Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Методи управління мобільними пристроями персоналу в корпоративній мережі

(тема)

Виконав:

здобувач 2 року навчання,

групи СПм-23-3

Ярослав ТАРАПАТА
(власне ім'я, прізвище)

Спеціальність

123 «Комп'ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма

Системне програмування
(повна назва освітньої програми)

Керівник: доцент Дмитро ГОЛУБНИЧИЙ
(посада, власне ім'я, прізвище)

Допускається до захисту

Зав. кафедри ЕОМ _____ Андрій КОВАЛЕНКО
(підпис) (прізвище, ініціали)

2025 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Тарапаті Ярославу Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Методи управління мобільними пристроями персоналу в корпоративній мережі

затверджена наказом по університету від " 21 " квітня 2025 р. № 296 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 16 червня 2025 р.

3. Вхідні дані до роботи 1) Операційна система – Android;
2) Технології мобільності корпоративних мереж: BYOD, COPE і CYOD;
3) Системи управління корпоративною мобільністю: AirWatch by VMWare, MobileIron, SOTI, Microsoft, Citrix;
4) Механізм реалізації моделі "клієнт-сервер": push-сповіщення;
5) мова програмування: PERL.

4. Перелік питань, що потрібно опрацювати у роботі
1. Аналіз проблеми управління мобільністю в корпоративних мережах
2. Модель управління корпоративною мобільністю
3. Метод управління корпоративної мобільністю
4. Рекомендації щодо проектування системи управління мобільними пристроями пристроями персоналу на основі ОС Android

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Слайд-презентація – 14 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Огляд технологій управління мобільними	22.04.25-29.04.25	
	пристроями персоналу в корпоративних		
	комп'ютерних мережах		
2	Вибір та обгрунтування методу управління	30.04.25-05.05.25	
	корпоративної мобільністю		
3	Вибір інструментальних засобів	06.05.25-09.05.25	
4	Розробка моделі управління корпоративною	10.05.25-21.05.25	
	мобільністю		
5	Проведення експериментів	22.05.25-02.06.25	
6	Оформлення матеріалів кваліфікаційної роботи	03.06.25-05.06.25	
7	Подання кваліфікаційної роботи керівникові та	06.06.25-09.06.25	
	її попередній захист		
8	Подання кваліфікаційної роботи на рецензу-	10.06.25-12.06.25	
	вання		

Дата видачі завдання " 21 " квітня 2025 р.

Здобувач _____ (підпис)

Керівник роботи _____ (підпис) доцент Дмитро ГОЛУБНИЧИЙ. (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 100 с., 47 рис., 8 табл., 1 дод., 30 джерело.

МОБІЛЬНІ ПРИСТРОЇ, КОРПОРАТИВНА МЕРЕЖА, МОБІЛЬНИЙ ЗАСТОСУНОК, МОБІЛЬНИЙ КОНТЕНТ, ВЕБЗАСТОСУНОК, PUSH-ПОВІДОМЛЕННЯ, ANDROID.

Метою кваліфікаційної роботи є підвищення ефективності управління та контролю мобільного доступу до корпоративних інформаційних ресурсів через удосконалення таких напрямів: керування пристроями, управління програмними застосунками, а також забезпечення захисту й конфіденційності корпоративного контенту.

У ході виконання кваліфікаційної роботи було визначені об'єкт та предмет дослідження.

Об'єкт дослідження – процеси організації та управління мобільною активністю в межах корпоративної мережі, включно з аналізом її основних складових: пристроїв, застосунків і даних.

Предмет дослідження – мобільні корпоративні мережі та окремі сегменти розподілених корпоративних обчислювальних систем, де вузлами виступають мобільні пристрої, їхні застосунки та контент.

Методи дослідження – методи системного аналізу, теорії управління, тривимірну модель масштабованості, ресурс-орієнтована архітектура, метод обміну повідомленнями, методи тестування та проектування мережевих та мобільних додатків.

Аналіз, висновки і пропозиції, що міститься в роботі, можуть бути також використані для управління мобільністю в мережах підприємства, які включають управління: пристроями, застосунками і контентом.

ABSTRACT

Master’s thesis: 100 pages, 47 figures, 8 tables, 1 appendices, 30 sources.

MOBILE DEVICES, CORPORATE NETWORK, MOBILE APPLICATION, MOBILE CONTENT, WEB APPLICATION, PUSH NOTIFICATIONS, ANDROID.

The major goal of this thesis is to increase the efficiency of managing and controlling mobile access to corporate information resources by improving the following areas: device management, application management, and ensuring the protection and confidentiality of corporate content.

The object of research is the processes of organizing and managing mobile activity within a corporate network, including the analysis of its main components: devices, applications, and data.

The subject of research is mobile corporate networks and individual segments of distributed corporate computing systems, where mobile devices, their applications, and content act as nodes.

Research methods – systems analysis methods, control theory, three-dimensional scalability model, resource-oriented architecture, messaging method, testing methods and design of network and mobile applications.

The analysis, conclusions and suggestions contained in the work can also be used for mobility management in enterprise networks, which include management of: devices, applications and content.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ІТ – інформаційні технології

ОС – операційна система

ПЗ – програмне забезпечення

УКМ – управління корпоративного мобільністю

УМЗ – управління мобільними застосунками

BYOD – (англ. Bring Your Own Device) принесіть свій власний пристрій

COPE – (англ. Corporate Owned Personally) корпоративні пристрої, які доступні персонально

CSS – (англ. Cascading Style Sheets) каскадні таблиці стилів

CYOD – (англ. Choose Your Own Device) виберіть свій власний пристрій

ECID – (англ. Exclusive Chip ID or Electronic Chip ID) унікальний ідентифікатор чіпу

HTML – (англ. HyperText Markup Language) мова розмітки гіпертексту

HTTP – (англ. Hyper Text Transfer Protocol) протокол передачі гіпертекстових документів

IMEI – (англ. International Mobile Station Equipment Identity) міжнародна ідентифікація обладнання мобільної станції

MAG – (англ. Mobile Access Gateway) шлюз мобільного доступу

MDM – (англ. Mobile Device Management) управління мобільними пристроями

MEAP – (англ. Mobile Enterprise Application Platform) платформа для корпоративних мобільних застосунків

MQTT – (англ. Message Queue Telemetry Transport) спрощений мережевий протокол, що працює на TCP/IP

OAuth – (англ. Open standard for Authorization) відкритий стандарт з

автентифікації

QR – (англ. Quick Response) швидке реагування

RPC – (англ. Remote Procedure Call) віддалений виклик процедур

SAML – (англ. Security Assertion Markup Language) мова розмітки декларації безпеки

URI – (англ. Uniform Resource Identifier) Уніфікований ідентифікатор ресурсу

UUID – (англ. Universally Unique Identifier) універсальний унікальний ідентифікатор

VDI – (англ. Virtual Desktop Infrastructure) віртуалізація робочих місць

VPN – (англ. Virtual Private Network) віртуальна приватна мережа

WLAN – (англ. Wireless Local Area Network) бездротова локальна мережа

ВСТУП

На сьогоднішній день мобільні пристрої стали доступними за ціною та широко інтегрованими як у повсякденне життя людини, так і в корпоративне середовище. Використання мобільних технологій для виконання бізнес-завдань є сучасною тенденцією. Працівники компаній за допомогою особистих портативних пристроїв можуть у будь-якому куточку світу підключатися до конфіденційної корпоративної інформації (листування, проєктної документації, планів, персональних даних тощо) через спеціалізовані корпоративні додатки. Така модель взаємодії отримала назву корпоративної мобільності. Вона сприяє підвищенню продуктивності праці та ефективності взаємодії співробітників у межах компанії.

Для досягнення бажаного рівня ефективності корпоративної мобільності необхідно забезпечити надійне та безперервне з'єднання мобільних пристроїв із корпоративними ресурсами відповідно до чинних політик безпеки, використовуючи захищені канали передачі даних. Для вирішення цих завдань розроблено системи управління корпоративною мобільністю (УКМ), які не лише гарантують захищений доступ до корпоративних даних, а й забезпечують управління користувачами та пристроями.

Системи УКМ відіграють ключову роль у діяльності сучасних організацій, особливо в частині моніторингу, координації та оптимізації процесів, що підтримують корпоративні бізнес-процеси. Через стрімке розширення ринку мобільних технологій в останні роки питання інтеграції мобільних пристроїв у вже наявні інформаційно-комунікаційні інфраструктури стало особливо актуальним для підприємств. Використання мобільних пристроїв у бізнесі сприяє підвищенню ефективності роботи та оптимізації процесів, однак водночас створює нові виклики, пов'язані з кібербезпекою та управлінням пристроями. Крім того, існують певні

обмеження у впровадженні систем УКМ в окремі бізнес-сегменти.

Таким чином, виникає потреба у розробці комплексної методології та впровадженні автоматизованої системи контролю та управління мобільним доступом до корпоративних інформаційних ресурсів.

У наукових роботах, що аналізувалися, розглянуто існуючі підходи до побудови мережевих архітектур із використанням мобільних пристроїв і запропоновано рішення для управління мобільністю корпоративних мереж з урахуванням концепцій BYOD (Bring Your Own Device), CYOD (Choose Your Own Device), COPE (Corporate Owned, Personally Enabled) та інших моделей. Однак виявлено ряд недоліків:

У науковій літературі відсутній цілісний підхід до аналізу якості, моделювання, проектування та впровадження систем УКМ.

Більшість наявних рішень УКМ є комерційним програмним забезпеченням із закритою архітектурою, що ускладнює аналіз їх структурних компонентів, моделей і механізмів на концептуальному рівні.

Існує багато розрізнених підходів до побудови систем УКМ, при цьому методики їх використання переважно описані на теоретичному рівні, без належної практичної оцінки їх ефективності.

Мета дослідження – підвищення ефективності управління та контролю мобільного доступу до корпоративних інформаційних ресурсів через удосконалення таких напрямів: керування пристроями, управління програмними застосунками, а також забезпечення захисту й конфіденційності корпоративного контенту.

Об'єкт дослідження – процеси організації та управління мобільною активністю в межах корпоративної мережі, включно з аналізом її основних складових: пристроїв, застосунків і даних.

Предмет дослідження – мобільні корпоративні мережі та окремі сегменти розподілених корпоративних обчислювальних систем, де вузлами виступають мобільні пристрої, їхні застосунки та контент.

Основними завданнями дослідження є:

а) проведення аналізу особливостей організації та управління корпоративною мобільністю на базі сучасних комп’ютерних мережевих інфраструктур;

б) впровадження масштабованої корпоративної моделі управління мобільними пристроями, яка враховує такі параметри, як характер взаємодії, ідентифікація пристроїв та механізми адміністративного контролю;

в) розроблення методичних рекомендацій щодо ефективного управління мобільними пристроями працівників з метою підвищення рівня корпоративної мобільності;

г) побудова алгоритму керування мобільними пристроями персоналу із використанням сучасних веб-технологій;

д) проєктування архітектури корпоративної системи управління мобільністю;

е) проведення експериментального дослідження f)щодо оцінювання продуктивності сервісів Push-сповіщень та навантаження на сервер у процесі підключення мобільних пристроїв.

1 АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ МОБІЛЬНІСТЮ В КОРПОРАТИВНИХ МЕРЕЖАХ

1.1 Особливості сучасних корпоративних мереж

Тут наведено приклади оформлення основних структурних елементів пояснювальної записки. Формат тексту підрозділу відповідає цьому стилю.

Сьогодні мобільні пристрої є настільки доступними за вартістю, що стали стандартним інструментом у багатьох корпоративних середовищах. Співробітники можуть зі своїх особистих гаджетів отримувати доступ до конфіденційної корпоративної інформації – листування, планів, подій, документів, персональних даних – незалежно від місця перебування. Деякі пристрої навіть підтримують повноцінну роботу з електронними таблицями та іншими офісними додатками. Це суттєво підвищує ефективність робочих процесів та продуктивність персоналу. Водночас гостро постає питання забезпечення інформаційної безпеки та захисту даних компаній [13].

Корпоративна мобільність дозволяє забезпечувати доступ до необхідної інформації у потрібний момент, що значно сприяє підвищенню загальної продуктивності, ефективності та конкурентоспроможності бізнесу. Серед основних проявів цієї тенденції можна виділити:

- збільшення кількості мобільних працівників, які працюють на контрактній основі;

- розширення доступу для співробітників через спеціалізовані мобільні застосунки;

- отримання бізнес-переваг завдяки масштабованості, зручності використання, оптимізації витрат та підвищенню якості обслуговування клієнтів при контрольованих рівнях ризику.

У таблиці 1.1 наведено порівняльний аналіз характеристик корпоративних мереж у минулому та сьогодні.

Таблиця 1.1 – Порівняльна характеристика мережі корпорації в минулому і сьогоденні

Показник	Минулий час	Теперішній час
Місце роботи	використання локально	незалежно від місця
Технологія	залежить від конкретної технології	незалежно від технології
Ресурси	у приміщенні; власник корпорації	у приміщенні та поза приміщенням, в режимі хмари; власник корпорації чи співробітники
Користувачі	працівники корпорації	співробітники корпорації; партнери та дистриб'ютори
Мета	самообслуговування	самообслуговування; широке поширення сервісу

Сучасні корпоративні мережі вирізняються широким залученням мобільних пристроїв до обробки корпоративних даних. У зв'язку з цим постає необхідність розроблення стратегії управління мобільними пристроями в мережі компанії, що має охоплювати такі аспекти [1]:

- контроль пристроїв, які підключаються до корпоративної мережі;
- організація ефективного та безпечного зв'язку з користувачами;
- моніторинг місцезнаходження та переміщення пристроїв;
- управління мобільними застосунками, які взаємодіють із корпоративними ресурсами.

Виконання такої стратегії реалізується через визначення життєвого циклу мобільних пристроїв у корпоративній мережі (рисунок 1.1).

За результатами аналітичного звіту «Світові постачання пристроїв за типами у 2019–2024 роках» побудовано діаграму динаміки змін на ринку мобільних пристроїв (рисунок 1.2) [2].

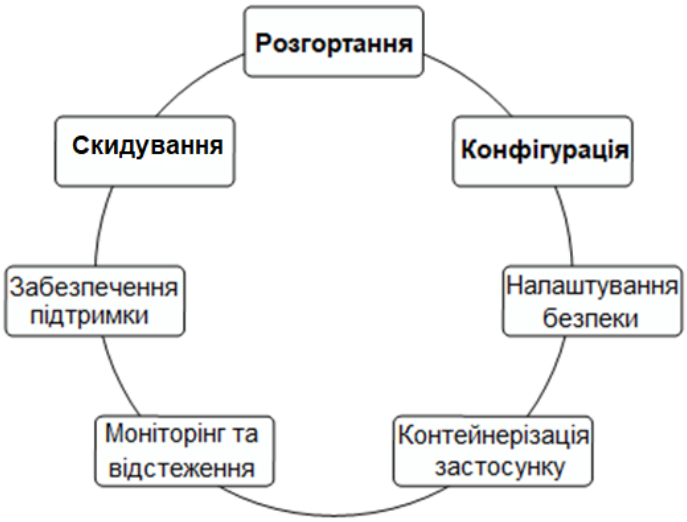

Рисунок 1.1 – Життєвий цикл мобільних пристроїв у корпоративній мережі

Рисунок 1.2 – Світові постачання пристроїв за типами у 2019–2024 роках

Аналіз показує, що, хоча сегмент смартфонів демонструє позитивну динаміку, порівняно із сегментами планшетів та ноутбуків, глобальна структура ринку мобільних пристроїв залишається відносно стабільною без суттєвих зрушень.

Сукупні продажі пристроїв на базі Android та iOS у другому кварталі 2023 року становили 99,1% загального обсягу реалізованих смартфонів, що більше, ніж 96,8% за аналогічний період 2022 року. З цього обсягу платформа Android утримує 86,2% ринку. У другому кварталі 2022 року було

реалізовано близько 272 мільйонів пристроїв на базі Android.

Серед виробників Android-смартфонів компанія Samsung залишається лідером із часткою продажів 22,3% у першому кварталі року.

1.2 Технології мобільності корпоративних мереж: BYOD, COPE і CYOD

Дослідження [3, 4] свідчать: коли працівники використовують власні пристрої для роботи або мають змогу застосовувати корпоративні гаджети в особистих цілях, їхня ефективність помітно зростає. Це дає їм змогу гнучко планувати час і місце праці, не обмежуючись офісом. Для роботи їм достатньо мати під рукою пристрій, зарядний кабель і базові аксесуари – наприклад, гарнітуру. Крім того, працівник залишається на зв’язку за єдиним номером, користуючись зручними для себе засобами.

Наразі найпоширенішими моделями корпоративної мобільності є BYOD, COPE та CYOD.

1.2.1 BYOD: «Принеси власний пристрій»

Концепція Bring Your Own Device (BYOD) передбачає, що співробітники залучають особисті мобільні пристрої для виконання професійних завдань, за згодою або без формального дозволу роботодавця (рисунок 1.3).

Основні сценарії застосування BYOD [5, 6]:

- сценарій 1: пристрій використовується переважно для особистих цілей; однак роботодавець може зв'язатися зі співробітником поза робочим часом;

- сценарій 2: пристрій також використовується для виконання службових обов'язків, з доступом до корпоративної пошти, календарів та

контактів. При цьому витрати на зв’язок сплачує співробітник, а компанія компенсує їх;

- сценарій 3: співробітник використовує особистий пристрій для роботи, але договір на послуги зв'язку оформлений на роботодавця.

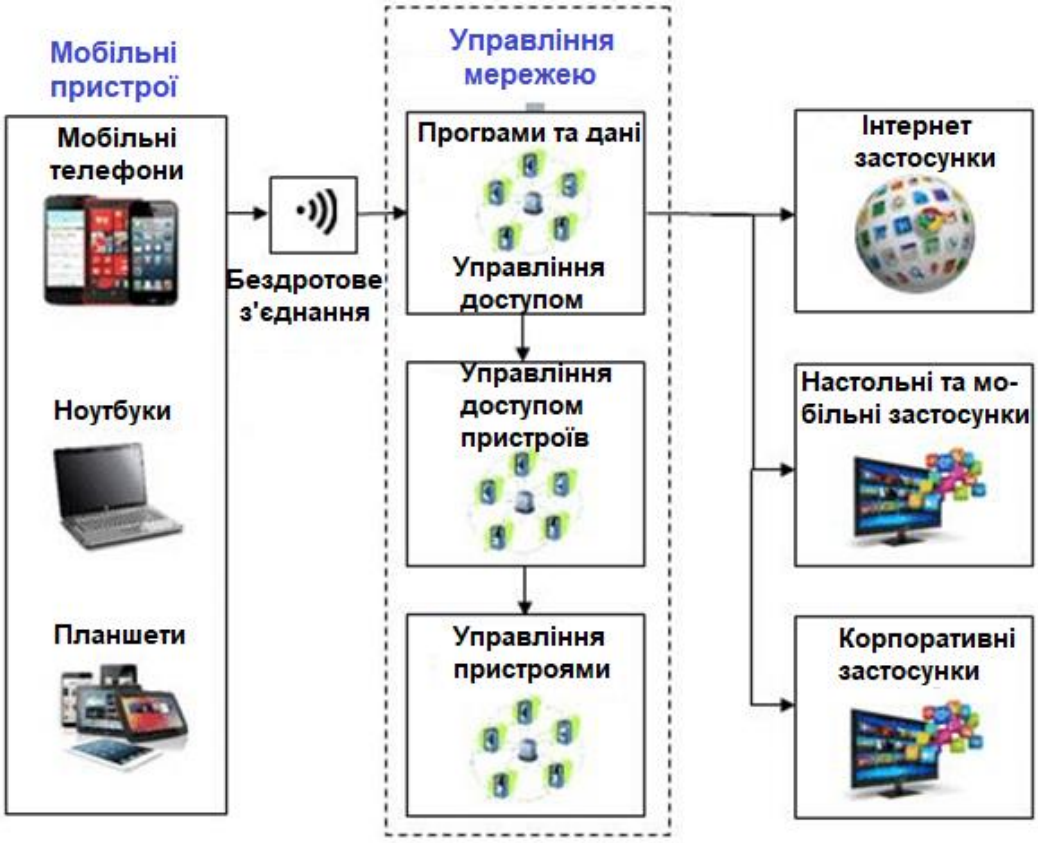

Рисунок 1.3 – Базова архітектура BYOD

Перший сценарій є юридично найпростішим, але потребує чітких правил, інакше працівник може стати «черговим» у неробочий час. Також обов'язково врегулювати доступ до корпоративної WLAN та забезпечити дотримання стандартів інформаційної безпеки.

Крім того, необхідно перевірити та врегулювати використання такими пристроями корпоративної бездротової локальної мережі (Wireless Local Area Network, WLAN) та їх відповідність встановленим вимогам до безпеки. Хоч BYOD і дозволяє компанії скоротити витрати на обладнання, зростають витрати на підтримку різноманітних пристроїв і платформ. Плюс працівники

часто хочуть користуватися найновішими моделями, що може не узгоджуватися із внутрішніми корпоративними політиками.

Реалізація сценаріїв 2 і 3 вимагає уважного врегулювання питань власності пристроїв, відповідальності за їх використання та обслуговування через системи управління мобільними пристроями (Mobile Device Management, MDM) [7].

Оскільки BYOD має високі юридичні ризики, його потрібно впроваджувати лише в межах чітких IT-політик, супроводжуючи це офіційними письмовими угодами.

1.2.2 COPE: «Корпоративний пристрій для особистого використання»

Технологія Corporate Owned Personally Enabled (COPE) менш відома. Вона передбачає надання співробітникам корпоративних смартфонів або планшетів із дозволом на їх особисте використання [5, 9]. На відміну від інших моделей, співробітник самостійно відповідає за базове налаштування і технічне обслуговування пристрою.

У межах концепції COPE усі витрати на придбання обладнання покладаються на роботодавця, однак витрати на його базове обслуговування практично відсутні. Зазвичай пристрій передається співробітнику, який самостійно налаштовує його відповідно до стандартів IT-відділу або адаптує типову конфігурацію під свої потреби. У випадку технічних несправностей працівник звертається безпосередньо до постачальника пристрою, тоді як рутинне обслуговування (установлення оновлень, виправлень тощо) виконується власними силами. Співробітник зобов’язується підтримувати програмне забезпечення в актуальному стані та, в межах своїх компетенцій, самостійно здійснювати технічну підтримку пристрою. Інтервенція служби технічної підтримки відбувається лише у виняткових випадках, що суттєво економить час і ресурси. Водночас такий підхід вимагає від працівників певного рівня технічної обізнаності.

Додатково при впровадженні цієї моделі важливо заздалегідь врегулювати питання відповідальності за можливі непрямі збитки через неправильне використання обладнання. Оскільки співробітнику делегуються окремі обов'язки, застосовуються загальні норми відповідальності: працівник несе відповідальність за навмисне пошкодження обладнання або прояв грубої недбалості.

Рекомендовано чітко розподіляти обов’язки за принципом «безпека передусім»: працівникам слід звертатися по консультацію при виникненні будь-яких сумнівів, а роботодавцю – детально визначити межі відповідальності. Крім укладання письмових угод, доцільно регулярно надавати працівникам актуальні рекомендації та інструкції щодо безпечної роботи (наприклад, попередження про ризики використання ненадійних застосунків, поради з оновлення системи тощо).

1.2.3 CYOD: «Вибір корпоративного пристрою»

Відповідно до моделі Choose Your Own Device (CYOD), роботодавець забезпечує працівників обраними ними пристроями із запропонованого списку, при цьому постачання супроводжується оформленням договору надання послуг зв’язку [5, 8]. Співробітник має можливість самостійно обрати з обмеженого асортименту мобільних телефонів, смартфонів або планшетних комп’ютерів той пристрій, який найкраще відповідає його професійним завданням та особистим вподобанням.

На відміну від концепцій BYOD і COPE, сама назва CYOD не дає чіткої відповіді щодо допустимості особистого використання корпоративної техніки. Тому слід розрізняти дві модифікації підходу: «суворий» варіант, що передбачає використання пристрою виключно для службових цілей, та «гнучкий», який допускає обмежене особисте користування.

При цьому застосування пристроїв має відповідати внутрішнім політикам організації та регламентам управління мобільними пристроями

(MDM). За моделлю CYOD роботодавець самостійно фінансує закупівлю техніки, однак завдяки стандартизації моделей досягається оптимізація витрат на технічну підтримку та обслуговування. Важливо також встановити чіткі правила щодо строків експлуатації обладнання та умов його використання.

Оскільки придбання пристроїв здійснюється безпосередньо компанією, виникає можливість мінімізувати ризики шляхом обмеження функціоналу пристрою лише робочими завданнями. Якщо ж передбачається особисте використання, можуть виникнути проблеми, аналогічні до тих, що характерні для концепції BYOD, зокрема питання оподаткування фінансової вигоди працівників та дотримання ліцензійних вимог при змішаному використанні програмного забезпечення, мультимедійного контенту тощо.

