ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТАЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія управління мобільними користувачами корпоративної інформаційної системи на базі концепції BYOD»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Іван ІСАЄНКО
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-62
ІСАЄНКО Іван
(прізвище, ім'я)

Керівник к.держ.у. СКИБУН Олександр
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

APN – Apple Push Notification Service

BYOD – Bring Your Own Device

GDPR - General Data Protection Regulation

MAM –Mobile Application Management

MDM – Mobile Device Management

Mishing – mobile-targeted phishing

RBDA – Рольовий доступ до пристрою

КІС - корпоративна інформаційна система

ВСТУП

Актуальність обраної теми дослідження зумовлена глибокими змінами, які відбуваються у сучасному бізнес-середовищі під впливом цифрових технологій та глобальної мобільності. Стрімке зростання кількості мобільних пристроїв — смартфонів, планшетів, ноутбуків — та їх інтеграція у робочі процеси підприємств висувають принципово нові вимоги до архітектури, безпеки та управління корпоративними інформаційними системами (КІС).

Концепція BYOD (Bring Your Own Device) передбачає використання співробітниками власних мобільних пристроїв для доступу до корпоративних ресурсів, набула масового поширення як в Україні, так і світі. Цей підхід є привабливим для бізнесу, оскільки він дозволяє значно знизити капітальні витрати на придбання обладнання, підвищити продуктивність праці завдяки використанню звичних та зручних для користувача інструментів, а також покращити задоволеність та мобільність персоналу. Однак, широке впровадження BYOD несе в собі комплексні та багатогранні ризики, які потребують негайного вирішення.

Основна проблема полягає у балансі між зручністю доступу та інформаційною безпекою. Неконтрольоване підключення особистих пристроїв, які можуть не відповідати корпоративним політикам безпеки, створює широкий вектор загроз. До них відносяться витоки конфіденційних даних, несанкціонований доступ до КІС, зараження корпоративної мережі шкідливим програмним забезпеченням, втрата пристроїв, що містять критичну інформацію, а також проблеми, пов’язані з розділенням особистих та робочих даних.

Існуючі традиційні механізми управління, такі як Mobile Device Management (MDM) або Mobile Application Management (MAM), є гнучкими або можуть інтегруватися в мобільне середовище, характерного для BYOD.

Отже, розробка технології набуває критичного значення, яке включатиме методику ідентифікації, автентифікації, управління доступом, сегментації даних та моніторингу мобільних користувачів в режимі реального часу. Це дозволить підприємствам не лише безпечно використовувати переваги BYOD, але й

забезпечити відповідність зростаючим вимогам регуляторних органів щодо захисту персональних та корпоративних даних.

Об'єкт дослідження – управління мобільними користувачами корпоративної інформаційної системи організації.

Предмет дослідження – технологія управління мобільними користувачами корпоративної інформаційної системи організації на базі концепції BYOD.

Мета роботи – розробка варіанту технології управління мобільними користувачами корпоративної інформаційної системи організації та розробки рекомендацій щодо її застосування.

Наукові завдання:

дослідити сутність проблеми управління мобільними користувачами корпоративної інформаційної системи організації;

проаналізувати основні загрози мобільним користувачам корпоративної інформаційної системи організації;

проаналізувати підходи до вирішення проблеми управління мобільними користувачами корпоративної інформаційної системи організації;

проаналізувати існуючі технології управління мобільними користувачами корпоративної інформаційної системи організації;

проаналізувати методи та засоби управління мобільними користувачами корпоративної інформаційної системи організації;

розробити рекомендації щодо застосування технології управління мобільними користувачами корпоративної інформаційної системи організації.

Методи дослідження: опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, практичне використання засобів захисту віддалених користувачів.

Практичне значення одержаних результатів: запропоновано рекомендації щодо управління мобільними користувачами корпоративної інформаційної системи організації.

Апробація результатів.

Ісаєнко І.І. Управління мобільними пристроями в сучасному корпоративному середовищі: виклики сьогодення та стратегії подолання. *Актуальні проблеми кібербезпеки:* матеріали всеукраїнської наук.-практ. конф., м. Київ: ДУІКТ, 29 жовт. 2025р. Київ. С 44-45.

1 АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ МОБІЛЬНИМИ КОРИСТУВАЧАМИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

1.1. Проблема управління мобільними користувачами корпоративної інформаційної системи організації

Сутність та класифікація мобільних пристроїв у корпоративному середовищі

Електронний мобільний пристрій у широкому сенсі – це портативний, автономний, багатофункціональний обчислювальний пристрій, здатний до безпроводового зв'язку та забезпечення доступу до даних і сервісів незалежно від місця розташування користувача. У контексті корпоративної інформаційної системи (КІС), мобільні пристрої перестали бути лише засобом комунікації, перетворившись на повноцінні робочі інструменти, критично важливі для забезпечення безперервності бізнес-процесів, особливо у сферах логістики, продажів, менеджменту та віддаленої роботи [1, 12].

До категорії корпоративних мобільних пристроїв [1], які використовують в корпоративній інформаційній системі відносять (рис. 1.1):

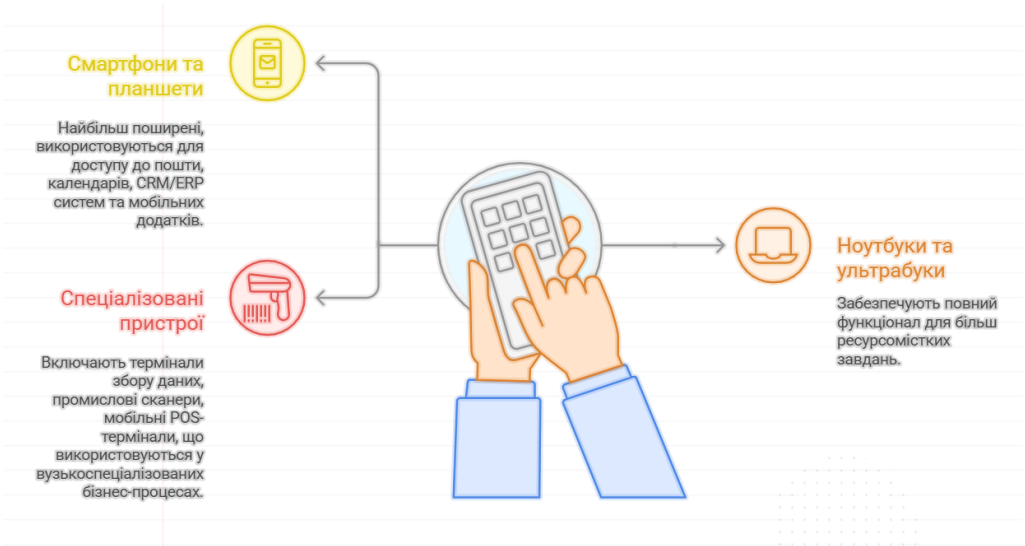


Рис.1.1. Категорії мобільних пристроїв

Смартфони та планшети, які є найбільш поширені і використовуються для доступу до корпоративної пошти, календарів, CRM/ERP систем та спеціалізованих мобільних додатків.

Ноутбуки та ультрабуки забезпечують повний функціонал для більш ресурсомістких завдань.

Спеціалізовані пристрої включають у себе термінали збору даних, промислові сканери, мобільні POS-термінали, що використовуються у вузькоспеціалізованих бізнес-процесах.

Впровадження мобільних технологій у бізнес стало повсюдним. Згідно з актуальними глобальними та українськими звітами, понад 60% всього інтернет-трафіку генерується мобільними гаджетами, що підкреслює їх домінуючу роль у взаємодії користувачів з цифровим контентом (рис.1.2).

Рис.1.2. Розподіл інтернет-трафіку за пристроями

За оцінками, більшість (понад 80%) організацій у світі вже інтегрували або планують інтегрувати стратегії управління мобільністю, а значна частина корпоративних користувачів регулярно використовує мобільні пристрої для виконання щонайменше однієї робочої задачі на день [1-3].

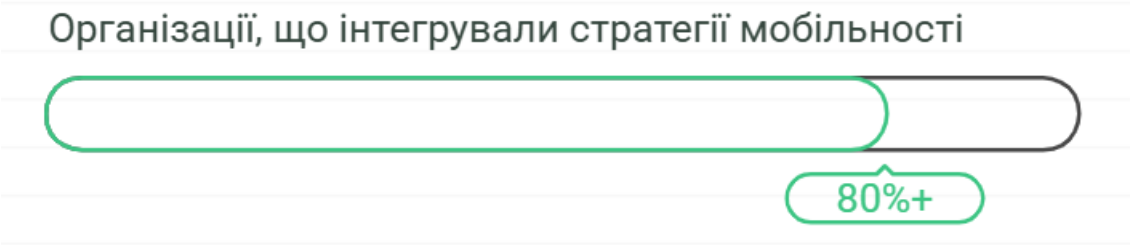


Рис.1.3. Інтеграція стратегій мобільності

Ця статистика підтверджує, що мобільність є не просто трендом, а фундаментальною необхідністю сучасної корпоративної інфраструктури.

Концепції організації мобільності в КІС

Управління мобільними пристроями в КІС неможливе без чіткої політики щодо володіння пристроєм та його використання. Існує чотири основні концепції (моделі) організації мобільності, які представлені у таблиці 1.1:

Таблиця 1.1.

Основні концепції (моделі) організації мобільності

Концепція	Розшифровка	Сутність	Володіння	Контроль IT
BYOD	Bring Your Own Device	Співробітники використовують власні пристрої для роботи.	Особисте	Низький / Середній (фокус на даних)
COPE	Corporate-Owned, Personally Enabled	Компанія володіє пристроєм, але дозволяє особисте використання.	Корпоративне	Високий (повний)
COBO	Corporate-Owned, Business Only	Компанія володіє пристроєм, який використовується виключно для роботи.	Корпоративне	Максимальний (жорсткий)

CYOD	Choose Your Own Device	Співробітник обирає пристрій із затвердженого компанією списку.	Корпоративне	Високий

1. BYOD є найбільш гнучкою, але й найбільш ризикованою моделлю. Її сутність полягає у перенесенні відповідальності за придбання, обслуговування та психологічне звикання до пристрою на самого співробітника.

Переваги BYOD:

– Економія витрат. Компанія не несе прямих витрат на купівлю обладнання.

– Підвищення продуктивності. Співробітники більш ефективні на звичних пристроях.

– Задоволеність персоналу. Збільшення гнучкості та автономності.

Недоліки BYOD:

– Безпека. Змішування особистих і корпоративних даних, ризик зараження через особисті додатки.

– Складність управління. Велика різноманітність операційних систем, версій ПЗ та моделей пристроїв.

– Конфіденційність. Проблеми з віддаленим стиранням даних (Wipe) у разі звільнення.

2. COPE (Corporate-Owned, Personally Enabled)Сутність: Пристрій належить компанії, але співробітнику дозволено використовувати його для особистих потреб (дзвінки, особиста пошта, соцмережі) у вільний від роботи час. IT-відділ встановлює суворі політики безпеки.

Переваги COPE

Повний контроль IT: Легкість централізованого налаштування, оновлення та вирішення проблем.

Уніфікація: Однакове апаратне та програмне забезпечення спрощує підтримку та навчання.

Висока безпека: Можливість жорсткого шифрування, встановлення корпоративних сертифікатів і віддаленого стирання даних (Wipe) всього пристрою без правових колізій.

Недоліки

Конфіденційність користувача: Співробітники можуть відчувати, що компанія моніторить їхнє особисте життя (геолокація, особисті додатки).

Обмежений вибір: Користувачі можуть бути незадоволені виділеною моделлю пристрою.

Вища вартість: Компанія несе витрати на придбання, обслуговування та заміни пристроїв.БезпекаВисока безпека:

3. Концепція COBO. Пристрій належить компанії і використовується виключно для робочих цілей. Це найсуворіша та найбезпечніша модель.

Переваги

Максимальний захист: Мінімальний ризик зараження, оскільки особисті програми та вебсайти заборонені. Ідеально підходить для висококонфіденційних даних.

Простота аудиту: Чітке розділення відповідальності та відсутність необхідності керувати особистим вмістом пристрою.

Відповідність вимогам (Compliance): Найкращий варіант для галузей із суворими регуляторними вимогами (фінанси, охорона здоров'я).

Недоліки

Низька зручність: Співробітники змушені носити два пристрої (особистий та робочий), що знижує мобільність.

Найвища вартість: Необхідність фінансувати не лише пристрій, а й пов'язані з ним комунікаційні послуги (мобільний зв'язок).

Зниження продуктивності: У деяких випадках співробітники можуть не мати доступу до звичних та ефективних інструментів.

4. Концепція CYOD. Пристрій належить компанії, але співробітнику надається право обрати модель пристрою зі списку, попередньо затвердженого IT-відділом. Це компроміс між BYOD та COPE/COBO.

Переваги

Мотивація персоналу: Надання вибору підвищує задоволеність та сприйняття корпоративної політики.Управління різноманіттям: IT-відділу все одно доводиться підтримувати обмежений, але різноманітний набір пристроїв (декілька моделей Android, декілька моделей iOS).

Високий рівень контролю: Оскільки список пристроїв обмежений, IT-відділ може протестувати та гарантувати сумісність кожного з них із корпоративними стандартами безпеки.

Баланс: Поєднує переваги контролю (як у COPE) зі зручністю вибору для користувача."Ефект вибору": Обмежений список може розчарувати тих, хто очікував більшої свободи, як у BYOD.

