних оновлень безпеки є важливим для зменшення цих ризиків. Крім того, поширення бездротових пристроїв може спричиняти перешкоди, погіршуючи якість відео або спричиняючи розриви з'єднання. Пристрої, що працюють на подібних частотах, такі як Bluetooth або сусідні мережі Wi-Fi, можуть порушувати цілісність сигналу та знижувати ефективність спостереження. Вирішення цих проблем вимагає комплексного підходу до управління мережею, кібербезпеки та технологічної стійкості, щоб забезпечити надійність та безпеку систем відеоспостереження Wi-Fi у різних операційних середовищах. Хоча системи відеоспостереження Wi-Fi пропонують значні переваги в галузі безпеки та експлуатації, вони також викликають значні проблеми щодо конфіденційності, які організації повинні вирішувати відповідально. Забезпечення дотримання законів і правил захисту даних, таких як Загальний регламент про захист даних (GDPR) у Європі або аналогічні рамки в усьому світі, має вирішальне значення для запобігання правовим наслідкам та підтримки довіри громадськості. Організації, що впроваджують ці системи, повинні встановити чітку політику щодо збору, зберігання та доступу до даних, зі суворими протоколами для запобігання нав'язливим практикам спостереження, які можуть порушувати права особистої конфіденційності. Такі заходи, як анонімізація відеозаписів, обмеження доступу для уповноваженого персоналу, та надання прозорої інформації про діяльність зі спостереження допомагає досягти балансу між перевагами безпеки та повагою до конфіденційності. Більше того, отримання інформованої згоди від осіб, коли це необхідно, та регулярний аудит практики спостереження можуть запобігти зловживанням та забезпечити дотримання вимог. З розвитком технологій спостереження важливість етичних міркувань та дотримання законодавства стає ще

більш критичною, сприяючи відповідальному підходу, який використовує технологічні переваги без шкоди для особистих свобод. Навігація цим делікатним балансом вимагає тонкого розуміння правових стандартів, організаційної відповідальності та соціальних наслідків повсюдного спостереження, гарантуючи, що покращення безпеки не відбувається за рахунок прав особистої конфіденційності.

Заглядаючи вперед, майбутнє систем відеоспостереження Wi-Fi готове до швидких інновацій, зумовлених новими технологіями та потребами безпеки, що розвиваються. Інтеграція технології 5G обіцяє революціонізувати швидкість передачі даних, значно покращивши можливості систем спостереження в режимі реального часу та дозволивши розгортання камер з вищою роздільною здатністю без проблем із затримкою. Цей прогрес сприятиме точнішій аналітиці, швидшому реагуванню та безперебійному віддаленому доступу навіть у густонаселених середовищах або середовищах з обмеженою пропускною здатністю. Крім того, інтеграція штучного інтелекту (ШІ) та машинного навчання переведе системи спостереження від реактивного моніторингу до прогнозної аналітики, що дозволить раннє виявлення потенційних загроз та моделей поведінки, що передують інцидентам безпеки. Ці інтелектуальні системи можуть навчатися на основі історичних даних, щоб прогнозувати ризики, оптимізувати розподіл ресурсів та покращувати загальні стратегії безпеки. Екологічна стійкість також відіграє важливу роль у майбутніх розробках; енергоефективне обладнання, датчики з низьким енергоспоживанням та екологічно чисті матеріали розробляються для зменшення вуглецевого сліду інфраструктури спостереження. Такі інновації, як камери на сонячних батареях та системи, що адаптують свою роботу до умов навколишнього середовища, зроблять спостереження більш сталим та економічно ефективним. У міру розвитку цих технологій очікується, що відеоспостереження через Wi-Fi стане більш інтелектуальним, стійким та екологічно свідомим, узгоджуючи покращення безпеки з ширшими суспільними та екологічними цілями.

На завершення, системи відеоспостереження Wi-Fi нового покоління пропонують безліч переваг, які значно підвищують безпеку, операційну ефективність та масштабованість системи в різних середовищах. Їхня здатність до моніторингу в режимі реального часу, зображення високої чіткості та інтеграція з аналітикою штучного інтелекту робить їх безцінними інструментами для сучасного управління безпекою. Економічна ефективність та функції дистанційного керування також дозволяють організаціям оптимізувати ресурси та швидко реагувати на нові загрози. Крім того, притаманна цим бездротовим системам масштабованість та гнучкість дозволяють безперешкодно розширюватися та адаптуватися до різних потреб організації. Однак ці переваги повинні бути збалансовані з такими викликами, як надійність мережі, ризики кібербезпеки та проблеми конфіденційності. З розвитком технологій майбутні тенденції, включаючи впровадження 5G, прогнозної аналітики на основі штучного інтелекту та стійких інновацій, обіцяють підняти Wi-Fi-спостереження на нові висоти ефективності та інтелекту. Зрештою, відповідальне використання цих досягнень може призвести до безпечніших, розумніших та стійкіших екосистем безпеки, які служать як організаційним інтересам, так і правам особистості, формуючи майбутній ландшафт технологій безпеки.

2. МОЖЛИВОСТІ ІНТЕГРАЦІЇ ІОТ ТА МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ П’ЯТОГО ПОКОЛІННЯ В СУЧАСНІ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ

2.1. IoT-підхід до побудови інтелектуальних систем відеонагляду

Швидкий розвиток технології Інтернету речей (IoT) спричинив революцію в багатьох секторах, включаючи безпеку та спостереження. Традиційні системи відеоспостереження часто працюють на централізованих архітектурах, які можуть бути обмежені затримкою, проблемами масштабованості та управлінням даними. Натомість, системи відеоспостереження на основі IoT використовують взаємопов'язані датчики, камери та обчислювальні ресурси для створення інтелектуальних, адаптивних та масштабованих мереж безпеки. У розділі досліджується архітектура систем спостереження на базі IoT, ключові технології, що сприяють їхньому розвитку, та значні переваги, які вони пропонують для підвищення безпеки та ситуаційної обізнаності [12].

Архітектура систем відеоспостереження на основі Інтернету речей (IoT) принципово характеризується розподіленою мережею датчиків і камер, які забезпечують збір даних у режимі реального часу в різних середовищах. На відміну від традиційних систем, що покладаються на централізований запис і обробку, архітектури IoT стратегічно розгортають датчики для моніторингу певних зон, забезпечуючи детальне та безперервне охоплення спостереженням. Ці датчики з'єднані між собою за допомогою надійних протоколів зв'язку, таких як MQTT, CoAP або Wi-Fi, що гарантує безперебійну передачу даних навіть у складних або віддалених місцях. Інтеграція з хмарними та периферійними обчислювальними ресурсами ще більше покращує цю архітектуру, дозволяючи локалізовану обробку даних на периферії — ближче до датчиків — зменшуючи затримку та споживання пропускної здатності. Наприклад, периферійні пристрої можуть фільтрувати нерелевантні кадри або виявляти аномалії, перш ніж передавати лише відповідні дані в хмару для подальшого аналізу. Такий багаторівневий підхід гарантує

оперативну обробку критично важливої інформації, підтримуючи прийняття рішень у режимі реального часу та мінімізуючи затримки у часі реагування. Загалом, архітектура IoT сприяє створенню стійкої, масштабованої та ефективної мережі спостереження, здатної адаптуватися до різноманітних потреб безпеки (рис. 2.1).

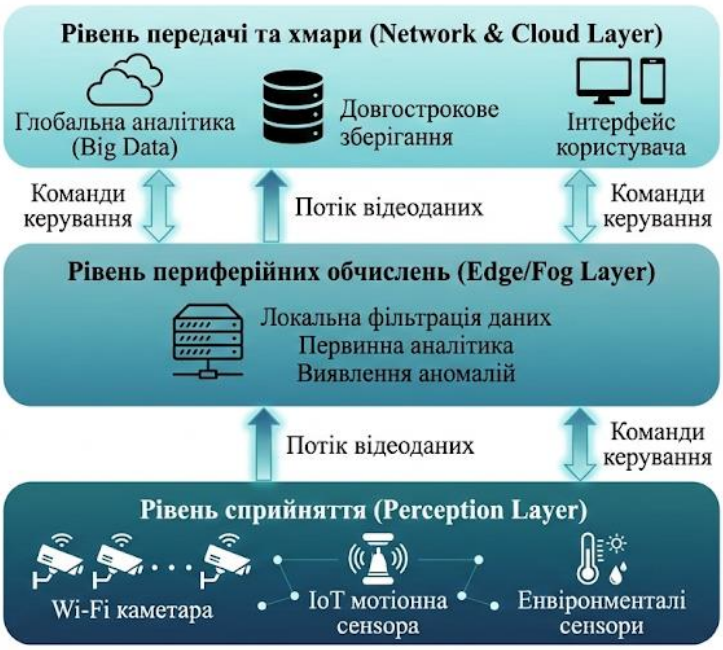


Рис. 2.1. Багаторівнева архітектура системи відеоспостереження на базі IoT

Ключові технологічні досягнення лежать в основі ефективності систем спостереження на основі IoT. Вдосконалені датчики та камери IoT, оснащені високороздільною здатністю зображення, інфрачервоними можливостями та детекцією руху, значно покращують якість збору даних. Ці пристрої можуть працювати в різних умовах навколишнього середовища, забезпечуючи надійну роботу цілодобово. Крім того, алгоритми штучного інтелекту (ШІ) та машинного навчання (МН) відіграють ключову роль в аналізі величезних потоків генерованих даних. Наприклад, аналітика на основі ШІ може автоматично виявляти підозрілу поведінку, таку як байдикування або несанкціонований доступ, зменшуючи залежність від ручного моніторингу. Аналітика великих даних додатково доповнює ці можливості, розпізнаючи складні закономірності з часом, що дозволяє виявляти

нові загрози або аномальні дії. Наприклад, аналізуючи історичні дані про рух, системи можуть прогнозувати потенційні порушення безпеки або виявляти повторювані закономірності доступу, тим самим покращуючи профілактичні заходи. У сукупності ці технології перетворюють необроблені відеопотоки на інтелектуальні аналітичні дані, дозволяючи співробітникам служби безпеки швидко та точно реагувати на ситуації, що змінюються.

Інтеграція Інтернету речей (IoT) у системи відеоспостереження пропонує численні переваги, які значно покращують результати безпеки. Моніторинг у режимі реального часу, що забезпечується взаємопов'язаними датчиками та аналітикою на основі ШІ, дозволяє швидко виявляти інциденти, дозволяючи командам безпеки реагувати оперативно — іноді протягом кількох секунд — таким чином мінімізуючи потенційні збитки або загрози. Масштабованість та гнучкість мереж спостереження IoT означають, що вони можуть легко розширюватися, щоб охоплювати нові зони або включати додаткові пристрої без значного капітального ремонту інфраструктури. Це особливо корисно для масштабних або середовищ, що розвиваються, таких як розумні міста, промислові комплекси або транспортні вузли. Крім того, точність і повнота даних, зібраних за допомогою систем Інтернету речей, покращують загальну ситуаційну обізнаність, забезпечуючи цілісне уявлення про ландшафти безпеки. Наприклад, інтегровані системи можуть поєднувати відеопотоки з датчиками навколишнього середовища, такими як температура або якість повітря, щоб пропонувати контекстно-залежну аналітику, що дозволяє приймати більш обґрунтовані рішення. Зрештою, підхід Інтернету речей не тільки підвищує швидкість і масштаби спостереження, але й гарантує, що заходи безпеки будуть більш точними, адаптивними та ефективними для захисту активів і населення.

Незважаючи на численні переваги систем відеоспостереження на основі Інтернету речей, їх впровадження не обходиться без значних труднощів. Однією з основних проблем є вразливості безпеки; оскільки ці системи стають більш взаємопов'язаними, вони також стають привабливими цілями для кібератак. Хакери можуть використовувати слабкі місця в прошивці пристроїв або протоколах зв'язку,

щоб отримати несанкціонований доступ, що потенційно може призвести до витоків даних або зловмисного маніпулювання каналами спостереження. Крім того, проблеми конфіденційності даних є надзвичайно важливими, особливо коли системи спостереження збирають конфіденційну інформацію про переміщення та діяльність людей. Забезпечення захисту даних від несанкціонованого доступу та неправильного використання вимагає надійних заходів шифрування, автентифікації та контролю доступу. Проблеми сумісності також створюють суттєву перешкоду, оскільки пристрої Інтернету речей часто виготовляються різними виробниками та працюють на різних платформах, що ускладнює безперебійну інтеграцію. Різнорідні системи можуть мати проблеми з ефективним спілкуванням, що призводить до фрагментації даних або операційної неефективності. Крім того, високі початкові витрати, пов'язані з розгортанням інфраструктури відеоспостереження Інтернету речей, такі як придбання передових датчиків, камер та периферійних пристроїв, можуть бути непомірно високими. особливо для невеликих організацій або муніципалітетів. Вимоги до інфраструктури, включаючи надійне мережеве підключення та можливості обробки даних, збільшують фінансове та логістичне навантаження на створення комплексних мереж спостереження IoT (табл. 2.1) [13].