З огляду на це доцільним є розроблення чітко визначеного регламенту, у якому будуть закріплені правила використання пристроїв, перелік дозволених застосунків, технічні вимоги до підтримуваного обладнання та обмеження стосовно особистого користування. Особливу увагу слід приділити питанням регулювання робочого часу, а також контролю фінансових ризиків, таких як витрати на послуги роумінгу.

1.2.4 Порівняння корпоративних моделей мобільності

Серед трьох основних моделей організації мобільного доступу до корпоративної мережі явну перевагу має концепція BYOD. Її популярність значною мірою обумовлена тим комфортом, який забезпечують особисті пристрої працівників, що часто є більш сучасними та продуктивними порівняно з корпоративними аналогами.

На другій позиції, залежно від конкретної ситуації, опиняється модель CYOD або COPE. У межах CYOD співробітникам дозволяється обирати бажаний пристрій із затвердженого переліку, проте із певними обмеженнями у використанні. Концепція COPE, своєю чергою, надає працівникам більше

свободи в експлуатації техніки, проте вимагає від них відповідних технічних навичок – зокрема, самостійного встановлення, налаштування та обслуговування оновлень і програмного забезпечення.

У кожній із цих моделей важливу роль відіграють питання особистої відповідальності працівника, прав власності на обладнання та розподілу обов'язків із технічного обслуговування. Кожен із підходів має власні юридичні ризики, які необхідно враховувати під час впровадження. Додатково слід зважати на аспекти інформаційної безпеки, що також накладають певні обмеження на використання пристроїв.

Кожна з розглянутих моделей має свої переваги та недоліки, що обумовлює необхідність ретельного вибору стратегії відповідно до потреб організації. Основні характеристики та відмінності концепцій BYOD, CYOD та COPE наведено (таблиця 1.2).

Таблиця 1.2 – Порівняльний аналіз технологій мобільних пристроїв

Критерії	BYOD	CYOD	COPE
Власник пристрою	співробітник	корпорація	корпорація
Технічна підтримка	співробітник/корпорація	корпорація	співробітник
Ступінь задоволеності співробітників	висока	середня	середня
Ступінь відповідальності	відсутня	висока	висока
Ступінь безпеки	низька	висока	середня
Ступінь різноманіття пристроїв та ОС	висока	низька	низька
Ступінь мобільності	висока	низька	середня
Вартість придбання	ні	є	є
Придатність для практичного використання на корпорації	низька	висока	середня

Починаючи з певної кількості мобільних кінцевих пристроїв, їхнє ручне адміністрування без застосування автоматизованих технічних рішень стає неможливим. Лише регулярне проведення інвентаризації апаратного та програмного забезпечення, а також цілодобовий моніторинг пристроїв у режимі реального часу дають можливість забезпечити законне та регламентоване використання обладнання в межах корпоративної інфраструктури.

Неконтрольоване застосування особистих пристроїв створює значні загрози для інформаційної безпеки організації. Більше того, технічна підтримка та впровадження оновлень у середовищі великої кількості різнорідних пристроїв та операційних систем у межах реалізації концепції BYOD може виявитися настільки трудомістким процесом, що перевищить прийнятні межі витрат ресурсів.

У разі виникнення сумнівів щодо вибору моделі управління мобільними пристроями доцільно віддати перевагу концепціям CYOD або COPE, які із самого початку дозволяють стримувати різноманіття кінцевих пристроїв і типів операційних систем, що використовуються в корпоративному середовищі.

У випадку реалізації моделі BYOD обов’язковим є формування узгодженого переліку допустимих до використання пристроїв.

Такий підхід мінімізує проблеми сумісності, знижує адміністративне навантаження та скорочує ризики у сфері кібербезпеки.

Крім того, працівників необхідно завчасно інформувати про можливі загрози інформаційній безпеці та їхню особисту відповідальність за дотримання політик організації [5].

Незалежно від обраної моделі, усі три концепції мають спільну проблему: поступове стирання межі між професійною та особистою сферами використання пристроїв.

1.3 Виклики корпоративної мобільності

Інновації у сфері мобільних технологій відкрили шлях до появи мобільних додатків, соціальних мереж, хмарних обчислень, інтернету речей, мобільної співпраці та бездротових рішень. Проте технологічний розвиток відбувається швидше, ніж корпорації встигають адаптувати свої процеси. IT-підрозділи, що не зможуть вчасно перебудуватися під нові реалії, ризикують поступитися конкурентам [18].

Сучасні умови суттєво відрізняються від тих часів, коли існували чіткі правила, достатньо часу та ресурси для розгортання необхідної інфраструктури моніторингу й управління. Нині на IT-сферу чинять тиск численні фактори: регуляторні вимоги, безпекові й конфіденційні обмеження, питання вартості, внутрішньоорганізаційні бар'єри та застарілі технології, що ускладнюють оперативну відповідь на зміни.

У подальшому розглянемо проблеми мобільності крізь призму чотирьох ключових аспектів: інфраструктури, елементів мобільності, безпеки та ідентифікації користувачів.

Інфраструктура – це базис, на якому будується корпоративна мобільність. Вона охоплює технології бездротового доступу WLAN, операторські мережі мобільного зв’язку, VPN-рішення, корпоративні каталоги та системи віртуалізації. Окрім того, мобільна інфраструктура має включати спеціалізовані засоби керування мобільними пристроями, що забезпечують відповідність стандартам і знижують ризики [18].

Основні вимоги до інфраструктури включають:

- надання високопродуктивного сервісу для щоденних потреб користувачів при забезпеченні повної мобільності;
- мінімізацію часу очікування у відповідь на стрімке зростання кількості мобільних пристроїв та обсягів трафіку;
- модернізацію систем, оскільки більшість існуючих інфраструктур не пристосовані до нових умов мобільності;

- забезпечення сумісності політики BYOD (Bring Your Own Device) з корпоративними системами.

Щоб відповідати цим вимогам, IT-службам необхідно розгортати повноцінні «end-to-end» рішення, що вимагає значних інвестицій часу та фінансів для підвищення надійності, продуктивності й керованості інфраструктури.

Елементи корпоративної мобільності (користувачі, пристрої, застосунки та дані) підлягають управлінню відповідно до вимог мобільного середовища з метою розробки рішень, що забезпечують працівникам доступ до необхідної інформації в будь-який час, у будь-якому місці та з використанням будь-якого пристрою.

Основу корпоративної мобільної стратегії становлять три ключові компоненти:

- користувачі;
- пристрої та мобільні застосунки;
- дані.

Ключові елементи корпоративної мобільності включають користувачів, пристрої, застосунки та дані. Мета корпорацій – створити середовище, в якому користувачі зможуть безперешкодно отримувати доступ до необхідної інформації в будь-який момент, у будь-якому місці та з будь-якого пристрою.

Три основні стратегії розвитку мобільності (рисунок 1.4):

- надання користувачам права вибору пристроїв;
- адміністрування мобільних пристроїв та застосунків;
- захист корпоративних даних і контенту.

При цьому зростають вимоги до мобільних даних, що суттєво впливають на розробку застосунків і якість взаємодії з користувачем. Серед ключових факторів, які потрібно враховувати: введення/виведення даних, точність синхронізації, особливості зберігання, інтеграція із серверною частиною, складність обробки даних, ризики втрати конфіденційної інформації та реагування на непередбачувані ситуації.

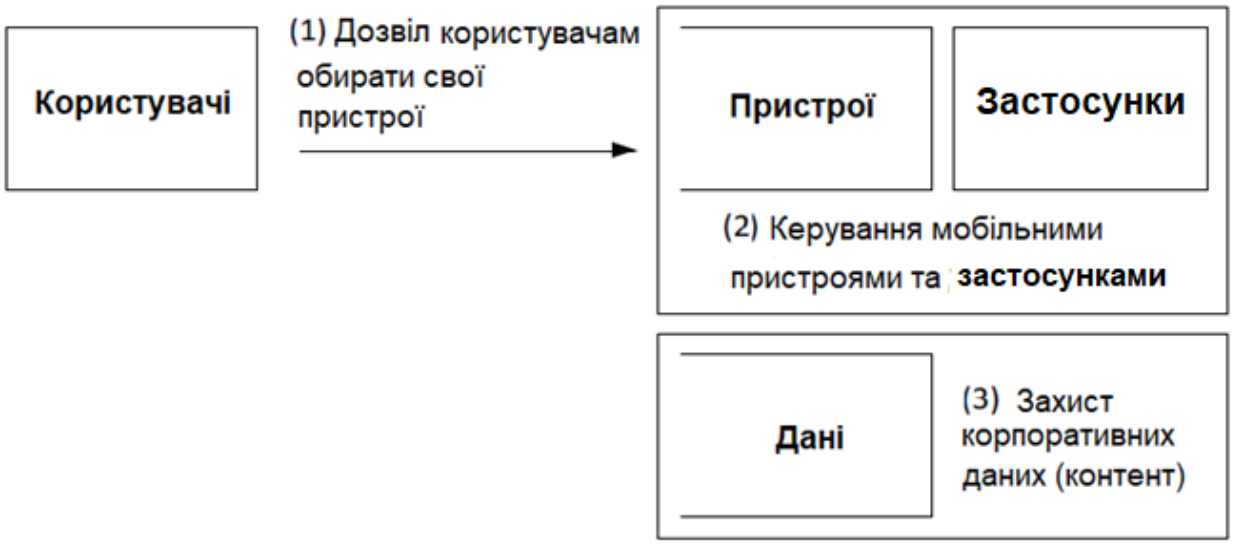

Рисунок 1.4 – Три основні сценарії розширення корпоративної мобільності

При цьому зростають вимоги до мобільних даних, що суттєво впливають на розробку застосунків і якість взаємодії з користувачем. Серед ключових факторів, які потрібно враховувати: введення/виведення даних, точність синхронізації, особливості зберігання, інтеграція із серверною частиною, складність обробки даних, ризики втрати конфіденційної інформації та реагування на непередбачувані ситуації.

Основні виклики у сфері мобільних застосунків та управління даними включають:

- обмеження витоку критичних корпоративних даних без шкоди для продуктивності;
- створення інтерфейсів, зручних для використання на різних розмірах екранів;
- належне регулювання використання соціальних медіа у корпоративному середовищі;
- подолання проблем, пов'язаних із коротким життєвим циклом пристроїв, нестачею оптимізованих застосунків та дефіцитом кваліфікованих розробників.

Комбінація цих викликів із постійно зростаючими очікуваннями користувачів значно ускладнює розробку мобільних рішень.

Проблеми безпеки та ідентифікації у корпоративній мобільності залишаються критичними. Хоча основні загрози – такі як шкідливе ПЗ, крадіжки або втрата пристроїв – не нові, мобільність додає нові ризики:

- недостатній контроль за використанням незахищених пристроїв співробітниками;
- відсутність єдиних стандартів для мобільних систем;
- різні рівні безпеки між різними типами пристроїв (шифрування, керування застосунками тощо);
- короткий термін експлуатації мобільних пристроїв;
- обмеження традиційного ПЗ для захисту інформації на мобільних пристроях;
- розповсюдження неконтрольованих корпоративних даних на особистих пристроях.

Щоб мінімізувати ці ризики, корпорації повинні гарантувати, що доступ до корпоративних систем мають тільки авторизовані користувачі, а також впроваджувати належні процедури перевірки пристроїв перед наданням доступу.

1.4 Концепції управління корпоративною мобільністю за функціональним підходом

Аналітична компанія Gartner визначає управління корпоративною мобільністю (УКМ) як окремий клас програмного забезпечення, який інтегрує мобільні пристрої у бізнес-процеси компаній. Це досягається шляхом їх включення до IT-інфраструктури та систем безпеки на всіх етапах життєвого циклу IT. УКМ забезпечує мобільних співробітників новими інструментами для ефективної роботи зі смартфонами та планшетами, сприяючи підвищенню їх продуктивності.

Завдяки швидкому технологічному розвитку та зростаючій

споживацькій орієнтації, УКМ сформувався як незалежне рішення для мобільної роботи. Підхід до мобільної незалежності кінцевих пристроїв дає змогу корпораціям керувати сервісами й застосунками, не зважаючи на тип пристрою користувача.

Система УКМ повинна охоплювати повний життєвий цикл мобільного пристрою: від налаштування та початкової конфігурації до забезпечення відповідності політикам безпеки та підтримки користувачів у разі виникнення проблем (рисунок 1.5).

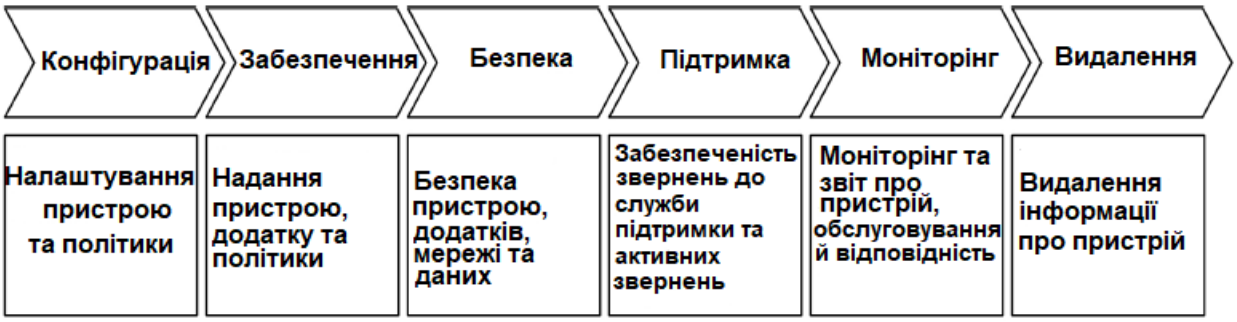

Рисунок 1.5 – Життєвий цикл системи УКМ

Щоб повністю реалізувати поставлені завдання, система УКМ об'єднує передові засоби управління мобільними пристроями (УМП), управління мобільними застосунками (УМЗ) і управління мобільним контентом (УМК).

УМП - концентрується на адмініструванні пристроїв.

УМЗ - забезпечує контроль доступу та розгортання застосунків.

УМК - управляє доступом до корпоративних даних через дозволені застосунки.

Крім того, важливим компонентом УКМ є корпоративний магазин застосунків, який підтримує розповсюдження і оновлення мобільного ПЗ.

Управління мобільними пристроями (УМП)займається налаштуванням пристроїв, їх розгортанням, моніторингом безпеки та інтеграцією в корпоративне середовище. Його головне завдання – забезпечення безпеки і функціональності пристроїв при збереженні цілісності корпоративної мережі.

Інструменти УМП повинні підтримувати як пристрої корпоративної, так і приватної власності (рисунок 1.6).

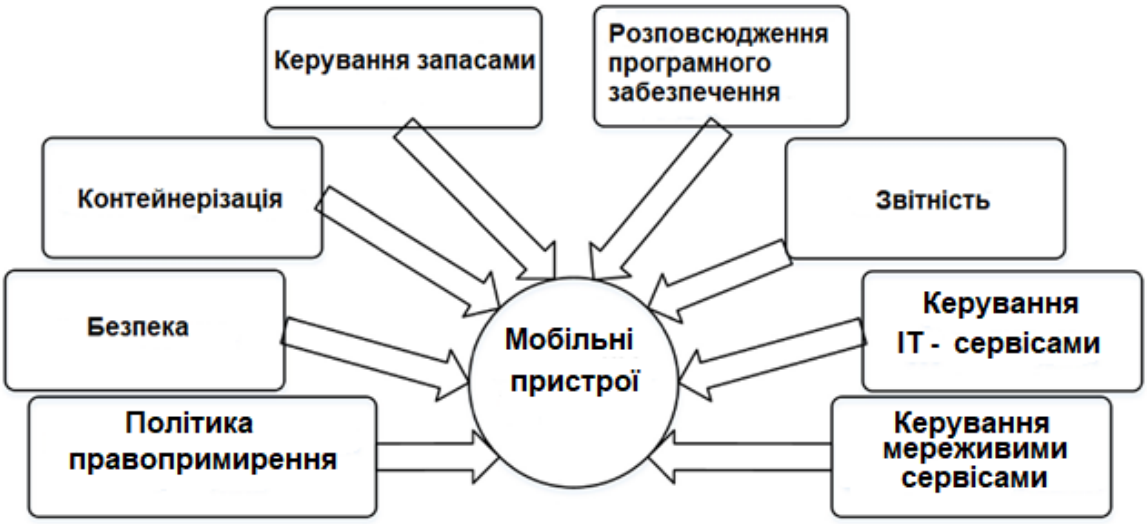

Рисунок 1.6 – Функції системи УМП (підсистеми)

Основні функції УМП включають:

- розподіл і обслуговування застосунків, управління кількома ОС;
- конфігурацію налаштувань пристроїв і політик безпеки;
- моніторинг мережевого трафіку через технологію GPS і бездротової локальної мережі(WLAN);
- адміністрування обладнання та його облік;
- забезпечення інформаційної безпеки шляхом автентифікації, шифрування, використання VPN і контейнеризації.

Управління мобільними застосунками (УМЗ) – відповідає за доставку та контроль корпоративних застосунків для пристроїв працівників. Його ключові можливості включають:

- формування політик і правил для мобільних застосунків;
- автоматичне розгортання необхідних застосунків відповідно до типу пристрою та ОС;
- безпечне видалення застосунків і даних у разі втрати або виведення

пристрою з експлуатації;

- створення корпоративного магазину застосунків для самообслуговування;
- організацію захищеного тунелю до внутрішніх систем компанії;
- управління застосунками, що використовують штучний інтелект.

Управління мобільним контентом (УМК) – орієнтоване на захист корпоративних даних через створення ізольованих шифрованих контейнерів. Тільки авторизовані користувачі мають доступ до даних і можливість їх передачі.

Ключові функціональні можливості УМК:

- надійне зберігання файлів на мобільних пристроях з доступом у режимі офлайн;
- безпечний перегляд електронної пошти через зашифровані програми;
- можливість доступу до внутрішнього HTML-контенту через захищений браузер без використання VPN-клієнта.

1.5 Огляд сучасних систем управління корпоративною мобільністю

1.5.1 AirWatch від VMware

AirWatch від компанії VMware вже п’ятий рік поспіль утримує лідируючі позиції у звіті Gartner Magic Quadrant за 2023 рік у категорії «Реалізація» в галузі корпоративного управління мобільністю. Протягом останніх трьох років AirWatch зберігає високу оцінку за свою здатність ефективно впроваджувати рішення (рисунок 1.7).

Переваги:

- широкі можливості масштабованого розгортання у різних галузях;
- зручна адміністративна панель із навчальними матеріалами, що спрощують процес освоєння для адміністраторів.

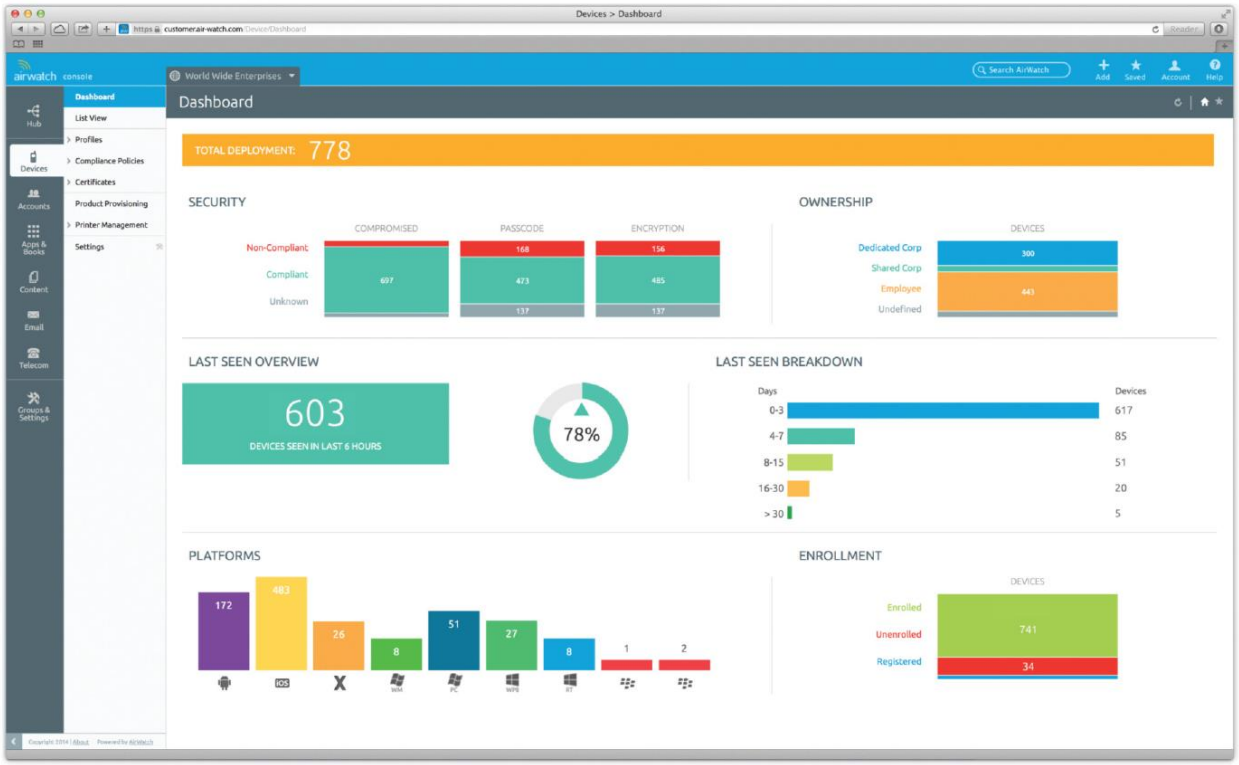

Рисунок 1.7 – Інтерфейс головного екрана системи управління корпоративною мобільністю AirWatch від VMware

Недоліки:

- висока вартість рішення;
- відсутність системи ведення банку довірених програм;
- серверна частина працює виключно на Windows-платформі;
- стабільність роботи залишається викликом;
- інколи виникають труднощі з підключенням поштового додатка Inbox до серверів AirWatch.

1.5.2 MobileIron

Продукти MobileIron спрямовані на вирішення завдання безпечного використання корпоративних даних на мобільних пристроях. Завдяки ним IT-відділи отримують можливість повного контролю за даними, що зберігаються або передаються через пристрої, забезпечуючи високий рівень захисту та зручність для кінцевих користувачів (рисунок 1.8).

Рисунок 1.8 – Головний екран системи централізованого керування мобільними пристроями MobileIron

Переваги:

- висока оцінка користувачів за якість обслуговування і відкритість до вдосконалень;
- єдиний постачальник УКМ-рішень, який дозволяє переглядати екран пристроїв iOS у реальному часі.

Недоліки:

- складна архітектура на основі appliance-ів ускладнює моніторинг доступності та продуктивності;
- обмежена підтримка API для Android;
- адміністративна консоль доступна лише англійською мовою.

1.5.3 SOTI MobiControl

SOTI MobiControl пропонує централізовану платформу для управління корпоративною мобільністю, яка підтримує різноманітні операційні системи. Система орієнтована на корпоративне управління пристроями і дозволяє

налаштовувати групи, політики та права доступу відповідно до вимог безпеки підприємства (рисунок 1.9).

Рисунок 1.9 – Інтерфейс користувача системи SOTI MobiControl

Переваги:

- потужний віддалений доступ і керування для Android-пристроїв;
- простота інтеграції та розширення функціоналу;
- гнучке створення профілів та правил для управління пристроями.

Недоліки:

- деякі недоліки в процесі реєстрації пристроїв;
- проблеми зі звітністю та аналітикою;
- недостатня підтримка iOS;
- потреба у вдосконаленні технічної підтримки та документації;
- обмежена налаштовуваність інформаційної панелі.

1.5.4 Microsoft Enterprise Mobility Suite (EMS)

Система EMS від Microsoft об'єднує кілька продуктів, серед яких Microsoft Intune, Azure Active Directory Premium, Advanced Threat Analytics, ConfigMgr та Azure Rights Management. Intune, який працює як хмарна служба, забезпечує базові функції управління мобільними пристроями, застосунками та контентом. Особливістю є унікальна інтеграція з мобільними версіями Office і можливість контролю над збереженням файлів та політиками копіювання (рисунок 1.10).