Недоліки

Високі початкові витрати: Компанія все одно купує пристрої, хоча і з певним урахуванням побажань працівників.

Управління різноманіттям: IT-відділу все одно доводиться підтримувати обмежений, але різноманітний набір пристроїв (декілька моделей Android, декілька моделей iOS).

"Ефект вибору": Обмежений список може розчарувати тих, хто очікував більшої свободи, як у BYOD.

Ці моделі демонструють спектр рішень: від максимальної свободи користувача (BYOD) до максимального контролю компанії (COBO).

Ключові виклики та проблема управління мобільними користувачами

Незважаючи на очевидні переваги мобільності, її інтеграція створює фундаментальну проблему: як забезпечити безперервний, гнучкий доступ до корпоративних ресурсів, не скомпрометувавши критично важливі дані та інфраструктуру КІС.

Проблема управління мобільними користувачами КІС на базі концепції BYOD є багатофакторною і охоплює три ключові аспекти: безпека, управління (Management) та відповідність (Compliance).

1. Безпека даних та пристроїв

Це найбільш гостра проблема. Особистий пристрій, що використовується для роботи, стає потенційною "діркою" у корпоративній мережі. Основні загрози включають:

Витоки даних (Data Leakage). Копіювання конфіденційної інформації з корпоративного контейнера на особисту пам'ять пристрою або у незахищені хмарні сервіси.

Шкідливе програмне забезпечення. Ризик інфікування пристрою через встановлення неперевірених додатків з публічних магазинів або зламаних сайтів.

Втрата/крадіжка. Фізична втрата пристрою, що містить корпоративні облікові дані та дані.

Скомпрометовані пристрої. Використання "джейлбрейкнутих" (iOS) або "рутованих" (Android) пристроїв, які обходять вбудовані системи безпеки ОС.

2. Адміністративне управління та підтримка

Технологія управління має долати складність гетерогенного середовища:

Фрагментація ОС. Різноманіття операційних систем (iOS, Android, Windows) та їх версій ускладнює єдине централізоване налаштування політик.

Налаштування та конфігурація. Необхідність віддалено встановлювати та оновлювати корпоративні програми, VPN-профілі, сертифікати без втручання в особисті дані користувача.

Автентифікація та доступ: Забезпечення надійного багаторівневого доступу (MFA) для кожного користувача, незалежно від його місця перебування та типу пристрою.

Розмежування: Критична необхідність створення на пристрої чіткого корпоративного контейнера, який ізолює робочі дані та додатки від особистих, щоб захистити конфіденційність працівника та IT-активи компанії.

3. Відповідність нормативним вимогам (Compliance)

Управління мобільністю має відповідати законодавчим та галузевим стандартам, зокрема:

GDPR (General Data Protection Regulation) / Закони про захист персональних даних: Необхідність гарантувати, що управління пристроєм (особистою власністю) не порушує право співробітника на приватність.

Галузеві стандарти. Наприклад, вимоги щодо захисту фінансових даних (PCI DSS) чи медичної інформації (HIPAA).

Таким чином, проблема управління мобільними користувачами КІС на базі BYOD полягає у відсутності комплексної, автоматизованої та адаптивної технології, здатної централізовано реалізувати: ізоляцію корпоративних даних на особистих пристроях, гранульований контроль доступу на основі контексту (користувач, пристрій, локація, стан безпеки) та швидке реагування на інциденти без порушення конфіденційності власника пристрою. Розробка такої технології є ключовою метою для забезпечення стабільності та безпеки сучасного мобільного підприємства.

1.2. Аналіз загроз мобільних користувачів корпоративної інформаційної системи організації

Характер кіберзагроз постійно розвивається, а зловмисники використовують дедалі складніші методи, щоб уникнути виявлення їх виявлення.

Звіт Zimperium «Global Mobile Threat Report 2025» виявляє, що зловмисники перейшли до стратегії mobile-first (спочатку мобільні пристрої), що робить критично важливим для організацій розуміння та зменшення мобільних ризиків [4].

Станом на кінець 2024 року у світі налічувалося приблизно 7,2 мільярда користувачів смартфонів. Мобільні пристрої тепер регулярно використовуються для доступу до конфіденційних систем, даних і робочих процесів, які раніше були обмежені захищеними настільними комп’ютерами, що значно розширює цифрову поверхню атаки.

Ключові факти, що підтверджують проблему BYOD:

Приблизно 70% організацій підтримують концепцію BYOD.

Середній пристрій, який використовується для роботи, налічує 80–100 встановлених програм, але лише 11 з них є робочими, згідно з Gartner [2]. Це вносить неконтрольовані поверхні атаки.

23,5% корпоративних пристроїв мають встановлені "sideloaded apps" (програми, встановлені не з офіційних магазинів).

25% мобільних пристроїв не можуть оновити свою операційну систему (ОС) через вік, що створює ризик компрометації даних через відомі вразливості ОС.

У звіті виділено три основні категорії загроз для корпоративного мобільного середовища:

1. Mishing (Мобільний фішинг)

Mishing (mobile-targeted phishing) став головною загальною мобільною загрозою [4].

Частка атак: Mishing становить приблизно третину загроз, виявлених zlabs.

Домінуючий вектор: Smishing (SMS-фішинг) становить понад дві третини (69,3%) всіх атак mishing.

Зростання: Кількість інцидентів Vishing (голосовий фішинг) зросла на 28%, а Smishing – на 22% у III кварталі 2024 року порівняно з II кварталом.

Нові вектори: Виник PDF-фішинг, який активно використовується через SMS-повідомлення (див. Рисунок 2) і становить 28,4% усіх mishing-атак

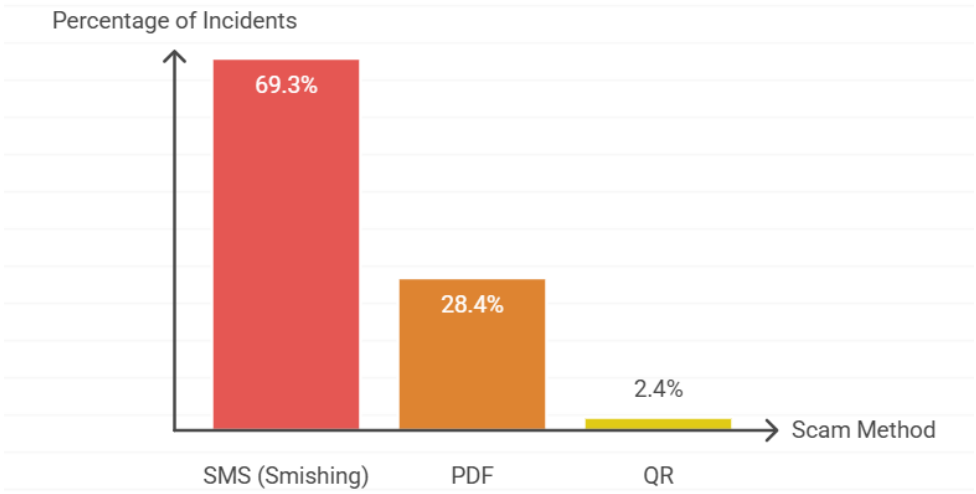


Рис.1.4. Частка атак мобільного фішингу

2. Мобільне шкідливе програмне забезпечення (Malware)

Шкідливе програмне забезпечення залишається основною зброєю як для кіберзлочинців, так і для складних, просунутих, постійних загроз, спрямованих на мобільні пристрої в усьому світі. Дослідження zLabs підтверджує поширений характер цієї загрози, виявивши, що на 18,1% пристроїв у нашому аналізованому наборі було встановлено мобільне шкідливе програмне забезпечення. Рисунок 1.5. наводить візуальний розподіл поширених типів шкідливого програмного забезпечення, які ми спостерігаємо [4].

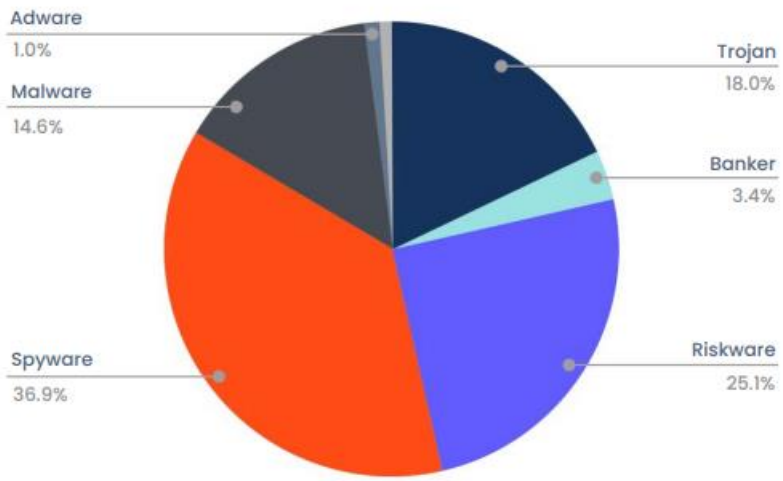


Рис. 1.5. Поширені типи загроз

3. Sideloading

Стороннє завантаження (sideloading) – це практика встановлення мобільних додатків на пристрій, які не походять з офіційних магазинів додатків. Зазвичай це робиться на рутованих пристроях Android або iOS з джейлбрейком. У 2024 році Закон ЄС про обробку даних призвів до появи сторонніх додатків на пристроях iOS, тому ми починаємо бачити їх присутність на iPhone. Зі стиранням меж між особистими та професійними особами сторонні додатки все частіше з'являються на особистих пристроях, що використовуються для роботи [4].

Бокове завантаження додатків може призвести до повної компрометації мобільного пристрою. zLabs виявив 23,5% мобільних пристроїв, на яких є один або кілька сторонніх додатків. Сторонньо завантажені додатки входять до 3 основних ризиків як для пристроїв iOS, так і для Android, згідно з zLabs [4].

1.3. Підходи до вирішення проблеми управління мобільними користувачами корпоративної інформаційної системи організації

Значною проблемою для ринку безпеки BYOD є управління різноманітними пристроями, які співробітники приносять на робоче місце. Ці пристрої відрізняються за операційними системами, конфігураціями обладнання та протоколами безпеки, що ускладнює для IT-команд підтримувати послідовний рівень безпеки в організації. Згідно з дослідженням 2024 року, 48% організацій мають труднощі з контролем над широким спектром пристроїв та програм, які використовують співробітники. Ця відсутність однаковості пристроїв та систем ускладнює впровадження єдиних заходів безпеки та створює значні труднощі для постачальників послуг безпеки [4].

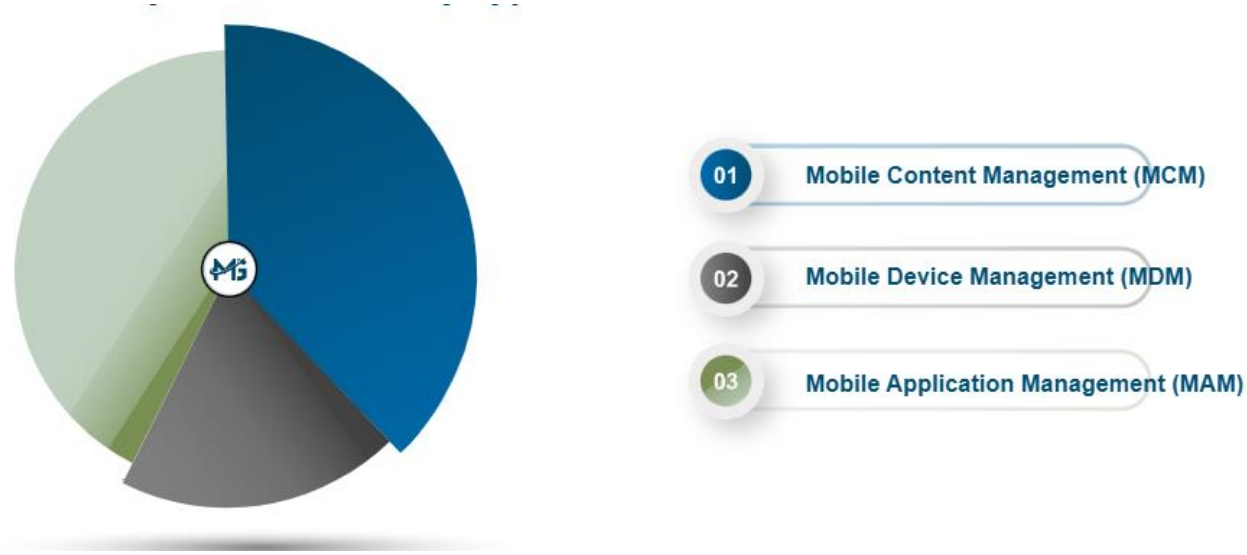


Рис.1.6. Сегментація ринку управління мобільними пристроями

Розглянемо підходи до управління мобільними пристроями за типом організації та застосування технологій

За типом організації

Великі підприємства: Великі підприємства швидко впроваджують політику BYOD через велику базу своїх співробітників та зростаючу потребу в мобільності. Тенденція до BYOD у великих організаціях значною мірою зумовлена бажанням підвищити продуктивність та покращити задоволеність співробітників. У 2023 році повідомлялося, що 65% великих підприємств впровадили політику BYOD,

порівняно з лише 45% серед малих та середніх підприємств. Зростаюче впровадження хмарних рішень та платформ корпоративної мобільності у великих компаніях сприяє цій тенденції.