Ефективне управління даними та їх зберігання є критично важливими компонентами систем спостереження на базі IoT, враховуючи величезні обсяги інформації, що генерується. Щоб запобігти перевантаженню даними та забезпечити змістовну аналітику, необхідні такі стратегії, як інтелектуальна фільтрація даних та визначення пріоритетів. Периферійні обчислення відіграють тут життєво важливу роль, обробляючи дані локально для виявлення відповідних подій або аномалій, гарантуючи, що до централізованого сховища передається лише важлива інформація, тим самим зменшуючи використання пропускної здатності та витрати на зберігання. Коли йдеться про рішення для зберігання даних, організації стикаються з вибором між хмарними платформами та локальними серверами.

Таблиця 2.1

Порівняльна характеристика традиційних систем відеоспостереження та систем на базі IoT

Характеристика	Традиційні системи відеоспостереження	Системи на базі технологій IoT
Архітектура мережі	Централізована: всі дані передаються на сервер для запису та обробки.	Розподілена: мережа взаємопов'язаних датчиків та камер з можливістю локальної обробки.
Обробка даних	Обробка на центральному сервері (хмарі), що створює затримки та навантаження на канал.	Периферійні обчислення (Edge Computing): фільтрація та аналіз даних безпосередньо на пристрої.
Масштабованість	Обмежена апаратною ємністю центрального реєстратора; складність розширення.	Висока: легке додавання нових пристроїв без капітального ремонту інфраструктури.
Реакція на події	Часто залежить від людського моніторингу; реакція постфактум.	Режим реального часу: автоматичне виявлення аномалій та миттєве сповіщення (секунди).
Функціональність	Переважно пасивний запис відеопотоку.	Інтелектуальна аналітика (ШІ/МН), контекстна обізнаність, інтеграція з іншими датчиками.

Хмарне сховище пропонує масштабованість, віддалений доступ та простоту управління, що робить його придатним для організацій зі змінними потребами в даних та обмеженою фізичною інфраструктурою. І навпаки, локальні сервери забезпечують більший контроль над даними, підвищену безпеку та переваги відповідності, що особливо важливо для конфіденційної або регульованої інформації. Незалежно від обраного підходу, підтримка цілісності даних є надзвичайно важливою; використання шифрування, регулярне резервне копіювання та контроль доступу допомагає запобігти пошкодженню або втраті даних. Крім того, дотримання правил захисту даних, таких як GDPR або місцеві закони про конфіденційність, має бути пріоритетним для захисту прав особистості та уникнення юридичних наслідків. Впровадження комплексних систем управління

даними гарантує, що дані спостереження управляються етично та відповідально протягом усього їхнього життєвого циклу.

Численні реальні застосування демонструють трансформаційний вплив систем спостереження на базі Інтернету речей у різних секторах. В ініціативах «розумного міста» датчики та камери Інтернету речей розгортаються для підвищення безпеки міста, моніторингу потоку транспорту та ефективнішого управління громадською безпекою. Наприклад, інтегровані мережі Інтернету речей можуть виявляти затори, аварії або позначати підозрілу діяльність у режимі реального часу, що дозволяє владі швидко реагувати та покращувати загальну якість життя в місті. У промислових та критично важливих інфраструктурних умовах спостереження за допомогою Інтернету речей відіграє життєво важливу роль у захисті активів та підтримці безперервності роботи. Датчики контролюють стан навколишнього середовища, структурну цілісність та продуктивність обладнання, попереджаючи персонал про потенційні небезпеки або порушення безпеки, перш ніж вони погіршаться. Безпека публічних заходів також значно підвищується завдяки інтегрованим системам Інтернету речей, які координують кілька пристроїв спостереження для моніторингу великих натовпів, виявлення незвичайної поведінки та безперешкодної координації реагування на надзвичайні ситуації. Наприклад, під час великих спортивних подій або фестивалів відеосистеми на базі Інтернету речей можуть відстежувати переміщення учасників, виявляти потенційні загрози та сприяти швидкому розгортанню персоналу безпеки. Ці тематичні дослідження показують, як рішення для спостереження на основі Інтернету речей не лише покращують безпеку, але й сприяють створенню більш стійких, ефективних та інтелектуальних середовищ у різних контекстах.

Заглядаючи в майбутнє, майбутнє систем відеоспостереження на основі Інтернету речей готове до значних технологічних досягнень, які ще більше розширять їхні можливості та ефективність. Одним з найперспективніших розробок є інтеграція мереж 5G, яка значно покращить зв'язок, пропонуючи вищу пропускну здатність, меншу затримку та надійнішу передачу даних. Цей стрибок у мережевих технологіях дозволить обмінюватися даними в режимі реального часу у

великих та густонаселених середовищах спостереження, сприяючи швидшому прийняттю рішень та більш оперативним заходам безпеки. Крім того, впровадження передової аналітики та алгоритмів глибокого навчання революціонізує аналіз даних у цих системах. Ці складні методи штучного інтелекту можуть забезпечити точніше розпізнавання об'єктів, прогнозування поведінки та виявлення аномалій навіть у складних сценаріях, що включають величезні обсяги даних. Такі досягнення дозволять системам спостереження стати більш автономними, зменшуючи потребу в людському нагляді, одночасно підвищуючи точність та швидкість. Однак, з розвитком цих технологічних можливостей, етичні міркування та розробка політики відповідального спостереження становитимуть критично важливими. Вирішення проблем щодо конфіденційності, неправомірного використання даних та потенційного перевищення повноважень вимагатиме встановлення чітких правил, заходів прозорості та систем підзвітності. Забезпечення відповідності досягнень у сфері спостереження за Інтернетом речей суспільним цінностям та правам людини матиме важливе значення для зміцнення довіри та прийняття цих систем у майбутньому [14].

Системи відеоспостереження на основі Інтернету речей (IoT) являють собою трансформаційний зсув у технологіях безпеки, що характеризуються інноваційною архітектурою, ключовими технологіями та численними перевагами, такими як моніторинг у режимі реального часу, масштабованість та покращена ситуаційна обізнаність. Багаторівнева архітектура, що інтегрує розподілені датчики, хмарні та периферійні обчислення, забезпечує ефективні, стійкі та чуйні мережі спостереження. Технологічні досягнення, такі як високороздільні датчики IoT, штучний інтелект, машинне навчання та аналітика великих даних, дозволили цим системам точно аналізувати величезні обсяги даних, що призводить до швидшого виявлення інцидентів та розумніших заходів безпеки. Незважаючи на ці переваги, необхідно ретельно керувати такими проблемами, як вразливості безпеки, проблеми конфіденційності даних, проблеми сумісності та високі витрати на розгортання. Для безпечного та етичного управління величезними потоками даних необхідні ефективні стратегії управління даними та продумане застосування

рішень для зберігання даних. Тематичні дослідження розумних міст, промислових об'єктів та публічних заходів демонструють глибокий вплив спостереження IoT на створення безпечніших та стійкіших середовищ. У міру розвитку технологій майбутні розробки, такі як інтеграція 5G, глибоке навчання та розширена аналітика, обіцяють ще більші можливості, але вони повинні супроводжуватися надійними етичними рамками для забезпечення відповідального використання. Загалом, відеоспостереження на базі Інтернету речей готове продовжувати своє зростання, пропонуючи розумніші, більш адаптивні рішення безпеки, які формуватимуть майбутнє безпеки у все більш взаємопов'язаному світі.

2.2. Роль та технічні можливості 5G для передачі мультимедійних потоків

Поява технології 5G означає трансформаційний стрибок у бездротовому зв'язку, обіцяючи безпрецедентний прогрес у передачі мультимедійних потоків. На відміну від своїх попередників, 5G розроблений для задоволення зростаючих потреб сучасних цифрових медіа, що характеризуються вищою якістю контенту, взаємодією в режимі реального часу та поширенням підключених пристроїв. У розділі досліджуються основні характеристики технології 5G, її технічні можливості для передачі мультимедіа та її ключова роль у забезпеченні захопливого досвіду доповненої та віртуальної реальності. Розглядаючи ці аспекти, ми можемо оцінити, як 5G не лише вдосконалює існуючі парадигми зв'язку, але й прокладає шлях для інноваційних мультимедійних застосувань, які раніше були недосяжні [15].

В основі технології 5G лежить кілька ключових функцій, які фундаментально переосмислюють бездротовий зв'язок. Одним з найважливіших удосконалень є збільшена пропускна здатність та швидкість передачі даних. Мережі 5G здатні забезпечувати пікову швидкість передачі даних до 20 гігабіт на секунду за оптимальних умов, що значно швидше, ніж мережі 4G LTE. Це суттєве збільшення дозволяє швидко передавати великі мультимедійні файли, такі як відео надвисокої

чіткості, без буферизації чи затримки. Крім того, 5G пропонує наднизьку затримку, часто менше однієї мілісекунди, що життєво важливо для програм реального часу та гарантує майже миттєву передачу пакетів даних. Висока надійність є ще одним наріжним каменем, що характеризується стабільною продуктивністю мережі навіть у години пікового навантаження, що є важливим для критично важливих мультимедійних послуг, таких як прямі трансляції чи дистанційні медичні консультації. Крім того, 5G підтримує масове підключення пристроїв, вміщуючи до мільйона пристроїв на квадратний кілометр. Ця висока щільність мережі забезпечує безперешкодну інтеграцію безлічі інтелектуальних пристроїв, датчиків та систем Інтернету речей, сприяючи створенню надійного середовища для обміну мультимедійними даними між різними платформами та галузями (рис. 2.2).

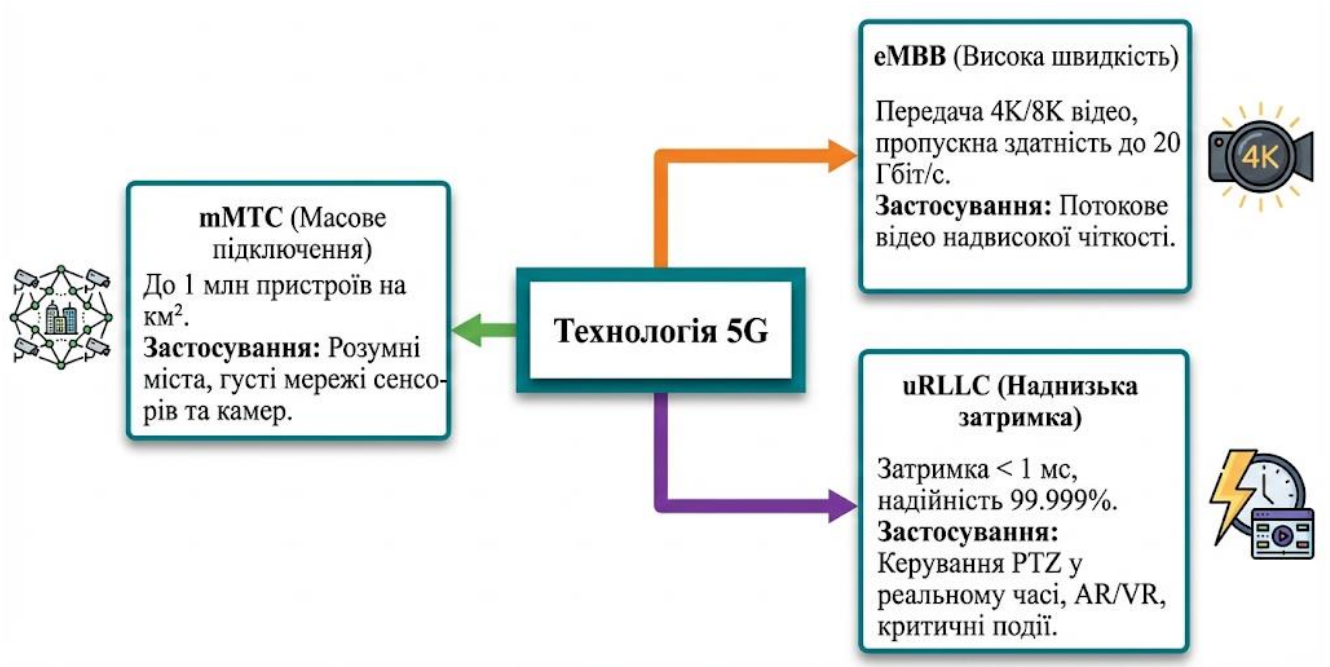


Рис. 2.2. Ключові сценарії використання 5G для мультимедіа та відеоспостереження

Технічні можливості 5G значно підвищують якість передачі та ефективність мультимедійних потоків. Для контенту високої чіткості 5G забезпечує пропускну здатність, необхідну для підтримки потокового відео 4K та навіть 8K, що вимагає значної пропускної здатності. Потокові сервіси можуть забезпечувати кришталево

чисте зображення з мінімальною затримкою, покращуючи враження користувачів у сфері розваг, освіти та професійного сектору. Крім того, підтримка 5G обробки в режимі реального часу та взаємодії з низькою затримкою є критично важливою для прямих трансляцій та інтерактивних медіа. Наприклад, прямі трансляції спортивних подій або концертів можна транслювати з майже миттєвими оновленнями, підтримуючи синхронізацію між мовником та глядачем. Крім того, 5G включає в себе передові методи стиснення даних та ефективніші протоколи передачі, що зменшує загальне навантаження даних без шкоди для якості. Ця ефективність дозволяє забезпечити більш стале використання мережі та потенціал для доставки високоякісного мультимедіа ширшій аудиторії навіть у середовищах з обмеженою пропускною здатністю. Поєднання цих технічних особливостей гарантує швидку, надійну та високоякісну доставку мультимедійного контенту, трансформуючи спосіб споживання та обміну цифровими медіа. Окрім звичайного потокового передавання, 5G відіграє життєво важливу роль у забезпеченні нових технологій, таких як доповнена реальність (AR) та віртуальна реальність (VR), які вимагають надзвичайно високої швидкості передачі даних та низької затримки для оптимальної продуктивності.