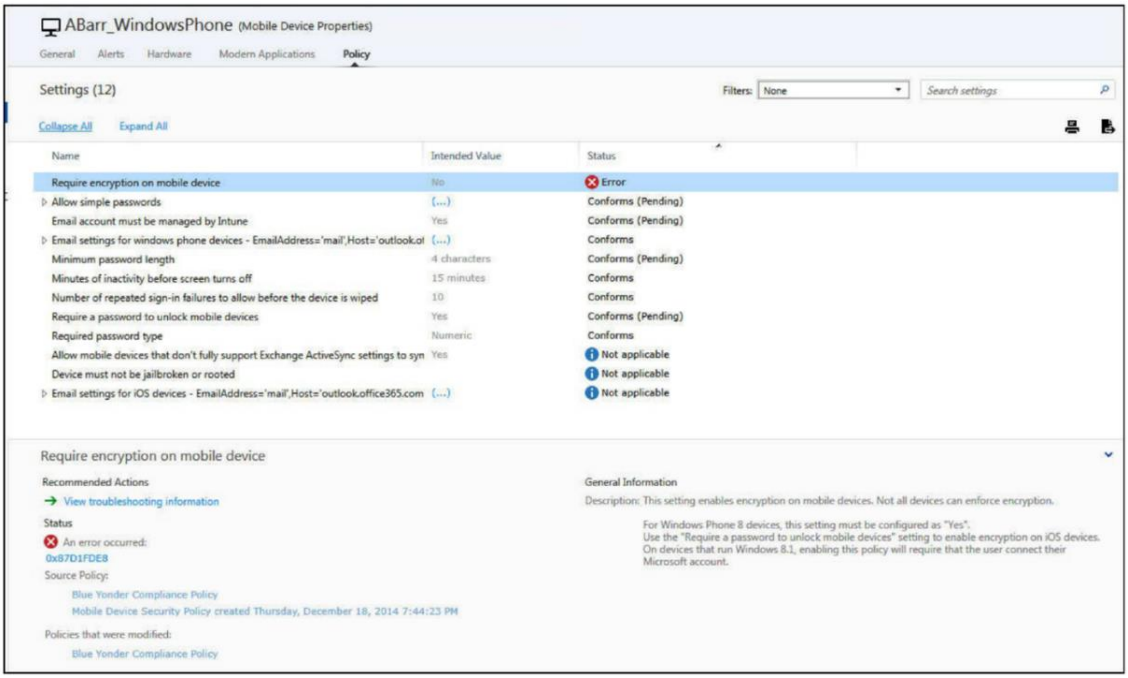

Рисунок 1.10 – Відображення інформації про пристрій на базі Windows Phone у середовищі Microsoft Enterprise Mobility Suite

Служба Microsoft Intune підтримує основні інтерфейси програмного керування (API), призначені для операційної системи Android, а також забезпечує базову інтеграцію з функціональними можливостями платформи Samsung Knox. Водночас Intune не надає підтримки середовища Android for Work та API-інтерфейсів, характерних для мобільних пристроїв інших виробників, таких як LG, HTC тощо.

Недоліки:

- нестабільна робота, особливо з Android- та Windows-пристроями;
- потреба в одночасному використанні трьох різних консолей для адміністрування.

1.5.5 Citrix XenMobile

Citrix XenMobile пропонує комплексне рішення для корпоративного управління мобільністю, об'єднуючи управління пристроями, застосунками і доступом до ресурсів в одному продукті. Система гарантує безпеку та зручність використання як корпоративних, так і особистих пристроїв (рисунок 1.11).

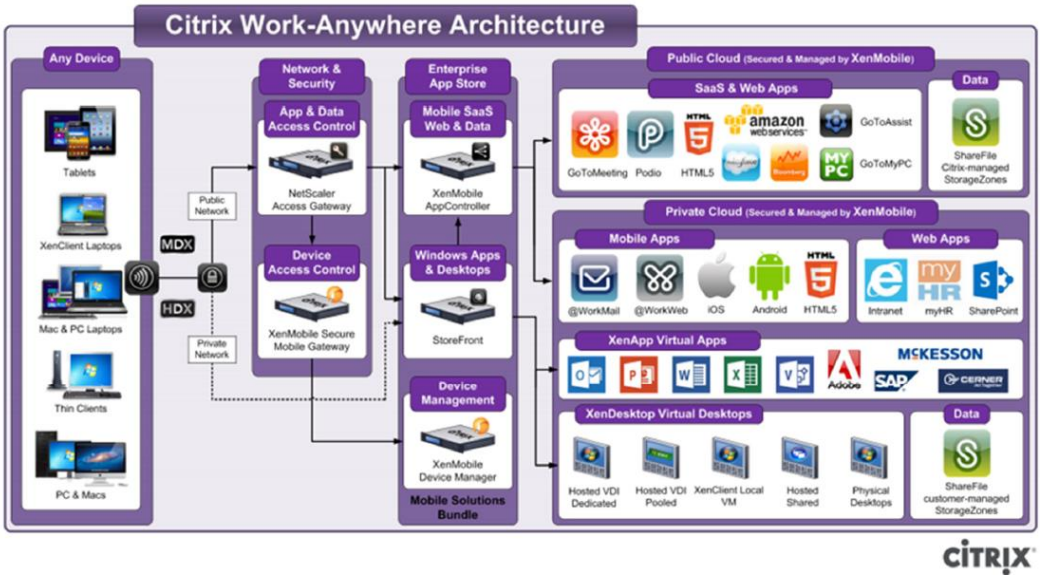

Рисунок 1.11 – Структурна архітектура платформи Citrix XenMobile

Переваги:

- платформа Citrix вирізняється наявністю високоякісних власних мобільних застосунків, які входять до пакету Worx Mobile Apps, а також інтеграцією зі сторонніми рішеннями, доступними через Worx App Store. Це забезпечує широкі можливості для розгортання корпоративних мобільних застосунків. Застосунок Citrix ShareFile вирізняється найповнішою

функціональністю серед аналогічних рішень у сфері управління корпоративною мобільністю (УКМ).

Компанія Citrix отримує схвальні відгуки клієнтів за якість технічної підтримки та високий рівень консультаційного супроводу.

Недоліки:

- функціональні можливості платформи можуть бути обмежені політикою виробників мобільних пристроїв;

- доступні функції здебільшого визначаються параметрами, які встановлює сам виробник обладнання, що значно звужує можливості керування;

- існує проблема довіри з боку користувачів: небажання надавати IT-службі доступ до особистих контактів і даних часто змушує працівників використовувати окремі пристрої для особистого та робочого використання, що призводить до необхідності носити два мобільні телефони.

1.5.6 Критерії оцінки систем УКМ

Проведений аналіз дозволив сформувати критерії оцінки функціональних можливостей систем управління корпоративною мобільністю, засновані на методі Smith Rob, рекомендованому компанією Gartner [20] (таблиця 1.3). Оцінювання проводилося за п’ятибальною шкалою: 1 – дуже низький рівень, 5 – дуже високий.

Виявлені основні проблеми у функціонуванні систем УКМ:

- велика різноманітність моделей і типів мобільних пристроїв;

- високі витрати на впровадження та підтримку УКМ залежно від масштабу підприємства;

- ризик виникнення проблем через самостійне обслуговування пристроїв співробітниками;

- зниження продуктивності системи при збільшенні кількості підключених пристроїв і користувачів.

Таблиця 1.3 – Порівняльна характеристика сучасних систем управління корпоративною мобільністю

Критерії	AirWatch by VMWare	MobileIron	SOTI	Microsoft	Citrix
Архітектура та масштабованість	4.9	4.0	4.0	3.0	2.5
Управління та зручність експлуатації	4.7	4.0	4.0	2.0	4.0
Конфігурація та керування пристрою	4.6	4.0	4.0	2.0	4.0
Управління мобільними програмами	4.8	4.0	3.5	2.0	4.5
Безпечні доступ та розподіл контенту	3.5	3.0	3.0	2.5	4.9
Мобільні ідентифікація та доступ	4.0	3.5	3.0	4.0	2.5
Політика стримування	2.5	4.0	2.0	4.5	4.5
Управління клієнтами	3.5	3.0	2.0	4.7	3.0
Безпека пристрою та відповідність вимогам	2.0	4.0	1.5	2.3	4.5

1.6 Вибір архітектури системи управління корпоративною мобільністю

Система управління корпоративною мобільністю (УКМ) складається з двох ключових елементів:

- сервер УКМ – центральний компонент, відповідальний за управління мобільними пристроями, застосунками, контентом і корпоративним магазином додатків;
- мобільний агент – застосунок, який встановлюється на пристрій користувача і виконує керуючі дії відповідно до команд сервера через бездротові мережі (3G–5G, Wi-Fi), незалежно від географічного розташування чи типу з'єднання [17].

Таким чином, вибір архітектури УКМ потребує визначення відповідних

рішень для обох складових системи.

Система УКМ є невід'ємною частиною корпоративної мобільної інфраструктури. Її архітектура подібна до архітектури інших корпоративних мобільних сервісів і слугує розширенням можливостей існуючих корпоративних платформ в умовах стрімкого розвитку мобільних технологій (рисунок 1.12).

Рисунок 1.12 – Розширення корпоративних сервісів для підтримки мобільних обчислень

Існують два підходи для інтеграції мобільних сервісів у корпоративне середовище:

- Point-to-Point рішення – передбачає індивідуальне розгортання додатків для мобільних працівників. Такий варіант більше підходить для організацій з невеликою кількістю співробітників;

- платформа для корпоративних мобільних додатків (Mobile Enterprise Application Platform, MEAP) – забезпечує повноцінне клієнт-серверне середовище та інструментарій для розробки мобільних застосунків, що можуть функціонувати на різних пристроях та операційних системах із підтримкою автономного режиму.

MEAP допомагає подолати виклики, пов’язані з різноманіттям пристроїв, мереж та груп користувачів, полегшуючи розробку, розгортання та підтримку мобільних рішень протягом усього їх життєвого циклу. Це рішення також сприяє зростанню гнучкості керування та оптимізації витрат,

що робить MEAP найбільш придатним варіантом для створення системи УКМ.

Мобільний агент, встановлений на пристрої користувача, має права адміністратора для виконання необхідних операцій. Існують чотири основні типи мобільних застосунків [10, 11]:

- рідний (native) застосунок – створений спеціально для певної платформи (наприклад, Android, iOS, Windows Phone) із використанням нативних інструментів розробника;

- веб-застосунок – працює на основі веб-технологій (HTML, CSS, JavaScript), є кросплатформовим, але має обмежений доступ до апаратних можливостей пристрою;

- гібридний застосунок – поєднує риси веб- та рідного застосунку, зазвичай реалізований як веб-додаток у контейнері нативного середовища;

- термінальний доступ – використання технологій віртуалізації робочих місць (Virtual Desktop Infrastructure, VDI) для доступу до Windows-додатків.

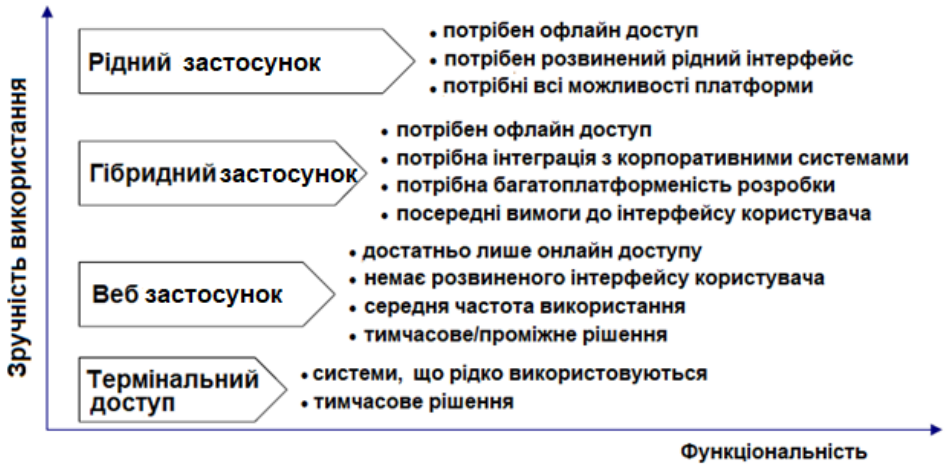

Рисунок 1.13 – Варіанти архітектурної побудови мобільних застосунків

Для об'єктивного аналізу типів застосунків складена таблиця переваг та недоліків (таблиця 1.4). Згідно з висновками з таблиці, найкращим вибором для створення мобільного агента системи УКМ є рідний застосунок.

Таблиця 1.4 – Переваги та недоліки видів мобільних застосунків

Модель	Переваги	Недоліки
1	2	3
Рідний застосунок	повна підтримка засобів та можливостей мобільної платформи; максимальна зручність використання; мокальне збереження даних та офлайн-режим роботи; безпека	спеціальна експертиза у розробці та тестуванні під конкретні мобільні платформи; більший час розробки
Гібридний застосунків	прискорена однакова розробка під різні мобільні платформи; прозора інтеграція з корпоративними системами; безпека	обмежені можливості використання специфіки мобільних платформ; спеціальна експертиза.
Веб-застосунок для використання в інтернет-браузері	одноразова розробка веб-програми	неможливість автономної роботи: відсутність локального збереження даних для роботи з документами та інформацією в автономному режимі; необхідний облік специфіки браузерів.

Продовження таблиці 1.4

1	2	3
Термінальний доступ до Windows-застосунків й віртуальний робочий стіл (VDI)	безпека; мінімальна модернізація інфраструктури	неможливість автономної роботи: відсутність локального збереження даних для роботи з документами та інформацією в офлайн-режимі; незручність і непристосованість мобільних пристроїв для роботи з інтерфейсом Windows-застосунків

2 МОДЕЛЬ УПРАВЛІННЯ КОРПОРАТИВНОЮ МОБІЛЬНІСТЮ

2.1 Контекстне середовище системи управління корпоративною мобільністю

Проблематика управління мобільними пристроями виникає у випадках, коли запити на доступ до корпоративних ресурсів надходять із зовнішнього середовища за межами корпоративної мережі. У ситуаціях, коли сервер шлюзу виявляє запити від невідомих або незареєстрованих мобільних пристроїв, вони автоматично перенаправляються на сервер системи УКМ для подальшої обробки. Після виконання встановлених процедур і налаштування мобільних пристроїв, сервер УКМ надає їм доступ до ресурсів і передає підтвердження цих дій до шлюзового сервера корпоративної мережі.

Корпоративна політика передбачає можливість використання працівниками як власних пристроїв для виконання службових обов’язків, так і корпоративних пристроїв для особистих потреб. Такий підхід сприяє більшій гнучкості планування робочого часу та місця, що позитивно впливає на загальну продуктивність співробітників.

Для більш наочного розуміння наведено (рисунок 2.1) контекстне середовище функціонування системи УКМ із залученням служб Push-сповіщень – важливого компонента, що забезпечує контекстну обізнаність застосунків та оперативне оновлення інформації на мобільних пристроях.

Основні процеси, що реалізуються у системі УКМ, включають:

- реєстрацію мобільних пристроїв у корпоративній інфраструктурі;
- централізоване управління пристроями, мобільними застосунками та корпоративним контентом;
- забезпечення захисту мобільних пристроїв;
- розподіл корпоративних ресурсів серед мобільних користувачів;
- моніторинг стану пристроїв та організацію системи сповіщень.

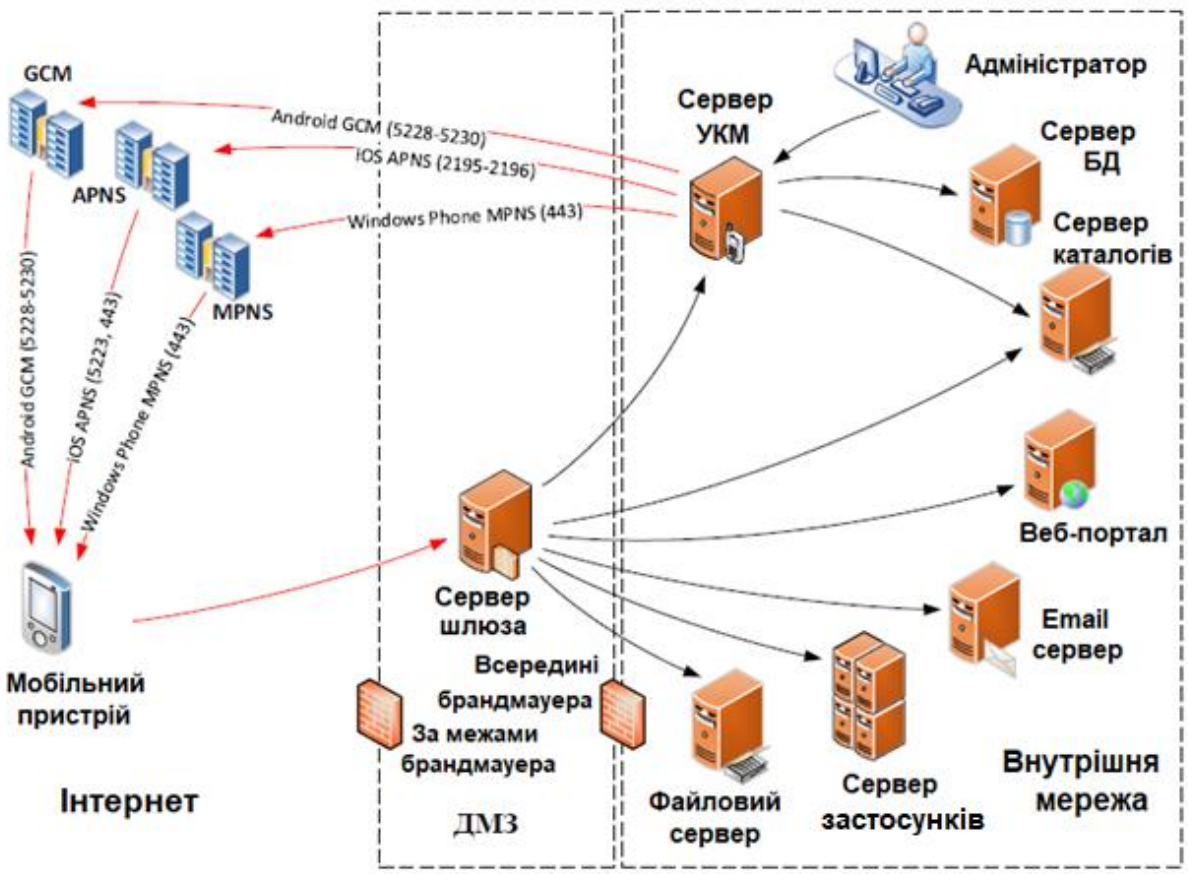

Рисунок 2.1 – Контекстне середовище системи УКМ

2.2 Масштабована модель керуючого простору

У системах управління корпоративною мобільністю (УКМ) ресурсна модель використовується для опису завдань, результатів операцій, обміну даними між функціональними сервісами на сервері та обміну керуючими повідомленнями між серверною частиною та мобільними пристроями.

Процеси в системі УКМ організовано за операційним принципом. На рисунку 2.2 наведено ресурсну модель, яка базується на трьох основних абстракціях: події, дії та властивості.

Події представляють зміни у стані мобільного пристрою під час взаємодії з сервером. Для кожного типу або конкретного пристрою формується перелік можливих подій. У ході обробки подій можуть виникати

одне чи декілька повідомлень. Кожна подія має бути ідентифікована за іменем та пов’язана із відповідними даними ресурсної моделі.

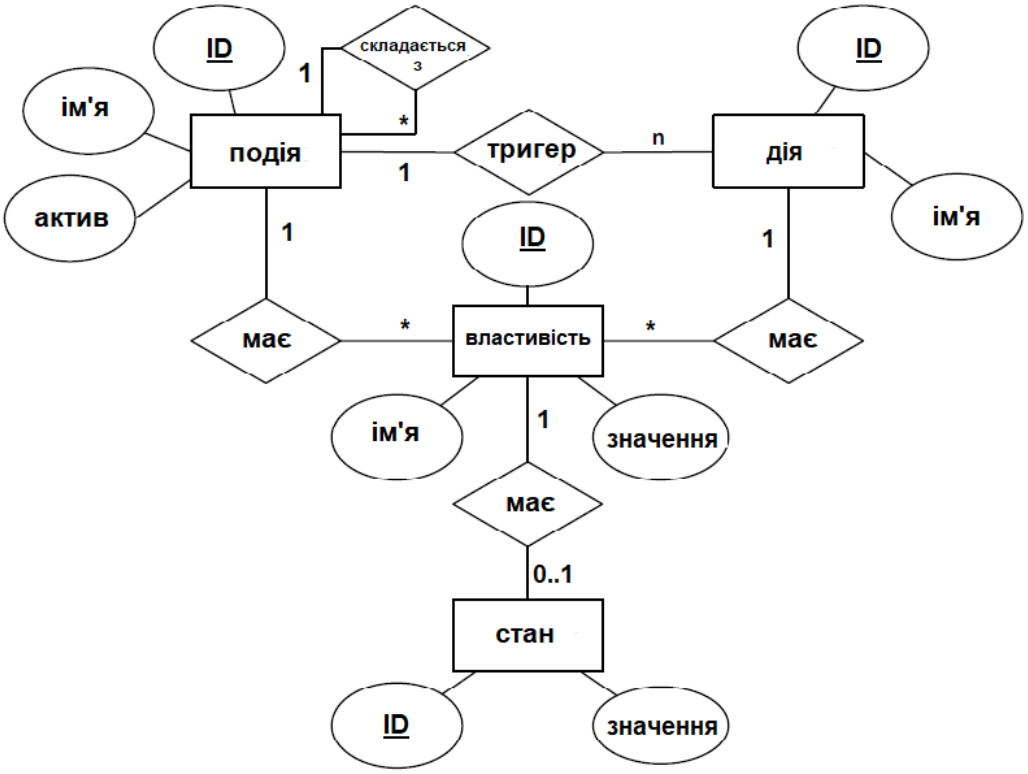

Рисунок 2.2 – Модель ресурсів операції з взаємозв'язками елементів подій

Дії визначають доступні методи взаємодії з пристроєм. Для виконання дій можуть знадобитися різні типи даних, такі як числа, логічні значення, рядки, масиви або об'єкти, які можуть містити вкладені дані. Виклик дій є асинхронним і може повертати результати, що відповідають структурі ресурсної моделі.

Властивості описують параметри, що характеризують стан, налаштування та конфігурацію пристрою, зокрема назву виробника, модель, поточні значення параметрів або конфігураційних налаштувань. Властивості можуть бути доступними лише для читання або для читання й запису та є об'єктами моніторингу змін.

Ресурсна модель УКМ зберігається у форматі JSON. Для оптимізації обміну даними допускається передача лише необхідних елементів без

дублювання повної структури подій, дій чи властивостей. Наприклад, наведено приклад структури JSON для операції зміни коду блокування екрану пристрою Android, зареєстрованого у системі УКМ:

- запит на пристрій:

```
json
{
  "operationID": {
    "lockCode": "1234"
  },
  "deviceID": "a5:90:g6:2f:8b:5c"
}
```

- отримана відповідь:

```
json
{
  "deviceID": "a5:90:g6:2f:8b:5c",
  "operationID": {
    "lockCode": "1234",
    "status": "COMPLETED"
  }
}
```

Архітектура системи УКМ побудована за принципом клієнт-серверної моделі і включає два основні компоненти:

- сервер – центральний елемент, що здійснює управління мобільними пристроями, застосунками, контентом і корпоративним магазином застосунків;

- агент, встановлений на мобільний пристрій, який виконує керуючі операції для конкретного пристрою.

На рисунку 2.3 представлено двоконтурну схему управління пристроєм у системі УКМ, де:

- суб'єкт управління – агент;

- об'єкт управління – мобільний пристрій;

- керуючий пристрій – модуль в агенті, що обробляє та виконує отримані операції;

- керуючий вплив – ресурсна модель операцій у форматі JSON;

- сам пристрій також виконує роль агента.

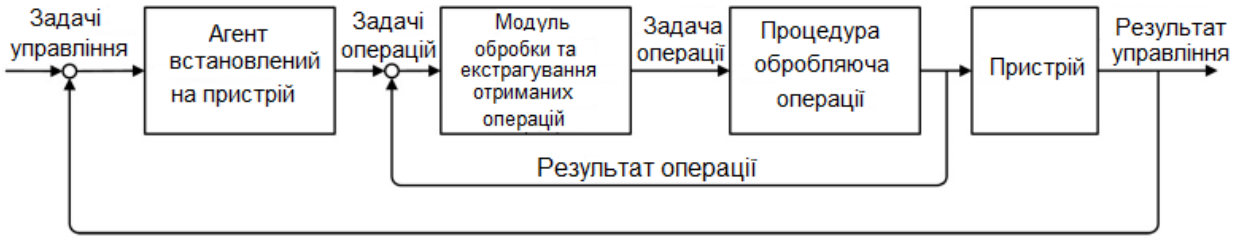

Рисунок 2.3 – Схема управління мобільністю в корпоративній середовищі на рівні пристроїв

Зворотній зв'язок у системі забезпечує аналіз результатів виконання операцій та поточного стану мобільного пристрою.

Функціональні компоненти та сервіси серверної частини обробляють різні типи керуючих операцій із відповідними ресурсними моделями. При виконанні операції operationID пристрій обмінюється ресурсами із сервісами серверної частини.

На основі проведеного аналізу системи УКМ, побудованої відповідно до концепції MEAP, доцільно використовувати ієрархічну структуру ресурсів та ресурсно-орієнтовану архітектуру. Згідно з "правилом трьох" Gartner і масштабованою моделлю куба AKF, ресурсні дані операцій описуються кортежем:

```
resource_data = {interaction_type, deviceID, operationID}
```

де:

`resource_data` – дані ресурсу (опис завдання або результату операції);

`interaction_type` – тип взаємодії в процесі виконання операції;

`deviceID` – унікальний ідентифікатор пристрою;

`operationID` – код операції, що виконується агентом.