Урядові організації: Урядові організації часто вважаються більш обережними у впровадженні політики BYOD через занепокоєння щодо національної безпеки та конфіденційності даних. Однак в останні роки багато урядових установ запровадили програми BYOD для підвищення операційної ефективності. Станом на 2023 рік приблизно 40% урядових установ у всьому світі запровадили політику BYOD, головним чином через необхідність забезпечити мобільну роботу для своїх співробітників, зберігаючи при цьому безпечні канали зв'язку.

Малий та середній бізнес (МСБ): МСБ все частіше впроваджують політику BYOD (придбання власних пристроїв), щоб скоротити витрати, пов’язані з наданням пристроїв співробітникам. Ці підприємства, як правило, є більш гнучкими та мають менше ресурсів безпеки, що робить їх більш залежними від сторонніх рішень безпеки BYOD. Дослідження показують, що близько 55% МСБ запровадили політику BYOD до кінця 2023 року, причому значна частина використовувала хмарні рішення MDM та MAM для захисту своїх мобільних пристроїв.

За застосуванням технологій

Керування мобільним контентом (MCM): MCM відіграє вирішальну роль в управлінні та захищенні контенту, доступ до якого здійснюється через пристрої, що належать співробітникам. Цей сегмент швидко розвивається, оскільки компанії прагнуть контролювати доступ, обмін та зберігання конфіденційних бізнес-даних на особистих пристроях. У 2023 році рішення MCM використовувалися понад 70% компаній з офіційною політикою BYOD, що допомагає їм захистити документи, електронні листи та інший важливий контент на мобільних пристроях.

Керування мобільними пристроями (MDM): MDM – це найпоширеніше рішення безпеки на ринку безпеки BYOD. Це рішення допомагає організаціям керувати, контролювати та захищати мобільні пристрої, забезпечуючи дотримання корпоративних політик. Згідно зі звітом за 2023 рік, впровадження рішень MDM

зросло на 30% порівняно з попереднім роком, оскільки все більше організацій шукали способи забезпечення дотримання стандартів безпеки на широкому спектрі мобільних пристроїв.

Керування мобільними додатками (MAM): Рішення MAM зосереджені на захисті додатків, встановлених на мобільних пристроях, забезпечуючи їх безпеку використання в корпоративному середовищі. Оскільки все більше компаній впроваджують культуру «принеси свій власний додаток», попит на рішення MAM зростає. У 2023 році повідомлялося, що приблизно 60% компаній із політикою BYOD впровадили рішення MAM для забезпечення безпечного використання додатків.

1.4. Аналіз технологій управління мобільними користувачами корпоративної інформаційної системи організації

Для вибору оптимальної технології, яка слугуватиме базою для розробки та моделювання запропонованої в магістерській роботі технології управління, необхідно провести порівняльний аналіз платформ.

Критеріями для вибору є:

Повнота реалізації EMM: Наявність не лише MDM, але й функцій MAM (управління програмами) та MCM (управління контентом).

Підтримка BYOD: Наявність спеціалізованих функцій для BYOD, зокрема контейнеризації, самостійної реєстрації та вибіркового стирання.

Функції безпеки: Здатність протидіяти ключовим загрозам (sideloading, витік даних, компрометація пристрою), виявленим у підрозділі 2.1.

Гнучкість розгортання: Можливість роботи як у хмарному, так і в локальному (on-premise) середовищі для гнучкості моделювання.

Основними технологіями для порівняння технологій управління мобільними пристроями є:

BES12 — це рішення для безпечного керування мобільністю пристроїв, програмами та контентом з інтегрованою безпекою та підключенням для

BlackBerry, iOS та Android. Розгортайте, керуйте та контролюйте як корпоративних користувачів, так і користувачів пристроїв BYOD за допомогою простої єдиної консолі [5].

Centrify пропонує рішення, яке захищає та керує не лише популярними мобільними пристроями, але й системами Mac OS X, UNIX та Linux. Хмарний сервіс Centrify for Mobile дозволяє централізовано захищати та керувати смартфонами й планшетами, використовуючи вашу існуючу інфраструктуру Active Directory. Centrify for Mobile використовує інструменти групової політики разом із Centrify Cloud Service для забезпечення налаштувань безпеки через надійне бездротове з'єднання та безпечний доступ до корпоративних мережевих служб [5].

Незалежно від того, чи належить компанія, чи власний пристрій, забезпечення безпечного доступу до програм починається із захисту та керування пристроями. Автоматично надсилайте електронну пошту, налаштування Wi-Fi та VPN, а також забезпечуйте відповідність пристроїв вимогам. Керуйте паролями, дистанційно блокуйте та видаляйте дані, а також використовуйте стан пристрою для політики єдиного входу в програмі — повний комплекс EMM, інтегрований з Identity [5].

Citrix XenMobile — це рішення для керування мобільними пристроями, програмами та даними. Користувачі мають доступ до всіх своїх мобільних, SaaS- та Windows-програм з єдиного корпоративного магазину програм, включаючи інтегровані програми для електронної пошти, браузера, обміну даними та підтримки. IT-відділ отримує контроль над мобільними пристроями з повними можливостями налаштування, безпеки, забезпечення та підтримки [5].

Заснована в 1992 році, компанія FileWave є лідером у сфері керування пристроями на різних платформах, що забезпечує простий, але потужний спосіб захисту, керування та обслуговування пристроїв, контенту, оновлень та налаштувань. Серед багатьох унікальних функцій FileWave найвизначнішою є підтримка всіх основних операційних систем – macOS, Windows, iOS, Chrome OS та Android – все в одній консолі. Це великий плюс для будь-якої організації, якій потрібна або знадобиться можливість керувати різноманітною та зростаючою

кількістю користувачів, пристроїв, контенту, програм, облікових записів тощо. Крім того, всі продукти та функції є комплексними, що гарантує, що IT-командам надані всі необхідні інструменти без додаткових компонентів [5].

Mobile Device Manager Plus — це масштабоване комплексне програмне забезпечення для керування мобільними пристроями, яке доповнює мобільну стратегію вашої організації, дозволяючи вам легко керувати мобільними пристроями та програмами та захищати їх. Воно підвищує продуктивність, оскільки ви можете швидко визначати профілі для корпоративних пристроїв та пристроїв, що належать співробітникам (BYOD) [5].

Завдяки Windows Server 2012 R2, Microsoft System Center 2012 R2 Configuration Manager, Windows Intune та Microsoft Azure, Microsoft створює рішення, яке підвищує продуктивність користувачів, одночасно підтримуючи потреби IT-фахівців у управлінні.

Enterprise Mobility Suite — це комплексне хмарне рішення від Microsoft для вирішення потреб споживача в IT та використання власних пристроїв (BYOD). Крім того, знижка на Enterprise Mobility Suite робить його найекономічнішим способом отримання хмарних служб, що входять до комплекту: Azure Active Directory (Azure AD) Premium для керування гібридними ідентифікаторами; Windows Intune для керування мобільними пристроями та ПК; та Azure Rights Management для захисту інформації. Microsoft Enterprise Mobility Suite доступний як хмарне рішення.

Таблиця 1.2.

Платформа	**Основний Фокус**	**Підтримка BYOD**	**Ключові Переваги**	**Обмеження / Специфіка**
BlackBerry UEM	UEM з високим рівнем безпеки	Дуже сильна (контейнери BlackBerry Dynamics)	Найкраща у своєму класі безпека "end-to-end", гранулярний контроль політик.	Може бути надлишковою або складною для середніх компаній; фокус на власну екосистему безпеки.

Centrify (Delinea)	Управління ідентифікацією (IAM) та доступом (PAM)	Часткова (через політики доступу на основі ідентичності)	Сильні SSO та MFA; інтеграція з Active Directory.	**Не є повноцінною MDM/EMM платформою**; управління пристроями є вторинною функцією.
Citrix Endpoint Management	UEM (інтеграція з цифровим робочим простором)	Дуже сильна (Micro-VPN, самостійна реєстрація)	Глибока інтеграція з VDI та віртуальними програмами (Citrix Workspace).	Найбільш ефективна в екосистемі Citrix; може бути складною, якщо VDI не потрібен.
FileWave	Мультиплатформенне UEM	Стандартна (EMM функції)	Єдине управління для macOS, Windows, iOS та Android.	Менш відома, може мати менш спеціалізовані функції MAM порівняно з лідерами.
ManageEngine Mobile Device Manager Plus	Комплексне EMM / MDM	Дуже сильна (Контейнеризація, самостійна реєстрація, профілі)	Широкий набір функцій (MDM, MAM, MCM); гнучкість (Cloud/On-premise).	Є частиною великого набору інструментів (Endpoint Central), що може вимагати інтеграції.

На основі проведеного аналізу, для подальшого моделювання та розробки технології управління мобільними користувачами в рамках концепції BYOD пропонується обрати платформу ManageEngine Mobile Device Manager Plus.

Цей вибір обґрунтовується такими причинами:

Найбільш збалансоване EMM-рішення: На відміну від Centrify, це повноцінна EMM-платформа, що охоплює MDM, MAM та MCM. На відміну від Citrix, її основний фокус – це управління кінцевими точками, а не віртуалізація. Порівняно з BlackBerry, вона пропонує більш гнучкий та універсальний набір функцій, не прив'язаний до пропрієтарної екосистеми безпеки.

Пряма відповідність загрозам BYOD: Функціонал платформи безпосередньо відповідає на виклики, зазначені у звіті Zimperium [4].

Для боротьби з Sideloaded Apps та шкідливим ПЗ платформа пропонує управління програмами (MAM), включно з чорними та білими списками.

Для боротьби з витоком даних (Data Leakage) вона надає управління контентом (MCM) та контейнеризацію для чіткого розділення особистих та корпоративних даних.

Для боротьби з компрометованими пристроями та застарілими ОС платформа дозволяє проводити аудит та застосовувати жорсткі політики безпеки.

Гнучкість розгортання та моделювання: Mobile Device Manager Plus доступний як у хмарній (SaaS), так і в локальній (On-premise) версії. Це робить його ідеальною моделлю для магістерської роботи, оскільки запропонована технологія може бути адаптована під будь-яку інфраструктуру підприємства.

Таким чином, ManageEngine Mobile Device Manager Plus надає найбільш повну, гнучку та збалансовану інструментальну базу, що необхідна для розробки та валідації комплексної технології управління мобільними користувачами в середовищі BYOD.

Висновки до розділу 1

1. Проведено аналіз проблеми управління мобільними користувачами корпоративної інформаційної системи організації, який показав необхідність впровадження заходів для користувачів мобільних пристроїв з концепцією BYOD для забезпечення захисту корпоративної інфраструктури.

2. Аналіз загроз підтвердив проблему BYOD, яку використовують 70% організацій та дозволив визначити основні категорії загроз.

3. Аналіз підходів до управління пристроями дозволив визначити основні підходи щодо впровадження відповідних технологій управління мобільними пристроями, на основі якого було проведено порівняльний аналіз існуючих технологій та визначено ManageEngine Mobile Device Manager Plus як найбільш повну, гнучку та збалансовану базу, що необхідна для управління мобільними користувачами в середовищі BYOD.

2 МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ МОБІЛЬНИМИ КОРИСТУВАЧАМИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

2.1. Архітектура ManageEngine Mobile Device Manager Plus

Технологія ManageEngine Mobile Device Manager Plus підтримує управління мобільними пристроями з однієї консолі для корпоративних інформаційних систем.. Mobile Device Manager Plus надає можливість керувати політиками, керування профілями, керування активами, керування програмами та керування безпекою різних типів мобільних пристроїв [6].

Mobile Device Manager Plus функціонально працює в двох рішеннях: хмарі та локально. Розглянемо архітектури цих рішень.

Більшість підприємств шукають хмарне рішення, щоб заощадити час і кошти, витрачені на апаратну та програмну інфраструктуру. Хмарні рішення не тільки викорінюють початкові інвестиції, але також служать рішенням, яке не потребує обслуговування. Це не потребує купувати, встановлювати, оновлювати чи обслуговувати будь-яке обладнання чи програмне забезпечення. Можна просто зареєструватися, створити обліковий запис у MDM і виконати кілька простих кроків, щоб почати керувати своїми мобільними пристроями.

ManageEngine Mobile Device Manager Plus Cloud підтримує безпечне керування мобільними пристроями з центральної точки. Це дозволяє реєструвати пристрої, попередньо налаштовувати параметри пристроїв, керувати програмами, розгортати команди безпеки та отримувати дані активів.