Застосунки AR та VR вимагають безперебійної передачі даних для забезпечення захопливого досвіду, будь то ігри, навчальні симуляції чи віддалена співпраця. Високі вимоги до швидкості передачі даних необхідні для передачі складних 3D-моделей, текстур високої роздільної здатності та просторового аудіо в режимі реального часу. Низька затримка не менш важлива; затримки навіть у кілька мілісекунд можуть порушити відчуття занурення та спричинити дискомфорт або дезорієнтацію. Щоб вирішити ці проблеми, 5G інтегрує інфраструктуру периферійних обчислень, наближаючи обчислювальну потужність до кінцевих користувачів та зменшуючи затримки, пов'язані з передачею даних до віддалених центрів обробки даних. Наприклад, у віртуальному класі студенти можуть взаємодіяти з 3D-моделями або брати участь у середовищах спільної роботи в режимі реального часу без помітної затримки. Ця синергія між високою швидкістю передачі даних, низькою затримкою та периферійними обчисленнями відкриває

нову сферу доповненої та віртуальної реальності, роблячи їх більш доступними, адаптивними та захопливими. Оскільки 5G продовжує розвиватися, його здатність підтримувати ці передові мультимедійні програми, ймовірно, прискорить інновації в багатьох секторах, включаючи охорону здоров'я, освіту, розваги та промисловий дизайн (табл. 2.2) [16].

Таблиця 2.2

Ключові технічні можливості мереж 5G та їх вплив на передачу мультимедіа

Технічний параметр 5G	Значення / Характеристика	Вплив на системи відеоспостереження та мультимедіа
Пропускна здатність	Пікова швидкість до 20 Гбіт/с.	Забезпечує передачу відео у роздільній здатності 4K та 8K без буферизації.
Затримка (Latency)	Менше 1 мілісекунди (Ultra-Low Latency).	Критично важлива для керування PTZ-камерами в реальному часі, AR/VR застосунків та синхронізації прямих ефірів.
Щільність підключень	До 1 мільйона пристроїв на 1 км².	Дозволяє розгортати щільні мережі камер та сенсорів у "Розумних містах" без перевантаження мережі.
Надійність	Стабільна продуктивність навіть у пікові навантаження.	Гарантує безперервність передачі для критично важливих об'єктів та служб екстреного реагування.
Обчислювальні можливості	Інтеграція з Mobile Edge Computing (MEC).	Наближає потужності обробки до користувача, дозволяючи рендеринг складної графіки та аналітику без затримок.

Поява технології 5G значно трансформувала послуги прямого мовлення та потокового передавання, покращивши як їхню стабільність, так і загальну якість. Завдяки високій пропускній здатності та низькій затримці, 5G дозволяє мовникам безперешкодно передавати контент високої та надвисокої чіткості, навіть у режимі реального часу. Це призводить до більш надійного потокового передавання для глядачів, мінімізуючи переривання, буферизацію та погіршення якості, які часто переслідували попередні покоління бездротових мереж. Крім того, здатність 5G підтримувати високоякісний мультимедійний контент у режимі реального часу

відкрила нові горизонти для подій у прямому ефірі, таких як спортивні змагання, концерти та висвітлення новин, дозволяючи глядачам сприймати події так, ніби вони фізично присутні. Крім того, 5G сприяє розвитку мобільних та дистанційних установок мовлення, надаючи журналістам, творцям контенту та мовникам можливість працювати практично з будь-якого місця. Можливість розгортати легке портативне обладнання для мовлення з високими можливостями передачі даних означає, що пряме висвітлення може бути... більш гнучким, динамічним та доступним. Як наслідок, індустрія розваг та медіа переживає зміну парадигми, коли більш захопливий та безпосередній прямий контент стає стандартним очікуванням для споживачів.

Попри численні переваги, розгортання та впровадження 5G у мультимедійній передачі стикається з кількома технічними труднощами та обмеженнями. Однією з основних проблем є ослаблення сигналу та прогалини в покритті, особливо в густонаселених міських районах, де високочастотні сигнали 5G насилу проникають крізь будівлі та інші перешкоди. Ці обмеження покриття можуть призвести до нестабільної якості послуг та перешкоджати широкому впровадженню, особливо в сільській місцевості або менш розвинених регіонах. Крім того, розгортання інфраструктури 5G пов'язане зі значними витратами та складністю, вимагаючи встановлення численних малих стільникових станцій та модернізації існуючих мережевих компонентів. Ці інвестиції в інфраструктуру можуть бути непомірними для деяких постачальників послуг та урядів, що потенційно може затримати повну реалізацію переваг 5G. Сумісність також створює проблему; багато існуючих пристроїв та мереж ще не оснащені для повного використання можливостей 5G, що вимагає розробки та впровадження нових апаратних та програмних стандартів. Подолання розриву між поточною інфраструктурою та мережами 5G наступного покоління залишається критичною перешкодою, яку необхідно вирішити, щоб максимально використати його потенціал для передачі мультимедіа.

Дивлячись у майбутнє, 5G обіцяє створити безліч інноваційних застосувань та технологічних досягнень у доставці мультимедійного контенту. Однією з найцікавіших перспектив є інтеграція штучного інтелекту (ШІ) з мережами 5G для

адаптивних потокових рішень. ШІ може оптимізувати розподіл пропускної здатності та динамічно регулювати якість відео на основі мережевих умов та уподобань користувача, забезпечуючи постійно високу якість, зберігаючи водночас мережеві ресурси. Крім того, очікується, що можливості 5G каталізуватимуть розвиток абсолютно нових мультимедійних застосувань, таких як повністю захопливий голографічний зв'язок, потокове відео на 360 градусів та інтерактивний досвід у реальному часі. Ці досягнення можуть революціонізувати такі галузі, як розваги, освіта, охорона здоров'я та промисловий дизайн, забезпечуючи багатший та цікавіший контент. Поєднання високих швидкостей передачі даних, низької затримки та периферійних обчислень також сприятиме передачі складних 3D-моделей та голографічних зображень, створюючи можливості для віддаленої діагностики, віртуальних зустрічей та захопливого сторітелінгу. Оскільки технологія 5G продовжує розвиватися, вона готова розпочати нову еру мультимедійних інновацій, трансформуючи те, як люди створюють, діляться та сприймають цифровий контент у всіх секторах.

Оскільки розгортання 5G революціонізує передачу мультимедіа, це одночасно викликає критичні занепокоєння щодо безпеки та конфіденційності. Збільшення зв'язку, що забезпечується 5G, що характеризується експоненціальним зростанням кількості підключених пристроїв та обміну даними, розширює поверхню атаки для кіберзагроз. Ця підвищена вразливість робить мережі більш вразливими до злому, витоків даних та зловмисних атак, які можуть поставити під загрозу конфіденційну інформацію користувачів або порушити надання послуг. Щоб зменшити ці ризики, надійні протоколи шифрування даних та засоби захисту конфіденційності користувачів є важливими компонентами інфраструктури 5G. Ці заходи включають наскрізне шифрування, безпечні механізми автентифікації та суворий контроль доступу, що захищає цілісність та конфіденційність мультимедійних потоків. Крім того, широке використання 5G для потокової передачі та взаємодії в режимі реального часу створює складні регуляторні та етичні проблеми. Уряди та організації повинні створити комплексні рамки для регулювання збору, зберігання та обміну даними, забезпечуючи дотримання законів

про конфіденційність та захищаючи права користувачів. Етичні міркування також виникають через потенційне нецільове використання мультимедійних даних, таке як несанкціоноване спостереження або маніпулювання контентом, що підкреслює необхідність прозорої політики та відповідальних інновацій. Оскільки 5G продовжує розвиватися, вирішення цих питань безпеки та конфіденційності залишається першочерговим для зміцнення довіри та забезпечення сталого технологічного прогресу в передачі мультимедіа.

Технологія 5G знаменує собою значну віху в еволюції бездротового зв'язку, фундаментально змінюючи ландшафт потокового передавання мультимедіа та взаємодії. Її основні характеристики – розширена пропускна здатність, наднизька затримка та масове підключення пристроїв – закладають основу для підтримки високоякісного контенту, обробки в режимі реального часу та поширення підключених пристроїв у різних галузях. Технічні можливості 5G забезпечують безперебійну доставку відео високої чіткості, захопливого досвіду доповненої та віртуальної реальності, а також надійного прямого мовлення, відкриваючи нові горизонти для розваг, освіти та віддаленої співпраці. Однак ці досягнення не позбавлені викликів, включаючи обмеження покриття, витрати на інфраструктуру та проблеми сумісності пристроїв, які необхідно вирішити для максимального впровадження. Заглядаючи вперед, майбутнє 5G обіцяє новаторські інновації, такі як адаптивне потокове передавання на основі штучного інтелекту та голографічне мультимедіа, які ще більше переосмислять цифровий досвід. Тим не менш, як і в будь-якій технологічній революції, збільшення підключення та потоку даних створює значні проблеми безпеки та конфіденційності, які вимагають пильних заходів безпеки та етичного нагляду. Загалом, 5G готовий революціонізувати передачу мультимедіа, сприяючи новій ері захопливого, ефективного та інноваційного цифрового зв'язку, підкреслюючи важливість безпечного та відповідального розгортання.

2.3. Виклики, обмеження та перспективи поєднання IoT і 5G у відеоспостереженні

Злиття технології Інтернету речей (IoT) та бездротових мереж п'ятого покоління (5G) сповіщає про нову еру у відеоспостереженні, обіцяючи безпрецедентний рівень підключення, обробку даних у режимі реального часу та розширені можливості безпеки. Ця інтеграція готова трансформувати системи спостереження в різних секторах, включаючи міську безпеку, транспорт та промисловий моніторинг. Однак шлях до повної реалізації потенціалу IoT та 5G у відеоспостереженні пов'язаний з численними викликами та обмеженнями. Технічні перешкоди, такі як високі вимоги до передачі даних та проблеми з надійністю мережі, загрожують продуктивності та масштабованості системи. Одночасно інфраструктурні та розгортальні бар'єри, особливо в різних географічних регіонах, перешкоджають широкому впровадженню. Крім того, проблеми щодо конфіденційності та безпеки створюють значні етичні та правові дилеми, що вимагає надійних гарантій для запобігання зловживанням. У розділі критично розглядаються багатогранні виклики, обмеження та перспективи, пов'язані з інтеграцією технологій IoT та 5G у відеоспостереження, надаючи уявлення про складний ландшафт, в якому зацікавлені сторони повинні орієнтуватися [17].

Однією з найважливіших технічних проблем інтеграції Інтернету речей (IoT) та 5G у системи відеоспостереження є управління величезним обсягом даних, що генеруються камерами високої чіткості та сенсорними мережами. Сучасні системи спостереження виробляють величезні обсяги даних у режимі реального часу, що вимагає швидких можливостей передачі та обробки. Мережі 5G розроблені для підтримки вищих швидкостей передачі даних — теоретично до 10 Гбіт/с — але фактична реалізація часто не відповідає вимогам через перевантаження мережі та обмеження інфраструктури, особливо в густонаселених міських районах. Крім того, затримка, властива передачі великих потоків даних, може погіршити можливості реагування в режимі реального часу, що є критично важливим для систем безпеки. Наприклад, затримки в передачі живого відео можуть

перешкоджати оперативному реагуванню правоохоронних органів на інциденти. Сумісність та стандартизація також створюють значні перешкоди; різноманітні пристрої від різних виробників часто працюють за різними протоколами, що призводить до проблем сумісності. Без єдиних стандартів інтеграція різнорідних пристроїв IoT з мережами 5G стає складною, ризикуючи фрагментацією системи та зниженням ефективності. Ці технічні бар'єри вимагають постійних досліджень та розробок для оптимізації стиснення даних, вдосконалення архітектури мережі та встановлення універсальних стандартів, які сприяють безперебійній інтеграції.

Окрім технічних перешкод, інфраструктурні обмеження значно обмежують розгортання систем відеоспостереження з підтримкою IoT та 5G. Хоча міські центри можуть поступово розширювати покриття 5G, багато сільських та недостатньо обслуговуваних районів все ще страждають від недостатньої мережевої інфраструктури, що перешкоджає розгортанню комплексних мереж спостереження. Високі витрати, пов'язані з встановленням та обслуговуванням передового обладнання для спостереження, включаючи камери та датчики, сумісні з 5G, ще більше посилюють проблему. Невеликі муніципалітети або приватні організації можуть вважати фінансовий тягар непосильним, обмежуючи їхні можливості щодо модернізації існуючих систем. Крім того, джерело живлення для цих пристроїв створює практичні проблеми; багато датчиків та камер Інтернету речей залежать від стабільних джерел електроенергії, які не завжди доступні у віддалених або недостатньо обслуговуваних місцях. Технічне обслуговування та довговічність пристроїв також створюють постійні проблеми, оскільки обладнання для спостереження необхідно регулярно ремонтувати або замінювати для забезпечення цілісності роботи. Отже, дефіцит інфраструктури не тільки перешкоджає початковому розгортанню, але й загрожує довгостроковій стійкості мереж спостереження з підтримкою Інтернету речей та 5G, що підкреслює необхідність економічно ефективних та енергоефективних рішень.