При побудові механізму взаємодії у системі УКМ важливим є узгодження взаємодії між компонентами клієнт-серверної архітектури. Агент на пристрої взаємодіє з різними сервісами серверної частини через різні стилі клієнт-серверної взаємодії, які класифікуються за двома вимірами:

а) тип взаємодії за кількістю об'єктів:

- один до одного – кожен запит обробляється одним екземпляром сервісу;

- один до багатьох – запит обробляється кількома екземплярами сервісу одночасно.

б) тип взаємодії за часом обробки:

- синхронна взаємодія – клієнт очікує на відповідь від сервісу;

- асинхронна взаємодія – клієнт не чекає відповіді та продовжує роботу незалежно від відповіді сервісу.

У таблиці 2.1 наведено порівняльну характеристику різних типів взаємодії у системі УКМ.

Таблиця 2.1 – Типи взаємодії

	Один до одного	Один до багатьох
Синхронна взаємодія	запит/відповідь	–
Асинхронна взаємодія	публікація	публікація /підписка
	запит/асинхронна відповідь	повідомлення / асинхронна відповідь

Існують наступні типи взаємодії один до одного:

- запит/відповідь – клієнт ініціює запит до сервісу і очікує на відповідь. Запит може блокувати потік програми під час очікування відповіді в межах встановленого часу;

- публікація – клієнт надсилає запит до сервісу, проте не очікує відповіді або її надання не є обов'язковим;

- запит/асинхронна відповідь – клієнт ініціює запит до сервісу, який відповідає асинхронно. Клієнт не блокується під час очікування відповіді, і відповідь може надійти через деякий час.

Існують також види взаємодії один до багатьох:

- публікація/підписка – клієнт публікує повідомлення, яке може бути отримано нульовою або кількома зацікавленими службами;

- публікація/асинхронна відповідь – клієнт публікує повідомлення із запитом і очікує відповіді від зацікавлених служб протягом певного часу.

У контексті системи УКМ, ідентифікація пристрою є важливим параметром для здійснення управлінських операцій на конкретному мобільному пристрої. Це унікальне значення, пов'язане з конкретним пристроєм. Існують два способи створення чи вилучення ідентифікації пристрою (deviceID) в залежності від операційної системи:

а) Device ID генерується з унікальної ідентифікації пристрою. Цей метод застосовується для пристроїв під управлінням Android та iOS.

Докладний опис методу створення та вилучення deviceID для пристроїв, що працюють під керуванням ОС Android або iOS, наведено нижче. Для Android-пристроїв deviceID є рядком ANDROID_ID – 64-бітовим шістнадцятирічним значенням, яке генерується випадковим чином під час первинного налаштування пристрою. Це значення залишається незмінним протягом усього терміну експлуатації пристрою. Отримати deviceID можна за допомогою наступного коду на мові Java:

```
import android.provider.Settings.Secure;
String deviceID = Secure.getString(this.getContentResolver(),
Secure.ANDROID_ID);
```

У випадку, коли Android-пристрій підтримує кілька користувачів (ця можливість доступна на пристроях, що працюють під керуванням Android 10 або новіших версій), кожен користувач розпізнається як окремий пристрій, що забезпечує унікальність значення ANDROID_ID для кожного конкретного користувача.

Щодо iOS-пристроїв, deviceID є унікальним ідентифікатором пристрою (UDID), який складається з шістнадцятирічного значення довжиною 40 символів (20 байт). Це значення UDID обчислюється за наступною методикою:

- для iPhone 4 і новіших моделей:

```
UDID = SHA1(serial + ECID + wifiMac + bluetoothMac);
```

- для інших пристроїв:

```
UDID = SHA1(serial + IMEI + wifiMac + bluetoothMac),
```

де serial – це серійний номер iOS-пристрою (довжина 11 символів для старих моделей або 12 символів для нових);

ECID (Exclusive Chip ID or Electronic Chip ID) – число ECID (довжина 13 - символів у десятковій системі числення без провідних нулів);

IMEI (International Mobile Station Equipment Identity) – число IMEI (довжина 15 – символів без пробілів); використання порожнього рядка для iPod touch та iPad моделі Wi-Fi;

wifiMac – MAC-адреса Wi-Fi (довжина 17-символів у нижньому регістрі, у тому числі двокрапкою). Для iPod touch першого покоління, використання "00:00:00:00:00:00";

MAC-адреса Bluetooth (довжина 17 символів у нижньому регістрі, у тому числі двокрапкою).

Device ID може бути також Universally Unique Identifier (UUID) – 128-бітове значення, що відповідає стандарту RFC 4122 [16].

Для візуалізації керуючої операції за допомогою масштабованої моделі куба AKF, кожна вісь куба (OX, OY, OZ) представляє різні аспекти масштабування системи. Найгірший варіант монолітної системи представлений на найнижчій лівій точці куба, де всі функції об'єднані в одній кодовій базі на одному сервері та/або одній IP-адресі.

Рисунок 2.4 ілюструє концепцію масштабованої архітектури системи УКМ, яка застосовує модель куба AKF для забезпечення масштабованості та гнучкості системи в різних умовах.

Три виміри масштабованого куба AKF для системи УКМ визначаються наступним чином:

а) вісь OX відображає горизонтальне дублювання та клонування сервісів і даних, а також типи взаємодії між компонентами системи. Тип взаємодії представляє собою метод чи механізм обміну повідомленнями між елементами системи. У контексті УКМ це визначає механізм виконання операцій управління мобільністю;

б) вісь OY відповідає за функціональну декомпозицію та сегментацію сервісів. Декомпозиція системи вздовж цієї осі передбачає поділ на кілька окремих сервісів, функцій або ресурсів. Кожен сервіс реалізує одну або кілька функцій управління пристроєм. Система УКМ складається з безлічі сервісів управління, при цьому кожен сервіс орієнтований на конкретну операцію або завдання з більш простим кодом. Існує кілька підходів до поділу системи на сервіси: один передбачає створення сервісів для реалізації окремих випадків використання, таких як отримання інформації від пристрою, а інший – формування сервісів, що відповідають за всі операції, пов'язані з певним об'єктом, наприклад, управління клієнтами;

в) вісь OZ описує розподіл сервісів і даних між кінцевими точками клієнта. Вона визначає множину точок операцій управління, що знаходяться на межі взаємодії з кінцевим користувачем.

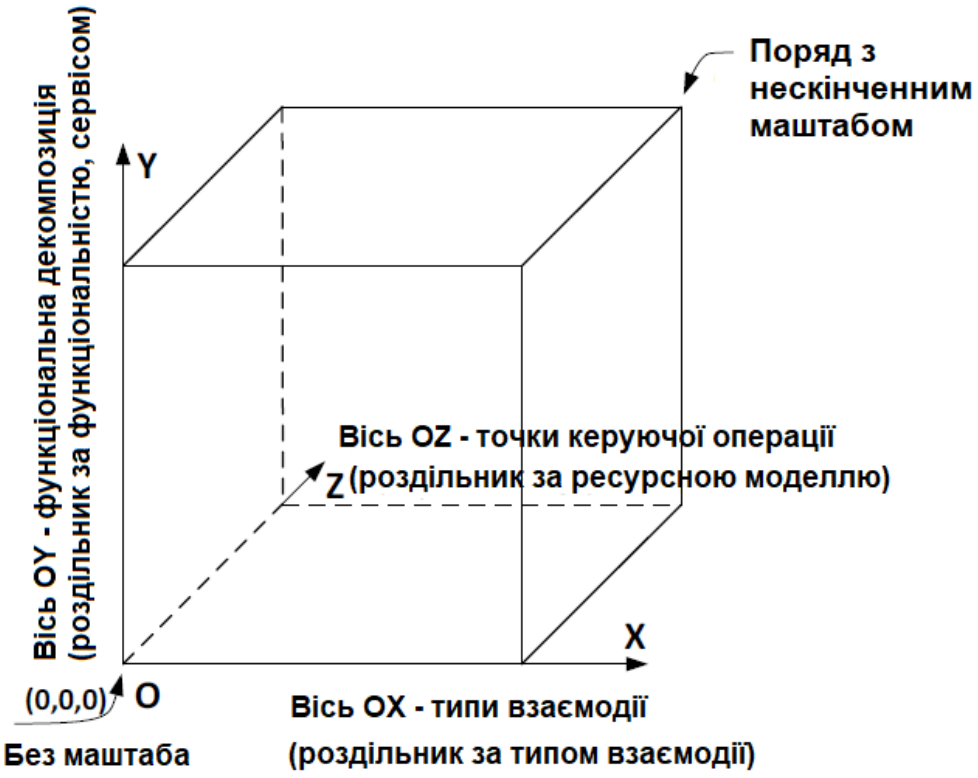

Рисунок 2.4 – Архітектура системи УКМ, побудована на основі моделі шкали куба AKF

2.3 Управління корпоративною мобільністю на основі ресурсно-орієнтованої архітектури

Рішення MEAP є оптимальним для побудови системи УКМ, оскільки пристрої та операції доступу до цієї системи можуть бути реалізовані через IP-адресу сервера. Операції в системі УКМ, що базується на ресурсно-орієнтованій архітектурі, здійснюються за допомогою HTTP-методів (з боку адміністратора) або протоколу MQTT (з боку пристрою). Для реалізації цієї архітектури необхідно виконати такі умови:

а) вміст обміну повідомленнями не повинен включати додаткову інформацію, таку як адреса пристрою чи операції;

б) ідентифікаційні дані пристрою та операції повинні бути представлені в HTTP-заголовках.

Ці вимоги вирішуються шляхом застосування унікальних URI-адрес для кожного пристрою та/або операції, що забезпечує чітке розмежування та контроль доступу.

Як приклад, нижче наведено принцип виконання конкретної операції `{operationID}` адміністратором для певного пристрою `{deviceID}` за допомогою командного рядка URI в типі HTTP-взаємодії:

```
curl -X GET -H "Content-Type: application/json" -H
"Authorization: Bearer <TOKEN>" -k -v
baseIP/{deviceID}/{operationID}
```

URI-стандарт складається з двох частин: host та path. Це можна побачити в наведеній команді, де адреса `baseIP/{deviceID}/{operationID}` розділяється на дві частини: `host baseIP` та `path part/{deviceID}/{operationID}`.

Операції в системі УКМ варіюються залежно від конкретних припущень і реалізуються через різні сервіси, використовуючи конструкцію `{deviceID}` та `{operationID}` для адресації операцій і пристроїв:

Існує m типів сервісів, що виконують m типів операцій;

Є n пристроїв, кожне з яких має унікальний ідентифікатор

`{deviceID}`.

Моделювання операцій управління мобільністю здійснюється на координатній площині OYZ масштабованого куба AKF. Приклад моделювання управління мобільністю через веб-сервіси RESTful для конкретних `{deviceIDi}` та `{operationIDj}` наведено (рисунок 2.5).

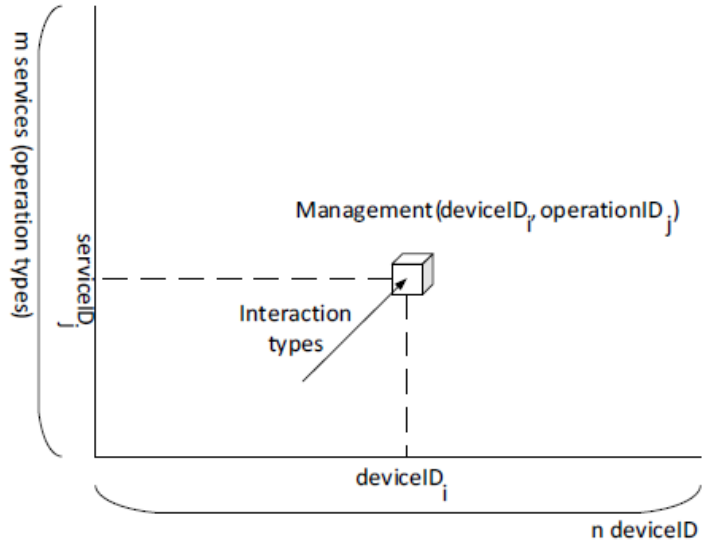

Рисунок 2.5 – Операція УКМ на основі ресурсно-орієнтованої архітектури

Наведено приклад операції управління корпоративною мобільністю (УКМ), що реалізується з використанням ресурсно-орієнтованої архітектури:

- на стороні адміністратора системи: керуюча операція здійснюється за допомогою HTTP-методів у архітектурному стилі REST (див. таблиця 2.2):

`GET/PUT/POST/DELETE baseIP/a590g62f8b5c/changelockcode`

- на стороні пристрою системи: операції передаються на пристрої за допомогою протоколу MQTT у моделі публікації/підписки:

`mqtt/+/emm/a590g62f8b5c/changelockcode/#`

Існують два типи підключення: синхронне (запит/відповідь) і асинхронне (публікація/підписка). У моделі публікації/підписки абоненти отримують лише частину загального потоку опублікованих повідомлень [15]. Процес вибору та обробки повідомлень для прийому реалізується через фільтрацію. Існує два основні підходи до фільтрації: за темою та за змістом:

- фільтрація за темою**:** у системі, організованій за принципом тем,

повідомлення публікуються на визначені теми або канали. Абоненти, що підписуються на певну тему, отримуватимуть всі повідомлення, опубліковані в цій темі. Якщо всі абоненти підписуються на одну й ту саму тему, вони отримуватимуть однакові повідомлення. Публікація відповідає за визначення класів повідомлень, до яких абоненти можуть підписуватись.

- фільтрація за змістом**:** у такій системі повідомлення доставляються абоненту тільки тоді, коли їх атрибути або вміст відповідають заданим критеріям, визначеним абонентом. Абонент здійснює класифікацію повідомлень відповідно до цих критеріїв.

- гібридна система**:** деякі системи комбінують обидва підходи: публікація відправляє повідомлення в тему, а абоненти реєструються на підписку з фільтрацією за змістом, однією або кількома темами.

У багатьох системах публікації/підписки повідомлення передаються через проміжний брокер повідомлень або шину подій. Абоненти реєструються для підписки на цей брокер, який виконує фільтрацію та маршрутизацію повідомлень до абонентів. Брокер також може виконувати функції зберігання та маршрутизації, визначаючи пріоритети повідомлень у черзі для їх подальшої доставки. Модель публікації/підписки має ряд переваг порівняно з моделлю запиту/відповіді [15].

Протокол MQTT (Message Queue Telemetry Transport) – це модель публікації/підписки, яка є простим і легким протоколом для обміну повідомленнями, спеціально розробленим для пристроїв з обмеженою пропускною здатністю, високою затримкою або ненадійними мережами. MQTT пропонує низку переваг порівняно з протоколом HTTP. HTTP був розроблений як протокол запиту/відповіді для клієнт-серверних обчислень і не оптимізований для мобільних середовищ. В умовах мобільних мереж критичними факторами є час відгуку, пропускна здатність та енергоспоживання, що є важливими параметрами при розробці.

Протокол MQTT забезпечує більш швидкий відгук, вищу пропускну здатність та зниження енергоспоживання, що робить його оптимальним для

використання в таких умовах:

- переміжне підключення;
- обмежена пропускна здатність;
- взаємодія корпоративного застосунку з одним або кількома мобільними додатками;
- мобільні додатки, які повинні передавати дані надійно без необхідності впровадження логіки повторних спроб.

Протокол HTTP не оптимізований для мінімізації енергоспоживання або зменшення потоку даних, в той час як MQTT має низьку латентність і забезпечує ефективний розподіл даних. MQTT споживає менше енергії для підтримки відкритого з'єднання та для прийому/надсилання повідомлень.

Архітектура протоколу MQTT зображена (рисунок 2.6).

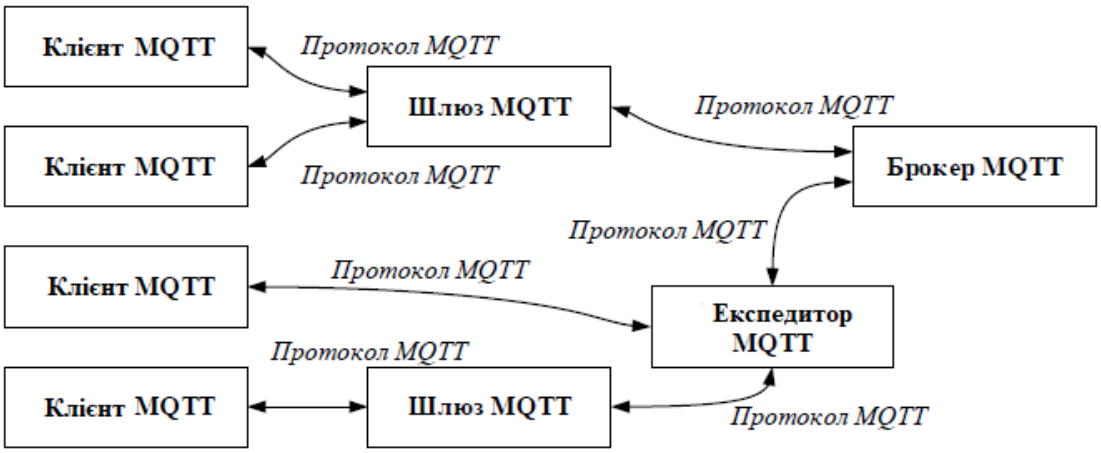

Рисунок 2.6 – Архітектура протоколу MQTT

У результаті викладених переваг моделі публікації/підписки, у системі УКМ для обміну повідомленнями між сервером та клієнтами застосовується протокол MQTT замість HTTP.

3 МЕТОД УПРАВЛІННЯ КОРПОРАТИВНОЇ МОБІЛЬНІСТЮ

3.1 Вибір механізму передачі керуючих операцій до пристроїв у системі управління корпоративною мобільністю

Система управління корпоративною мобільністю (УКМ) функціонує за архітектурною моделлю "клієнт-сервер" та включає два ключові компоненти:

- сервер УКМ – центральний елемент системи, що виконує адміністрування пристроїв, застосунків, корпоративного контенту та фірмового магазину застосунків;

- клієнтський агент**,** який інсталюється на мобільний пристрій і забезпечує виконання керуючих команд, що надходять від сервера системи. З'єднання між агентом і сервером реалізується через бездротовий канал, який є незалежним від фізичного розташування користувача або типу мережевого підключення.

У зв’язку з цим постає завдання вибору ефективного механізму передачі команд від сервера до агентів, встановлених на мобільних пристроях. Наразі у практиці застосовуються три основні підходи до реалізації такого обміну:

а) polling-механізм (опитування) на стороні клієнта**;**

б) тунельований механізм передачі**;**

в) push-сповіщення**.**

Polling-механізм (рисунок 3.1). Цей підхід вважається найпростішим з точки зору реалізації. При потребі виконання певної операції, адміністратор створює відповідний запит на сервері. Клієнтський агент із заданою періодичністю здійснює опитування сервера щодо наявності команд. У разі наявності таких, агент виконує операції та надсилає результати назад на сервер. Основною перевагою цього методу є низький рівень залежності між сервером і клієнтами, що суттєво знижує навантаження на сервер і дає змогу

ефективно обслуговувати значну кількість пристроїв.

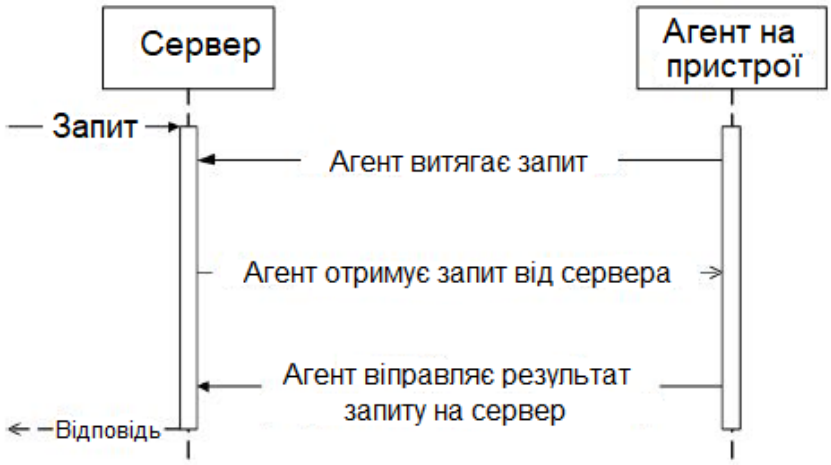

Рисунок 3.1 – Polling-механізм (опитування) на стороні клієнта

Тунельований механізм (рисунок 3.2). Передбачає створення стійкого каналу зв'язку (тунелю) між клієнтом та сервером при запуску програми. З'єднання підтримується в активному стані доти, поки пристрій має доступ до мережі. У разі розриву зв'язку, клієнт автоматично намагається відновити з'єднання. Така модель забезпечує оперативне надсилання команд від адміністратора через сервер без суттєвих затримок. Проте, утримання постійного з'єднання може спричинити додаткові витрати ресурсів системи.

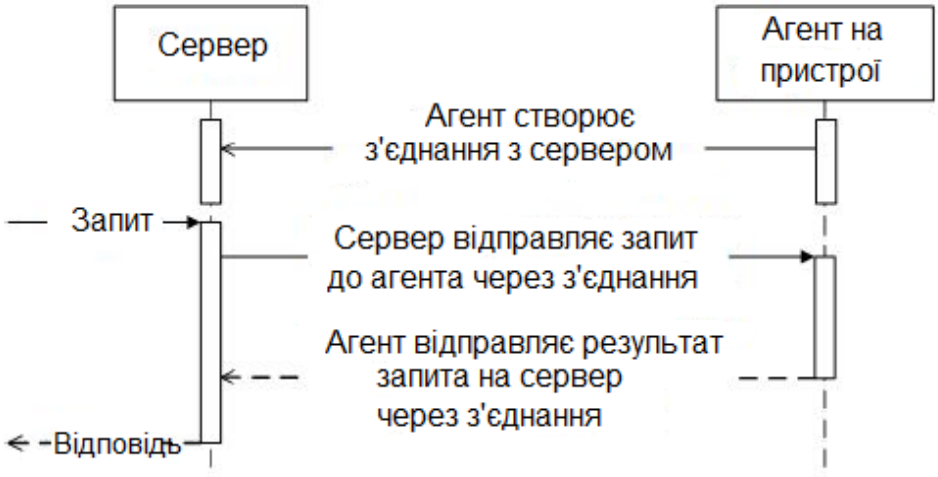

Рисунок 3.2 – Тунельований механізм

Push-сповіщення (рисунок 3.3). Даний механізм ґрунтується на використанні вбудованих сервісів Push-сповіщень, які підтримуються сучасними мобільними операційними системами. Для передачі керуючих операцій сервер надсилає відповідне повідомлення до пристрою через відповідну службу Push-сповіщень. Після отримання такого повідомлення агент виконує вказані дії.

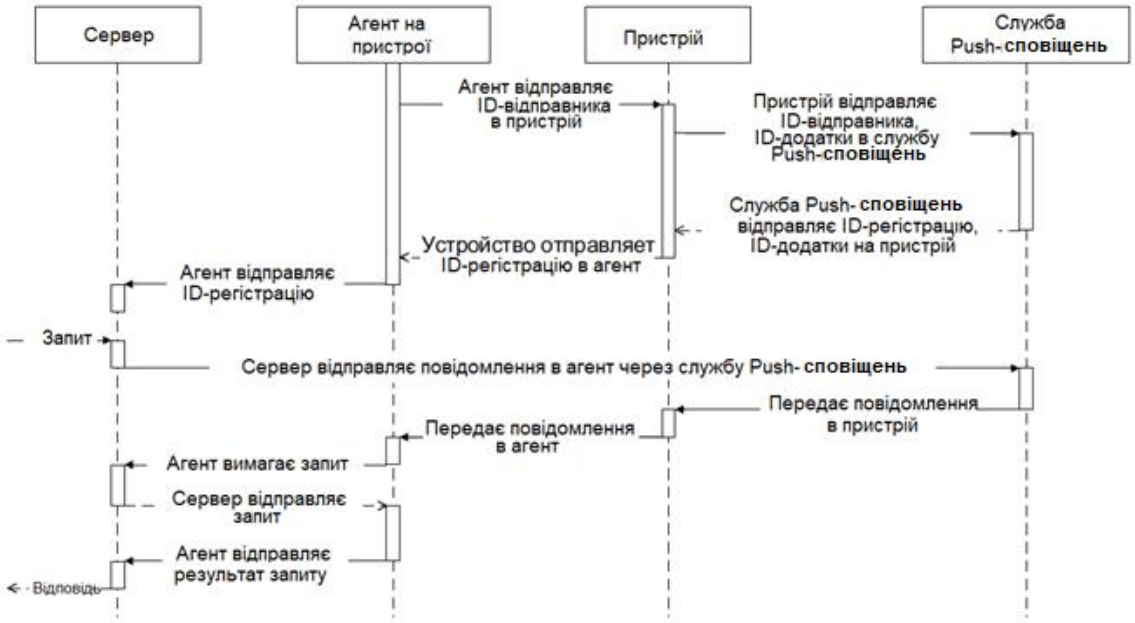

Рисунок 3.3 – Push-сповіщення

Усі розглянуті методи мають власні переваги та обмеження. У рамках проєктування системи УКМ було прийнято рішення реалізувати механізм Push-сповіщень**,** що зумовлено такими чинниками:

- повна інтеграція механізмів Push-сповіщень у сучасні мобільні операційні системи;

- миттєва доставка сповіщень до клієнтських агентів, що мінімізує затримки виконання операцій;

- відсутність потреби в постійному з'єднанні, як у випадку з тунельованим механізмом, що дозволяє уникнути зайвих витрат ресурсів;

- на відміну від Polling-механізму, Push-модель не створює надмірного навантаження на сервер і не потребує високої частоти опитувань.