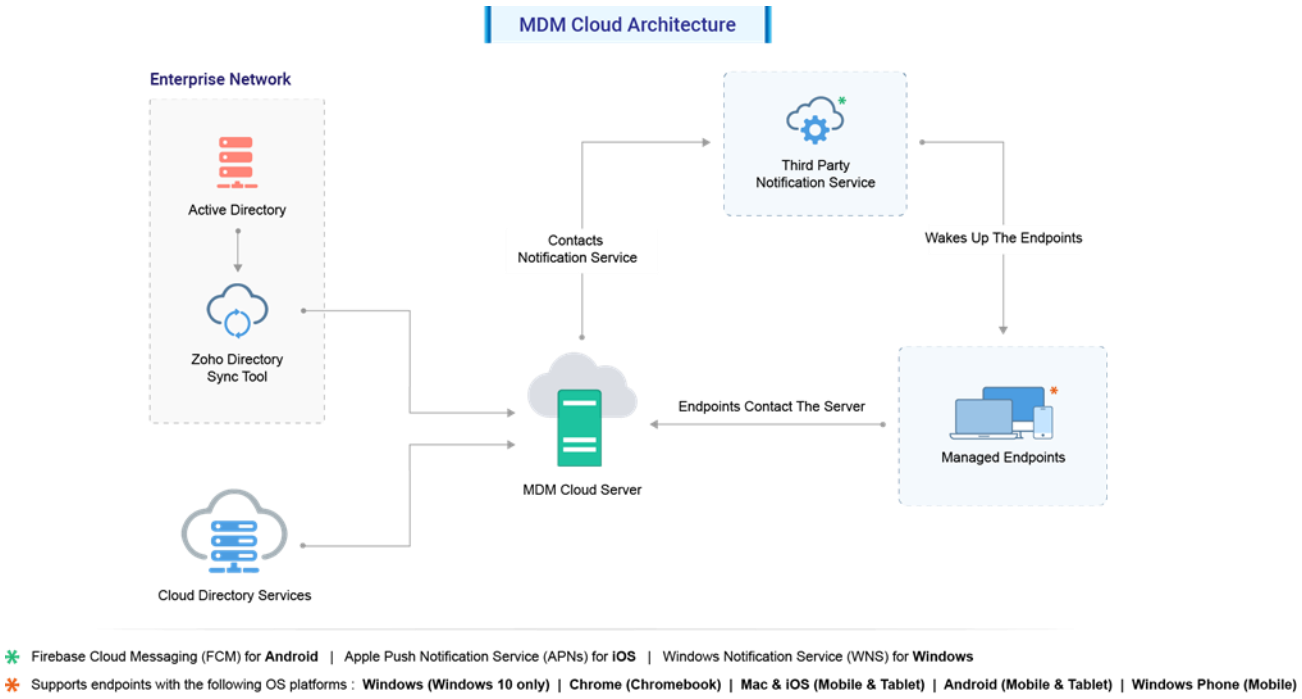


Рис. 2.1. Хмарна архітектура Mobile Device Manager Plus (MDM) [6]

Компоненти Mobile Device Manager Plus Cloud:

Хмарний сервер MDM;

Служби сповіщень;

Керовані пристрої;

Каталогові служби;

Веб-консоль.

Перйдемо до локальної архітектури Mobile Device Manager Plus.

На рис.2.1 представлено діаграму, яка відображає робочий процес локальної версії Mobile Device Manager Plus.

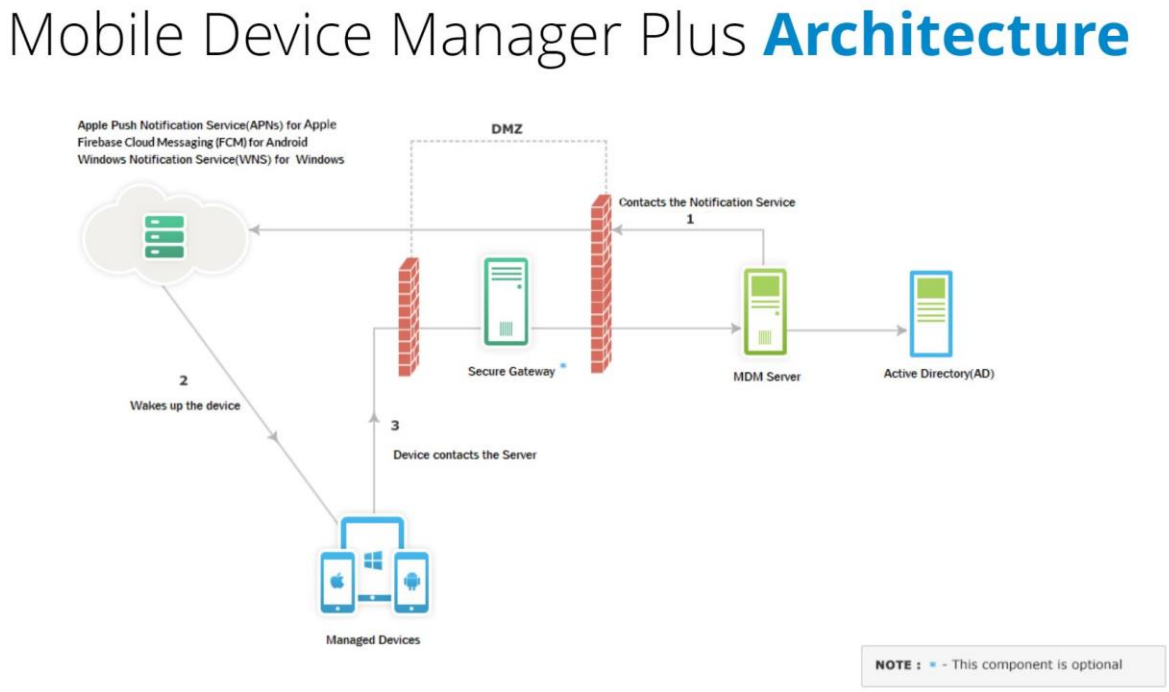


Рис.2.2. Архітектура локальної версії Mobile Device Manager Plus

Згідно з рис.2.2. архітектура Mobile Device Manager Plus працює з пристроями наступним чином:

1. Будь-який зв'язок від Mobile Device Manager Plus до мобільного пристрою передається через службу Apple Push Notification Service (APN) з використанням порту TCP-порт 443,який є спільним який як для пристроїв iOS, так і для пристроїв Android [6].

2. Усі пристрої iOS, згідно з протоколом MDM Apple iOS, підтримують виділене TCP-з'єднання з APN через TCP-порт 5223. Таким чином Mobile Device Manager Plus використовує це для активації пристрою за допомогою APN [6].

3. Мобільний пристрій зв'язується з MDM-сервером для того щоб отримати доступні інструкції через порт 9383. При цьому використовується захищене з'єднання [6].

4. Система виконує всі інструкції та безпечно надсилає всі звіти на MDM-сервер зі статусом/даними через портт 9383.

Для того щоб архітектура працювала, за умови мобільності користувача, слід виконати наступне: MDM-сервер має бути постійно доступним через публічну IP-адресу. Для того щоб увімкнути цю функцію, слід перетворити внутрішню IP-

адресу MDM-сервера на публічну IP-адресу через NAT. Якщо всі керовані пристрої знаходяться в локальній мережі, ця вимога не потрібна [6].

Розглянемо протоколи, які використовуються для Mobile Device Manager Plus. Для реєстрації пристроїв у MDM використовуються протоколи TCP та TLS .

Надаймо деталі щодо використання порту.

TCP-порти, які потрібно відкрити на MDM-сервері. Для MDM-сервера торти для iOS та Android будуть різними [6].

9383 – Використовується для захищеного зв’язку між агентом та Mobile Device Manager Plus.

TCP-порти для управління мобільними пристроями iOS, які потрібно відкрити:

1. 443 – має бути відкрито на брандмауері/проксі-сервере, щоб MDM-сервер міг отримати доступ до точок доступу (APN). Адреса хоста: api.push.apple.com

2. 5223 – якщо мобільний пристрій буде підключатися до Інтернету через Wi-Fi, цей порт необхідно відкрити. Для покращеної безпеки можна обмежити ці підключення діапазоном IP-адрес 17.0.0.0/8. Якщо всі мобільні пристрої КІС будуть мати доступ до стільникової мережі передачі даних, ця вимога для порту не потрібна.

TCP-порти, які потрібно відкрити для управління мобільними пристроями Android.

1. 443 – використовується для захищеного зв’язку між сервером MDM та сервером FCM.

2. Якщо мобільний пристрій підключається до Інтернету через Wi-Fi - порти з номерами 5228, 5229, 5230, 5235, 5236 мають бути відкриті на брандмауері. Це забезпечує зв'язок між мобільними пристроями та FCM.

MDM може керувати [6]:

iOS 4.0 або пізнішої версії

iPadOS 13.0 або пізнішої версії

macOS 10.7 або пізнішої версії

tvOS 7.0 або пізнішої версії

Android 5.0 або пізнішої версії

Android TV – Android 4.4 і вище

Chrome OS 57.0 або пізнішої версії

Windows Phone 8 або пізнішої версії

Ноутбуки з Windows 10 або вище

Таким чином, правильно налаштована архітектура дозволить управляти мобільними пристроями користувачів КІС.

2.2. Ключові характеристики Mobile Device Manager Plus

Розглянемо ключові характеристики Mobile Device Manager Plus.

Mobile Device Manager Plus – це рішення для керування мобільністю підприємства, яке знімає навантаження з адміністратора, автоматизуючи реєстрацію пристроїв за допомогою методів безконтактної та самостійної реєстрації. Зареєстровані пристрої забезпечуються необхідними політиками безпеки, програмами та ресурсами на основі ролей користувачів в організації [7].

Автоматизація налаштування Wi-Fi, VPN, електронної пошти, паролів, програм та інших параметрів організації мінімізують час простою критично важливих пристроїв за допомогою дистанційного керування, отримують сповіщення про важливі події, такі як низький рівень заряду батареї, на цих пристроях. Окрім сповіщень, можна планувати надсилання персоналізованих звітів у поштову скриньку для отримання детальної інформації про пристрої [7].

Основною характеристикою технології є забезпення управління кожним пристроєм на кожному етапі його *життєвого циклу управління мобільним пристроєм* (рис 2.3)

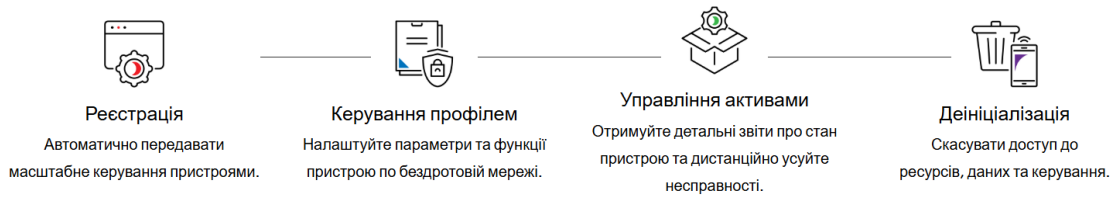


Рис.2.3. Життєвий цикл MDM

Життєвий цикл управління додатками дозволить КІС захистити та обліковувати кожен мобільний пристрій.

Управління додатками протягом усього їхнього життєвого циклу починається з попереднього налаштування параметрів та дозволів програм, щоб допомогти користувачам використовувати програми з мінімальним або нульовим налаштуванням. Розгортаються ці налаштовані програми на пристроях безшумно або на порталах самообслуговування, що відповідає певним групам каталогів та відділам, щоб забезпечити легкий доступ для потрібних користувачів [7].

Контроль версій користувацьких програм на всіх визначених пристроях, на основі відділів, дозволяє одночасно налаштовувати правила автоматичного оновлення для дозволених програм. Такий підхід захищає КІС від шкідливого програмного забезпечення, блокуючи програми зі зловмисними намірами та запобігаючи встановленню програм з ненадійних джерел [7].

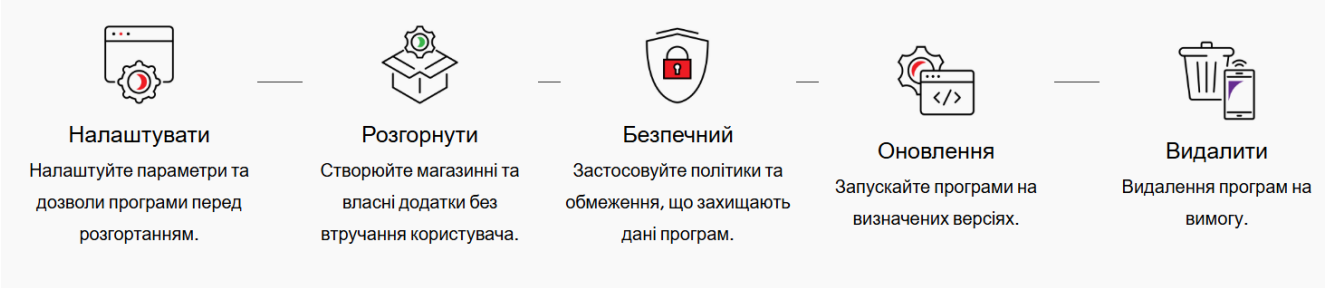


Рис.2.4. Життєвий цикл управління додатками мобільного пристрою

Захист даних незалежно від їхнього стану. Забезпечує безпеку пристроїв за допомогою шифрування пристроїв і SD-карт, а також встановлює політики входу за допомогою пароля та біометричних даних. Доповнюється це миттєво виправляючи вразливості ОС «нульового дня» за допомогою відповідних політик оновлення ОС. Щоб забезпечити відповідність вимогам, застосовуються політики геозонування та використання коригувальних заходів щоразу, коли пристрій входить у периметр або виходить з нього [7].

Данна характеристика забезпує безпеку даних, регулюючи копіювання та вставку, створення знімків екрана, резервне копіювання у сторонні хмарні ресурси, обмін даними з USB та мережею, а також обмін через несанкціоновані програми.

Це також забезпечує безпеку даних під час передачі, налаштовуючи та контролюючи параметри мережі, такі як Wi-Fi, Bluetooth, NFC, VPN, APN та проксі.