Питання конфіденційності та безпеки, мабуть, є найнагальнішими обмеженнями у розгортанні Інтернету речей та 5G для відеоспостереження. Поширення взаємопов'язаних пристроїв підвищує ризик витоків даних,

несанкціонованого доступу та кібератак, які можуть поставити під загрозу конфіденційну інформацію або дозволити зловмисну діяльність. Наприклад, хакери можуть використовувати вразливості системи безпеки для вилучення каналів спостереження, маніпулювання відеозаписами або повного виведення з ладу систем. Такі інциденти підривають довіру громадськості та викликають етичні питання щодо балансу між безпекою та правами на конфіденційність особистості. Потенційне зловживання даними спостереження для зловмисних цілей, таких як переслідування або політичні репресії, підкреслює важливість встановлення надійних протоколів безпеки та суворого контролю доступу. Впровадження наскрізного шифрування, безпечних механізмів автентифікації та постійного аудиту безпеки є важливими для зменшення цих ризиків. Однак динамічний характер кіберзагроз означає, що заходи безпеки повинні постійно розвиватися, вимагаючи значних інвестицій як у технології, так і в навчання персоналу. Оскільки системи спостереження стають все більш поширеними та складними, вирішення проблем конфіденційності та безпеки залишається суттєвим викликом, який зацікавлені сторони повинні пріоритезувати, щоб забезпечити відповідальне та етичне розгортання (табл. 2.3) [18].

Одна з критичних проблем, що стоять перед інтеграцією Інтернету речей та 5G у відеоспостереження, стосується обмежень управління даними та їх зберігання. Камери високої роздільної здатності та розгалужена мережа датчиків постійно генерують величезні обсяги даних, часто досягаючи терабайтів щодня навіть для систем середнього масштабу. Керування цим потоком інформації вимагає надійної інфраструктури, здатної обробляти дані в режимі реального часу, що залишається значною перешкодою. Обробка високоякісних відео в режимі реального часу передбачає складні алгоритми та значну обчислювальну потужність, що часто навантажує існуючі мережеві та серверні можливості. Крім того, потреба в масштабованих рішеннях для зберігання даних є надзвичайно важливою; з розширенням мереж відеоспостереження зростає і попит на більшу ємність для зберігання даних.

Таблиця 2.3

Класифікація викликів та обмежень при впровадженні систем відеоспостереження на базі IoT та 5G

Категорія викликів	Основні проблеми та перешкоди
Технічні проблеми	Управління даними: Величезні обсяги інформації (терабайти щодня), що потребують потужної обробки .Сумісність: Відсутність єдиних стандартів між пристроями різних виробників (фрагментація) .Реальна швидкість: Невідповідність теоретичних 10-20 Гбіт/с реальним умовам через перевантаження.
Інфраструктурні обмеження	Покриття: Слабке проникнення високочастотного сигналу 5G крізь стіни та відсутність мереж у сільській місцевості .Вартість: Високі капітальні витрати на обладнання та густу мережу базових станцій .Енергозабезпечення: Складність живлення віддалених датчиків.
Безпека та конфіденційність	Кіберзагрози: Збільшення поверхні атаки через велику кількість підключених пристроїв; вразливість прошивок .Захист даних: Ризики витоку конфіденційної інформації та відеозаписів.
Правові та регуляторні аспекти	Законодавство: Відмінності у регулюванні спостереження в різних регіонах; проблеми транскордонної передачі даних .GDPR: Необхідність суворого дотримання правил захисту персональних даних.

Традиційні методи зберігання можуть мати труднощі з врахуванням потоку даних, що призводить до потенційних проблем з їх отриманням та аналізом. Це створює труднощі для швидкого доступу до історичних відеоматеріалів або проведення судово-медичних розслідувань, особливо коли дані зберігаються в різних місцях. різнорідних систем або у застарілих форматах. Хмарне сховище пропонує перспективне рішення, але воно створює занепокоєння щодо затримки, безпеки даних та витрат. Проблема полягає в розробці ефективних методів стиснення даних, інтелектуальної фільтрації даних та масштабованих архітектур сховища, які можуть адаптуватися до зростаючих потреб спостереження без шкоди для швидкості чи безпеки.

Окрім технологічних та інфраструктурних бар'єрів, регуляторні та правові обмеження суттєво впливають на розгортання та експлуатацію систем

відеоспостереження на базі Інтернету речей та 5G. Нормативні бази, що регулюють спостереження, сильно відрізняються в різних регіонах, часто відстаючи від технологічного прогресу. Наприклад, деякі країни мають суворі закони про захист даних, які обмежують збір, зберігання та обмін записами спостереження, тоді як інші взагалі не мають чітких правил, що призводить до непослідовної практики. Транскордонний обмін даними створює додаткові труднощі, особливо коли дані спостереження, зібрані в одній юрисдикції, зберігаються або аналізуються в іншій, що порушує питання суверенітету даних та дотримання місцевих законів. Ці правові невизначеності можуть перешкоджати міжнародній співпраці та перешкоджати розвитку комплексних мереж спостереження. Крім того, відсутність стандартизованих рекомендацій щодо відповідальної практики спостереження створює неоднозначність щодо прийнятного використання, захисту конфіденційності та заходів підзвітності. Без чіткої правової та регуляторної бази організації стикаються з ризиком юридичних наслідків, негативної реакції громадськості або неправильного використання даних спостереження, що підкреслює важливість встановлення прозорої, послідовної політики, яка б збалансувала потреби безпеки з правами особистості.

Попри ці виклики, майбутні перспективи поєднання Інтернету речей та 5G у відеоспостереженні є багатообіцяючими, пропонуючи розширені можливості, які можуть революціонізувати управління та безпеку міст. Інтеграція цих технологій дозволяє покращити моніторинг у режимі реального часу, дозволяючи владі швидше та ефективніше реагувати на такі інциденти, як злочини, аварії чи стихійні лиха. Наприклад, високошвидкісні мережі 5G сприяють миттєвій передачі відео високої чіткості, що може бути вирішальним у термінових ситуаціях. Крім того, інтеграція штучного інтелекту (ШІ) у системи спостереження значно посилює їхні аналітичні можливості, забезпечуючи автоматизоване виявлення загроз, розпізнавання облич, аналіз поведінки та виявлення аномалій. Ці інтелектуальні системи можуть фільтрувати величезні обсяги даних, виявляти закономірності та попереджати операторів про потенційні проблеми без втручання людини, тим самим підвищуючи ефективність та точність. Крім того, синергія Інтернету речей

та 5G відкриває можливості для розробки додатків для розумних міст, інтегруючи спостереження з управлінням дорожнім рухом, моніторингом навколишнього середовища та ініціативами громадської безпеки. Такі взаємопов'язані системи можуть оптимізувати роботу міста, покращити розподіл ресурсів та сприяти безпечнішому та більш чутливому міському середовищу. Хоча ці перспективи є переконливими, реалізація їхнього повного потенціалу вимагає подолання існуючих технічних, інфраструктурних та регуляторних перешкод шляхом постійних інновацій та розробки політики [19].

Численні можливості та напрямки досліджень мають потенціал для вирішення поточних проблем та розкриття всіх можливостей інтеграції Інтернету речей (IoT) та 5G у відеоспостереження. Основна увага приділяється розробці енергоефективних пристроїв IoT, які можуть стабільно працювати в різних середовищах, особливо у віддалених або районах з дефіцитом інфраструктури. Інновації в малопотужних датчиках та технологіях збору енергії можуть значно знизити витрати на обслуговування та покращити термін служби пристроїв, зробивши широке розгортання більш можливим. Водночас, зусилля зі стандартизації мають вирішальне значення для встановлення універсальних протоколів та стандартів сумісності між різними виробниками та платформами. Така гармонізація сприятиме безперешкодній інтеграції, спрощуватиме управління системами та сприятиме конкурентоспроможній екосистемі, керованій інноваціями. Крім того, досягнення в периферійних обчисленнях та штучному інтелекті готові ще більше революціонізувати системи спостереження. Обробляючи дані локально на периферії, системи можуть зменшити затримку, зменшити використання пропускної здатності та покращити швидкість реагування в режимі реального часу. Аналітика на основі штучного інтелекту на периферії може забезпечити негайне виявлення загроз та прийняття рішень, не покладаючись виключно на централізовану хмарну інфраструктуру. Ці технологічні прориви, у поєднанні з поточними дослідженнями, відіграватимуть важливу роль у подоланні існуючих бар'єрів, прокладаючи шлях для створення розумніших, стійкіших та

етично відповідальних мереж спостереження, здатних підтримувати мінливі вимоги сучасного міського життя та безпеки.

Інтеграція технологій Інтернету речей та 5G у відеоспостереження пропонує трансформаційні перспективи для підвищення безпеки, управління міськими районами та громадської безпеки. Однак це багатообіцяюче майбутнє супроводжується значними викликами, включаючи технічні перешкоди, пов'язані з передачею даних та сумісністю пристроїв, обмеження інфраструктури та розгортання, нагальні проблеми конфіденційності та безпеки, обмеження управління та зберігання даних, а також складні регуляторні ландшафти. Вирішення цих проблем вимагає узгоджених зусиль у дослідженнях та розробках, розробці політики та технологічних інноваціях. Майбутні можливості, такі як енергоефективні пристрої, стандартизовані протоколи сумісності, передові периферійні обчислення та інтеграція штучного інтелекту, є ключем до подолання поточних обмежень. У міру того, як зацікавлені сторони орієнтуються в цих складнощах, збалансований підхід, що підкреслює етичні міркування, надійну безпеку та стійку інфраструктуру, буде необхідним для реалізації повного потенціалу Інтернету речей та 5G у створенні розумніших, безпечніших та більш чуйних екосистем спостереження в усьому світі [20].

3. РОЗРОБКА СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ НОВОГО ПОКОЛІННЯ НА БАЗІ WI-FI КАМЕР ІЗ ВИКОРИСТАННЯМ IOT ТА 5G

3.1. Концепція інтегрованої системи Wi-Fi–IoT–5G та її функціональна структура

У швидкозмінному ландшафті цифрового зв'язку інтеграція технологій бездротового зв'язку, таких як Wi-Fi, Інтернет речей (IoT) та 5G, стала ключовою для розвитку інтелектуальних систем та досягнення безперебійного обміну даними між різними платформами. Концепція інтегрованої системи Wi-Fi–IoT–5G втілює комплексну структуру, розроблену для використання унікальних сильних сторін кожної технології для задоволення складних вимог у різних сферах застосування, включаючи розумні міста, промислову автоматизацію та спостереження в режимі реального часу. Це есе має на меті з'ясувати функціональну структуру такої інтегрованої системи, проаналізувавши її фундаментальні вимоги, дослідивши її архітектурний дизайн та вивчивши механізми взаємодії між її основними компонентами. Розуміння цього інтегрованого підходу є важливим для розробки масштабованих, ефективних та надійних рішень для зв'язку, які можуть задовольнити зростаючий попит на високоякісне потокове відео, телеметрію та обробку даних у режимі реального часу [21].

Основою інтегрованої системи Wi-Fi–IoT–5G є чітке визначення її технічних вимог, які слугують основою для проектування та впровадження системи. Для таких застосувань, як потокове відео та телеметрія, система повинна підтримувати високоякісну передачу даних у режимі реального часу з мінімальною затримкою, щоб забезпечити швидке реагування та точний моніторинг. Наприклад, камери спостереження в розумних містах вимагають безперервної передачі відео високої чіткості без перерв, що вимагає значної пропускної здатності та надійної роботи. Тому система повинна враховувати різні навантаження даних, починаючи від телеметрії датчиків з низьким енергоспоживанням і закінчуючи відеопотоками з інтенсивним використанням пропускної здатності. Ключові параметри, такі як

пропускна здатність, повинні бути достатньо високими — часто в діапазоні від кількох сотень Мбіт/с до Гбіт/с для відео — тоді як затримка повинна бути мінімізована, в ідеалі менше 50 мілісекунд, щоб забезпечити майже миттєвий обмін даними. Надійність не менш важлива; втрата пакетів або збої в мережі можуть поставити під загрозу цілісність системи, особливо в критично важливих для безпеки сценаріях, таких як автономна навігація транспортних засобів або управління промисловими процесами. Визначення відповідних сценаріїв використання системи, таких як міське відеоспостереження, дистанційний моніторинг або автономні системи, спрямовує конфігурацію цих технічних вимог, забезпечуючи адаптацію системи до конкретних операційних вимог та обмежень навколишнього середовища (рис. 3.1).