3.2 Метод управління мобільністю з використанням механізму Push-сповіщень

Метод виконання операцій управління мобільністю містить 9 кроків (рисунок 3.4) [21].

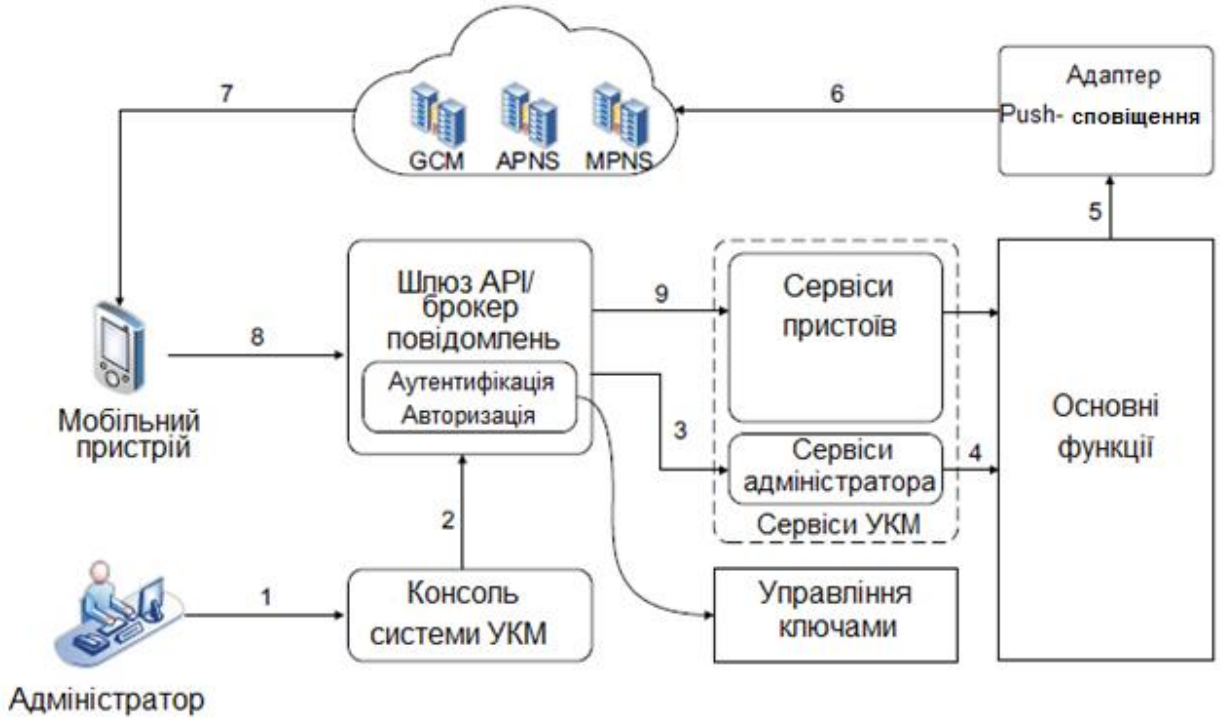

Рисунок 3.4 – Методика УКМ із використанням механізму Push – сповіщень

Крок 1. За допомогою веб-консолі системний адміністратор створює операції, що повинні виконуватися на пристрої.

Крок 2. Веб-консоль викликає API функції на шлюз API.

Крок 3. API-функція на шлюзі API запускає backend-сервіс адміністратора.

Крок 4. Сервіси адміністратора запускають активні операції для пристрою.

Крок 5. Після процесу підтвердження виконання операцій, викликається адаптер Push-сповіщень.

Крок 6. Адаптер викликає відповідну службу Push-сповіщень (GCM для Android, APNS для iOS, MPNS для Windows Phone).

Крок 7. Служба Push-сповіщень надсилає сповіщення на пристрій для оголошення початку певної операції.

Крок 8. Пристрій викликає теми на брокері обміну повідомленнями, щоб отримати операції.

Крок 9. Брокер обмінюється повідомленнями з пристроєм, підписаним та опублікованим за певними темами.

9 кроків об'єднуються у два етапи:

- створення операцій на сервері (рисунок 3.5);
- агентне управління виконанням операцій з використанням методів RESTful або протоколу MQTT (рисунок 3.6).

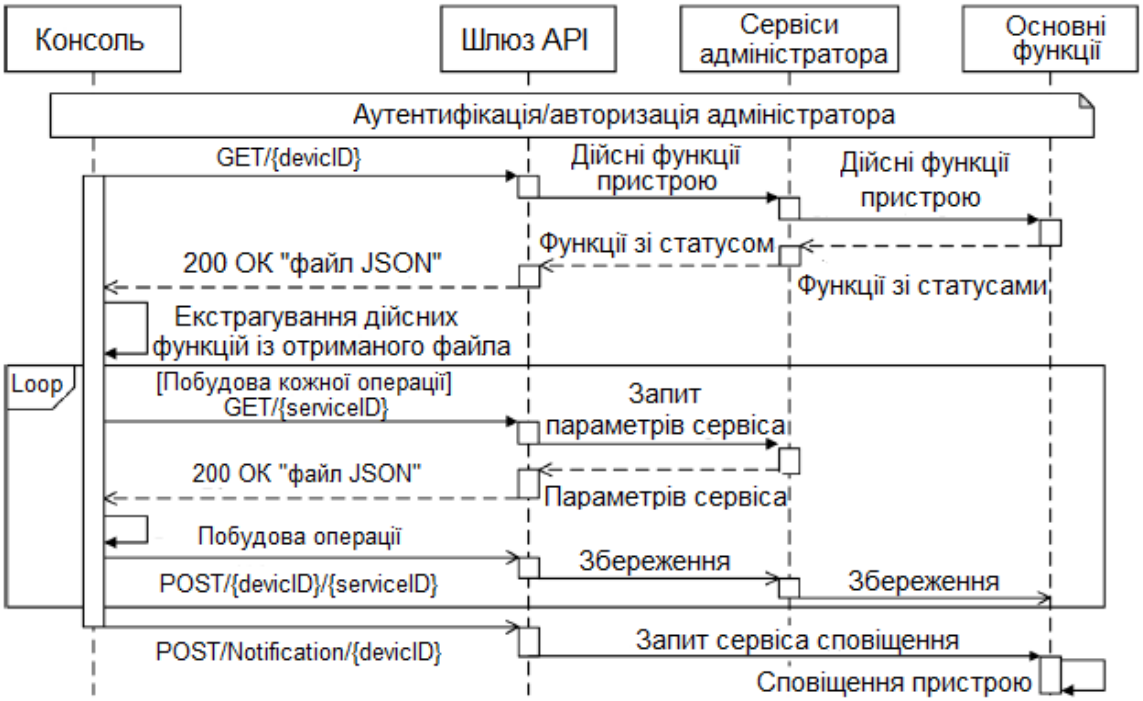

Рисунок 3.5 – Створення операцій на сервері УКМ

3.3 Процеси реєстрації пристроїв та автентифікації/авторизації

Методика УКМ містить 4 процеси:

- реєстрація пристрою в системі УКМ [17];

- автентифікація пристрою [14];

- автентифікація/авторизація користувача за допомогою протоколу OAuth;

- обмін повідомленнями між сервером та мобільними пристроями. Цей розділ визначає перші три процеси в рамках методики управління корпоративною мобільністю для пристроїв під керуванням операційною системою (ОС) Android.

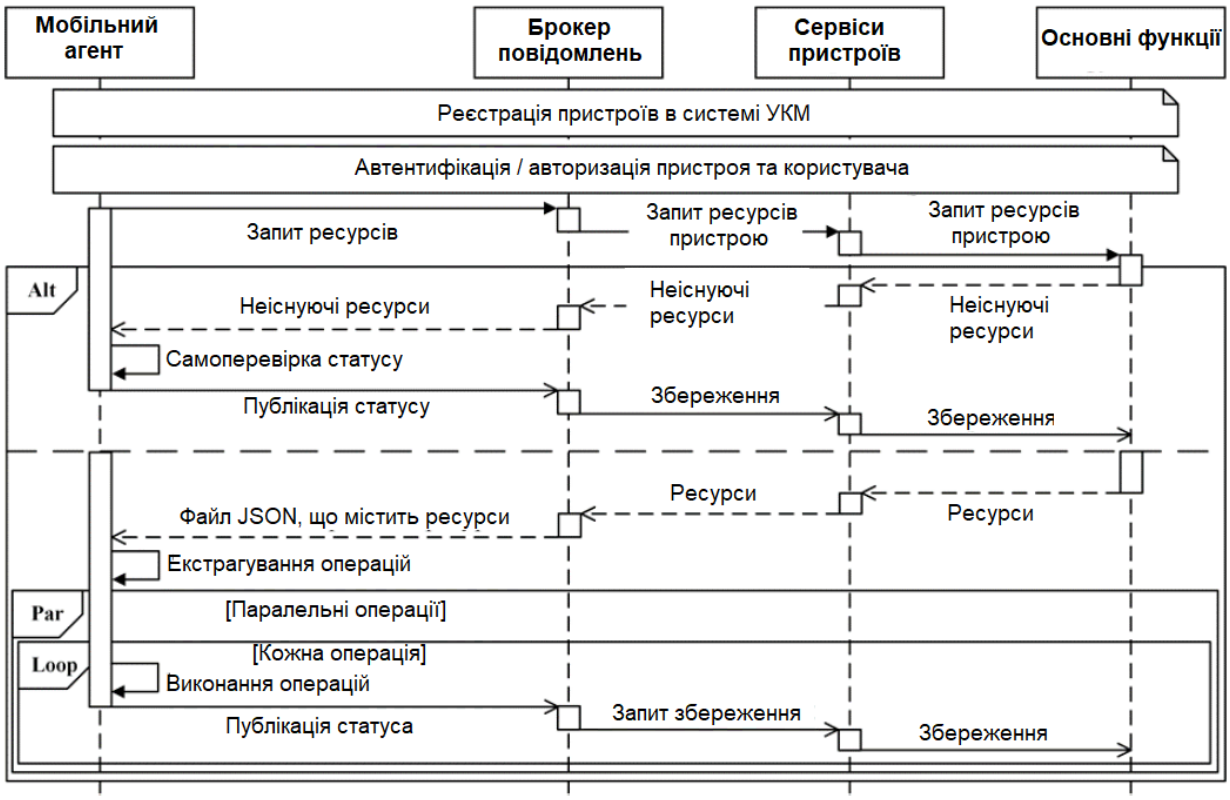

Рисунок 3.6 – Агентне управління виконанням операцій

3.3.1 Процес реєстрації мобільного пристрою в системі управління корпоративною мобільністю

У зв’язку з підвищеними ризиками, пов’язаними з процесом реєстрації пристроїв на базі ОС Android у системі управління корпоративною мобільністю (УКМ), до процедури безпечної реєстрації висуваються наступні вимоги:

- адреса для реєстрації має передаватися лише уповноваженим користувачам через захищені канали, зокрема електронну пошту та/або у вигляді QR-коду (Quick Response);

- пристрій, що ініціює запит на реєстрацію, повинен відповідати вимогам безпеки, встановленим в операційній системі Android;

- до початку завантаження клієнтського агента, сервер УКМ зобов'язаний здійснити автентифікацію як пристрою, так і користувача із застосуванням стандарту Security Assertion Markup Language (SAML)**;**

- після інсталяції агент повинен виконати попередню перевірку параметрів безпеки пристрою (наявність адміністративних та root-повноважень, реєстрація ідентифікатора у службі Google Cloud Messaging (GCM), наявність keystore-файлу тощо), а потім передати ці дані на сервер УКМ;

- автентифікація агента, пристрою та користувача має бути додатково підтверджена відповідно до протоколу OAuth**;**

- увесь процес реєстрації має перебувати під контролем системного адміністратора.

Процедура безпечної віддаленої реєстрації Android-пристрою в системі УКМ включає сім основних етапів (рисунок 3.7):

а) надсилання реєстраційної URL-адреси користувачеві**:** здійснюється через захищений електронний лист або шляхом передавання QR-коду;

б) процес автентифікації пристрою**:** користувач проходить авторизацію, відкривши надану адресу через мобільний браузер або за допомогою QR-сканера;

в) ідентифікація типу пристрою на сервері**:** сервер аналізує заголовок User-Agent у HTTP-запиті, щоб перевірити відповідність пристрою вимогам (зокрема, використання ОС Android з активованими модулями безпеки);

г) автентифікація пристрою за допомогою SAML**:** проводиться перевірка легітимності пристрою відповідно до стандарту (рисунок 3.8);

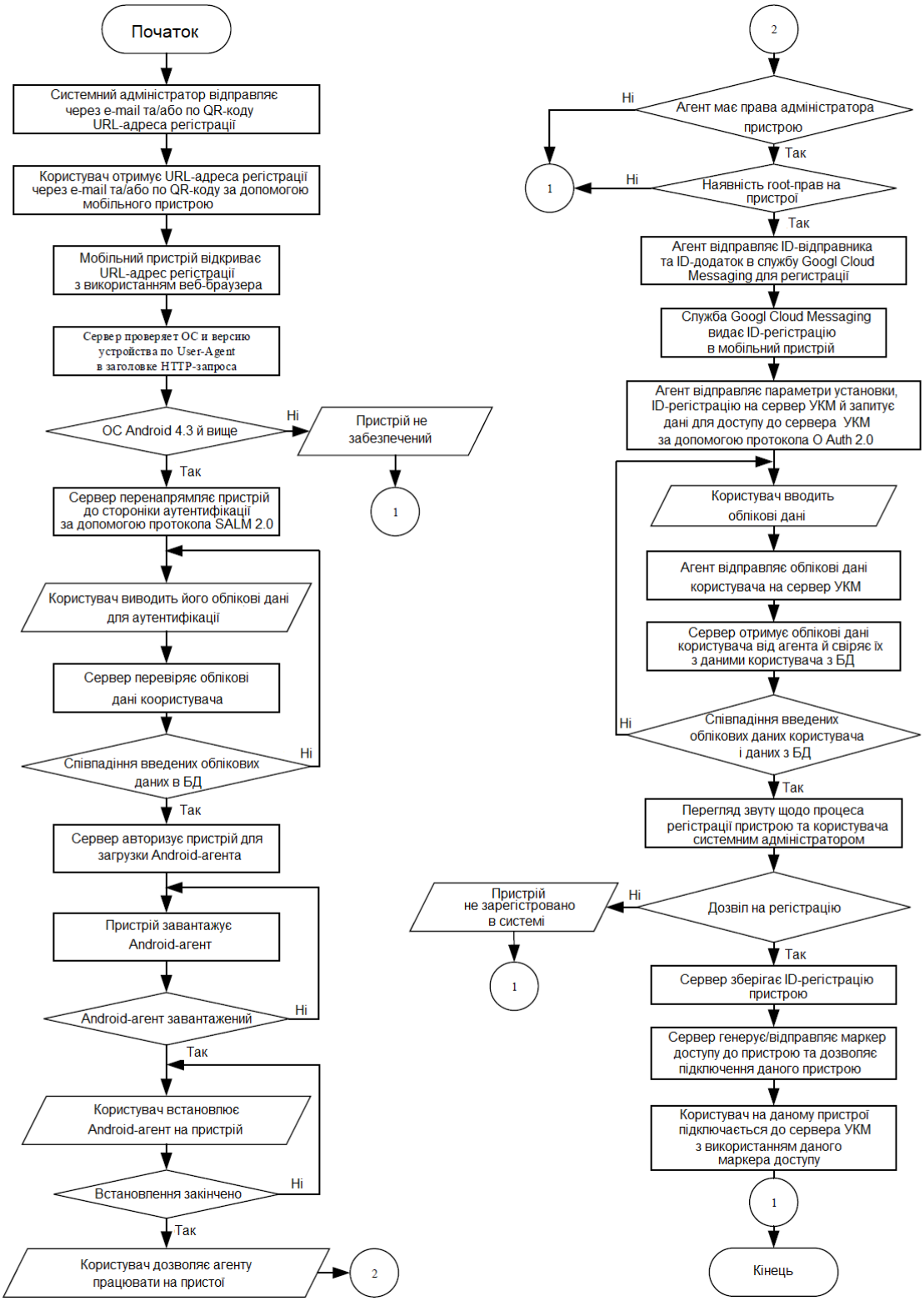

Рисунок 3.7 – Алгоритм безпечної віддаленої реєстрації Android - пристрою в системі УКМ

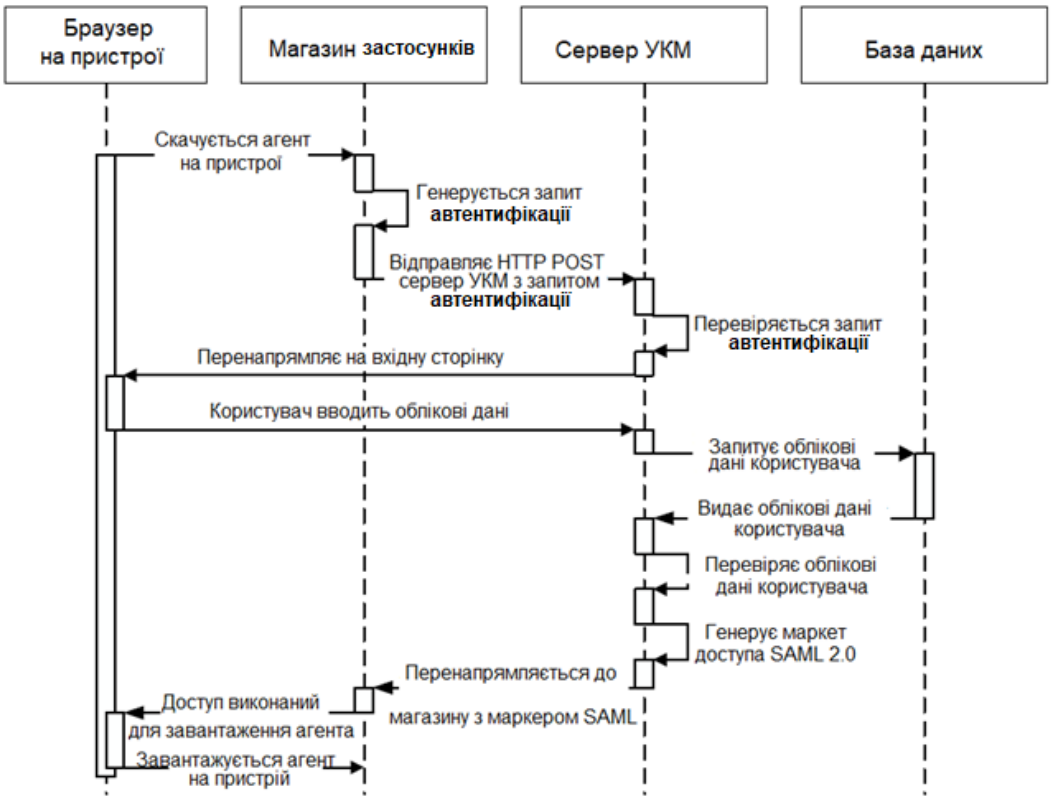

Рисунок 3.8 – Схема автентифікації пристрою за допомогою SAML

д) завантаження агента**:** після успішної автентифікації пристрій отримує інсталяційний файл агента з сервера;

е) установлення агента користувачем**:** користувач встановлює програмне забезпечення на свій мобільний пристрій;

є) реєстрація у системі**:** після інсталяції агент ініціює процедуру авторизації через OAuth-протокол та виконує реєстрацію пристрою на сервері, включаючи підключення до служби Push-сповіщень (GCM) (рисунок 3.9).

3.3.2 Процес автентифікації та авторизації пристрою і користувача

а) Автентифікація мобільного пристрою

Автентифікація пристрою здійснюється після запуску агентного програмного забезпечення на мобільному пристрої. Агент функціонує у

фоновому режимі, без прямої взаємодії з користувачем. Оскільки для ідентифікації пристрою використовуються Push-сповіщення, необхідно налаштувати мережеву інфраструктуру (зокрема, брандмауер) для забезпечення зв'язку з відповідними сервісами. Для пристроїв на платформі Android це означає відкриття портів 5228, 5229, 5230 для доступу до Google Cloud Messaging (GCM).

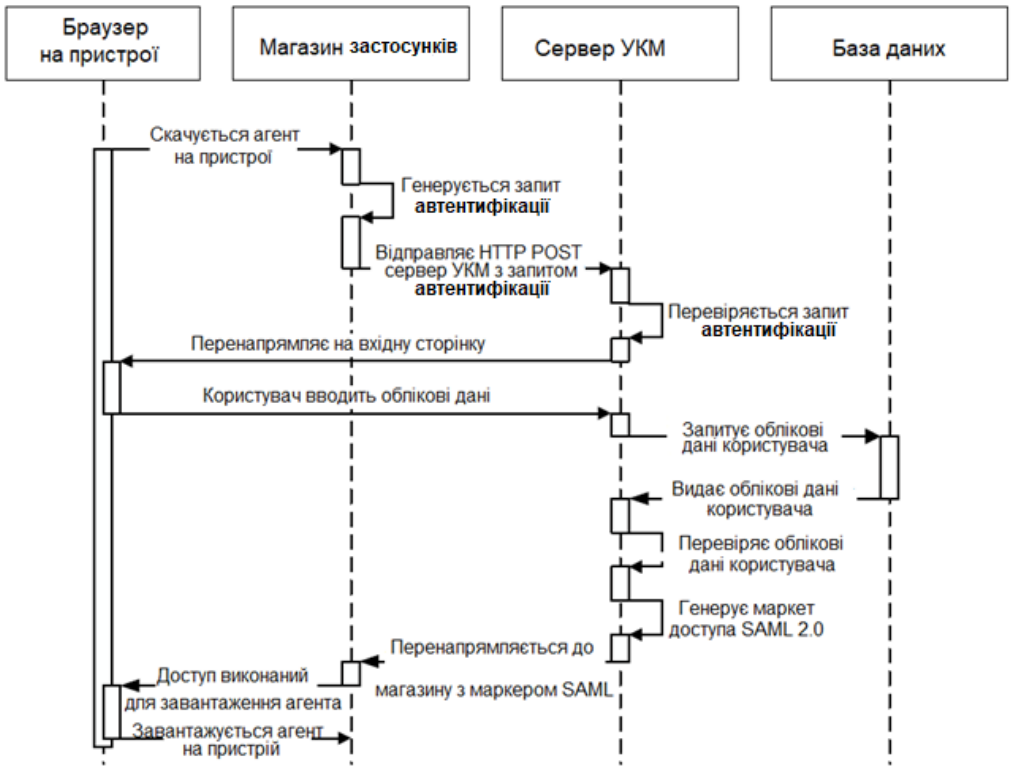

Рисунок 3.9 – Схема реєстрації пристрою на сервері та GCM

Алгоритм автентифікації пристрою включає наступні етапи:

1) користувач активує агент на мобільному пристрої (встановлений нативний застосунок);

2) агент виконує перевірку безпекових параметрів пристрою;

3) здійснюється перевірка доступу до служби Push-сповіщень;

4) агент ініціює запит на підключення до сервера УКМ;

5) сервер отримує ідентифікатор реєстрації (ID) та мітку часу доступу;

6) сервер звертається до бази даних для перевірки наявності відповідного ID-пристрою;

7) база даних повертає ідентифікатор, якщо такий вже зареєстрований;

8) після успішного порівняння ID з бази та агента, сервер підтверджує існування пристрою та приймає запит на підключення;

9) сервер генерує ID-доступу на основі хешування (SHA-256) ID-реєстрації та часу доступу, і надсилає запит до агента;

10) агент очікує отримання ID-доступу через Push-сповіщення;

11) сервер передає згенерований ID-доступ до служби Push-сповіщень разом з відповідним ID-реєстрації;

12) служба Push-сповіщень ідентифікує агент за ID-застосунку, витягує ID-доступ та пересилає його на мобільний пристрій;

13) пристрій приймає повідомлення з ID-доступом, витягує його та передає агенту;

14) агент надсилає ID-доступ безпосередньо на сервер для верифікації;

15) сервер виконує порівняння отриманого ID-доступу з раніше згенерованим. Якщо значення співпадають – підтверджується автентичність пристрою;

16) сервер формалізує встановлення безпечного з'єднання з мобільним пристроєм.

У цій фазі (рисунок 3.10) ідентифікатор доступу генерується шляхом хешування ID-реєстрації пристрою та часу доступу з використанням алгоритму SHA-256. Це забезпечує унікальність з'єднання між агентом та сервером і унеможливлює повторну ідентифікацію через підміну.