Рис.2.5. Захист даних незалежно від їхнього стану

Управління доступом до корпоративного контенту, електронної пошти та робочих просторів

Дана характеристика дозволяє розповсюджувати корпоративний контент на керовані пристрої за допомогою політик DLP, щоб обмежити спільний доступ. Ці політики також можна застосовувати для захисту даних корпоративних програм як на керованих, так і на некерованих пристроях. Забезпечує проактивне блокування доступу будь-яких неавторизованих пристроїв до корпоративної електронної пошти та даних.

Дозволяє налаштовувати облікові записи електронної пошти у великих масштабах та обмежувати доступ до вкладень для керованих програм, для яких налаштовано політики DLP. Інтегрується з Microsoft 365, Google Workspace та Zoho Workplace, щоб налаштовувати програми електронної пошти та робочі програми, застосовувавши умовний доступ та встановлювати політики DLP, навіть якщо пристрої не керуються.

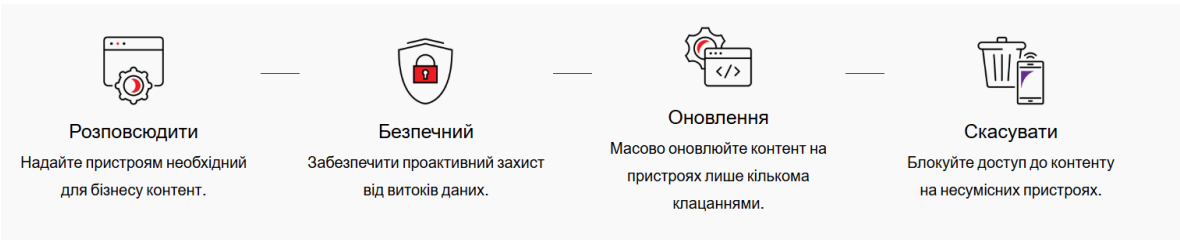


Рис.2.6. Управління доступом до корпоративного контенту, електронної пошти та робочих просторів

Захист особистих пристроїв (BYOD)

Дана характеристика дозволяє гнучко реєструвати мобільні примтрої відповідно до концепції BYOD, за рахунок ізоляції мобільного контенту та забезпечення повної конфіденційності.

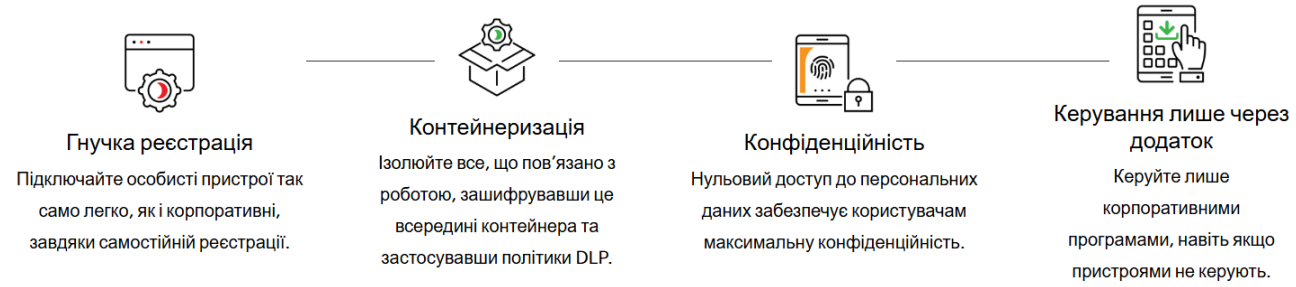


Рис.2.7. Захист особистих пристроїв

2.3. Рольовий доступ до пристрої для управління користувачами

Кожний адміністратор, часто відчуває вплив від звичайної рутинної роботи. Mobile Device Manager Plus надає можливість адміністратору призначати певні ролі з різними привілеями для інших технічних спеціалістів за допомогою модулів User & Role-Based Device Management.

Рольовий доступ до пристрою (RBDA)

Модуль даної технології дозволяє вибирати ролі з найбільш часто використовуваних ролей в розділі «Попередньо визначені ролі». Крім цього є можливість визначати ролі, які найкраще відповідають вимогам організації, у межах ролей, визначених користувачем, і надавати відповідні дозволи. Надаймо короткий опис попередньо визначених користувачем ролей.

Визначена користувачем роль

Mobile Device Manager Plus дозволяє створити будь-яку кількість ролей за допомогою і надати їм дозволи на свій вибір відповідно до потреб організації. Ці налаштовані ролі належать до категорії, визначеної користувачем. За допомогою цього адміністратор може надати користувачам доступ лише до необхідних модулів. Таким чином, необхідно визначити область управління, надаючи доступ лише окремим групам і пристроям. Наприклад, якщо організація має офіси в різних

місцях, адміністратор може дозволити користувачам переглядати пристрої та керувати ними лише у своїх місцях.

Розглянемо алгоритм, як створити роль, визначену користувачем. Щоб створити нову роль, визначену користувачем, необхідно виконати наступні дії.

На веб-консолі обрати вкладку «Адміністратор» і натиснути «Адміністрування користувачів». Відкриється сторінка адміністрування користувачів.

Вибрати вкладку «Роль» і натисніть кнопку «Додати роль».

Вказати назву ролі та невеликий опис.

Визначення модульного рівня дозволу для ролі можна в розділі Select Control.

Рівні дозволів в загальному випадку поділяються на:

– Повний доступ — для виконання всіх операцій, як адміністратор, для певного модуля.

– Читання — для перегляду лише деталей у цьому модулі.

– Запис — для виконання таких дій, як асоціація та розповсюдження в цьому модулі. Немає дозволу на створення або зміну будь-яких налаштувань у модулі.

– Без доступу - щоб приховати модуль від користувача.

Натиснувши кнопку «Додати», адміністратор створює нову роль.

Роль, яку було створено, відтепер буде доступна в списку ролей модуля «Адміністрування» користувачів на вкладці «Адміністратор». Видалити роль неможливо, якщо ця роль пов’язана навіть з одним користувачем. Однак є можливість змінити рівні дозволів для всіх ролей, визначених користувачем.

Лише адміністратори матимуть дозвіл змінювати дані користувача, створювати чи видаляти користувача.

Mobile Device Manager Plus дозволяє використовувати попередньо визначені ролі. Це можливо зробити у категорії «Попередньо визначені ролі», а саме такі ролі:

– адміністратор;

– технік;

– гість;

– ревізор;

– менеджер IT-активів.

Роль адміністратора означає суперадміністратора, який здійснює повний контроль над усіма модулями. Операції ролі для «Адміністратор», включають:

– Додавання нових користувачів і створення нових ролей;

– Зміна налаштувань поштового сервера;

– Зміна налаштувань проксі;

– Параметри персоналізації, як-от зміна тем, встановлення закінчення сеансу тощо;

– Перегляд журналів дій Mobile Device Manager Plus;

– Резервне копіювання бази даних;

– Має повний доступ до модуля Inventory;

– Має повний контроль над модулем звітів;

– Має повний контроль над модулем Profiles;

– Має повний контроль над модулем додатків;

– Вносити зміни в цю роль суворо заборонено.

Роль «Технік» має чітко визначений набір дозволів для виконання певних операцій. Користувачам із роллю «Технік» заборонено виконувати всі операції, перелічені на вкладці «Адміністратор». Техніку також заборонено використовувати налаштування MDM.

Операції, які можуть виконувати користувачі, пов’язані з роллю «Технік», включають:

– Може виконувати операції сканування.

– Має дозвіл на запис для таких елементів, як інвентаризація, звіти, профілі та програми в управлінні мобільними пристроями.

MDM дозволяє технікам виконувати певні дії для груп. Спеціалісту можна дозволити доступ до різних груп на сервері, додаючи, змінюючи або видаляючи групи залежно від потреб організації.

Інші ролі, які мають повний доступ до керування додатками, керування профілями, керування вмістом, керування оновленнями ОС, дистанційне керування та параметри сповіщень, також матимуть доступ до груп.

Адміністратори з ролями запису для керування додатками, керування профілями та керування вмістом автоматично отримують доступ «Читання» до груп.

Адміністратори з ролями запису для реєстрації автоматично отримують доступ на запис до груп.

Роль гостя зберігає дозвіл лише на читання для всіх модулів — для перегляду, деталей інвентаризації MDM, звітів, профілів і програм мобільних пристроїв. Користувач, пов’язаний із роллю Гість, матиме повноваження сканувати та переглядати інформацію про IT-активи. Вносити зміни в цю роль суворо заборонено.

Роль аудитора спеціально створена для цілей аудиту. Ця роль допоможе надати дозволи аудиторам переглядати деталі інвентаризації програмного забезпечення, перевіряти відповідність ліцензії тощо.

Менеджер IT-активів має повний доступ до модуля управління активами. Менеджер IT-активів може переглядати деталі інвентаризації всіх мобільних пристроїв. Усі інші функції недоступні.

Таким чином, технологія управління доступом на основі ролей (Role-Based Device Access, RBDA) у Mobile Device Manager Plus є критично важливим інструментом для децентралізації управління та підвищення операційної ефективності.

Вона вирішує проблему надмірного навантаження на головного адміністратора, дозволяючи безпечно делегувати рутинні завдання іншим технічним спеціалістам, аудиторам або менеджерам.

Технологія надає два рівні гнучкості:

– Попередньо визначені ролі: Набір із п'яти фіксованих ролей (Адміністратор, Технік, Гість, Ревізор, Менеджер IT-активів) забезпечує швидке

налаштування для найпоширеніших сценаріїв використання, кожна з чітко визначеними правами.

– Визначені користувачем ролі: Можливість створювати необмежену кількість кастомних ролей дозволяє організації точно реалізувати принцип найменших привілеїв.

Ключовою перевагою є можливість гранулярного налаштування дозволів (Повний доступ, Запис, Читання, Без доступу) для кожного окремого модуля платформи. Крім того, функція обмеження області управління (scoping) дозволяє призначати ці ролі лише для конкретних груп пристроїв (наприклад, за географічним розташуванням офісу), що є необхідним для масштабованих та територіально-розподілених організацій.

Висновки 2 розділу

1. Отримано локальну та хмарну архітектуру Mobile Device Manager Plus, яка показує компоненти та основні можливості підключення мобільних пристрої до корпоративної інформаційної системи організації.

2. Отримано ключові характеристики Mobile Device Manager Plus в основу яких покладено життевий цикл мобільного пристрою, та життевий цикл роботи додатку.

3. Надано основні етапи створення ролей на основі технології управління доступом на основі ролей (Role-Based Device Access, RBDA) у Mobile Device Manager Plus, яка критично важливим інструментом для децентралізації управління та підвищення операційної ефективності.

3 ТЕХНОЛОГІЯ УПРАВЛІННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ ОРГАНІЗАЦІЇ НА БАЗІ MOBILE DEVICE MANAGER PLUS

3.1. Технологія комплексної моделі життєвого циклу мобільного пристрою

Ефективне управління мобільними пристроями (MDM) є циклічним процесом, який охоплює весь життєвий цикл мобільного пристрою в корпоративній інформаційній системі. На базі платформи Mobile Device Manager Plus цей процес можна розділити на чотири ключові етапи, які забезпечують повний контроль та безпеку.

Загальний життєвий цикл управління мобільним пристроєм (рис.3.1):

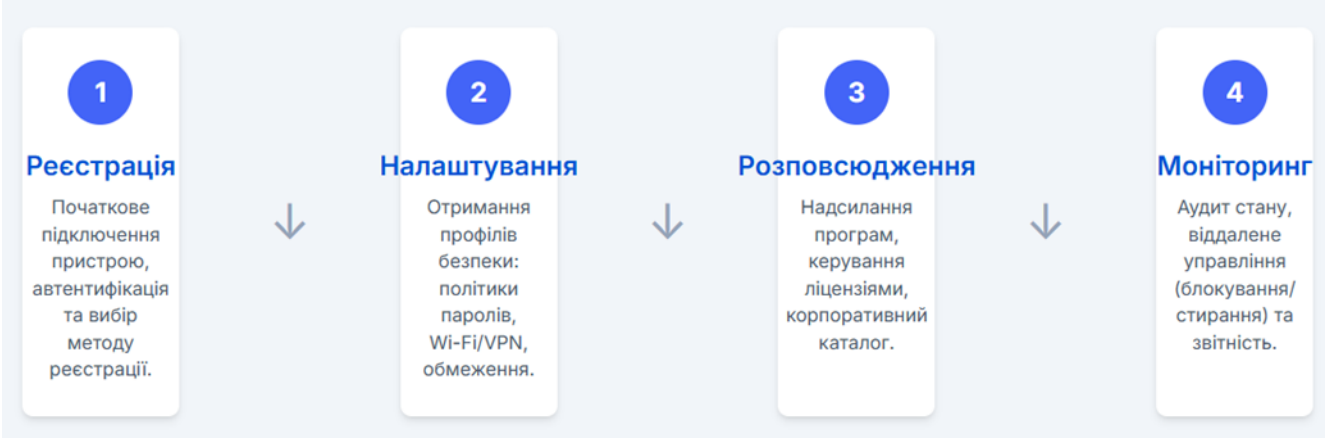


Рис.3.1. Загальний життєвий цикл управління мобільним пристроєм

1. *Етап 1. Реєстрація пристроїв (Enrollment).* Це початковий етап підключення пристрою до системи управління. Він включає автентифікацію користувача та вибір методу реєстрації (самостійна, за запрошенням, масова).