Рис. 3.1. Трирівнева архітектура інтегрованої системи Wi-Fi–IoT–5G

Побудова архітектури інтегрованої системи Wi-Fi–IoT–5G передбачає проектування логічних рівнів, які розмежовують ролі та взаємодію між складовими технологіями. На вищому рівні систему можна концептуалізувати у три основні рівні: рівень Wi-Fi, рівень IoT та рівень 5G. Wi-Fi в першу чергу обслуговує локальний високошвидкісний зв'язок на короткі відстані, ідеальний для приміщень

та локалізованої передачі даних, наприклад, підключення камер до периферійних серверів. Рівень IoT охоплює широкий спектр датчиків, виконавчих механізмів та блоків обробки даних, які збирають та попередньо обробляють дані з різних джерел, слугуючи посередником, який консолідує інформацію про конкретний пристрій. Рівень 5G забезпечує покриття широкої зони з наднадійним зв'язком з низькою затримкою, необхідним для передачі агрегованих даних на хмарні платформи або центральні сервери. Для забезпечення безперебійної роботи між цими рівнями має бути створена структура взаємодії, що включає стандартизовані протоколи зв'язку та інтерфейси обміну даними. Наприклад, пристрої Інтернету речей можуть передавати дані датчиків через Wi-Fi до локальних шлюзів, які потім використовують канали 5G для надсилання критично важливої інформації до віддалених центрів обробки даних. Розробка функціональної карти компонентів, включаючи маршрутизатори, шлюзи, датчики та хмарні сервіси, забезпечує чіткість потоку даних та дозволяє ефективно керувати всією системою, підтримуючи масштабованість та сумісність у різних сценаріях розгортання [22].

Ключовим аспектом інтегрованої системи є взаємодія між Wi-Fi камерами та інфраструктурою Інтернету речей, що передбачає створення безпечних та надійних механізмів для підключення пристроїв, автентифікації та передачі даних. Wi-Fi камери, які часто розгортаються в системах спостереження, повинні безперешкодно підключатися до локальних мереж та автентифікуватися в централізованих системах управління, щоб запобігти несанкціонованому доступу. Цього можна досягти за допомогою надійних протоколів безпеки, таких як WPA3 та автентифікація на основі сертифікатів, які гарантують, що в мережі беруть участь лише авторизовані пристрої. Після підключення ці камери повинні передавати відеопотоки високої чіткості разом із допоміжними службовими даними, такими як часові позначки, стан камери та показники навколишнього середовища, через надійні канали. Зазвичай це забезпечується безпечними високошвидкісними каналами Wi-Fi з'єднаннями Wi-Fi з резервними варіантами переходу на стільникове або дротове з'єднання, якщо це необхідно. Крім того, інтеграція даних датчиків з пристроїв Інтернету речей, таких як датчики руху або датчики

навколишнього середовища, в єдиний потік даних покращує ситуаційну обізнаність. Ця агрегація може відбуватися за допомогою периферійних обчислювальних блоків, які попередньо обробляють відео та дані датчиків перед передачею об'єднаних потоків через мережі 5G або Wi-Fi на віддалені сервери. Така інтеграція не тільки оптимізує використання пропускної здатності, але й забезпечує аналітику в режимі реального часу, що дозволяє системним операторам оперативно реагувати на події та підтримувати безперервність роботи [23].

Фундаментальним компонентом інтегрованої системи Wi-Fi–IoT–5G є розробка ефективного та надійного механізму передачі даних через мережі 5G. Для цього важливо визначити оптимальний маршрут передачі відео від шлюзу Інтернету речей до основної мережі 5G. Цей процес включає вибір найбільш підходящого інтерфейсу — чи то через виділені сегменти 5G, динамічний розподіл спектру, чи сегментацію мережі — для забезпечення високої пропускної здатності та низької затримки передачі великих відеофайлів. Правильний вибір маршруту мінімізує затримки та запобігає перевантаженню, особливо в густонаселених середовищах з кількома потоками даних. Налаштування підтримки якості обслуговування (QoS) та пріоритезації трафіку є не менш важливим; шляхом призначення рівнів пріоритету різним типам даних, таким як відео в реальному часі проти фонової телеметрії, система може ефективно розподіляти мережеві ресурси, забезпечуючи пріоритет потоків, чутливих до затримки. Крім того, формування чітких правил доступу до хмарної інфраструктури є життєво важливим для підтримки безпеки та ефективного управління потоком даних. Ці правила визначають дозволи для пристроїв та служб, диктуючи, як і коли дані передаються на хмарні платформи для зберігання, аналізу або подальшої обробки. Впровадження цих механізмів гарантує, що дані передаються безпечними, оптимізованими шляхами, підтримуючи загальні цілі системи щодо високої продуктивності, надійності та безпеки в різних операційних контекстах.

Система управління та моніторингу інтегрованої архітектури Wi-Fi–IoT–5G має вирішальне значення для підтримки операційної стабільності, оптимізації продуктивності та превентивного вирішення проблем. Розробка централізованої

логіки керування пристроями передбачає створення єдиної платформи управління, яка контролює всі підключені пристрої — від камер і датчиків до шлюзів і мережевих вузлів. Ця платформа повинна підтримувати віддалене налаштування, оновлення прошивки та управління несправностями, що дозволяє швидко реагувати на несправності пристроїв або порушення безпеки. Щоб забезпечити якість відеопотоків та загальний стан системи, необхідно встановити певні показники. До них належать такі параметри, як частота кадрів, роздільна здатність, бітрейт, втрата пакетів, тремтіння та затримка, які разом слугують показниками якості потоку та продуктивності мережі. Моніторинг цих показників у режимі реального часу дозволяє операторам оперативно виявляти погіршення стану та вживати коригувальних заходів. Крім того, інтеграція інструментів аналізу стану мережі, таких як мережеві аналізатори, системи виявлення вторгнень та панелі моніторингу продуктивності, забезпечує комплексне розуміння моделей мережевого трафіку, потенційних вразливостей та вузьких місць. Такий проактивний підхід до управління та моніторингу гарантує безперебійну роботу інтегрованої системи, підтримку високої якості передачі даних та динамічну адаптацію до змінних умов навколишнього середовища або експлуатаційних вимог (табл. 3.1).

Таблиця 3.1

Технічні вимоги до інтегрованої системи Wi-Fi–IoT–5G для різних типів даних

Параметр	Телеметрія (IoT)	Відеопотік (Камери спостереження)
Характер даних	Дані з низьким енергоспоживанням, періодичні	Інтенсивне використання пропускної здатності, безперервний потік
Пропускна здатність	Низька (кбіт/с)	Висока (сотні Мбіт/с — Гбіт/с) для HD/4K
Затримка (Latency)	Допустима середня	Мінімальна (< 50 мс) для реагування в реальному часі
Вимоги до надійності	Висока (гарантована доставка)	Критична (відсутність втрат кадрів та збоїв)

Безпека є першочерговим завданням в архітектурі інтегрованої системи Wi-Fi–IoT–5G через чутливий характер переданих даних та широку поверхню атаки, створену кількома взаємопов'язаними компонентами. Розробка надійної моделі кібербезпеки передбачає встановлення суворих політик автентифікації та авторизації, які контролюють доступ до пристроїв та привілеї даних у всіх сегментах. Наприклад, використання багатофакторної автентифікації, цифрових сертифікатів та контролю доступу на основі ролей допомагає запобігти несанкціонованому доступу пристроїв або користувачів. Методи шифрування між сегментами Wi-Fi, IoT та 5G однаково важливі; для захисту цілісності та конфіденційності даних слід впроваджувати такі протоколи, як AES (Advanced Encryption Standard) для даних у стані спокою та TLS (Transport Layer Security) для даних під час передачі. Необхідно впроваджувати безпечні методи управління ключами, щоб запобігти компрометації ключів та несанкціонованому розшифруванню. Крім того, розробка процедур виявлення та реагування на атаки є важливою для раннього виявлення таких загроз, як спроби вторгнення, зараження шкідливим програмним забезпеченням або витоки даних. Це включає розгортання систем виявлення вторгнень (IDS), алгоритмів виявлення аномалій та автоматизованих протоколів реагування, які можуть ізолювати скомпрометовані пристрої, сповіщати адміністраторів та ініціювати коригувальні дії. Побудова цієї комплексної системи кібербезпеки забезпечує стійкість інтегрованої системи до кіберзагроз, що розвиваються, захищаючи критичні операції та цілісність даних на всіх рівнях мережі [24].

Важливим аспектом проектування інтегрованої системи Wi-Fi–IoT–5G є оцінка її сумісності та масштабованості, щоб гарантувати, що вона зможе відповідати майбутнім вимогам та технологічним досягненням. Перевірка відповідності встановленим стандартам, таким як IEEE 802.11 для Wi-Fi, різні протоколи зв'язку Інтернету речей, такі як MQTT та CoAP, а також специфікації 3GPP для 5G, має вирішальне значення для безперебійної сумісності між пристроями та компонентами. Дотримання стандартів не тільки сприяє інтеграції з існуючою інфраструктурою, але й гарантує, що система залишається адаптивною в

міру появи нових пристроїв та технологій. Крім того, аналіз масштабованості включає оцінку того, чи може архітектура вмістити велику кількість пристроїв, таких як сотні або тисячі камер, у розгортанні розумного міста. Це вимагає вивчення пропускної здатності мережі, забезпечення пропускної здатності та надійності протоколів контролю та управління для підтримки збільшених навантажень даних без погіршення продуктивності. Також важливо враховувати потенційні обмеження, такі як апаратні обмеження, перевантаження мережі або несумісність протоколів, які можуть перешкоджати розширенню. Раннє виявлення цих обмежень дозволяє системним архітекторам впроваджувати масштабовані рішення. рішення, такі як ієрархічні мережеві структури, розподілена обробка та модульні компоненти, які можуть органічно зростати, зберігаючи стабільність та продуктивність. Визнання цих факторів гарантує, що інтегрована система залишається гнучкою та стійкою, здатною розвиватися разом з технологічними та операційними вимогами [25].

Підсумовуючи, концепція інтегрованої системи Wi-Fi–IoT–5G охоплює комплексну структуру, розроблену для задоволення високих вимог сучасних рішень для підключення. Базовий крок включає чітке визначення технічних специфікацій для високоякісного потокового відео та телеметрії, з акцентом на пропускній здатності, затримці та надійності, що відповідають різним операційним сценаріям. Архітектурно, проектування логічних рівнів та встановлення механізмів взаємодії між компонентами Wi-Fi, IoT та 5G створюють цілісну, масштабовану інфраструктуру, здатну підтримувати різноманітні програми (табл. 3.2).

Таблиця 3.2

Функціональні рівні архітектури системи

Рівень архітектури	Основні технології	Функціональне призначення
Рівень Wi-Fi	Wi-Fi 6 (802.11ax)	Локальний високошвидкісний зв'язок на короткі відстані (приміщення)
Рівень IoT	Сенсори, MQTT, CoAP	Збір, попередня обробка та консолідація даних з датчиків
Рівень 5G	5G NR, Network Slicing	Покриття широкої зони, надійна передача агрегованих даних у хмару

Взаємодія між Wi-Fi камерами та пристроями IoT ілюструє, як безпечна, ефективна передача даних та інтеграція сприяють обізнаності про ситуацію в режимі реального часу. Крім того, впровадження надійних механізмів передачі даних через 5G, разом із централізованим управлінням, моніторингом та протоколами кібербезпеки, забезпечує операційну стабільність, високу продуктивність та цілісність даних. Нарешті, оцінка сумісності та масштабованості системи гарантує, що архітектура може розвиватися, щоб враховувати зростання щільності пристроїв без шкоди для функціональності. У сукупності ці елементи підкреслюють важливість добре структурованої, безпечної та адаптованої інтегрованої системи для задоволення майбутніх потреб взаємопов'язаних середовищ, сприяючи розвитку розумніших міст, галузей та громад [26].

3.2. Реалізація прототипу, оптимізація відеопередачі та оцінка ефективності

У цьому технічному звіті описано комплексний процес розробки, оптимізації та оцінки передової інтегрованої системи Wi-Fi–IoT–5G, призначеної для високоякісної передачі відео. Основною метою є створення надійного прототипу, який бездоганно поєднує стандарти бездротового зв'язку з інтелектуальною обробкою даних для забезпечення надійної передачі відео в режимі реального часу в складних мережевих середовищах. Розглядається створення функціонального прототипу, ретельне налаштування параметрів Wi-Fi для забезпечення стабільної передачі та впровадження адаптивних алгоритмів, які динамічно оптимізують якість відео на основі мережевих умов. Ці зусилля мають вирішальне значення для розвитку застосувань в інтелектуальному спостереженні, дистанційному моніторингу та автономних системах, де безперебійні відеопотоки мають першорядне значення. Кожен етап підтримується детальними технічними стратегіями та емпіричними міркуваннями, що підкреслює важливість інтегрованого проектування системи, налаштування мережі та адаптивного

управління даними для задоволення високих вимог сучасних інфраструктур бездротового зв'язку [27].

Основою системи була розробка комплексного прототипу, який інтегрує сегменти Wi-Fi, IoT та 5G в єдину операційну структуру. Центральним елементом цих зусиль було створення детальної структурної схеми, що ілюструє взаємодію між Wi-Fi камерою, шлюзом IoT та вузлом мережі 5G.

Ключовою відмінністю розробленого прототипу від типових рішень є інтеграція авторського алгоритму адаптивного керування передачею відеоданих, логіка роботи якого представлена на рис. 3.3.