Завдяки довжині ID-доступу у 256 біт передача через Push-сповіщення є ефективною та захищеною від зовнішніх атак.

б) Автентифікація та авторизація користувача за протоколом OAuth

Після завершення процедури автентифікації пристрою необхідно

провести автентифікацію користувача для надання прав доступу до ресурсів системи. Дана процедура реалізується відповідно до стандарту OAuth**.**

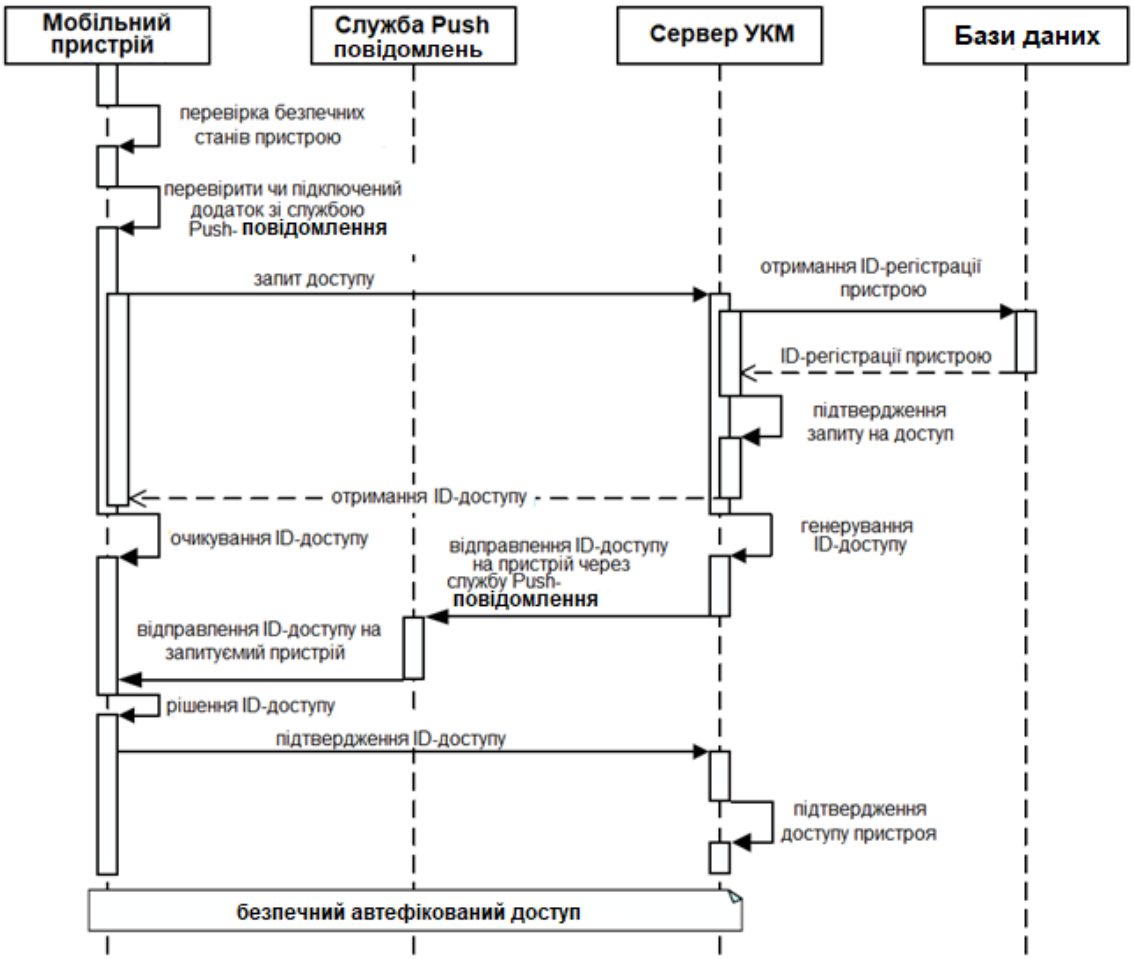

Рисунок 3.10 – Автентифікація пристрою

Послідовність дій наступна.

Агент на пристрої ініціює інтерфейс входу (Login) для введення облікових даних користувача.

Користувач вводить облікові дані.

Агент надсилає запит з обліковими даними на сервер УКМ.

Сервер зберігає отримані дані та формує запит до бази даних.

База даних повертає облікову інформацію, пов’язану з відповідним користувачем.

Сервер порівнює два набори даних (отримані від агента та бази даних).

У разі відповідності користувач вважається автентифікованим.

Після успішної автентифікації сервер генерує токен доступу (access token).

Токен надсилається агенту на пристрої.

Сервер підтверджує авторизований доступ користувача.

Агент зберігає налаштування, пов’язані із політикою безпеки, і встановлює адміністративні привілеї.

Пристрій використовує токен для взаємодії із системними ресурсами.

У фіналі пристрій реєструється в системі як авторизований, підтверджується справжність і правомірність доступу відповідно до встановленої політики безпеки.

Повна логіка цього етапу представлена на схемі (рисунок 3.11).

Рисунок 3.11 – Автентифікація та авторизація користувача

3.4 Обмін повідомленнями між сервером та мобільними пристроями за протоколом MQTT

Протокол MQTT (Message Queuing Telemetry Transport) було обрано

для реалізації комунікації між серверною інфраструктурою та мобільними агентами завдяки його низькому споживанню ресурсів та високій пропускній здатності порівняно з традиційним HTTP. Зважаючи на це, саме MQTT застосовується як основний механізм обміну повідомленнями в системі управління корпоративною мобільністю (УКМ).

Архітектура взаємодії між сервером і мобільними пристроями (рисунок 3.12) побудована на основі брокера MQTT, через якого агенти та сервери взаємодіють за допомогою спеціалізованого MQTT-адаптера. Цей адаптер виконує роль посередника між MQTT-повідомленнями та внутрішніми процесами корпоративної мережі, реалізуючи логіку запитів через HTTP-методи типу GET, POST, PUT і DELETE.

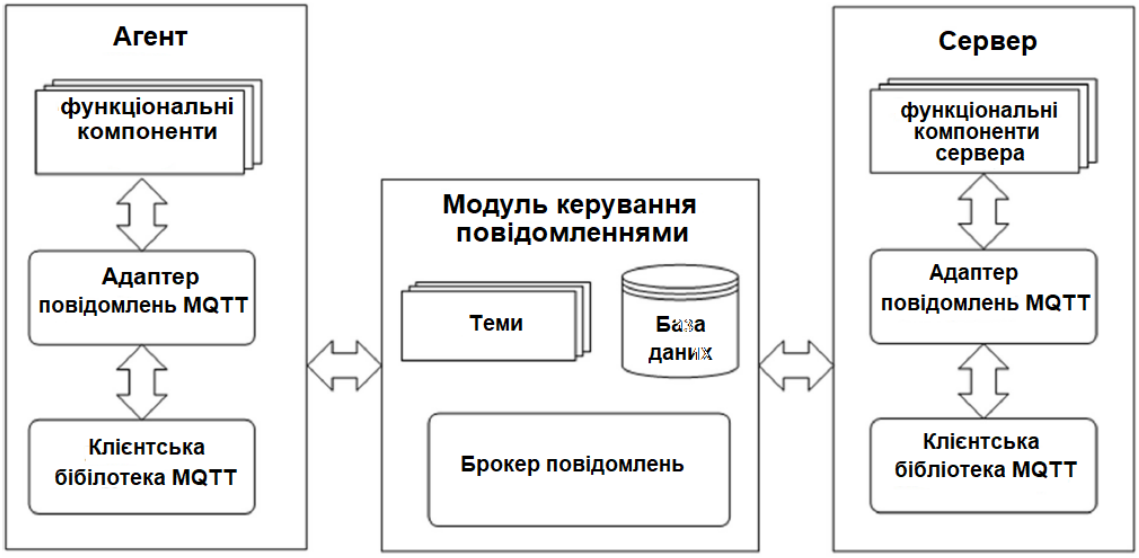

Рисунок 3.12 – Архітектурна схема модуля обміну повідомленнями з використанням MQTT

Ключові елементи архітектурної моделі та функціональні операції системи узагальнені (таблиці 3.1 – 3.2).

Зважаючи на публікаційно-підписний характер MQTT, для реалізації взаємодії у форматі запит/відповідь було запропоновано спеціалізовану структуру тем, що дозволяє моделювати класичний обмін.

Таблиця 3.1 – Основні розроблені операції в межах моделі

Інтерфейс	Операції
УМП	УМП управляє налаштуванням конфігурації пристроїв: надходження, розгортання, забезпечення безпеки моніторингу, інтеграції тощо на робочому місці
УМЗ	УМЗ фокусується на контролі доступу і адмініструванні корпоративного програмного забезпечення для кінцевих користувачів корпоративних та особистих мобільних пристроїв

Таблиця 3.2 – Основні структурні компоненти архітектури

Компонент	Опис
Брокер повідомлень	Брокер повідомлень розроблений у моделі та забезпечує повідомленнями, на яких пристрої/сервер публікують свої дані. Клієнти можуть також робити передплати. Коли корисні дані публікуються в брокері повідомлення на певну тему, дані доставляються клієнтам, підписаними до цієї теми
Клієнтська бібліотека MQTT	Для розробки моделі використана бібліотека Eclipse Paho, яка є класом клієнта з підтримкою MQTT та містить деякі допоміжні функції, що значно спрощують публікацію MQTT-повідомлень
Адаптер повідомлень MQTT	Агенти та сервер використовують адаптер MQTT, що дозволяє з'єднувати з брокером та переводити керуючі операції за допомогою протоколу MQTT
База даних	База даних MySQL призначена для зберігання даних повідомлень, виконаних операцій

Цей процес може бути описаний наступним кодом:

```
perl
mqtt/+/{corporation_name}/{deviceID}/{operationID}/#
```

де:

`mqtt/S/...` – канал для надсилання запитів;
`mqtt/R/...` – канал для отримання відповідей.

4 РЕКОМЕНДАЦІЇ ЩОДО ПРОЕКТУВАННЯ СИСТЕМИ УПРАВЛІННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ ПЕРСОНАЛУ НА ОСНОВІ ОС ANDROID

4.1 Основні алгоритмічні принципи управління мобільністю в Android-додатках

Для ефективного управління Android-додатками необхідно глибоко розуміти архітектурні принципи та ключові компоненти, що визначають функціонування застосунків у цій операційній системі. Android-додатки постачаються у вигляді архівного виконуваного файлу формату APK, який містить скомпільовані ресурси, код та мета-інформацію, що забезпечують цілісне функціонування програми.

У межах архітектури Android виділяють чотири основних типи компонентів, кожен із яких виконує визначену роль:

- активності (Activities): компоненти, що безпосередньо реалізують взаємодію з користувачем. Кожен екран програми зазвичай представлений окремою активністю. У випадку запуску нової активності, виконання попередніх тимчасово призупиняється, забезпечуючи фокусування на поточному інтерфейсі;

- службові компоненти (Services): Забезпечують виконання фонових операцій без необхідності взаємодії з інтерфейсом. Сервіси підтримують багатопоточну обробку та можуть надавати інтерфейси для віддалених викликів процедур (Remote Procedure Call, RPC), включаючи обробку зворотних викликів;

- приймачі широкомовних повідомлень (Broadcast Receivers): Реагують на системні або прикладні трансляції подій, таких як завершення завантаження файлів або надходження SMS. Додатки також можуть ініціювати власні трансляції в залежності від потреб;

- контент-провайдери (Content Providers): Використовуються для

організації доступу до структурованих даних, що можуть зберігатися у базах даних (наприклад, SQLite), файловій системі або в мережі. Доступ до контенту здійснюється через об'єкт ContentResolver**,** що дозволяє виконувати операції читання, запису, оновлення та видалення за допомогою відповідних методів (query(), insert(), update(), delete()). Контент-провайдери взаємодіють з іншими компонентами через URI, що унікально ідентифікує ресурси.

Опис конфігурації застосунку міститься у системному файлі AndroidManifest.xml**,** який відіграє ключову роль у процесі ініціалізації програми. Основна інформація, що міститься в маніфесті:

- унікальне ім’я пакета, яке слугує ідентифікатором додатку;
- перелік компонентів застосунку (активностей, сервісів, приймачів та провайдерів);
- опис дозволів (permissions), необхідних для роботи програми;
- вимоги до зовнішніх бібліотек та рівня API;
- умови запуску компонентів та їхній процес виконання.

Процедура інсталяції Android-застосунку реалізується за допомогою системного компонента PackageInstaller**,** який забезпечує інтерактивний інтерфейс для встановлення програм. Графічний інтерфейс цього процесу позначається як InstallAppProgress (рисунок 4.1).

Видалення застосунку реалізується аналогічно його встановленню, через ініціювання відповідного Intent з користувацького інтерфейсу пристрою. Для цього достатньо викликати цей код:

```
Uri packageURI = Uri.parse("package:"+packageName);
Intent intent = new Intent(Intent.ACTION_DELETE, packageURI);
startActivity(intent);
```

Для перевірки наявності оновлень мобільного додатку використовується Package Manager, який зберігає мета-інформацію про встановлені пакети у системних файлах, розташованих за шляхом /data/system/:

а) packages.xml – містить інформацію про дозволи та зареєстровані пакети;

б) packages.list – включає дані про ідентифікатор користувача, ім’я пакета, прапори й каталоги;

в) packages-stopped.xml – відображає статуси застосунків, зокрема позначення зупинених пакетів, які не мають права приймати трансляції.

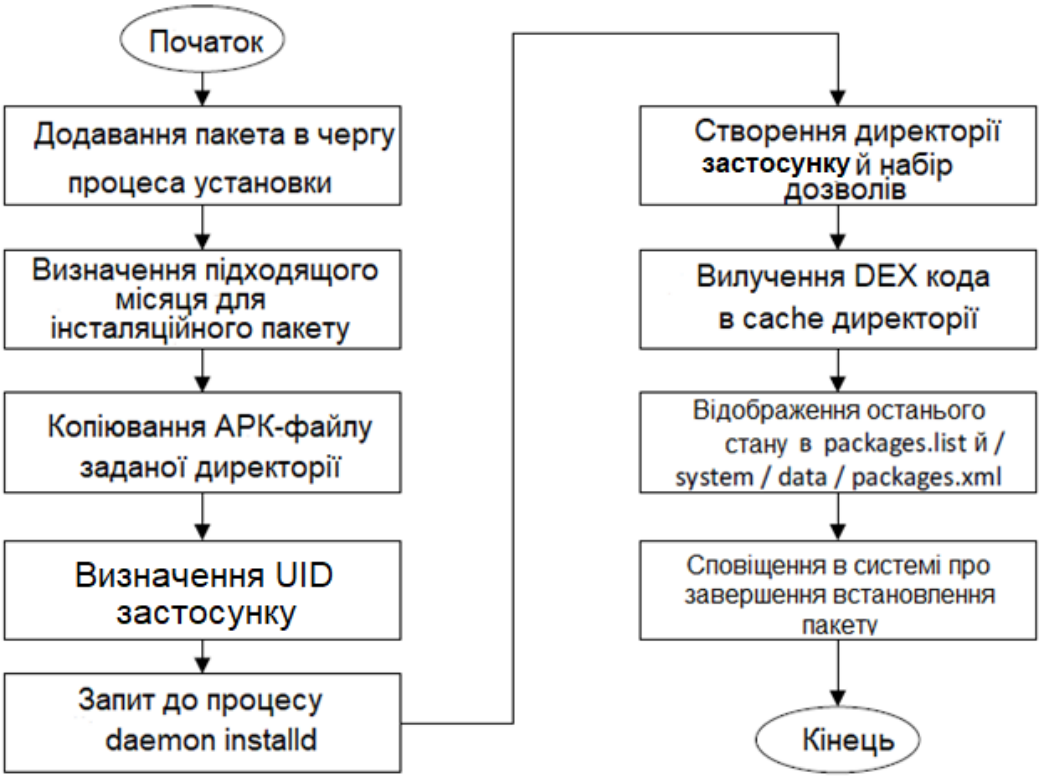

Рисунок 4.1 – Етапи встановлення програмного забезпечення на Android-пристрої

Оновлення застосунку передбачає попередню перевірку встановленої версії та у разі виявлення новішої – повторне встановлення пакета, внаслідок чого застосунок оновлюється.

4.2 Архітектура системи управління корпоративною мобільністю

Узагальнена структура системи управління корпоративною мобільністю (УКМ) представлена (рисунок 4.2). Для чіткого визначення

ключових компонентів системи, а також встановлення взаємозв'язків між ними, було проведено структурно-функціональний аналіз.

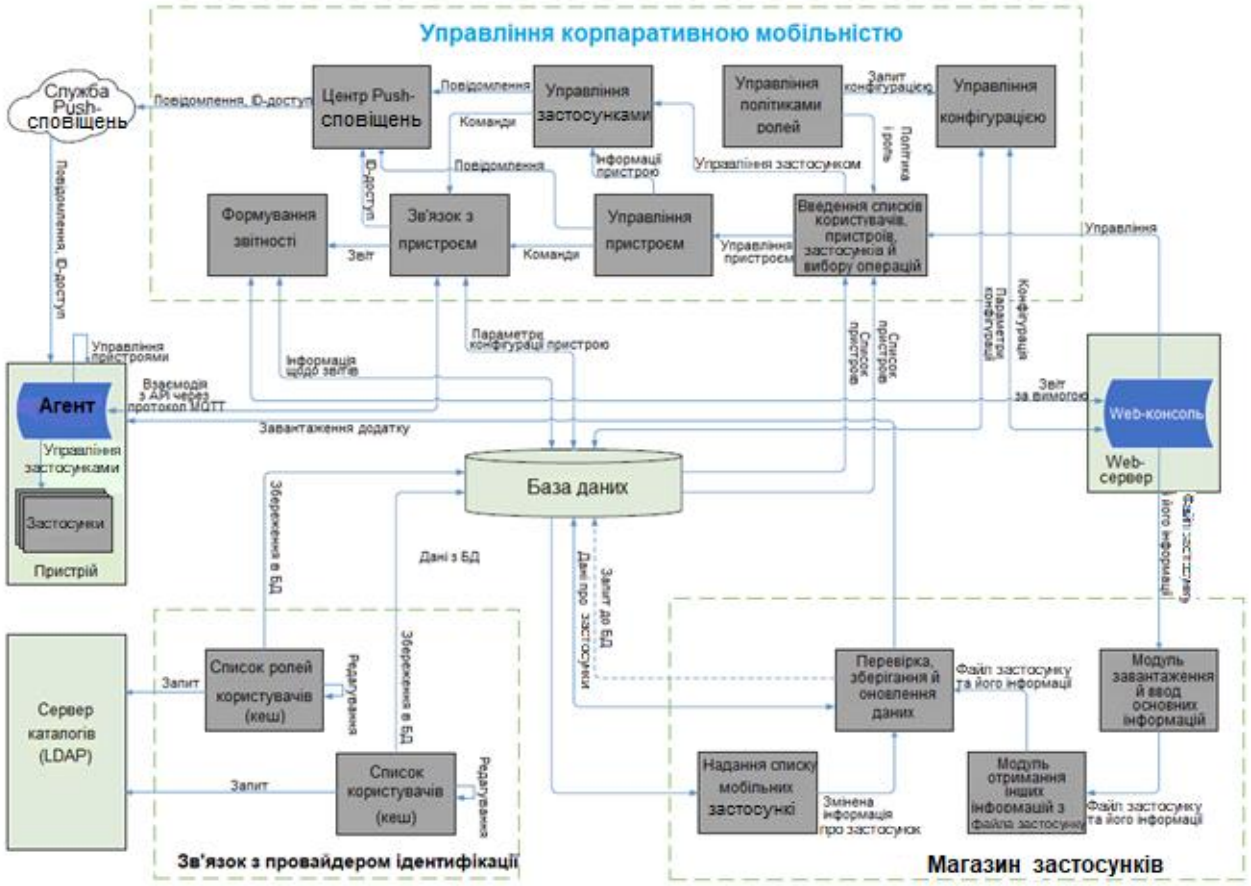

Рисунок 4.2 – Структура архітектури системи управління корпоративною мобільністю

У результаті встановлено, що система УКМ включає такі основні складові:

а) підсистема управління корпоративною мобільністю. Цей компонент охоплює ряд функціональних модулів, кожен з яких відповідає за певні аспекти керування:

- модуль управління пристроями та контентом – реалізує адміністрування мобільних пристроїв та супровідного інформаційного контенту.

- модуль керування застосунками – забезпечує централізоване

управління мобільним програмним забезпеченням, зокрема: встановлення, оновлення, видалення програм, перегляд списку інстальованих застосунків на пристрої, віддалене адміністрування версій.

- модуль управління політиками та ролями – відповідає за налаштування політик безпеки, а також розподіл ролей між користувачами, пристроями та застосунками.

- модуль конфігурації – виконує функції налаштування системних параметрів, забезпечуючи централізоване управління конфігурацією системи.

- модуль звітності – дозволяє створювати та обробляти звіти щодо здійснених дій у системі.

- модуль зв’язку з пристроями – забезпечує безпосередню взаємодію із встановленими на пристроях агентами.

- модуль Push-сповіщень – виконує функції розсилки сповіщень на мобільні пристрої користувачів. Повідомлення можуть відображатися як у центрі сповіщень, так і в рядку стану пристрою.

- модуль ведення обліку користувачів, пристроїв і застосунків – надає засоби для перегляду зареєстрованих об'єктів системи, формування операційних звітів та вибору дій адміністрування.

б) корпоративний магазин застосунків;

Призначений для централізованого зберігання, перегляду та розповсюдження корпоративних застосунків. Забезпечує зручний доступ до каталогів програмного забезпечення та його самостійне встановлення користувачами. Після вибору застосунку та цільового пристрою система автоматично розгортає програму через бездротове з'єднання.

в) служба Push-сповіщень;

Відповідає за оперативну передачу контекстної інформації або важливих системних оновлень на мобільні пристрої. Застосовується для ініціювання критично важливих подій, що вимагають миттєвої реакції пристроїв.

г) мобільний агент;

Це програмний компонент, інстальований на мобільному пристрої, який здійснює комунікацію з серверною частиною системи УКМ. Обмін даними між агентом і сервером відбувається через захищений бездротовий канал, незалежно від фізичного розташування пристрою чи типу мережевого з'єднання.

д) підсистема зв’язку з провайдером ідентифікації;

Здійснює інтеграцію з корпоративною службою каталогів. Виконує аутентифікацію, зберігає дані про користувачів та їх ролі у вигляді кешу, оптимізуючи доступ до сервісів системи.

е) база даних системи УКМ;

Централізоване сховище інформації, яке містить структуровані дані про користувачів, ролі, пристрої та інші системні об'єкти, необхідні для функціонування УКМ.

є) веб-консоль адміністратора;

Інтерфейс управління, призначений для адміністраторів системи. Надає повний набір інструментів для моніторингу, налаштування та керування всіма компонентами системи УКМ.

4.3 Вимоги до системи управління корпоративною мобільністю

Система управління корпоративною мобільністю (УКМ) повинна відповідати низці ключових вимог, що забезпечують її функціональність, безпеку та зручність використання. Основні вимоги до системи включають:

- реєстрація та авторизація користувачів**:** для отримання доступу до функціоналу системи, користувач (адміністратор або звичайний користувач) повинен встановити агентське програмне забезпечення на свій пристрій та пройти процедуру авторизації;
- адміністрування користувачів**:** система повинна надавати можливість адміністратору додавати нових користувачів, редагувати їх облікові дані

(логін, пароль тощо) та керувати правами доступу;

- керування корпоративним магазином застосунків: повинна бути реалізована можливість адміністрування каталогу застосунків – додавання, редагування, видалення програмного забезпечення, зберігання відповідних метаданих;

- управління мобільними застосунками на пристроях**:** система повинна забезпечити функціонал для перегляду встановлених застосунків, перевірки їх версій, віддаленого оновлення, встановлення та видалення;

- забезпечення інформаційної безпеки**:** усі операції повинні проходити з перевіркою прав доступу користувача, використовуючи надійні механізми авторизації та шифрування даних.

Відповідно до зазначених вимог, була сформована функціональна структура системи, яка включає наступні основні компоненти:

- модуль управління користувачами та пристроями**:** забезпечує додавання нових користувачів, авторизацію пристроїв, керування персональними обліковими та технічними даними;

- корпоративний магазин застосунків**:** реалізує механізми додавання, редагування та видалення застосунків, обробку інформації, отриманої з APK-файлів;

- модуль керування мобільними застосунками**:** дозволяє проводити віддалене встановлення застосунків, переглядати перелік інстальованого ПЗ, здійснювати їх деінсталяцію та генерувати звіти про виконані дії.

На рисунках 4.3 та 4.4 наведено загальну функціональну архітектуру системи УКМ та типовий сценарій її використання в рамках корпоративного середовища. Після запуску системи користувачу відкривається сторінка авторизації, де необхідно ввести облікові дані (логін та пароль) для входу в систему. Успішна авторизація відкриває доступ до панелі керування, яка відображає функціональні можливості відповідно до ролі користувача. Для адміністратора, зокрема, передбачено додаткові розділи: Users, Add User, Upload App (рисунок 4.5).