2. *Етап 2. Налаштування політик (Policy Configuration).* Після реєстрації пристрої автоматично групуються та отримують необхідні профілі безпеки: політики паролів, налаштування Wi-Fi/VPN, обмеження (камера, веб-вміст) та конфігурації пошти.

3. *Етап 3. Розповсюдження програм (App Distribution).* На керовані пристрої надсилаються необхідні корпоративні або публічні програми, керуються ліцензії та налаштовується корпоративний каталог додатків.

4. *Етап 4. Моніторинг та Звітність (Monitoring & Reporting).* Це безперервний процес моніторингу стану пристрою, аудиту відповідності політикам, віддаленого управління (блокування/стирання) та створення детальних звітів.

Далі розглянемо кожен етап детально.

Етап 1: Деталізація процесу реєстрації пристроїв

Реєстрація є фундаментальним етапом, який починається з автентифікації користувача та пристрою (рис.3.2).

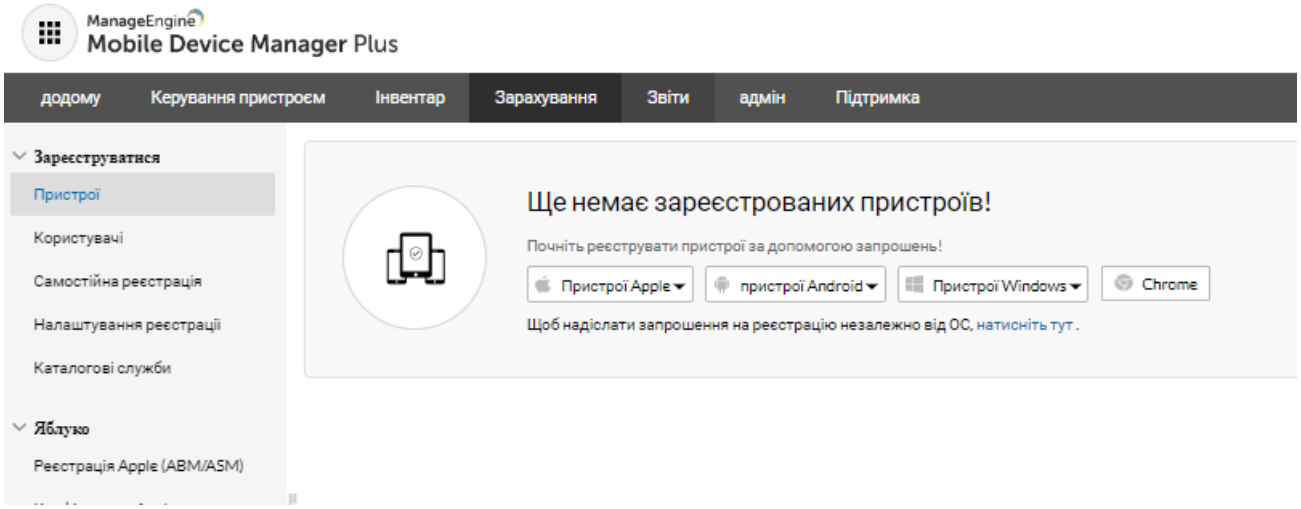


Рис. 3.2. Етап початку реєстрації пристроїв

Автентифікація користувачів

Mobile Device Manager Plus підтримує гнучкі методи автентифікації:

– *Одноразовий пароль (OTP)* Адміністратор надсилає користувачеві запрошення на реєстрацію, яке містить унікальний одноразовий пароль. Цей пароль дійсний 7 днів і може бути використаний лише один раз для реєстрації одного пристрою.

– *Автентифікація Active Directory (AD/Azure).* Є обов'язковою для методу самостійної реєстрації. Користувачі використовують свої корпоративні облікові дані для підтвердження особи.

Методи реєстрації пристроїв

Платформа пропонує гнучкі методи реєстрації, які поділяються на дві категорії:

1. Користувацькі методи (рекомендовані для BYOD)

– *Через запрошення.* Адміністратор надсилає індивідуальні запрошення (з OTP або обліковими даними AD) на електронні пошти користувачів.

– *Самостійна реєстрація.* Кінцеві користувачі можуть самостійно реєструвати пристрої, перейшовши за єдиною URL-адресою (http://<ім’я сервера:номер порту>/MDM/enroll).

2. Адміністративні методи (рекомендовані для корпоративних пристроїв)

– *Масова реєстрація***:** Дозволяє одночасно реєструвати велику кількість пристроїв шляхом завантаження .csv файлу з даними користувачів (ім'я, домен, email, платформа, власник) .

– *Реєстрація адміністратора (Apple Business Manager, Apple Configurator)*. Ці методи забезпечують *обов'язкове управління*, тобто користувач не може скасувати реєстрацію MDM з пристрою. Вони також дозволяють "Нагляд за пристроями" (Supervision) для глибшого контролю, наприклад, тихого встановлення програм.

Налаштування самостійної реєстрації (для BYOD)

Оскільки URL-адреса самореєстрації є загальнодоступною, MDM дозволяє адміністраторам налаштувати суворі обмеження:

1. *Обмеження за групами AD***.** Можна дозволити реєстрацію лише певним групам AD (наприклад, "IT_Відділ") або дозволити всім, за винятком певних груп.

2. *Обмеження за кількістю пристроїв.* Щоб уникнути проблем з безпекою, адміністратор може встановити ліміт пристроїв, які один користувач може зареєструвати (наприклад, "2 пристрої на користувача").

3. *Автоматичне призначення груп.* Пристрої можна автоматично додавати до певних груп на основі платформи (iOS/Android) або типу власності (особистий/корпоративний). Це дозволяє миттєво застосувати до них необхідні політики (Етап 2) одразу після реєстрації.

Обов'язкова передумова для iOS: Створення сертифікату APN

Для керування пристроями Apple (iOS та Mac) сервер MDM повинен мати зв'язок зі службами Apple Push Notification (APN). Це вимагає одноразового створення сертифікату APN.

Рекомендація: Слід використовувати загальну корпоративну пошту (Apple ID), а не особисту, оскільки сертифікат потребує щорічного оновлення.

Процес створення APN показано на рис 3.3 та рис.3.4.

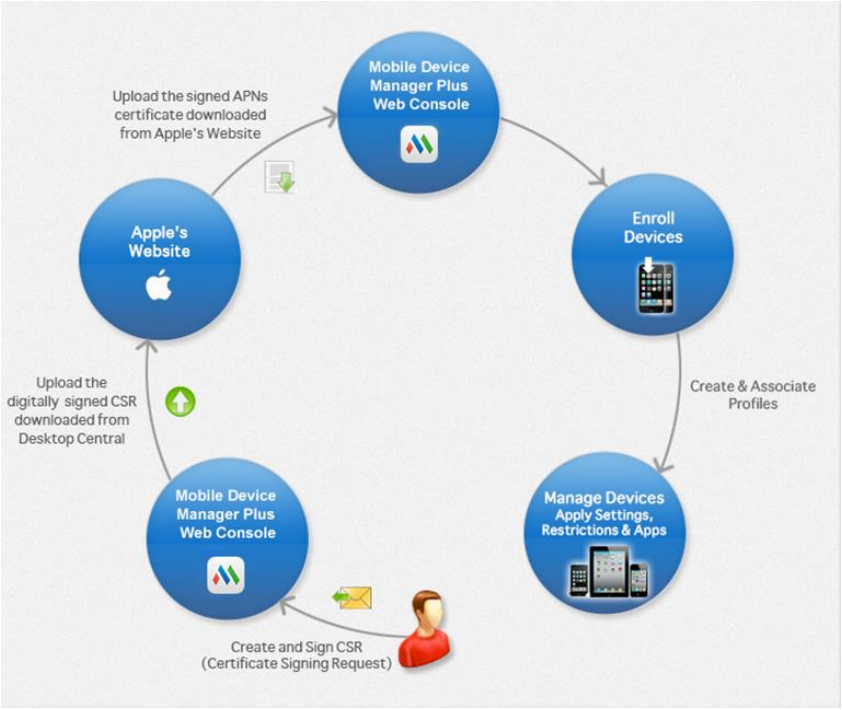


Рис.3.3. Процес створення APN

1. На консолі MDM завантажити CSR (запит на підписання сертифіката), підписаний ManageEngine.

2. Увійти на портал Apple Push Certificate Portal, використовуючи корпоративний Apple ID.

3. Натиснути «Створити сертифікат» та прийняти умови.

4. Завантажити раніше отриманий CSR-файл.

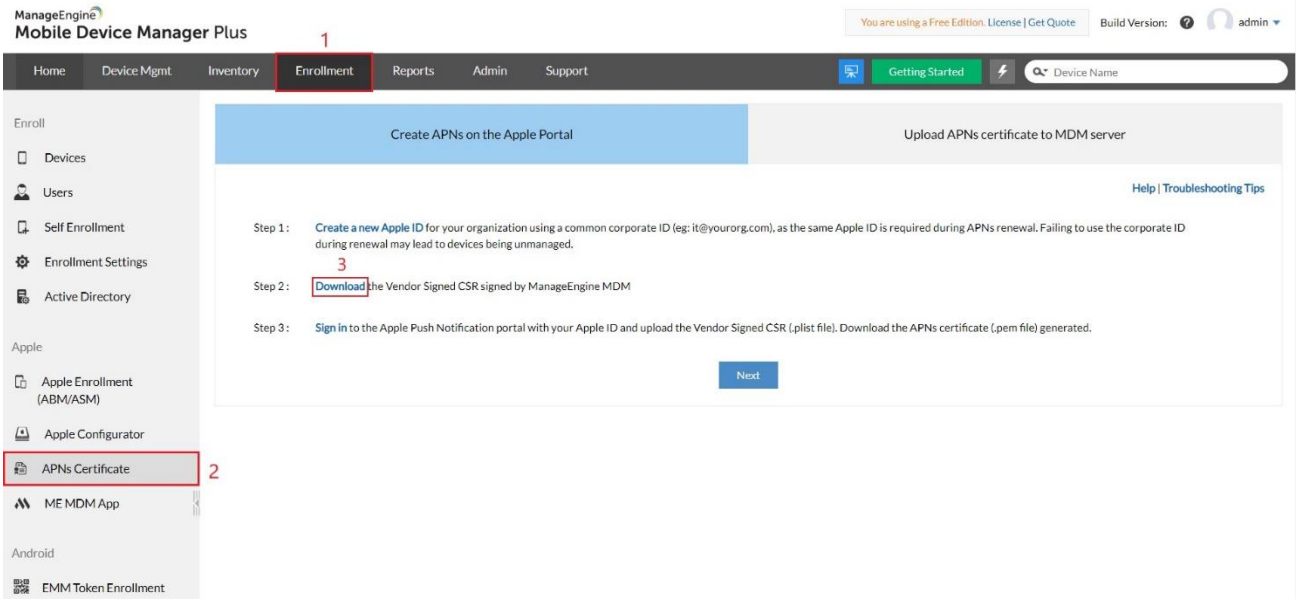


Рис.3.4. Завантаження CSR, підписаного постачальником

5. Завантажити з порталу Apple згенерований сертифікат (.pem).

6. Повернутися до консолі MDM та завантажити цей .pem файл, вказавши Apple ID, який використовувався для його створення.

7. Після успішного завантаження (Рис. 3.5 та рис.3.6) система готова до реєстрації пристроїв Apple.