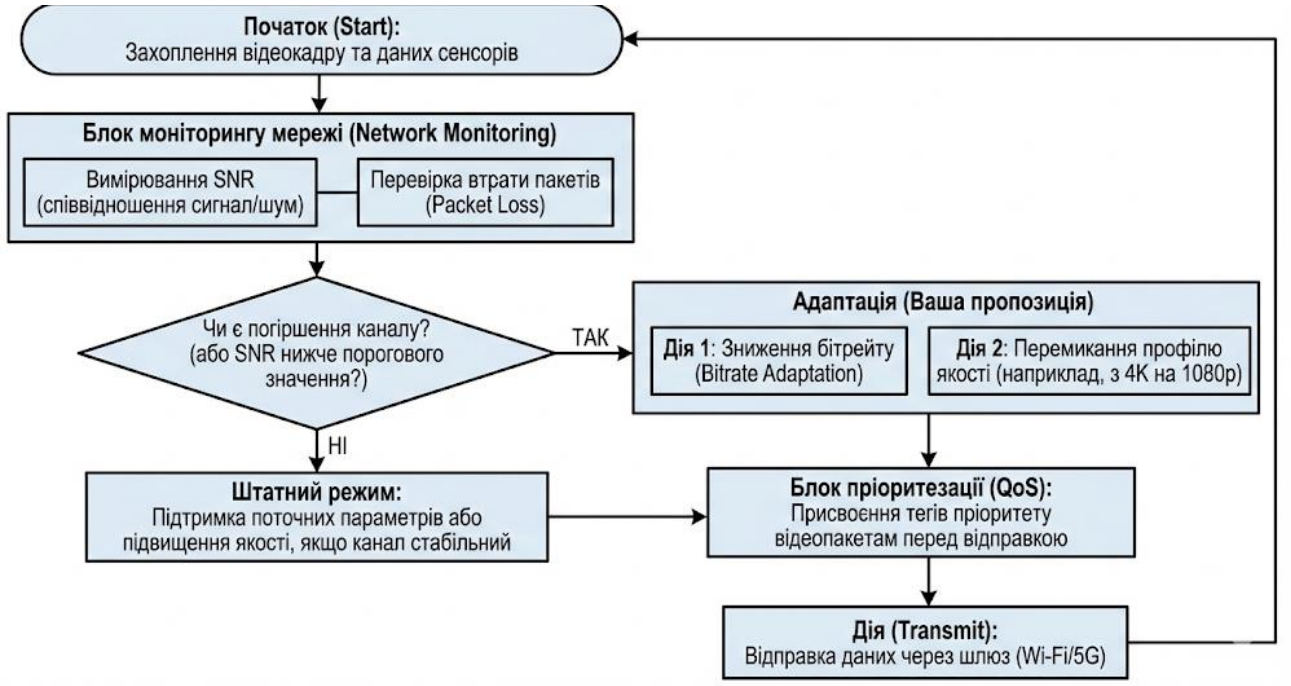


Рис. 3.3. Блок-схема алгоритму адаптивного керування передачею відеоданих

Запропонований алгоритм вирішує проблему нестабільності бездротового каналу шляхом впровадження циклу зворотного зв'язку в реальному часі. На відміну від стандартних механізмів, які часто реагують на погіршення зв'язку лише після втрати з'єднання, наша пропозиція передбачає превентивну адаптацію параметрів потоку.

Алгоритм функціонує за наступним сценарієм:

1. Моніторинг стану каналу: Система безперервно аналізує метрики якості мережі (SNR, рівень джиттера та відсоток втрачених пакетів).

2. Прийняття рішень: При виявленні відхилення показників від норми (наприклад, падіння SNR нижче порогового значення), блок прийняття рішень ініціює зміну профілю кодування.

3. Динамічна адаптація: Залежно від ступеня деградації каналу, алгоритм виконує одну з двох дій:

– *М'яка корекція:* зниження бітрейту (Bitrate Throttling) без зміни роздільної здатності.

– *Жорстка корекція:* перемикання на профіль з нижчою роздільною здатністю (наприклад, з 4K на 1080p або 720p) для збереження плавності руху (FPS) за рахунок деталізації.

4. Пріоритезація (QoS): Сформовані відеопакети маркуються тегами високого пріоритету перед відправкою на шлюз, що забезпечує їх першочергову обробку в черзі маршрутизатора.

Саме ця програмна логіка дозволяє системі утримувати з’єднання та передавати інформативне зображення навіть в умовах, коли традиційна Wi-Fi камера втратила б зв’язок або передавала б пошкоджене зображення.

Ця схема окреслює шляхи потоку даних, сигнали керування та протоколи взаємодії, необхідні для синхронізованої роботи. Наприклад, Wi-Fi камера захоплює відео високої чіткості та передає телеметричні дані через захищене бездротове з'єднання до шлюзу IoT, який діє як посередник, обробляючи та упаковуючи дані для ефективної передачі через сегмент 5G. Налаштування мережевих інтерфейсів передбачало вибір відповідних протоколів зв'язку, таких як MQTT для телеметрії та RTP/RTSP для потокового відео, що забезпечувало сумісність та низьку затримку. Інтеграція цих компонентів в єдиний програмний модуль вимагала ретельного програмування для полегшення збору, кодування та передачі даних у режимі реального часу. Цей модуль об'єднує відеопотоки та телеметричні дані, забезпечуючи синхронізовану обробку та передачу, що є

критично важливим для застосувань, що вимагають мінімальної затримки та високої надійності. Успіх цього прототипу заклав основу для подальшої оптимізації та оцінки продуктивності, демонструючи, що безперебійна сумісність між різнорідними сегментами мережі досяжна завдяки ретельному проектуванню системи та інтеграції протоколів (табл. 3.3).

Таблиця 3.3

Параметри оптимізації бездротового каналу Wi-Fi для відеопередачі

Параметр налаштування	Обране значення / Метод	Очікуваний ефект
Частотний діапазон	5 ГГц	Зменшення перешкод, покращення пропускної здатності
Режим роботи	802.11ax (Wi-Fi 6)	Використання OFDMA та MU-MIMO для зниження затримки
Кодек відео	H.264 / H.265	Ефективне стиснення та адаптивне керування бітрейтом
Керування якістю (QoS)	Пріоритет відеотрафіку	Мінімізація втрат пакетів та повторних передач

Досягнення стабільної та високоякісної передачі відео через Wi-Fi вимагає точного налаштування параметрів бездротового каналу. З цією метою було проведено масштабну оптимізацію налаштувань Wi-Fi, зосереджуючись на виборі каналу, пропускній здатності, потужності передачі та режимі роботи. Наприклад, вибір оптимальної пропускної здатності каналу 5 ГГц зменшив перешкоди та покращив пропускну здатність, а регулювання рівнів потужності передачі мінімізував втрату пакетів та підвищив стабільність сигналу. Крім того, вибір режиму Wi-Fi, такого як 802.11ax (Wi-Fi 6), забезпечив розширені функції, такі як OFDMA та MU-MIMO, що збільшило пропускну здатність та зменшило затримку. Вибір кодека, бітрейт та налаштування частоти кадрів були ретельно налаштовані; наприклад, використання кодека H.264 або H.265 з адаптивним керуванням бітрейтом дозволило системі підтримувати плавні відеопотоки за різних мережевих умов. Динамічно регулюючи бітрейт і частоту кадрів на основі зворотного зв'язку з мережі в режимі реального часу, система могла запобігти вичерпанню буфера та зменшити тремтіння. Втрата пакетів була додатково зменшена за допомогою

мережевих налаштувань, таких як увімкнення тегів якості обслуговування (QoS) та оптимізація розмірів буферів, що приділяло пріоритет відеопакетам і мінімізувало повторні передачі. Ці заходи разом сприяли створенню стійкого каналу Wi-Fi, здатного підтримувати стабільні відеопотоки високої роздільної здатності в динамічних середовищах, що характеризуються коливаннями перешкод та обмеженнями пропускної здатності [28].

Для подальшого підвищення стійкості передачі було впроваджено адаптивні алгоритми передачі відео, що дозволило системі динамічно реагувати на зміну мережевих умов. Однією з ключових функцій була адаптація бітрейту, яка включала постійний моніторинг стану каналу, такого як співвідношення сигнал/шум (SNR) та втрата пакетів, і регулювання бітрейту в режимі реального часу для оптимізації якості відео без перевантаження мережі. Наприклад, у періоди високих перешкод система зменшувала бітрейт, тим самим зменшуючи навантаження на мережу та запобігаючи перевантаженню. Крім того, було запроваджено механізм динамічного перемикання профілів якості, що дозволяє системі перемикатися між різними налаштуваннями роздільної здатності та стиснення, такими як від 4K до 1080p, на основі поточних показників продуктивності мережі. Такий підхід гарантував, що критично важливі відеопотоки підтримували прийнятний рівень якості навіть за несприятливих умов. Політики QoS також були точно налаштовані, щоб надавати пріоритет відеотрафіку над менш конфіденційними даними, враховуючи показники навантаження як з сегментів Wi-Fi, так і з сегментів 5G. Завдяки інтеграції цих адаптивних алгоритмів система досягла балансу між якістю відео та стабільністю передачі, значно покращуючи загальну продуктивність у змінних мережевих середовищах. Емпіричні тести показали, що такі адаптивні механізми можуть зменшити затримку, мінімізувати втрату пакетів та підтримувати високоякісні відеопотоки, тим самим підтверджуючи їхню ефективність для реальних розгортань.

Критичним аспектом функціональності системи є безперешкодна інтеграція даних датчиків Інтернету речей з відеопотоком для забезпечення комплексного моніторингу. Ця інтеграція була досягнута завдяки розробці спеціалізованого

каналу доставки даних датчиків, який працює одночасно зі шляхом передачі відео. Конструкція гарантує, що телеметричні дані, такі як температура, вологість, виявлення руху або стан пристрою, інкапсулюються в легкі пакети та передаються разом із відеокадрами. Підтримка часової кореляції між даними та візуальною інформацією. Для точної синхронізації пакетів Інтернету речей з відеокадрами були реалізовані механізми позначення часу, які сприяють точному узгодженню показань датчиків з відповідними мітками часу відео. Ця синхронізація є життєво важливою для таких застосувань, як відеоспостереження або моніторинг навколишнього середовища, де співвіднесення подій датчиків з візуальними доказами покращує ситуаційну обізнаність. Крім того, були впроваджені процеси фільтрації та агрегації телеметрії для оптимізації використання пропускної здатності; фільтрація видаляє надлишкові або нерелевантні дані, тоді як агрегація об'єднує показання кількох датчиків у консолідовані звіти. Такий підхід зменшує навантаження на мережу, мінімізує затримку та гарантує передачу лише відповідної інформації, тим самим підвищуючи ефективність та надійність системи. Інтегровані дані Інтернету речей, синхронізовані з високоякісними відеопотоками, підвищують здатність системи надавати комплексні ситуаційні дані в режимі реального часу в складних операційних середовищах [29].

Продуктивність усієї системи значною мірою залежить від ефективної конфігурації протоколів маршрутизації та політик якості обслуговування (QoS) у сегменті мережі 5G. Пріоритет відеотрафіку над іншими типами даних є важливим для підтримки низької затримки та високої надійності відеопотоків у режимі реального часу. З цією метою в мережі 5G було визначено спеціальні класи QoS, що призначають відеотрафіку вищі рівні пріоритету, забезпечуючи мінімальну затримку та джиттер під час передачі. Стратегії маршрутизації були оптимізовані шляхом вибору транспортних маршрутів від шлюзу Інтернету речей до центральних серверів або хмарного сховища, з акцентом на найкоротші та найменш перевантажені шляхи для зменшення часу проходження та втрати пакетів. Для адаптації до різних умов, підтримуючи оптимальну пропускну здатність, використовувалися такі методи, як динамічне коригування маршруту на основі

показників мережевого навантаження. Крім того, в рівень управління мережею були інтегровані механізми контролю затримки та джиттера, такі як стратегії буферизації, формування трафіку та планування пакетів. Ці заходи допомагають згладити тимчасові коливання мережі, мінімізуючи мінливість часу надходження пакетів та забезпечуючи стабільну якість відтворення відео. Поєднання пріоритетної маршрутизації, адаптивного вибору шляху та механізмів зменшення затримки разом підвищує стійкість та стабільність продуктивності системи доставки відео в інфраструктурі 5G (табл. 3.4).