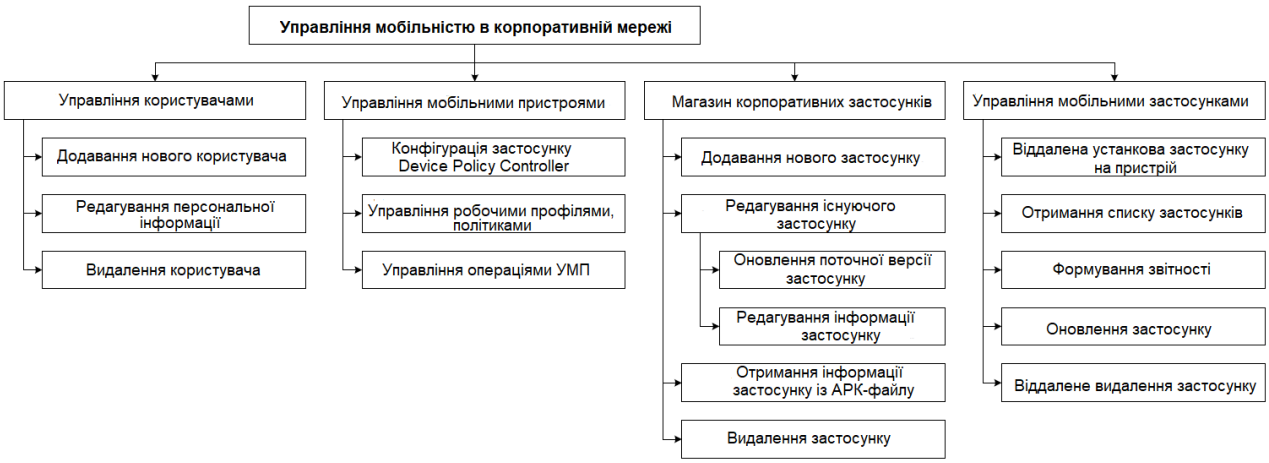

Рисунок 4.3 – Функціональна структура системи УКМ

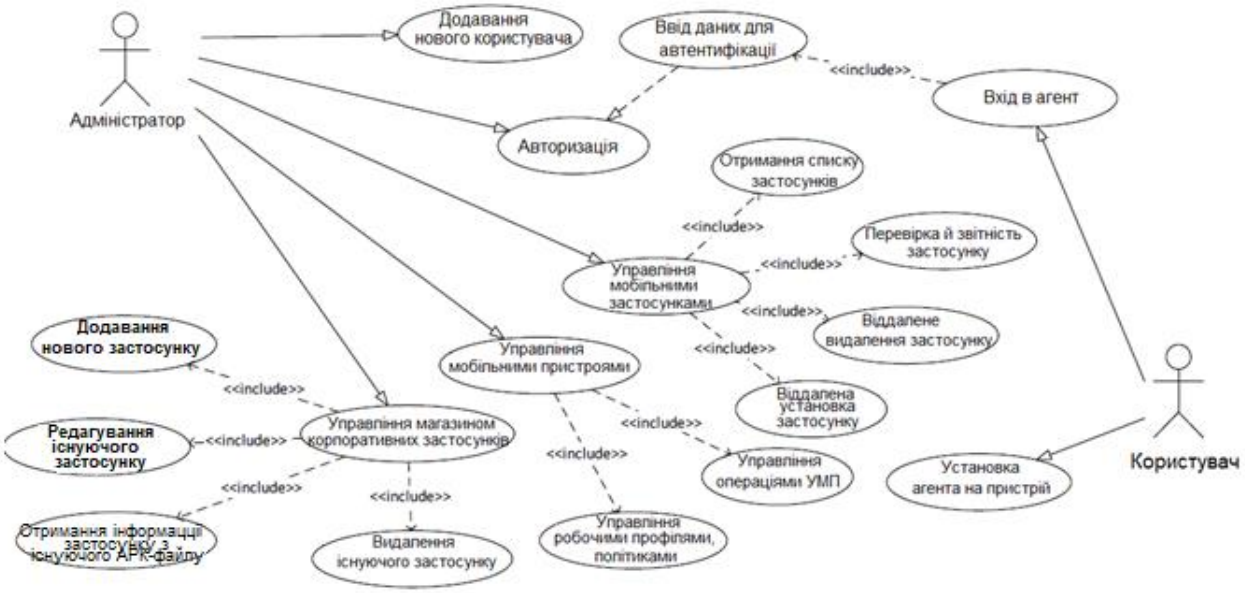

Рисунок 4.4 – Типовий сценарій функціонування системи УКМ

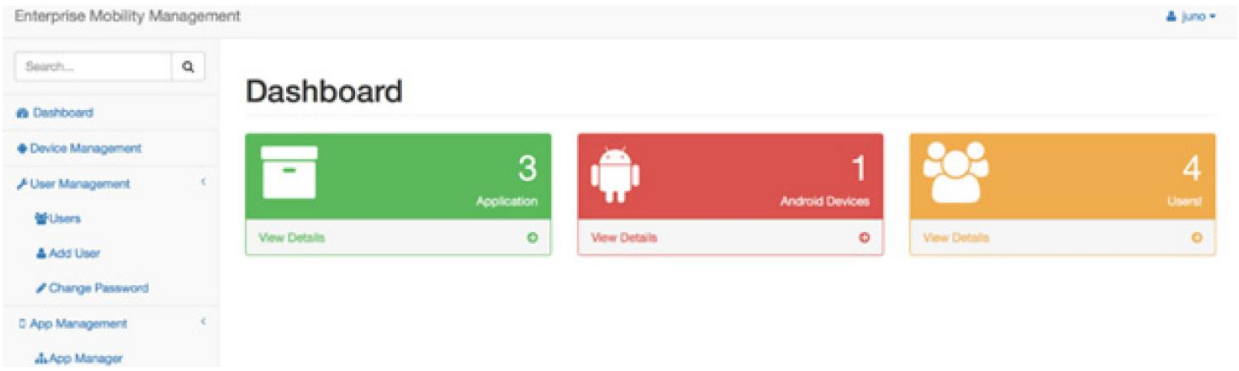

Рисунок 4.5 – Інтерфейс «Панель керування»

Управління обліковими записами користувачів здійснюється через відповідні елементи інтерфейсу: для додавання, редагування або видалення даних необхідно заповнити відповідні форми. Інтерфейси керування наведено на рисунках 4.6 – 4.8.

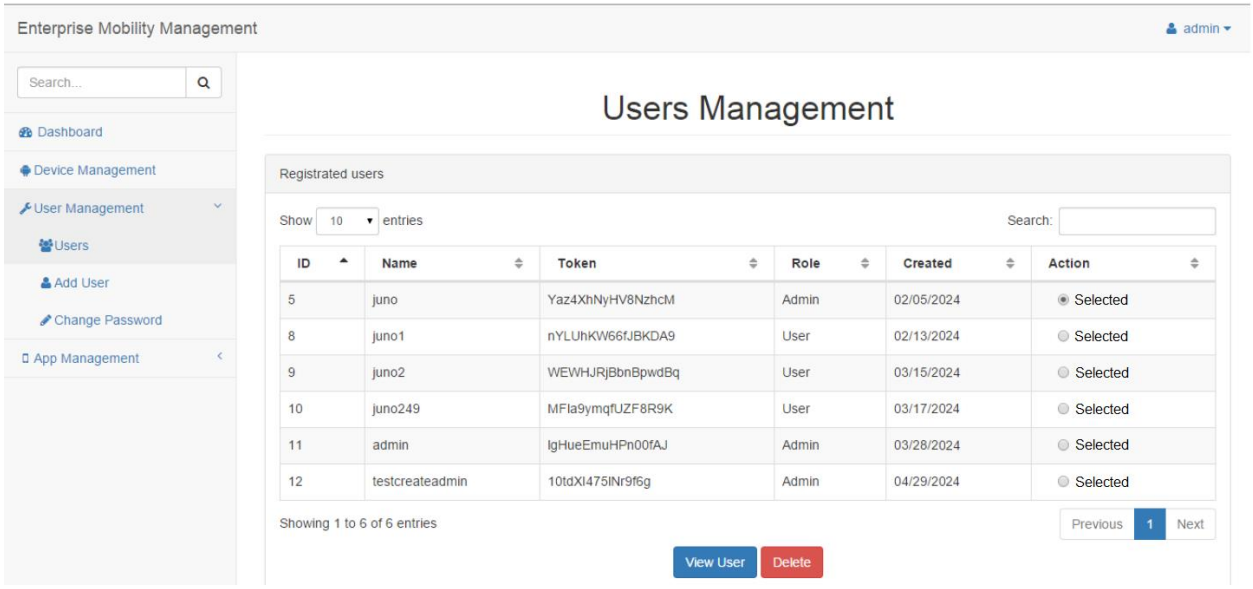

Рисунок 4.6 – Сторінка «Керування користувачами»

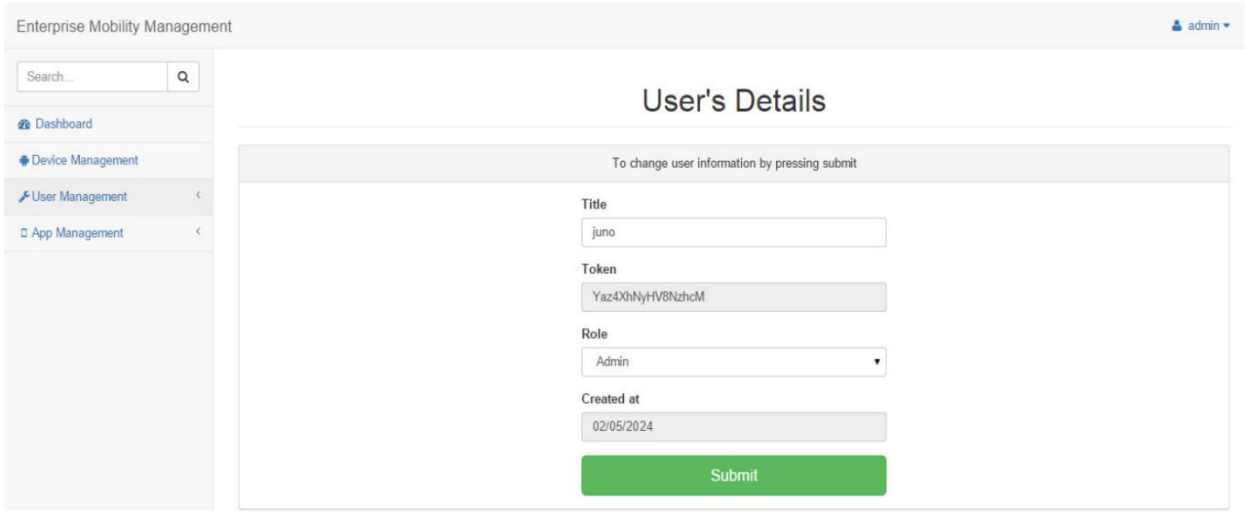

Рисунок 4.7 – Сторінка «Перегляд інформації про користувача»

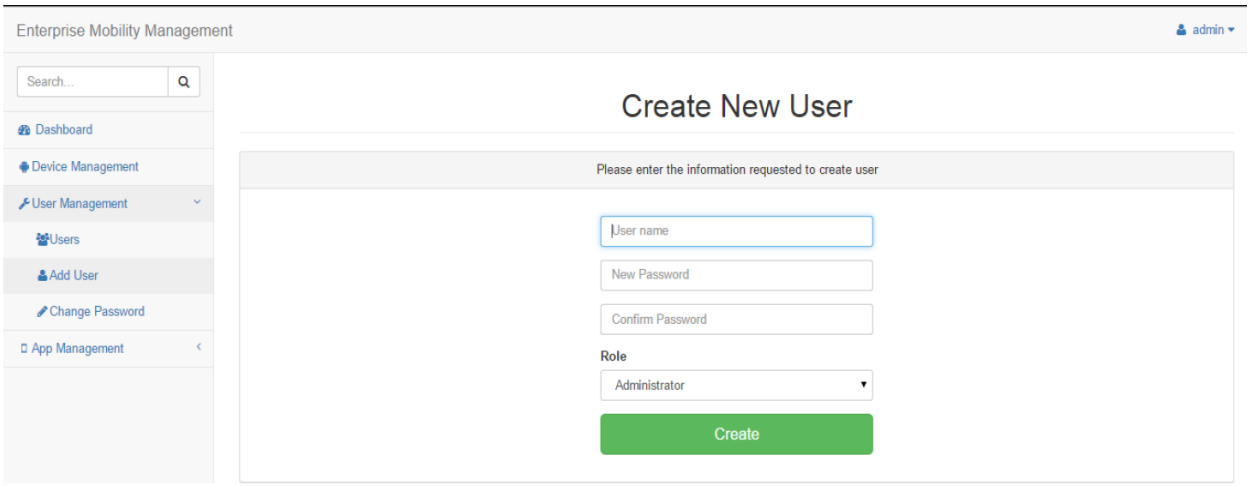

Рисунок 4.8 – Сторінка «Додавання нового користувача»

Для завантаження нового застосунку до системи використовується кнопка Upload New App**.** Після вибору файлу та заповнення необхідних відомостей, потрібно натиснути кнопку Submit для підтвердження дії (рисунок 4.9).

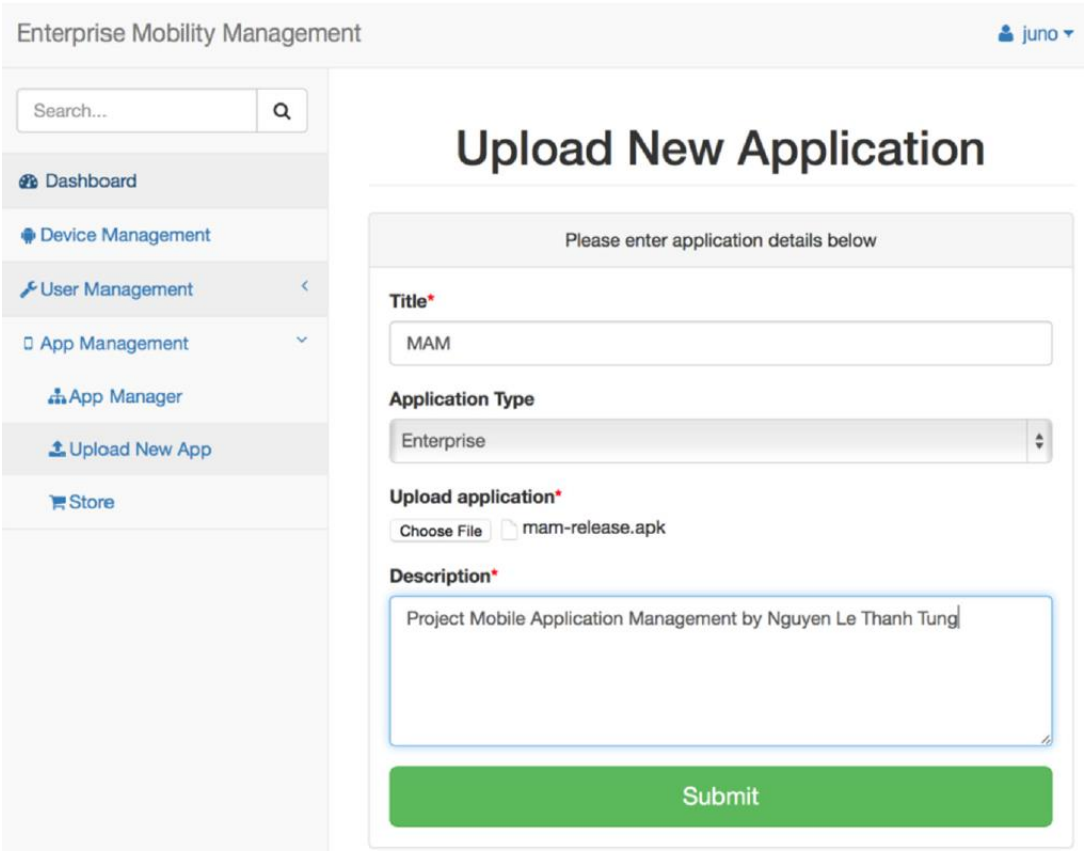

Рисунок 4.9 – Сторінка «Завантаження нового застосунку»

У разі успішного завантаження, користувачу відкривається доступ до переліку наявних програм у магазині корпоративних застосунків (рисунок 4.10). Тут можна переглядати, оновлювати або видаляти наявні застосунки, а також додавати нові (рисунок 4.11).

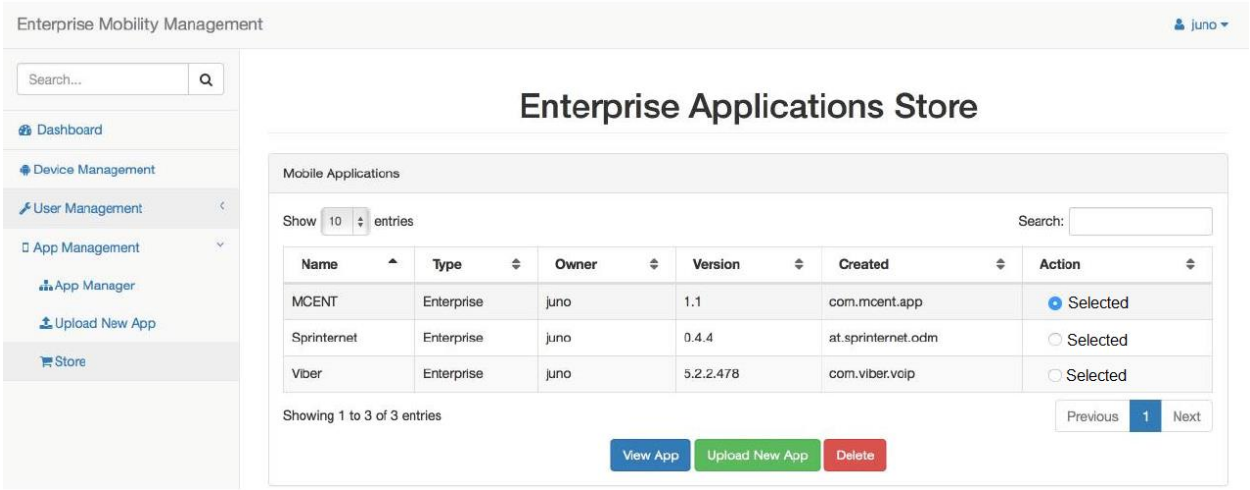

Рисунок 4.10 – Сторінка «Магазин корпоративних застосунків»

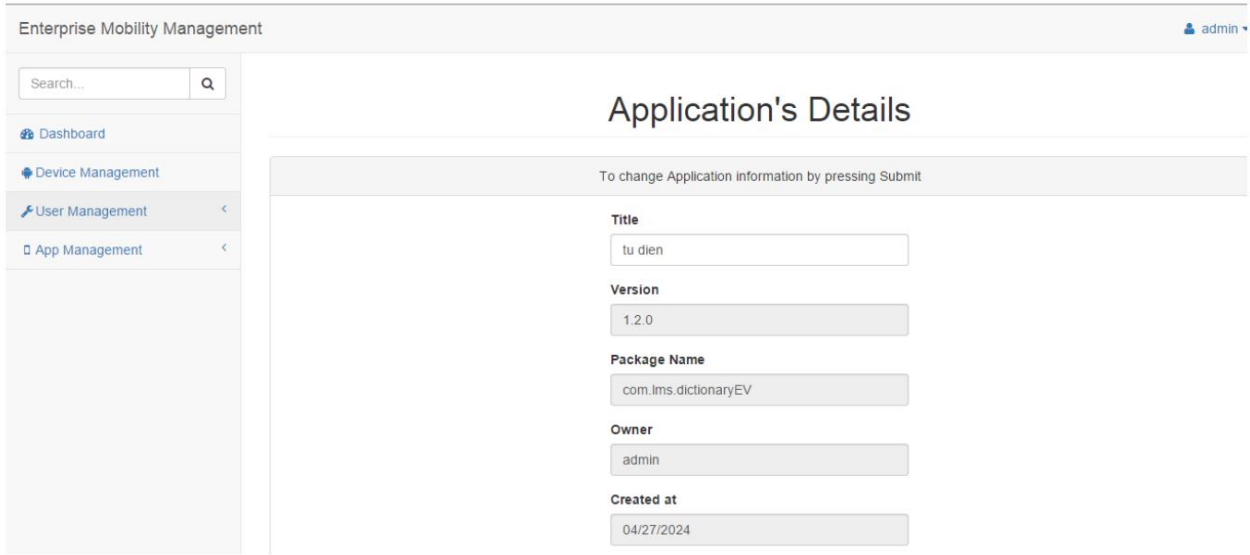

Рисунок 4.11 – Сторінка «Перегляд інформації про застосунок»

Для адміністрування зареєстрованих пристроїв передбачено спеціальний інтерфейс, що дозволяє переглядати, змінювати або видаляти інформацію про них (рисунок 4.12).

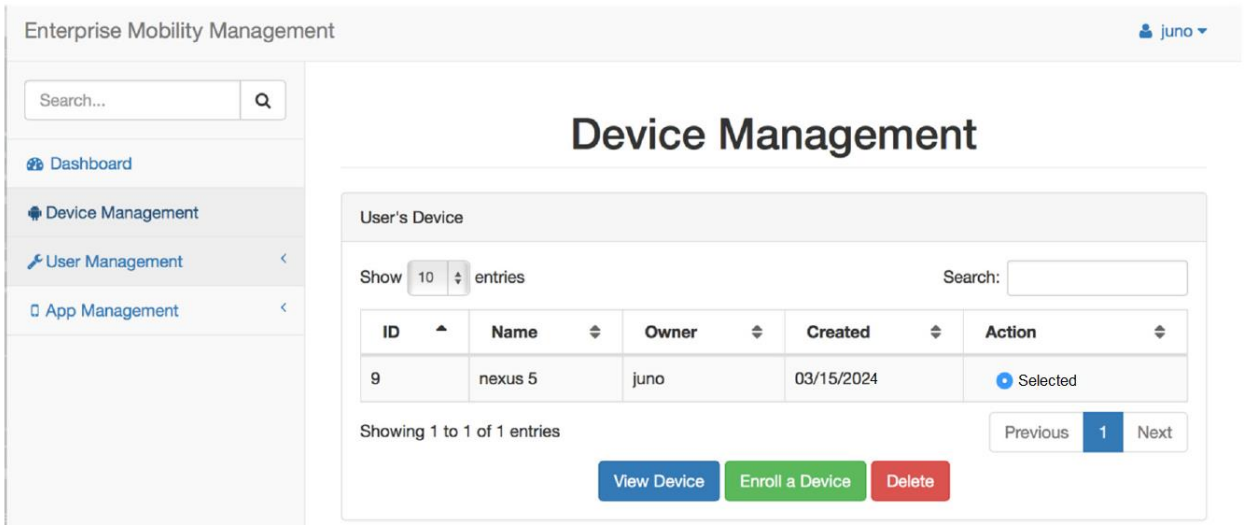

Рисунок 4.12 – Сторінка «Керування пристроями»

Головна сторінка інтерфейсу системи орієнтована на керування корпоративними застосунками. Вона дозволяє користувачам переглядати перелік програм, виконувати операції (встановлення, оновлення, видалення, генерація звітів) та керувати процесами встановлення на обрані пристрої. Для виконання конкретної дії необхідно обрати програму, пристрій та натиснути кнопку Submit (рисунок 4.13).