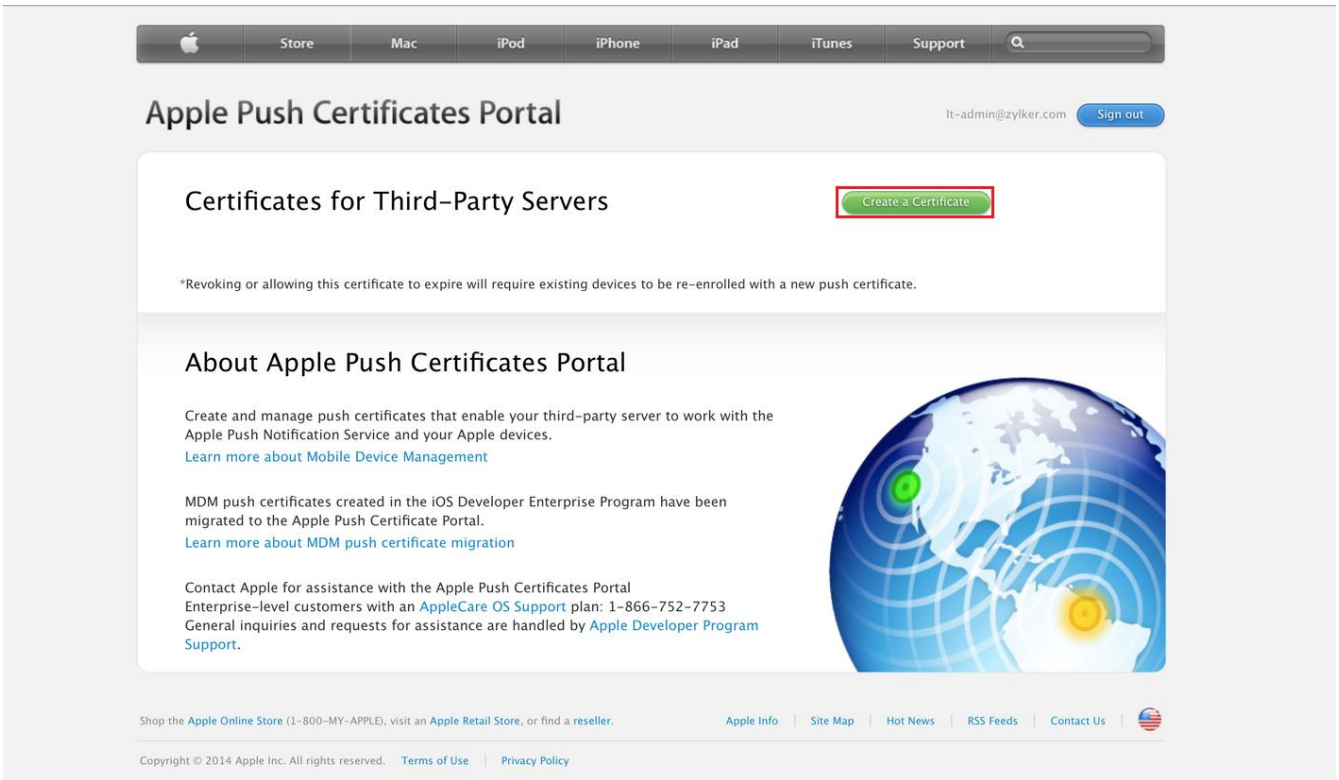
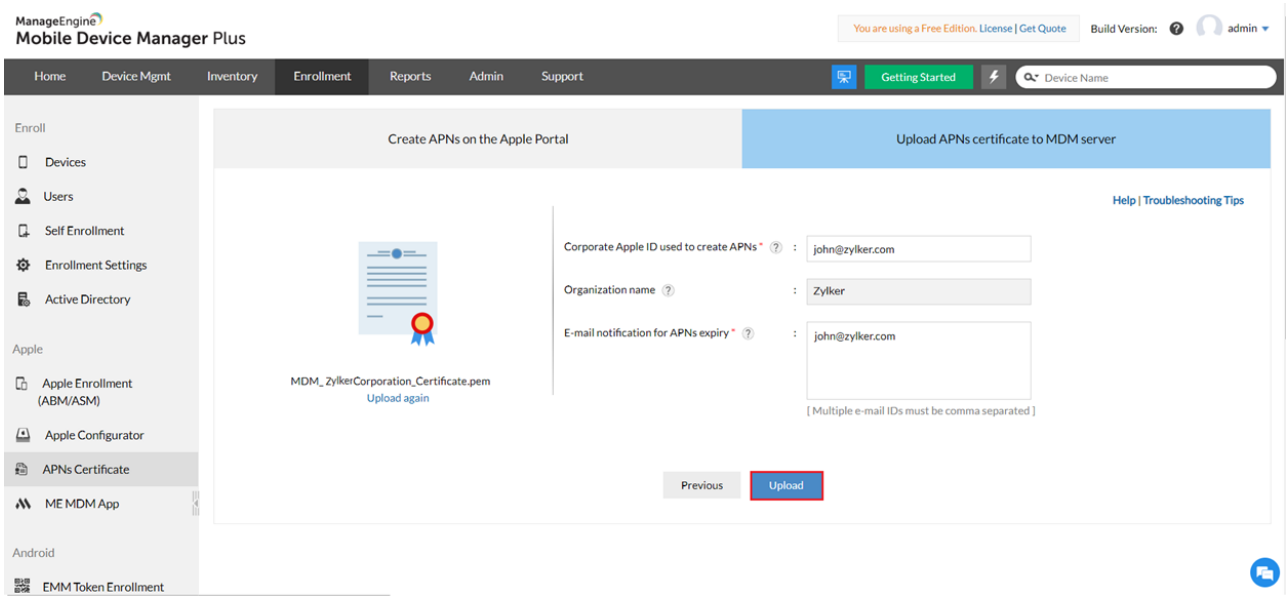


Рис.3.5. Створення сертифікату на порталі Apple



3.6. Успішна реєстрація сертифікату APN [10]

Етап 2: Налаштування та розповсюдження політик

Після успішної реєстрації пристрою (Рис. 3.5) він має бути автоматично або вручну доданий до групи (Рис. 3.6). Платформа MDM дозволяє створювати профілі та політики для груп пристроїв (рис.3.7).

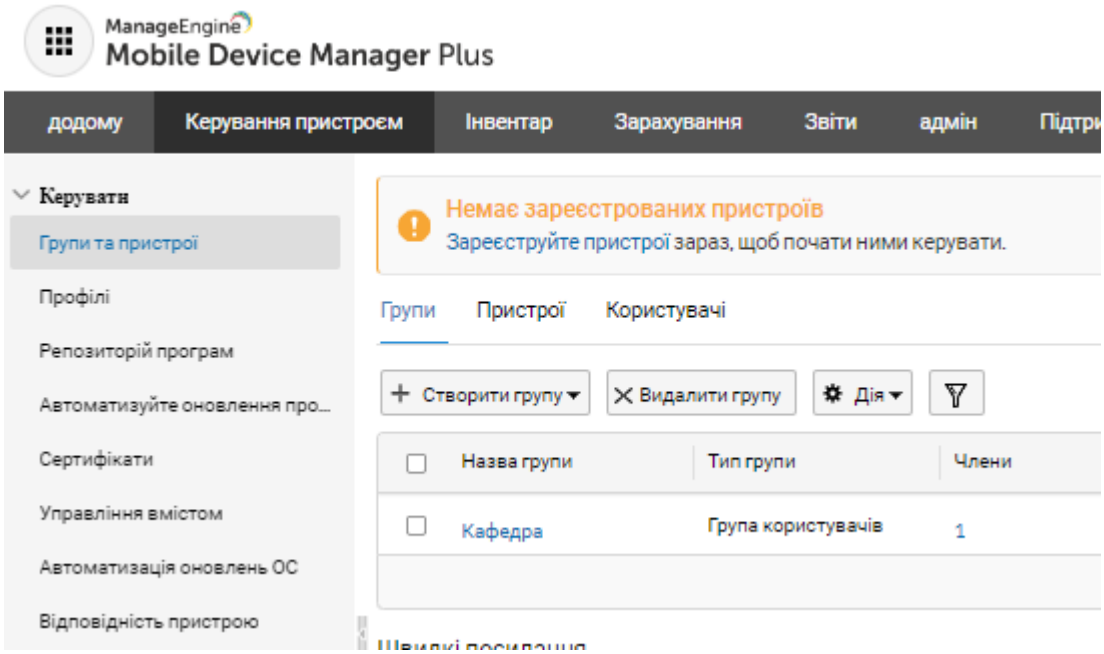


Рис. 3.7. Створення групи пристроїв [10]

Основні політики включають:

– *Безпека.* Налаштування складності пароля, політики шифрування, обмеження камери, Bluetooth тощо.

– *Мережа.* Автоматичне налаштування корпоративних Wi-Fi, VPN та поштових клієнтів (Exchange ActiveSync).

– *Обмеження.* Блокування доступу до певних веб-сайтів, програм (наприклад, App Store) або функцій пристрою.

– *Режим термінала (Kiosk Mode).* Блокування пристрою для роботи лише з однією або визначеним набором програм.

Етап 3: Управління програмами та контентом

Цей етап передбачає надання користувачам необхідних робочих інструментів.

– *Розповсюдження програм:* Адміністратор може надсилати (push) корпоративні (внутрішні) або публічні (з App Store/Play Market) програми на пристрої.

– *Каталог додатків:* Користувач бачить на своєму пристрої корпоративний "App Catalog", звідки може самостійно встановлювати дозволені програми.

– *Управління ліцензіями:* Платформа дозволяє керувати оптовими закупівлями програм (через Apple VPP або Android Managed Google Play).

– *Встановлення агента ME MDM.* На зареєстровані пристрої розповсюджується додаток ME MDM. Цей додаток надає розширений контроль, зокрема дозволяє відстежувати геолокацію пристрою (Рис. 3.8) та ідентифікувати пристрої зі зламаною ОС (Rooted/Jailbroken).

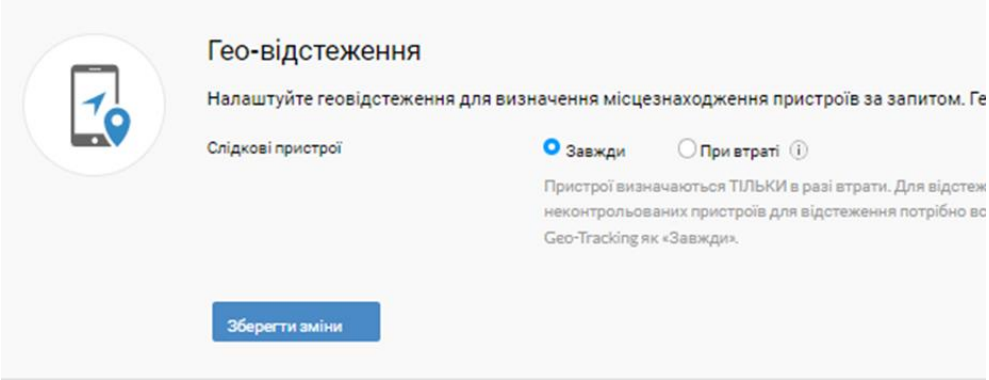


Рис. 3.8. Геолокація пристроїв [10]

Етап 4: Моніторинг, аудит та звітність

Управління є безперервним процесом, що вимагає постійного моніторингу.

– *Моніторин.* Інтуїтивно зрозуміла інформаційна панель надає адміністратору огляд стану всіх пристроїв.

– *Віддалені дії.* У разі втрати або крадіжки пристрою адміністратор може дистанційно його заблокувати, подати звуковий сигнал або стерти корпоративні дані (Selective Wipe) чи весь пристрій (Full Wipe).

– *Аудит відповідності*. Система автоматично перевіряє пристрої на порушення політик (наприклад, встановлення заборонених програм) та сповіщає адміністратора.

– *Звітність* (Рис. 3.9). Платформа надає потужні інструменти для створення детальних звітів за різними категоріями:

- Звіти про додатки. Встановлені програми, пристрої з програмами з "чорного списку".
- Звіти про обладнання: Пристрої за моделлю, деталі SIM-карти, історія батареї.
- Звіти про реєстрацію: Неактивні пристрої, пристрої за часом реєстрації.
- Звіти про місцезнаходження: Історія переміщень, статус гео-відстеження.
- Звіти безпеки: Пристрої Jailbroken/Rooted, стан шифрування, статус режиму втрати, атестація пристрою.

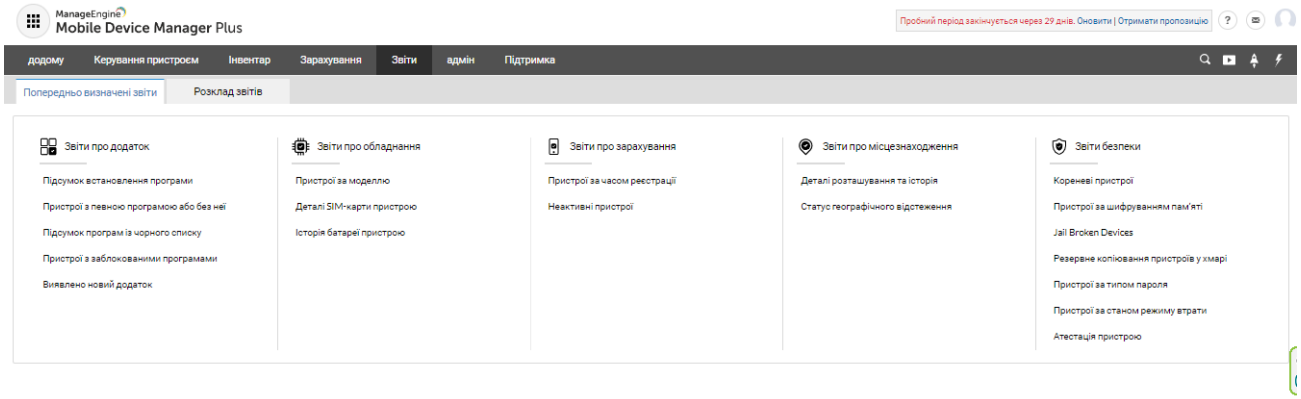


Рис. 3.9. Меню створення звітів [10]

Отже, запропонована технологія полягає в обґрунтуванні та розробці комплексної 4-етапної моделі життєвого циклу мобільного пристрою (реєстрація, налаштування, розповсюдження, моніторинг), яка, на відміну від фрагментарних підходів, розглядає управління мобільним користувачем як єдиний, автоматизований та безперервний процес.

3.2. Рекомендації щодо впровадження Mobile Device Manager Plus в інфораційній системі організації

Найкращі практики MDM полегшують роботу адміністраторів інформаційної системи організації за рахунок упорядкованих кроків:

1. Автоматизація завдань з управління.
2. Впровадження комплексних політик безпеки.
3. Забезпечення безпечної доступності до корпоративних ресурсів.
4. Використання заходів для забезпечення конфіденційності BYOD.
5. Перепризначення пристроїв, щоб отримати від них максимум користі.

Рис. 3.10. Основні кроки для ефективного управління

Автоматизація завдання з управління часто заощаджує час адміністраторів, який можна витратити на більш продуктивну діяльність. Для цього слід уникати ручних та повторюваних завдань, виконуючи наступні кроки:

Реєструйте та налаштовуйте пристрої масово.