Таблиця 3.4

Метрики оцінки продуктивності системи

Метрика	Опис показника	Значення для системи
Пропускна здатність	Максимальна швидкість передачі даних (відео + IoT)	Визначає здатність мережі витримувати навантаження без деградації
Затримка (Latency)	Час проходження сигналу (End-to-End)	Критично для керування PTZ та реакції на події
Джиттер (Jitter)	Варіація затримки пакетів	Впливає на плавність відтворення відео
Втрата пакетів	% втрачених даних при передачі	Впливає на цілісність зображення та артефакти

Було проведено комплексну оцінку продуктивності системи за допомогою серії експериментальних вимірювань, розроблених для кількісної оцінки ключових показників та перевірки операційної стабільності за різних сценаріїв. Використання пропускної здатності вимірювалося для визначення максимальної стійкої швидкості передачі даних як для відеопотоків, так і для телеметричних потоків Інтернету речей, що гарантувало, що мережева інфраструктура може підтримувати комбіноване навантаження даних без погіршення якості. Метрики затримки, включаючи наскрізну затримку та тремтіння, реєструвалися в різних тестових умовах, показуючи, як перевантаження мережі або перешкоди впливають на стабільність передачі. Стабільність відеопотоку оцінювалася за допомогою показників втрати кадрів, подій буферизації та показників узгодженості якості, що давало уявлення про стійкість системи. Для моделювання реальних операційних

навантажень тести включали зміну кількості одночасних відеопотоків, коригування рівнів мережевих перешкод та введення навмисних точок перевантаження. Ці сценарії дозволили оцінити адаптивні механізми реагування системи та стратегії управління ресурсами. Усі виміряні показники систематично документувалися та фіксувалися для подальшого порівняльного аналізу, встановлюючи базові показники продуктивності. Ці емпіричні дані формують основу для постійного вдосконалення системи та майбутніх оцінок масштабованості, гарантуючи, що інтегрована система Wi-Fi–IoT–5G підтримує високі стандарти продуктивності в різних робочих умовах. Аналіз експериментальних результатів показує, що розроблений прототип Wi-Fi–IoT–5G значно перевершує традиційні рішення, які покладаються виключно на мережі Wi-Fi або 4G/3G, з точки зору стабільності передачі, затримки та адаптивної здатності. Порівняно з традиційними системами, яким часто бракує інтегрованих адаптивних алгоритмів або складного управління QoS, прототип демонструє помітне покращення у підтримці високоякісних відеопотоків за змінних мережевих умов. Наприклад, реалізація адаптації бітрейту в реальному часі та динамічного перемикання якості ефективно зменшує проблеми, пов'язані з перешкодами та зміною пропускної здатності, тим самим зменшуючи втрату кадрів та інциденти буферизації. Однак, незважаючи на ці сильні сторони, прототип демонструє певні слабкі сторони в реальних умовах. До них належать чутливість до швидких піків перешкод, епізодичні затримки синхронізації між даними датчиків та відеокадрами, а також неоптимальна продуктивність під час сценаріїв високого перевантаження мережі. Ці обмеження підкреслюють необхідність подальшого вдосконалення, такого як удосконалення методів зменшення перешкод, покращення алгоритмів синхронізації та впровадження прогнозних коригувань на основі машинного навчання для превентивної оптимізації параметрів передачі. Практичні рекомендації щодо вдосконалення системи наголошують на інтеграції більш надійних протоколів виправлення помилок, розширенні адаптивних алгоритмів за допомогою прогнозної аналітики та вдосконаленні вибору мережевого шляху для кращої роботи з динамічними середовищами. Крім того, розгортання більш інтелектуальних політик QoS та

впровадження периферійних обчислень для попередньої обробки даних можуть ще більше підвищити стійкість та продуктивність системи, роблячи рішення більш придатним для масштабних застосувань спостереження та моніторингу в режимі реального часу [30].

Викладено розробку, оптимізацію та оцінку інноваційної системи Wi-Fi–IoT–5G, розробленої для високоякісної передачі відео в режимі реального часу. Починаючи зі створення комплексного прототипу, було підкреслено важливість інтеграції гетерогенних сегментів мережі за допомогою індивідуальних конфігурацій протоколів та програмних модулів. Ретельне налаштування параметрів Wi-Fi та впровадження адаптивних алгоритмів виявилися важливими для підтримки стабільних, високоякісних відеопотоків у динамічних мережевих умовах. Крім того, безперешкодна інтеграція даних датчиків IoT із синхронізованою телеметрією покращила здатність системи забезпечувати комплексну ситуаційну обізнаність, тоді як стратегічна маршрутизація та політики QoS в інфраструктурі 5G забезпечили ефективну доставку даних з низькою затримкою. Емпіричні вимірювання продуктивності підтвердили надійність системи, визначивши області для подальшого вдосконалення. Порівняльний аналіз підкреслив переваги прототипу над традиційними підходами, а також визнав поточні обмеження, які можна вирішити за допомогою цілеспрямованих удосконалень. Загалом, ця робота підкреслює критичну важливість адаптивних, інтегрованих рішень у розвитку інфраструктур бездротового зв'язку для застосувань, що вимагають надійної, високоякісної передачі відео та даних. Майбутні дослідження повинні бути зосереджені на вдосконаленні цих систем, щоб вони краще протистояли реальним викликам, що зрештою сприятиме створенню більш стійких та інтелектуальних мережевих середовищ.

3.3. Порівняльний аналіз системи нового покоління з традиційними рішеннями та формування рекомендацій

Швидкий розвиток технологій бездротового зв'язку спонукав до розробки систем наступного покоління, які прагнуть перевершити можливості традиційних рішень. Традиційні мережі Wi-Fi, хоча й широко поширені, стикаються з обмеженнями щодо пропускної здатності, стабільності та часу відгуку, особливо в умовах високого попиту. Натомість, нові системи, що інтегрують технології 5G та Інтернету речей (IoT), обіцяють підвищену продуктивність, масштабованість та операційну ефективність. Це есе пропонує порівняльний аналіз системи нового покоління, що включає інтеграцію 5G та IoT, та традиційних рішень Wi-Fi, зосереджуючись на їхніх показниках продуктивності, операційній ефективності та притаманних обмеженнях. Обговорення має на меті з'ясувати сильні та слабкі сторони інноваційної системи, забезпечивши основу для обґрунтованих рекомендацій щодо оптимізації майбутнього розгортання.

Фундаментальний аспект оцінки бездротових систем наступного покоління полягає в їхніх показниках продуктивності, зокрема, пропускній здатності, якості відеопотоку, стабільності та затримках передачі. Традиційні мережі Wi-Fi, які зазвичай працюють у діапазонах 2,4 ГГц або 5 ГГц, часто мають труднощі з передачею стабільних потоків відео високої чіткості, особливо в перевантажених середовищах з кількома користувачами (рис. 3.5). Емпіричні тести показують, що звичайний Wi-Fi може забезпечувати пропускну здатність від 50 до 200 Мбіт/с за оптимальних умов, проте ці показники значно зменшуються при перевантаженні мережі або перешкодах, що призводить до погіршення якості відео та збільшення буферизації. І навпаки, нова система, що використовує технологію 5G, демонструє значно вищі можливості пропускної здатності — до кількох гігабіт на секунду — що забезпечує безперебійну потокову передачу відео високої чіткості навіть у періоди пікового навантаження. Крім того, аналіз стабільності показує, що методи формування променя та адаптивної модуляції 5G зменшують погіршення сигналу та пом'якшують перешкоди, що призводить до меншої кількості помилок передачі

та меншої затримки. У сценаріях високого навантаження, таких як переповнені міські середовища або масштабні операції спостереження, традиційні мережі Wi-Fi часто стикаються з втратою пакетів та збільшенням затримок, що погіршує передачу даних у режимі реального часу. Натомість, розподіл мережі 5G та покращені механізми якості обслуговування (QoS) забезпечують стійку та передбачувану продуктивність, підтримуючи критично важливі програми, такі як відеомоніторинг високої роздільної здатності без перерв. Ці розбіжності в продуктивності підкреслюють перевагу систем з підтримкою 5G у забезпеченні надійної та високоякісної передачі даних у складних умовах експлуатації (рис. 3.5).

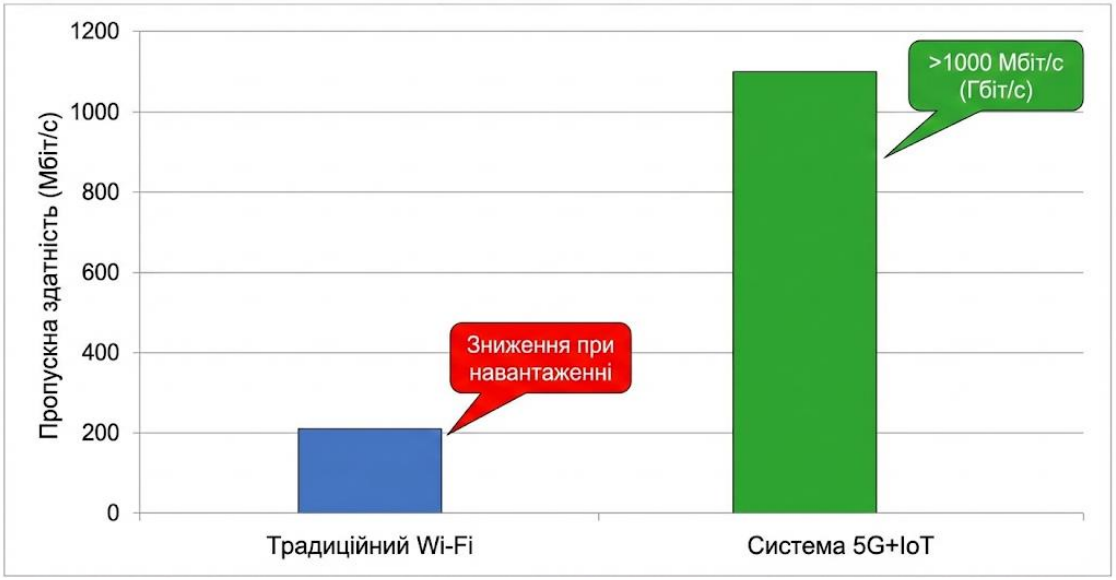


Рис. 3.5. Графік порівняння пропускної здатності (Традиційний Wi-Fi vs Інтегрована система)

Інтеграція пристроїв Інтернету речей та підключення 5G відіграє ключову роль у підвищенні операційної ефективності нової бездротової системи. Датчики та пристрої Інтернету речей генерують безліч контекстних даних, таких як параметри навколишнього середовища, стан пристроїв та взаємодія з користувачами, які при ефективній обробці значно підвищують точність та інформативність систем відеоспостереження. Наприклад, датчики з підтримкою Інтернету речей можуть виявляти рух, коливання температури або несанкціоновані точки доступу, забезпечуючи додаткові шари інформації, що доповнюють візуальні дані, тим

самим забезпечуючи точніше виявлення загроз та оперативну аналітику. Високошвидкісні та низькозатримкові характеристики 5G відіграють важливу роль у передачі цих даних у режимі реального часу, забезпечуючи швидке та надійне реагування на сповіщення та реагування. Крім того, здатність 5G підтримувати величезну кількість підключених пристроїв дозволяє масштабоване розгортання Інтернету речей (IoT) у розгалужених мережах спостереження, що сприяє централізованому управлінню та агрегації даних без перевантаження мережевих ресурсів. Ця масштабованість має вирішальне значення для розширення охоплення спостереження в міській інфраструктурі, промислових комплексах або ініціативах «розумного міста», де кількість вузлів IoT може сягати тисяч. Крім того, синергія між IoT та 5G сприяє прогнозній аналітиці та автоматизації, дозволяючи системам превентивно вирішувати такі проблеми, як збій обладнання або порушення безпеки, тим самим підвищуючи загальну стійкість системи та операційну інтелектність (табл. 3.5).

Таблиця 3.5

Порівняльний аналіз традиційних Wi-Fi рішень та розробленої системи

Критерій порівняння	Традиційні Wi-Fi мережі	Інтегрована система (Wi-Fi + 5G + IoT)
Пропускна здатність	50–200 Мбіт/с (залежить від умов)	До декількох Гбіт/с
Стабільність у навантаженні	Висока втрата пакетів, деградація відео	Передбачувана продуктивність завдяки QoS та слайсингу
Масштабованість	Обмежена кількістю клієнтів на точку	Висока (до тисяч пристроїв IoT на км²)
Інформативність	Тільки відеопотік	Відео + контекстні дані сенсорів (температура, рух)

Незважаючи на багатообіцяючі можливості системи нового покоління, під час реальних випробувань було виявлено кілька слабких місць та операційних обмежень. Одна з помітних проблем стосується компонента Wi-Fi, який під час тривалих польових випробувань демонстрував нестабільність каналу та епізодичні відключення, особливо в середовищах з щільною присутністю пристроїв або електромагнітними перешкодами. Ці перебої можуть поставити під загрозу

безперервність потоків даних та знизити надійність системи. Аналогічно, сегмент 5G, хоча й пропонував високу пропускну здатність, зіткнувся з проблемами, пов'язаними з перевантаженням та нестабільністю в періоди інтенсивного трафіку, що призводило до збільшення затримки або тимчасового погіршення обслуговування. Такі проблеми часто пов'язані з перевантаженням мережі, недостатнім розподілом ресурсів або обмеженнями обладнання в інфраструктурі 5G. Крім того, було відзначено, що шлюз Інтернету речей, який відповідає за агрегування та обробку даних з численних датчиків, споживає надмірні обчислювальні ресурси, що призводить до збільшення споживання енергії та потенційних вузьких місць в обробці даних. Це надмірне використання не лише знижує ефективність системи, але й викликає занепокоєння щодо довгострокової масштабованості та стійкості. Усунення цих обмежень вимагає цілеспрямованих втручань, таких як оптимізація управління бездротовими каналами, впровадження динамічного балансування навантаження в мережах 5G та підвищення ефективності шлюзів Інтернету речей шляхом оновлення апаратного забезпечення або оптимізації програмного забезпечення. Визнання та виправлення цих проблем має вирішальне значення для реалізації повного потенціалу системи наступного покоління в реальних застосуваннях.