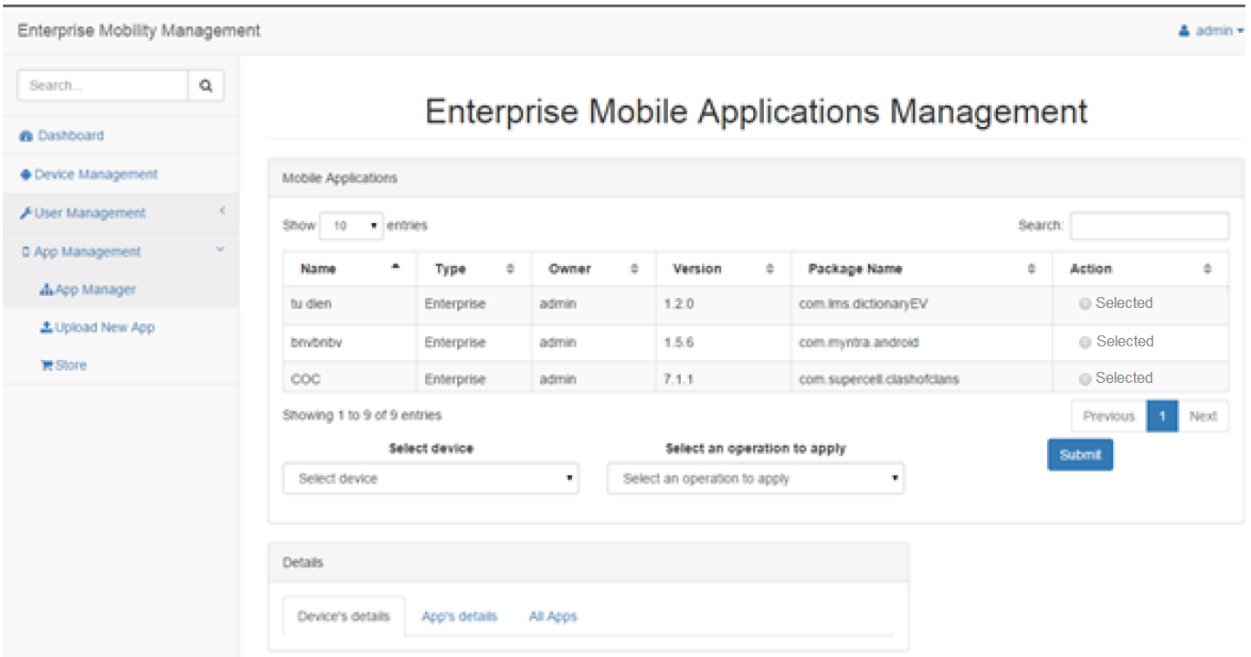

Рисунок 4.13 – Сторінка «Керування корпоративними застосунками»

4.4 Опис клієнтської частини системи

Клієнтський компонент системи управління корпоративною мобільністю (УКМ), призначений для користувачів мобільних пристроїв, реалізовано під операційну систему Android із використанням інтегрованого середовища розробки Android Studio**.**

Для початку роботи з клієнтською частиною застосунку необхідно пройти процедуру первинної реєстрації, яка передбачає введення ідентифікаційних даних. До обов'язкових полів належать: назва пристрою**,** адреса сервера (URL)**,** а також облікові дані користувача (логін і пароль). Приклад інтерфейсу реєстраційної форми наведено на рисунку 4.14.

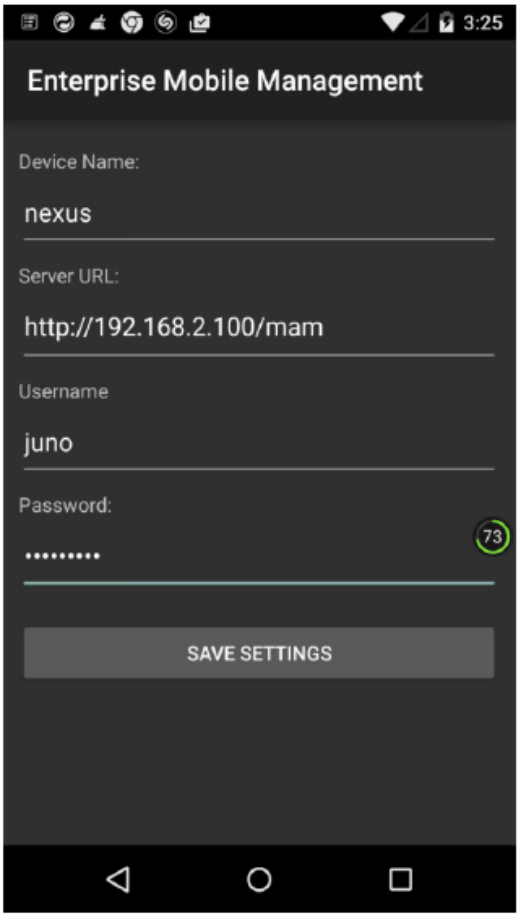

Рисунок 4.14 – Форма реєстрації користувача

Вся введена під час реєстрації інформація зберігається у

централізованій базі даних, реалізованій на платформі MySQL, яка використовується серверною частиною системи для автентифікації користувача, а також для забезпечення взаємодії з механізмами надсилання сповіщень.

Після успішного завершення реєстраційного процесу, користувачу надається доступ до функціоналу керування корпоративними мобільними застосунками, зокрема:

- розповсюдження програмного забезпечення на мобільні пристрої;
- оновлення існуючих застосунків;
- віддалене видалення застосунків;
- перегляд переліку встановленого програмного забезпечення;
- перевірка актуальності версій застосунків.

Таким чином, клієнтська частина є важливою складовою системи УКМ, яка забезпечує інтерактивну взаємодію користувача з інфраструктурою корпоративного мобільного середовища.

4.5 Оцінювання якості мобільного доступу

Для аналізу якості мобільного доступу використано три критерії якості (табл. 4.1):

- продуктивність служб Push-сповіщень;
- навантаження сервера при підключенні пристроїв;
- якість сервісу.

В рамках експериментального дослідження було виконано серію тестів, спрямованих на визначення параметрів продуктивності служби Push-сповіщень, а також на вимірювання навантаження на сервер у випадках підключення пристроїв із показниками QoS, рівними 1 або 2.

Таблиця 4.1 – Критерії оцінки якості мобільного доступу

Рівень	Опис
QoS=0 - максимум одноразова доставка	публікатор виконує одноразове надсилання повідомлення, але не робить кроки
QoS=1 - мінімум одноразова доставка	доставка повідомлення перевіряється, однак дозволяється доставляти його більше ніж один раз
QoS = 2 - одноразова доставка	доставка повідомлення гарантується лише один раз

Мета тестування:

- push-сповіщення**:** встановити величину затримки між моментом формування повідомлення на сервері та його доставкою на цільові мобільні пристрої;

- навантаження серверу**:** оцінити здатність серверної частини системи обробляти масові підключення мобільних клієнтів із паралельним обміном інформацією.

Кожне повідомлення Push-сповіщення містить JSON-структуру, яка включає унікальний індекс повідомлення та серверну часову мітку, що фіксує час його створення. Клієнтські додатки для приймання повідомлень реалізовано для операційних систем Android, iOS та Windows Phone. Після отримання повідомлення, мобільний пристрій витягує корисні дані з JSON-об’єкта та передає їх до SQL-бази даних разом із власною тимчасовою міткою отримання.

Для забезпечення об’єктивності тестування всі повідомлення мали однаковий розмір у 254 байти, що є мінімальним допустимим значенням для усіх протестованих платформ, що дозволяє виключити вплив транспортного шару на результати.

Методика тестування:

Повідомлення надсилалися з інтервалом в одну секунду протягом 15 секунд (серія з 15 повідомлень), після чого слідувала 30-хвилинна пауза, та

повторювалася ще одна аналогічна серія. Цикл повторювався протягом 8 годин, у результаті чого було передано 240 повідомлень. Частота надсилання повідомлень вибиралася таким чином, щоб мінімізувати ризики, пов’язані з виявленням зловмисних дій (наприклад, атаки типу «відмова в обслуговуванні»), а також забезпечити справедливі умови перевірки стабільності служби повідомлень при різних рівнях навантаження.

Крім того, тестування здійснювалося у різні періоди доби з метою врахування змін навантаження на мережу та серверні ресурси.

Результати проведеного дослідження зображено на рисунку 4.15, де наведено порівняльну характеристику швидкості доставки повідомлень у різних системах Push-сповіщень, зокрема Google Cloud Messaging (GCM), Apple Push Notification Service (APNS) та Microsoft Push Notification Service (MPNS).

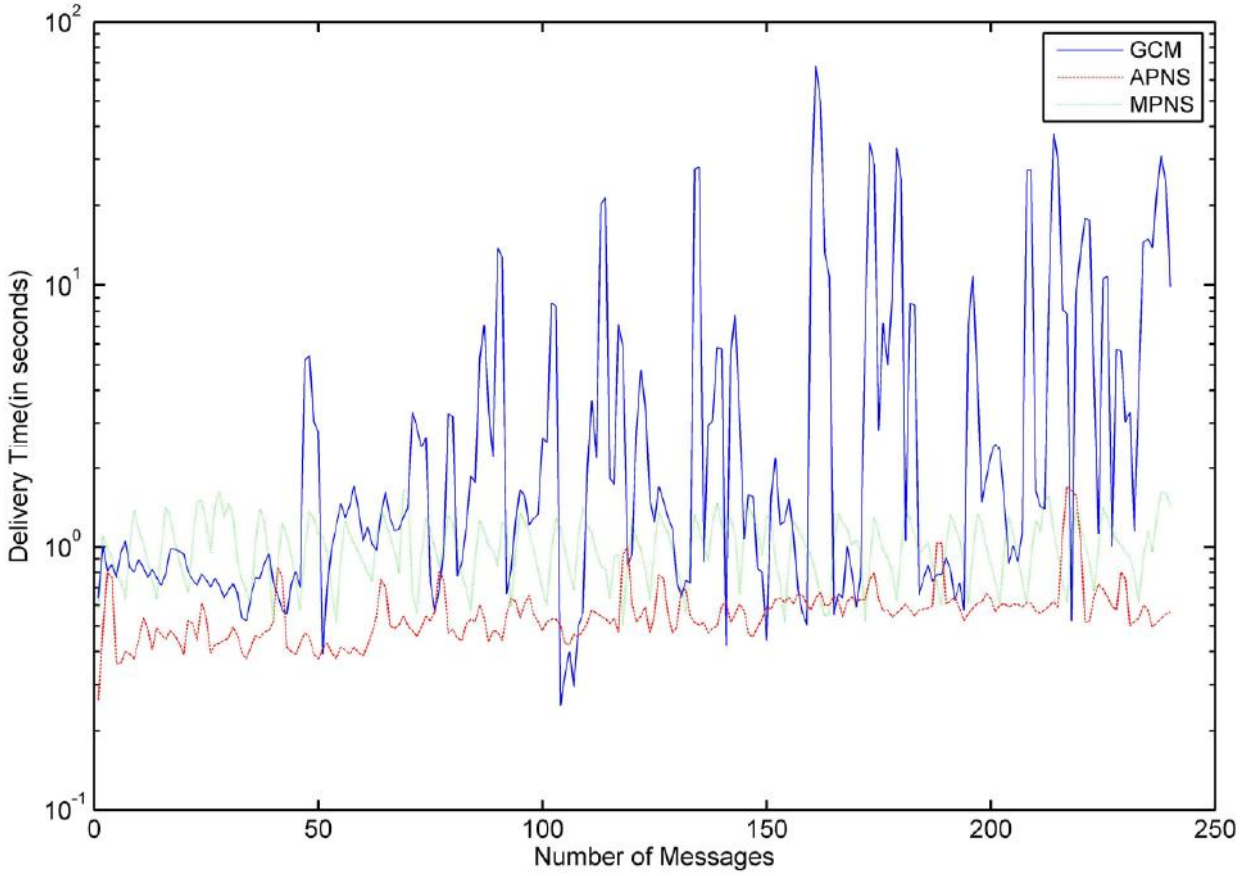

Рисунок 4.15 – Порівняльний аналіз швидкості доставки повідомлень у різних службах Push-сповіщень

Таким чином, результати проведеного тестування засвідчили наступне:

- сервіс Google Cloud Messaging (GCM) продемонстрував найменшу надійність у режимі реального часу. Середній час доставки повідомлень становив близько 4,83 секунди, медіанне значення – 0,99 с, а стандартне відхилення – 11,22. Аналіз графіка розподілу швидкості доставки свідчить про зниження якості сервісу з плином часу та збільшенням кількості повідомлень. Крім того, доставка повідомлень здійснюється без дотримання порядку їх відправлення;

- apple Push Notification Service (APNS) виявився більш стабільним та надійним механізмом. Середній час доставки повідомлень становив 0,57 секунди, медіана – 0,54 с, стандартне відхилення – 0,20. У більшості випадків повідомлення доставляються у відповідному порядку, що свідчить про ефективний розподіл навантаження між серверами служби;

- microsoft Push Notification Service (MPNS) також демонструє непослідовну доставку повідомлень. Середній час – 1,01 секунди, медіана – 1,02 с, стандартне відхилення – 0,14. Порядок доставки повідомлень не гарантується.

У рамках дослідження навантаження серверної частини системи при підключенні великої кількості пристроїв було проведено вимірювання часу прийому та передачі запитів (round-trip time, RTT). Для цього використовувалися інструменти Wireshark, Tshark та TCPDump, що забезпечили моніторинг та аналіз мережевого трафіку. Було згенеровано 1000 імітованих пристроїв, кожен з яких виконували одну з чотирьох операцій – battery, ram, location або policy – із застосуванням базової аутентифікації (логін/пароль).

Кожен пристрій упродовж 15-хвилинного періоду обмінювався повідомленнями з сервером, використовуючи модель публікації/підписки з відповідними темами (deviceID та operationID). Передача здійснювалася у форматі JSON, обсягом від 256 байт до 1 кілобайта. Для забезпечення доставки повідомлень використовувався протокол MQTT із параметрами QoS

= 1 та QoS = 2. Кожен експеримент повторювався тричі, після чого обчислювалося середнє значення результатів. Підсумкові дані наведені (рисунок 4.16).

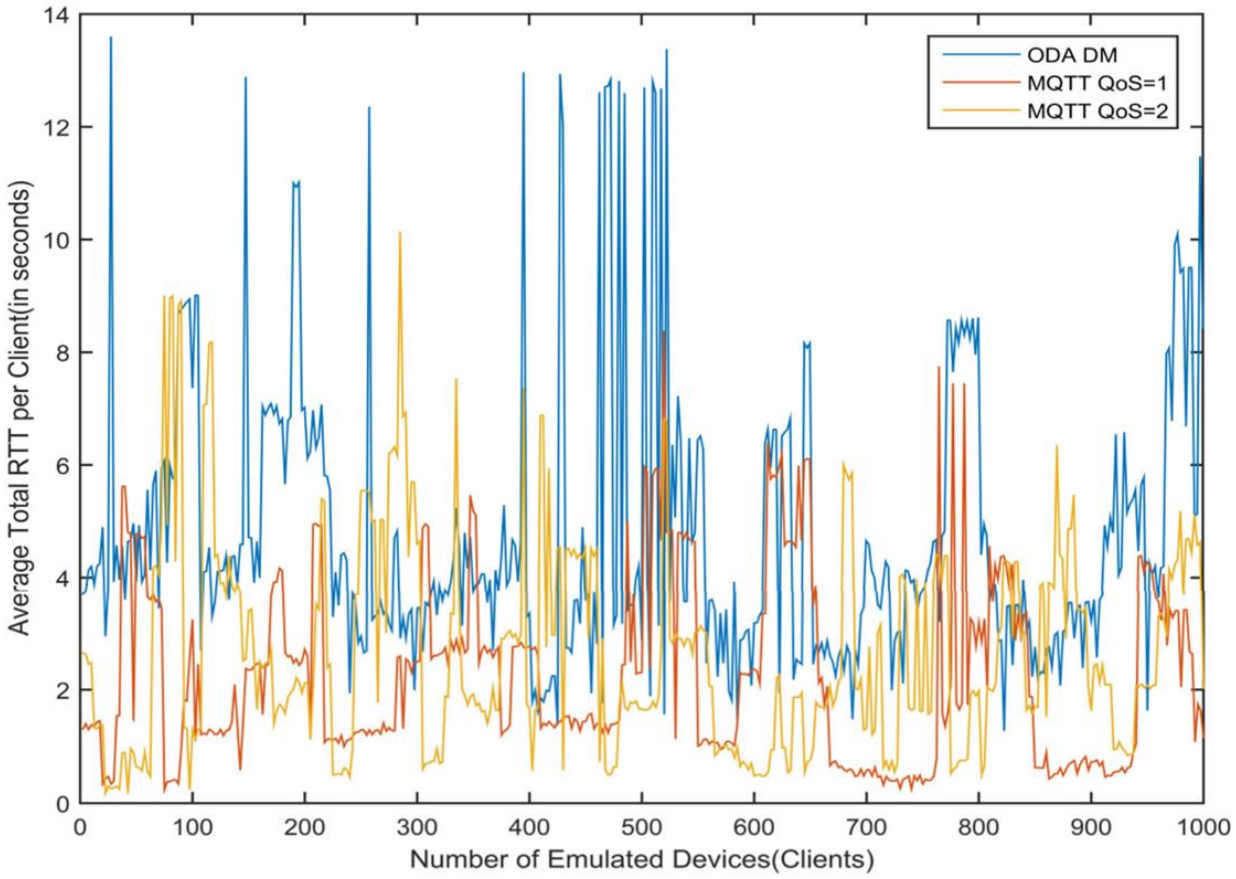

Рисунок 4.16 – Графік часу прийому-передачі запитів у різних протоколах

Аналіз отриманих результатів дозволяє зробити такі висновки:

- із збільшенням кількості активних пристроїв спостерігається зростання часу прийому-передачі запитів. Так, у системі SOTI MobileControl при використанні протоколу OMA DM цей показник зростає з 1,28 до 13,6 секунди, тоді як у розробленій системі із застосуванням MQTT значення для QoS=1 змінюється з 0,24 до 8,38 секунди, а для QoS=2 – з 0,17 до 10,14 секунди. Причиною цього є зростання кількості запитів, що створює додаткове навантаження на сервер і потребує більшого часу обслуговування клієнтських запитів;

- середній час обробки запитів за QoS=1 є меншим порівняно з QoS=2,

оскільки перший не передбачає повноцінного чотириетапного узгодження (four-way handshake), що значно спрощує процес взаємодії. Натомість QoS=2, хоча і гарантує високу надійність доставки, може суттєво впливати на серверну продуктивність при великій кількості запитів;

- загалом, розроблена система показала вищу ефективність: приблизно у 2,1 раза швидше для QoS=1 та у 1,8 раза швидше для QoS=2, порівняно з аналогічними платформами.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було розв’язано науково-технічну задачу підвищення ефективності управління мобільним доступом до корпоративних інформаційних ресурсів за рахунок удосконалення методів контролю пристроїв, управління мобільними застосунками та забезпечення інформаційної безпеки корпоративного контенту.

Основні результати дослідження можна сформулювати наступним чином:

а) проведено комплексне дослідження предметної області управління корпоративною мобільністю. Встановлено основні технології, функціональні вимоги та проблеми, які виникають під час адміністрування мобільних пристроїв у корпоративному середовищі. В результаті аналізу існуючих рішень було виокремлено ключові функції та базові компоненти архітектури систем УКМ;

б) розроблено масштабовану модель управління корпоративною мобільністю, що включає:

- концепцію контекстно-орієнтованого середовища функціонування системи;
- ресурсну модель керуючих операцій;
- модель масштабованої архітектури з використанням принципів декомпозиції простору управління відповідно до AKF Cube (взаємодія, ідентифікація, операція);
- визначення серверного архітектурного стилю REST та застосування моделі публікації/підписки (MQTT) для комунікації з пристроями;
- побудову ресурсно-орієнтованої архітектури системи УКМ.

в) розроблено методику реалізації функцій управління мобільністю, яка передбачає:

- обґрунтування вибору технології Push-сповіщень серед можливих

моделей комунікації;

- формування процесів взаємодії між сервером і клієнтами (реєстрація, автентифікація, авторизація, обмін повідомленнями);
- реалізацію механізмів управління пристроями в реальному часі.

г) розроблено алгоритм управління мобільними пристроями на базі операційної системи Android, що враховує особливості структури програмного забезпечення та надає можливості для централізованого адміністрування;

д) спроєктовано архітектуру програмної системи УКМ, реалізовану у вигляді клієнт-серверного рішення. Система охоплює компоненти для управління мобільними застосунками та пристроями, а також інтерфейс взаємодії з адміністратором через веб-консоль;

е) запропоновано методику оцінки ефективності мобільного доступу, що включає:

- тестування продуктивності служб Push-сповіщень;
- аналіз навантаження серверної частини при підключенні великої кількості пристроїв;
- використання QoS-рівнів (1 та 2) з метою підвищення достовірності результатів;

є) проведено практичне впровадження та експериментальне тестування системи управління корпоративною мобільністю. На підставі отриманих результатів розроблено методичні рекомендації щодо подальшого використання системи та її вдосконалення.

Таким чином, поставлені у кваліфікаційній роботі завдання вирішено повністю, що підтверджується результатами розробки, тестування та аналізу ефективності запропонованого підходу.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Mobile Device Management [Electronic resource]. – Access mode: https://www.manageengine.com/mobile-device-management/.

2. Worldwide Devices Shipments to Continue 2022 Decline in 2023 [Electronic resource]. – Access mode: https://displaydaily.com/worldwide-devices-shipments-to-continue-2022-decline-in-2023/.

3. BYOD, CYOD, COPE: Which Approach Should You Take? [Electronic resource]. – Access mode: https://blog.talkspirit.com/en/byod-cyod-cope-which-approach-should-you-take/

4. Mobile Blog [Electronic resource]. – Access mode: https://www.facebook.com/MobileBlogSite/

5. Himmelsbach, R. What is hidden behind the concepts of BYOD, CYOD, COPE [Electronic resource] / R. Himmelsbach // Journal of network solutions LAN. - 2023, No. 06. – Pp. 26 – 44.

6. Bring Your Own Device [Electronic resource]. – Access mode: https://www.willowbank.school.nz/8/pages/6-bring-your-own-device-byod/

7. Mobile Device Management [Electronic resource]. – Access mode: https://en.wikipedia.org/wiki/Mobile_device_management/

8. Choose Your Own Device [Electronic resource]. – Access mode: https://www.techtarget.com/searchmobilecomputing/definition/CYOD-choose-your-own-device/

9. COPE (corporate-owned, personally enabled) [Electronic resource]. – Access mode: https://www.techtarget.com/searchmobilecomputing/definition-/COPE-corporate-owned-personally-enabled.

10. Marin M.A., Technologies for the implementation of mobile applications / M.A. Marin // Proceedings of the Internet conference of the State Professional Educational Institution "Innovations: Developments and Technologies", № 3, 2024.

11. Sokolova, V. Development of mobile applications: a tutorial / V. Sokolova // Viena Polytechnic University. - Viena: Publishing house of Viena Polytechnic University. - 2021. – Pp. 7 – 50.

12. XenMobile - Mobile Device Management for Enterprise Mobility [Electronic resource]. – Access mode: http://www.citrix.cz/products/xen-mobile/overview.html.

13. Mobile Security Solution for Enterprise Network / A.G. Kravets, Duong Bui Ngoc, M.S. Al-Ashwal // Knowledge-Based Software Engineering [Electronic resource]. – Access mode: https://www.researchgate.net/publication/-278658390_Mobile_Security_Solution_for_Enterprise_Network.

14. Enterprise mobility management [Electronic resource]. – Access mode: https://en.wikipedia.org/wiki/Enterprise_mobility_management.

15. Publish–subscribe pattern [Electronic resource]. – Access mode: https://en.wikipedia.org/wiki/Publish%E2%80%93subscribe_pattern

16. What's a UUID? What are Universal Unique Identifiers and how do they work? [Electronic resource]. – Access mode: https://www.uuidtools.com/what-is-uuid.

17. Android Device Information Security [Electronic resource]. – Access mode: https://security.stackexchange.com/questions/149084/how-to-theft-protect-my-android-device.

18. Enterprise Mobility and Its Impact on IT [Electronic resource]. – Access mode: https://www.gartner.com/en/documents/1985016.

19. MobileIron User Reviews [Electronic resource]. – Access mode: https://www.itqlick.com/mobileiron/feedback.

20. Critical Capabilities for Enterprise Mobility Management Suites [Electronic resource]. – Access mode: https://www.gartner.com/en/documents/3345017.

21. Designing the transition to operations in large inter-organizational projects: Strategy, structure, process, and people [Electronic resource]. – Access mode: https://www.researchgate.net/publication/373658604_Designing_the_-

transition_to_operations_in_large_inter-organizational_projects_Strategy_structure_process_and_people.

22. Peterson L.L. Computer Networks: A Systems Approach (The Morgan Kaufmann Series in Networking)/ L.L. Peterson, B.S. Davie. – Morgan Kaufmann, 2021. – 920 p.

23. Smith R.E. Authentication: From Passwords to Public Keys / R.E. Smith. – Addison-Wesley Professional, 2022. – 549 p.

24. Kaufman C. Network Security: Private Communication in a Public World / C. Kaufman, R. Perlman, M. Speciner. – Prentice Hall, 2022. – 752 p.

25. Тарасюк М. В. Захищені інформаційні технології. Проектування та застосування / М. В. Тарасюк. - К.: СЛОН-Прес, 2024. – 192 с.

26. Ігнатенко А. П. Протидія атакам на відмову в мережі Інтернет: вибір середовища моделювання / О. П. Ігнатенко, Д. В. Ціцкун // Проблеми програмування. – 2018. № 2-3. Спеціальний випуск. – Стор. 579-586.

27. ISO/IEC 27035-1:2023 Information technology. Information security incident management. Part 1: Principles and process [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/78973.html.

28. RFC 2475: An Architecture for Differentiated Services [Електронний ресурс]. – Режим доступу:https://tools.ietf.org/html/rfc2475

29. Cannady J. A Comparative Analysis of Current Intrusion Detection Technologies [Електронний ресурс]. – Режим доступу: http://www.scis.nova.edu/~cannady/TISC96.pdf.

30. Технологія аналізу даних. BaseGroup Labs [Електронний ресурс]. - Режим доступу: http://www.basegroup.com/library/analysis/regression/knn/