Забезпечте автоматичну реєстрацію ваших корпоративних пристроїв за допомогою готових інструментів реєстрації, таких як Android zero-touch enrollment, Apple Business Manager, Apple School Manager та Windows Autopilot.

Додатково, можна налаштувати MDM- рішення так, щоб воно автоматично забезпечувало пристрої необхідними політиками, програмами та контентом одразу після реєстрації. Це усуне необхідність вручну налаштовувати кожен пристрій перед тим, як роздати їх усім вашим співробітникам, заощадивши купу часу. Пасивно стежте за вашими керованими пристроями, автоматизуючи звіти про їхні деталі, програми та стан безпеки, а також будь-яку іншу інформацію, яка допоможе бути в курсі їхнього стану та приймати обґрунтовані рішення. Це також звільнить від необхідності вручну моніторити керовані пристрої.

Впроваджуйте комплексні політики безпеки. Зі зростанням загроз безпеки, надзвичайно важливо підтримувати мобільні кінцеві точки у вашій організації захищеними. Сфери, на яких слід зосередитися, щоб забезпечити безпеку пристроїв:

Підтримуйте відповідність пристроїв. Налаштуйте пристрої так, щоб вони відповідали політикам безпеки вашої організації, керуючи їхніми налаштуваннями на гранулярному рівні, впроваджуючи обмеження та блокуючи будь-які непотрібні функції пристроїв. Наприклад, блокування основних функцій, таких як камера та мікрофон, запобігає їхньому використанню для витоку корпоративних даних та розмов. Ви також можете примусово ввімкнути шифрування пристрою та вимагати пароль блокування, щоб захистити дані на пристрої від несанкціонованого доступу.

Забезпечення безпечної доступності до корпоративних ресурсів. Забезпечте безпечні комунікації. Захист даних від атак типу "людина посередині" (man-in-the-middle) може дати змогу вашій мобільній робочій силі функціонувати віддалено без будь-яких турбот. Щоб захистити дані при передачі, можна налаштувати пристрої

на підключення лише до відомих Wi-Fi з'єднань та на автоматичне встановлення VPN-з'єднання при запуску робочої програми. Також при можливості необхідно налаштувати SSO для безпечного, зручного доступу до корпоративних даних та розповсюджувати сертифікати безпеки, щоб підтримувати підключені пристрої перевіреними. Додатково, налаштуйте безпечні протоколи безпеки, які будуть використовуватися, коли співробітники надсилають або отримують електронні листи, для додаткової безпеки.

Будьте готові вживати реактивних заходів безпеки Хоча вищезгадані політики безпеки слугують проактивними заходами, ви маєте завжди бути готовими на випадок надзвичайної ситуації. Якщо мобільний пристрій загублено, віддалена команда на його блокування зі зміною пароля має захистити дані від несанкціонованого доступу. Щоб захистити пристрій ще більше, ви можете обмежити всі функції пристрою та відстежувати його місцезнаходження, увімкнувши режим втрати (lost mode). Якщо пристрій виявиться неможливим повернути, ви маєте переконатися, що корпоративні дані на ньому не потраплять до чужих рук, стерши всі конфіденційні дані на ньому. Забезпечте безпечну доступність корпоративних ресурсів Якщо робочий пристрій не забезпечений усіма необхідними інструментами, співробітники можуть вдатися до "тіньових IT" (shadow IT) для доступу до ресурсів зі сторонніх джерел. "Тіньові IT" можуть привнести кілька загроз безпеці в мережу організації через неавторизовані та потенційно шкідливі програми. Щоб запобігти цьому, ви маєте переконатися, що всі необхідні ресурси доступні співробітникам.

Встановлюйте безпечні програми з мінімальною взаємодією Переконатися, що всі робочі програми встановлені, - це перший крок до того, щоб ваші співробітники могли використовувати мобільні пристрої для роботи. Встановлюйте критично важливі для бізнесу програми без будь-якого втручання з боку співробітників та додавайте необов'язкові програми до порталу самообслуговування, щоб співробітники мали свободу встановлювати їх за потреби. Також, керуйте та попередньо налаштовуйте дозволи програм, щоб запобігти відмові критичним програмам у необхідних дозволах. Коли програми

потребують оновлення, попереднє тестування оновлень критично важливих бізнес-додатків гарантує, що все працює гладко, тоді як автоматизація оновлень несуттєвих програм економить час. Блокуйте шкідливі програми та веб-вміст Щоб підтримувати корпоративні пристрої в безпеці, слід блокувати встановлення програм, які відомі як шкідливі або походять зі сторонніх джерел. Як додатковий крок, будь-яка програма, що може зашкодити продуктивності співробітників, також має бути заблокована. Блокування доступу до не вартих довіри веб-сайтів також захистить пристрої від веб-загроз та прихованих шкідливих навантажень.

Запобігайте несанкціонованому доступу до даних Окрім програм, співробітникам потрібен доступ до корпоративних документів на їхніх мобільних пристроях. Ви маєте безпечно ділитися цими файлами з пристроями через довірені програми, підтримувати файли оновленими та видаляти їх, коли співробітники їх більше не потребують. Дозвіл лише довіреним пристроям на доступ до корпоративних серверів, автоматизація регулярних атестацій безпеки пристроїв та видалення вразливих пристроїв з мережі можуть допомогти вам налаштувати середовище Нульової Довіри (Zero Trust). Також, переконайтеся, що всі останні патчі безпеки та оновлення ОС протестовані та заплановані до встановлення на пристрої поза робочими годинами.

Вживайте заходів для забезпечення конфіденційності BYOD При роботі з середовищем BYOD часто буває складно запевнити співробітників, що їхні особисті дані не відстежуються IT-адміністраторами. Для цього будь-які особисті пристрої, що підпадають під політику BYOD, мають управлятися інакше, ніж корпоративні пристрої, щоб забезпечити як конфіденційність співробітників, так і безпеку корпоративних даних. Контейнеризуйте та керуйте корпоративними даними На пристроях BYOD має бути створений окремий, віртуальний робочий контейнер. Таким чином, адміністратор може керувати лише цим ізольованим корпоративним робочим простором замість усього пристрою, одночасно сприяючи безпеці корпоративних даних та конфіденційності співробітників. Будь-які спільні робочі ресурси та впроваджені політики безпеки стосуватимуться лише цього контейнера. Щоб запобігти передачі конфіденційних корпоративних даних та

файлів неавторизованим особам, обмежте експорт або копіювання даних за межі корпоративного контейнера.

Перепризначайте пристрої, щоб отримати від них максимум користі. Ви можете усунути необхідність купувати нові пристрої для нових співробітників, перепризначивши пристрої, які вже є у вашому IT-середовищі. Це заощадить вашій організації час та гроші. Коли співробітник залишає вашу організацію, ви можете просто виконати скидання до заводських налаштувань на корпоративному пристрої, який він використовував, перепризначити його новому співробітнику та повторно забезпечити його необхідними програмами, дозволами та контентом.

Безпечне виведення пристроїв з експлуатації Коли пристрої більше не можуть використовуватися або вважаються застарілими, ви можете просто виконати скидання до заводських налаштувань і вивести їх з експлуатації, щоб переконатися, що ніхто не зможе отримати доступ до корпоративних даних через них. У середовищі BYOD потрібна додаткова обережність, щоб не видалити особисті дані на пристрої співробітника, коли він залишає організацію. На такому пристрої має бути виконано корпоративне стирання, щоб видалити лише корпоративний контейнер, залишивши особисті файли співробітника недоторканими.

Ще кілька моментів, про які варто пам’ятати.

Дослідіть різні типи управління пристроями, такі як власник пристрою (device owner), власник профілю (profile owner) та супервізор пристрою (device supervisor), а також рівень можливостей управління, що підтримується для кожного з них, щоб зрозуміти, який метод налаштування (provisioning) відповідає вашим потребам та парку пристроїв.

Дізнайтеся про можливості управління, що підтримуються кожним виробником ОС, перш ніж приймати рішення про покупку. Деякі виробники не підтримують реєстрацію пристроїв, тоді як інші OEM-виробники створюють пристрої з додатковими можливостями управління.

Делегуйте обов'язки з управління пристроями технічним спеціалістам та надайте їм рольовий доступ лише до необхідних модулів сервера. Керуйте рівнем

даних, що збираються з пристроїв, та тим, що відображається на сервері, для забезпечення конфіденційності.

Слідкуйте за журналами сервера та виконуйте регулярні аудити пристроїв та дій з управління, щоб виявити щось незвичайне. Автоматизуйте нагадування про поновлення вашого сертифіката та токенів сервера для служби Apple Push Notification (APNs), щоб забезпечити безперебійне управління вашими пристроями.

Підтримуйте резервні копії сервера та вторинний сервер, щоб зменшити ризик втрати ваших даних.

Отже Mobile Device Manager Plus ManageEngine– це веб-орієнтоване рішення для управління мобільними пристроями, яке допомагає керувати широким спектром пристроїв з центрального розташування. Воно автоматизує повний життєвий цикл управління мобільними пристроями, від реєстрації та захисту пристроїв до управління програмами, профілями та активами.

Висновки до розділу 3

1. Запропоновано технологію Mobile Device Manager Plus ManageEngine, яка полягає в обґрунтуванні та розробці комплексної 4-етапної моделі життєвого циклу мобільного пристрою яка, на відміну від фрагментарних підходів, розглядає управління мобільним користувачем як єдиний, автоматизований та безперервний процес.

2. Розроблено загальні рекомендації по впровадженню та використанню MDM, які полегшують роботу адміністраторів інформаційної системи організації за рахунок упорядкованих кроків роботи з технологією Mobile Device Manager Plus ManageEngine.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було отримано наступні результати:

1. Проведено аналіз проблеми управління мобільними користувачами корпоративної інформаційної системи організації, який показав необхідність впровадження заходів для користувачів мобільних пристроїв з концепцією BYOD для забезпечення захисту корпоративної інфраструктури.

2. Аналіз загроз підтвердив проблему BYOD, яку використовують 70% організацій та дозволив визначити основні категорії загроз.

3. Аналіз підходів до управління пристроями дозволив визначити основні підходи щодо впровадження відповідних технологій управління мобільними пристроями, на основі якого було проведено порівняльний аналіз існуючих технологій та визначено ManageEngine Mobile Device Manager Plus як найбільш повну, гнучку та збалансовану базу, що необхідна для управління мобільними користувачами в середовищі BYOD.

4. Отримано локальну та хмарну архітектуру Mobile Device Manager Plus, яка показує компоненти та основні можливості підключення мобільних пристрої до корпоративної інформаційної системи організації.

5. Отримано ключові характеристики Mobile Device Manager Plus в основу яких покладено життєвий цикл мобільного пристрою, та життєвий цикл роботи додатку.

6. Надано основні етапи створення ролей на основі технології управління доступом на основі ролей (Role-Based Device Access, RBDA) у Mobile Device Manager Plus, яка критично важливим інструментом для децентралізації управління та підвищення операційної ефективності.

7. Запропоновано технологію Mobile Device Manager Plus ManageEngine, яка полягає в обґрунтуванні та розробці комплексної 4-етапної моделі життєвого циклу мобільного пристрою яка, на відміну від фрагментарних підходів, розглядає

управління мобільним користувачем як єдиний, автоматизований та безперервний процес.

8. Розроблено загальні рекомендації по впровадженню та використанню MDM, які полегшують роботу адміністраторів інформаційної системи організації за рахунок упорядкованих кроків роботи з технологією Mobile Device Manager Plus ManageEngine.

ПЕРЕЛІК ПОСИЛАНЬ

1. Принеси власний пристрій. URL: https://www.kingston.com/ua/blog/data-security/bring-your-own-device-workplace-security
2. Gartner. Magic Quadrant for Unified Endpoint Management Tools 2024. Stamford, CT: Gartner Inc., 2024.
3. BYOD Security Market Overview URL: https://www.marketgrowthreports.com/market-reports/byod-security-market-100405
4. Звіт загроз використання мобільних пристроїв. URL: https://zimperium.com/hubfs/Reports/2025%20Global%20Mobile%20Threat%20Report.pdf
5. https://solutionsreview.com/mobile-device-management/mdm-buyers-guide-directory/
6. Архітектура ManageEngine Mobile Device Manager Plus. URL: https://www.manageengine.com/mobile-device-management/mobile-device-manager-plus-architecture.html?help.
7. Enterprise mobility management. URL: https://www.manageengine.com/mobile-device-management/enterprise-mobility-management-emm.html .
8. Управління мобильними пристоями мережі. URL: https://pirit.biz/reshenija/upravlenie-mobilnymi-ustrojstvami .
9. Програмне забезпечення для керування мобільними пристроями URL: https://www.manageengine.com/mobile-device-management/ .
10. Архітектура Mobile Device Manager Plus (MDMURL: https://www.manageengine.com/mobile-device-management/mobile-device-manager-plus-architecture.html?help .
11. Портал Mobile Device Manager Plus URL: https://mdm.manageengine.eu/webclient#/uems/mdm/home .
12. Ісаєнко І.І. Управління мобільними пристроями в сучасному корпоративному середовищі: виклики сьогодення та стратегії подолання. *Актуальні проблеми кібербезпеки:* матеріали всеукраїнської наук.-практ. конф., м. Київ: ДУІКТ, 29 жовт. 2025р. Київ. С 44-45.