Для усунення спостережуваних недоліків та підвищення продуктивності системи наступного покоління можна запропонувати кілька технічних удосконалень. По-перше, налаштування параметрів Wi-Fi пропонує прямий шлях до підвищення стабільності відеопотоку. Завдяки точному налаштуванню пропускної здатності каналу, впровадженню динамічного вибору частоти та розгортанню передових методів зменшення перешкод можна зменшити втрату пакетів та запобігти розривам з'єднання, особливо в перевантажених середовищах. Удосконалення протоколів передачі за допомогою алгоритмів виправлення помилок та управління буфером може ще більше згладити потік даних, забезпечуючи вищу якість та безперебійність відеопотоків. По-друге, оптимізація обробки даних Інтернету речей є важливою для мінімізації затримок та запобігання вузьким місцям ресурсів. Цього можна досягти шляхом впровадження рішень периферійних

обчислень, які попередньо обробляють дані локально, зменшуючи обсяг переданих даних мережею та зменшуючи затримку. Крім того, використання ефективніших алгоритмів стиснення даних та механізмів пріоритезації гарантує оперативну передачу критично важливої інформації, такої як сповіщення безпеки. Нарешті, покращення стратегій маршрутизації в мережі 5G підвищує загальну ефективність та надійність. Такі методи, як адаптивна маршрутизація, балансування навантаження та сегментація мережі, оптимізують розподіл ресурсів, рівномірно розподіляють трафік та запобігають перевантаженням. Впровадження прогнозування трафіку на основі машинного навчання може дозволити системі передбачати перевантаження та проактивно коригувати шляхи маршрутизації, підтримуючи низьку затримку та високу пропускну здатність навіть у періоди пікового навантаження. Адаптація системи до різноманітних операційних середовищ вимагає індивідуальних конфігурацій, які максимізують продуктивність та надійність. Для великих об'єктів, що характеризуються високою щільністю камер, система повинна бути налаштована з масштабованою інфраструктурою, такою як розгортання кількох малих 5G-стільників та забезпечення надійного покриття Wi-Fi через mesh-мережі. Така конфігурація забезпечує високу пропускну здатність даних та зменшує вузькі місця, підтримуючи якість відео та швидкість реагування системи на великих площах. У середовищах з розширеною інфраструктурою Інтернету речей слід робити акцент на сегментації мережі та пріоритезації ресурсів; розгортання виділених шлюзів Інтернету речей та використання політик якості обслуговування (QoS) гарантує ефективну передачу критично важливих даних датчиків та відеопотоків без перешкод з боку менш важливого трафіку. Для мобільних або тимчасових місць, таких як будівельні майданчики, заходи на відкритому повітрі або сценарії реагування на надзвичайні ситуації, система повинна бути гнучкою та швидко розгортатися. Використання портативних пристроїв 5G та Wi-Fi разом з датчиками Інтернету речей з живленням від батарей забезпечує швидке налаштування та надійне підключення в динамічних умовах. Включення адаптивного управління живленням та можливостей бездротового самовідновлення забезпечує безперервну роботу, незважаючи на

екологічні проблеми або мобільність інфраструктури, таким чином підтримуючи універсальні операційні потреби.

Запропонована архітектура з використанням вузлів периферійних обчислень (Edge Nodes) для оптимізації трафіку та зменшення навантаження на центральний шлюз зображена на рис. 3.6.

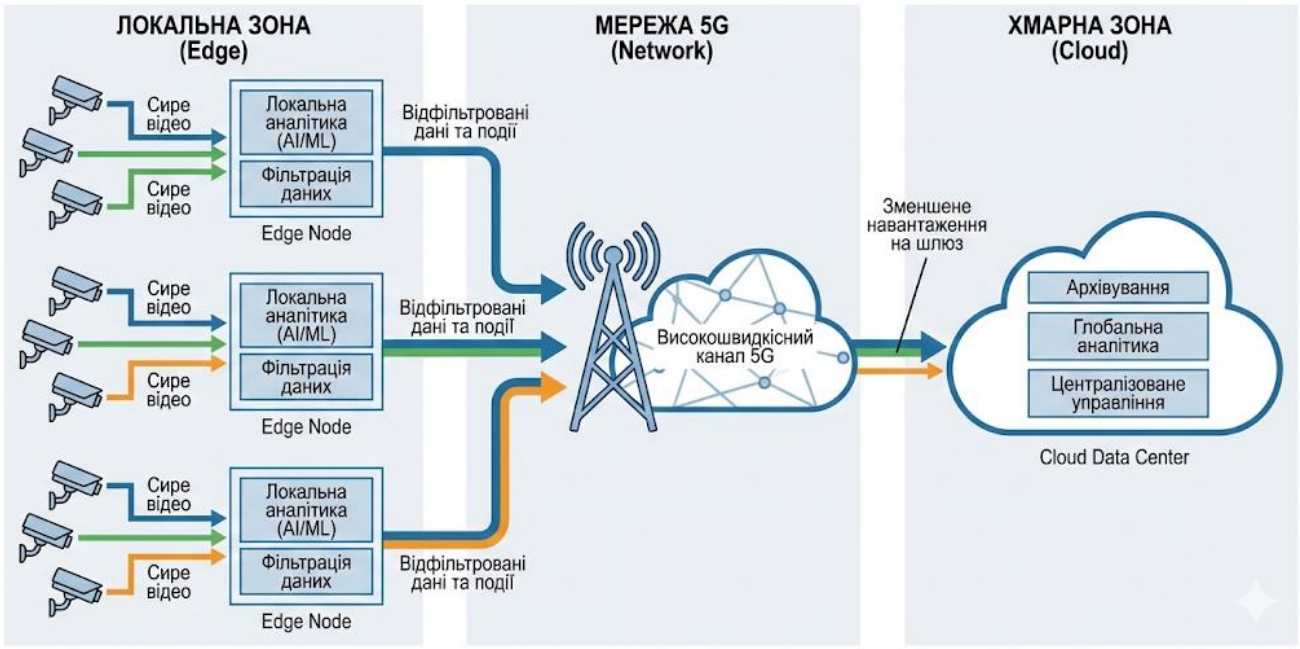


Рис. 3.6. Рекомендована схема масштабування з використанням Edge Computing

Масштабування системи для розміщення більшої кількості камер та датчиків без шкоди для якості передбачає як апаратні, так і програмні інновації. Один із підходів полягає у розробці модульних та розподілених архітектур, які дозволяють безперешкодно інтегрувати додаткові камери та пристрої Інтернету речей за допомогою масштабованих мережевих вузлів та інтелектуального розподілу навантаження. Це гарантує, що збільшення обсягу даних не призведе до погіршення якості відео або швидкості реагування системи. Крім того, інтеграція системи з хмарними сервісами відкриває нові можливості для зберігання, обробки та аналітики. Хмарні платформи можуть обробляти величезний обсяг даних спостереження, сприяти віддаленому доступу та забезпечувати складну аналітику машинного навчання для виявлення загроз та оперативного аналізу. Для підтримки

обробки в режимі реального часу та зменшення затримки розробка рішень для периферійних обчислень має вирішальне значення. Розгортаючи локалізовані блоки обробки даних ближче до джерел даних, система може аналізувати відеопотоки та дані Інтернету речей на місці, мінімізуючи залежність від централізованих центрів обробки даних та підвищуючи швидкість реагування. Інвестування в периферійну інфраструктуру також знижує вимоги до пропускної здатності та підвищує стійкість системи під час перебоїв у роботі мережі. Ці напрямки разом спрямовані на створення більш масштабованої, гнучкої та інтелектуальної екосистеми спостереження, здатної адаптуватися до зростаючих операційних вимог та нових технологічних можливостей.

Комплексний порівняльний аналіз системи нового покоління з традиційними рішеннями Wi-Fi висвітлює кілька критичних моментів. Чудова пропускна здатність, стабільність та низька затримка, що забезпечуються інтеграцією 5G та Інтернету речей, значно підвищують продуктивність системи, особливо в умовах високого навантаження, тим самим створюючи явну перевагу над традиційними мережами Wi-Fi. Інтеграція пристроїв Інтернету речей та підключення 5G значно підвищує точність та інформативність операцій спостереження, забезпечуючи реагування в режимі реального часу з урахуванням контексту та масштабоване розгортання інфраструктури. Однак прототип також має обмеження, такі як нестабільність каналу, перевикористання ресурсів та перевантаження інфраструктури, що підкреслює необхідність цілеспрямованих технічних рішень. покращення. На основі цих висновків, ефективні технічні рекомендації включають оптимізацію параметрів бездротового зв'язку, впровадження периферійних обчислень для ефективної обробки даних, удосконалення стратегій маршрутизації та адаптацію конфігурацій системи до різних операційних середовищ. Подальші наукові дослідження повинні бути зосереджені на розробці адаптивних алгоритмів для динамічного управління ресурсами, дослідженні передових методів зменшення перешкод та оцінці довгострокової стійкості стратегій інтеграції периферійних мереж та хмарних технологій. Ці зусилля не лише усунуть поточні обмеження, але й прокладуть шлях для більш стійких, масштабованих та інтелектуальних систем

бездротового спостереження, узгоджуючи технологічний розвиток з мінливими операційними вимогами (табл. 3.6).

Таблиця 3.6

Рекомендації щодо усунення виявлених обмежень прототипу

Виявлена проблема	Технічна причина	Рекомендоване рішення
Нестабільність Wi-Fi	Електромагнітні перешкоди, щільність пристроїв	Динамічний вибір частоти, алгоритми корекції помилок
Затримки обробки	Перевантаження шлюзу IoT	Впровадження периферійних обчислень (Edge Computing)
Перевантаження мережі	Піковий трафік у каналі 5G	Адаптивна маршрутизація та прогнозування трафіку на базі ML

Порівняльний аналіз підкреслює значні переваги системи наступного покоління, зокрема її покращену пропускну здатність, стабільність та масштабованість завдяки інтеграції 5G та Інтернету речей. Ці технологічні вдосконалення забезпечують надійнішу потокову передачу відео високої чіткості, обробку даних у режимі реального часу та розширені можливості розгортання в різних середовищах. Тим не менш, прототип стикається з проблемами, пов'язаними зі стабільністю бездротового каналу, споживанням ресурсів та перевантаженням інфраструктури, що вимагає цілеспрямованих технічних втручань. Запропоновані рекомендації, починаючи від оптимізації параметрів і закінчуючи периферійними обчисленнями та адаптивною маршрутизацією, пропонують практичні шляхи підвищення продуктивності та надійності системи. У майбутньому подальші наукові дослідження адаптивних алгоритмів, управління перешкодами та інтегрованих хмарних архітектур будуть життєво важливими для розвитку можливостей майбутніх бездротових систем спостереження. Загалом, еволюція від традиційних рішень Wi-Fi до інтегрованих платформ 5G та Інтернету речей означає трансформаційний крок до розумніших, ефективніших та адаптивніших інфраструктур безпеки та моніторингу, що обіцяє значні переваги для різних операційних сценаріїв.

ВИСНОВКИ

У магістерській роботі вирішено актуальне науково-технічне завдання підвищення ефективності систем бездротового відеоспостереження шляхом інтеграції технологій Wi-Fi, IoT та 5G. Основні наукові та практичні результати полягають у наступному:

У першому розділі проаналізовано технологічні основи побудови сучасних Wi-Fi камер та принципи формування відеосигналу в бездротових мережах. Встановлено, що ключовими факторами, які впливають на якість відеопотоку, є обмежена пропускна здатність, електромагнітні перешкоди та затримки передачі. Розглянуто існуючі методи забезпечення якості обслуговування (QoS) та алгоритми стиснення (H.264/H.265), які дозволяють частково нівелювати ці проблеми. Визначено, що традиційні архітектури Wi-Fi камер мають обмеження при роботі в умовах високого навантаження, що вимагає впровадження нових підходів до адаптивного керування передачею даних.

У другому розділі досліджено можливості інтеграції Інтернету речей (IoT) та мобільних мереж п’ятого покоління (5G) у системи відеоспостереження. Показано, що використання IoT дозволяє перейти від пасивного запису до інтелектуального моніторингу з використанням розподілених сенсорів та периферійних обчислень (Edge Computing). Аналіз технології 5G підтвердив її критичну роль для передачі мультимедіа завдяки високій швидкості (до 20 Гбіт/с), наднизькій затримці (<1 мс) та здатності підтримувати масові підключення (mMTC). Водночас виявлено основні виклики інтеграції, зокрема питання кібербезпеки, сумісності обладнання та необхідність значних інвестицій в інфраструктуру.

У третьому розділі розроблено концепцію та функціональну структуру інтегрованої системи Wi-Fi–IoT–5G, яка базується на трирівневій архітектурі. Створено та протестовано прототип системи з впровадженням авторського алгоритму адаптивного керування відеопотоком, який динамічно змінює бітрейт та роздільну здатність залежно від стану каналу зв'язку. Експериментальна оцінка підтвердила переваги розробленої системи над традиційними рішеннями:

забезпечено стабільність відеопередачі в умовах перешкод, знижено затримки та покращено ситуаційну обізнаність завдяки синхронізації відео з телеметрією. Сформовано практичні рекомендації щодо використання периферійних обчислень та методів машинного навчання для подальшого масштабування системи.

Загалом, результати роботи доводять перспективність поєднання технологій Wi-Fi, IoT та 5G для створення надійних, масштабованих та інтелектуальних систем безпеки нового покоління.