Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Порівняння MDM систем в задачах керування мобільними пристроями

Виконав: студент VI курсу, групи САм-61
спеціальності 124 Системний аналіз
(шифр і назва спеціальності)

_____ Пакон О.Д.
(підпис) (прізвище та ініціали)

Керівник _____ Небесний Р.М.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ _____
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ Тиш Є.В.
(підпис) (прізвище та ініціали)

Тернопіль
2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 124 Системний аналіз
(шифр і назва спеціальності)

Студенту Пакон Олег Дмитрович
(прізвище, ім'я, по батькові)

1. Тема роботи Порівняння MDM систем в задачах керування мобільними пристроями

Керівник роботи Небесний Руслан Михайлович, доктор філософії, доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 29 » листопада 2024 року № 4/7-1140

2. Термін подання студентом завершеної роботи 20 грудня 2024р.

3. Вихідні дані до роботи літературні джерела та наукові публікації з теми дослідження

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. Розділ 1. Огляд систем керування мобільними пристроями,
Розділ 2. Порівняльний аналіз систем керування мобільними пристроями
Розділ 3. Практичне дослідження MDM систем на прикладі knox manage та soti mobicontrol
Розділ 4. Охорона праці і безпека в умовах надзвичайних ситуацій
Висновки. Перелік джерел. Додатки(Додаток А, Публікації).

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1 Титульна сторінка. 2 Актуальність теми. 3 Визначення MDM систем. 4 Технології та протоколи систем керування мобільними пристроями. 5 Платформа Samsung Knox. 6 Особливості платформи Samsung Knox. 7 Платформа SOTI. 8 Особливості платформи SOTI. 9 Порівняння Knox Manage та SOTI MobiControl. 10 Ієрархія компонентів систем. 11 Заведення пристроїв. 12 Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Сенчишин В.С., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., ст. викладач		

7. Дата видачі завдання 15 листопада 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	15.11.2024	*Виконано*
2.	Підбір наукових джерел про мобільні пристрої та	16.11.2024-18.12.2024	*Виконано*
	системи керування мобільними пристроями		
3.	Опрацювання наукових публікацій та збір даних по	18.11.2024-22.11.2024	*Виконано*
	темі роботи		
4.	Виконання дослідження згідно мети кваліфікаційної	22.12.2024-25.11.2024	*Виконано*
	роботи		
5.	Оформлення розділу «Огляд систем керування	25.12.2024-02.12.2024	*Виконано*
	мобільними пристроями»		
6.	Оформлення розділу «Порівняльний аналіз систем	02.12.2024-10.12.2024	*Виконано*
	керування мобільними пристроями»		
7.	Оформлення розділу «Практичне дослідження MDM	10.12.2024-13.12.2024	*Виконано*
	систем на прикладі knox manage та soti mobicontrol»		
8.	Виконання завдання до підрозділу «Охорона праці»	13.12.2024-14.12.2024	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в	14.12.2024-15.12.2024	*Виконано*
	надзвичайних ситуаціях»		
10.	Оформлення кваліфікаційної роботи	15.12.2024-16.12.2024	*Виконано*
11.	Нормоконтроль	16.12.2024-17.12.2024	*Виконано*
12.	Перевірка на плагіат	18.12.2024	*Виконано*
13.	Попередній захист кваліфікаційної роботи	20.12.2024	*Виконано*
14.	Захист кваліфікаційної роботи	23.12.2024	

Студент _____ Пакон О.Д.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Небесний Р.М.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Порівняння МДМ систем в задачах керування мобільними пристроями // Кваліфікаційна робота освітнього рівня «Магістр» // Пакон Олег Дмитрович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група САм-61 // Тернопіль, 2024 // С. 69, рис. – 20, табл. – 0, кресл. – 0, додат. – 1, бібліогр. – 55.

Ключові слова: система керування мобільними пристроями, мобільні пристрої, smasung knox, soti.

У першому розділі кваліфікаційної роботи розглянуто актуальність теми, основні поняття та можливості систем керування мобільними пристроями (MDM).

У другому розділі кваліфікаційної роботи проведено порівняльний аналіз систем MDM на прикладі платформ Samsung Knox і SOTI. Проаналізовано історію розвитку кожної платформи, їх функціональні особливості та інструменти управління.

У третьому розділі кваліфікаційної роботи розглянуто практичний аспект роботи з MDM системами на прикладі Knox Manage та SOTI MobiControl. Проведено огляд веб-консолей, налаштування інфраструктури систем, огляд інструментів управління пристроями та зроблено підсумки дослідження.

У четвертому розділі розглянуто питання охорони праці та безпеки в умовах надзвичайних ситуацій. Проаналізовано механізми мінімізації впливу іонізуючих випромінювань на працівників підприємств та моделі оповіщення населення в умовах техногенних і природних надзвичайних ситуацій.

ANNOTATION

Comparison of MDM Systems in Mobile Device Management Tasks // The educational level "Master" qualification work // Oleh Dmytrovych Pakon // Ternopil Ivan Pulyuy National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Science, SAm-61 group // Ternopil, 2024 // P. 63, fig. - 14, tables - 17, posters - 17, annexes - 2, ref. - 55.

Key words: mobile device management system, mobile devices, samsung knox, soti.

The first chapter of the qualification work examines the relevance of the topic, key concepts, and capabilities of mobile device management (MDM) systems.

The second chapter provides a comparative analysis of MDM systems using Samsung Knox and SOTI platforms as examples. The history of each platform's development, functional features, and management tools are analyzed.

The third chapter focuses on the practical aspects of working with MDM systems using Knox Manage and SOTI MobiControl as examples. It reviews web consoles, system infrastructure settings, device management tools, and presents the conclusions of the research.

The fourth chapter addresses occupational safety and emergency response issues. It analyzes mechanisms to minimize the impact of ionizing radiation on enterprise workers and models for alerting the population in technological and natural emergencies.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

MDM (англ. Mobile Device Management) – Система керування мобільними пристроями.

Zero-touch реєстрація – Реєстрація пристроїв в MDM систему без необхідності додаткового налаштування.

EMM (англ. Enterprise Mobility Management) – Набір рішень і технологій, зосереджених на управлінні мобільними пристроями.

FOTA (англ. Firmware Over-The-Air) – Технологія оновлення прошивки пристроїв через бездротове з'єднання.

ОС (Операційна система) — комплекс програмного забезпечення, яке управляє апаратними ресурсами пристрою і забезпечує виконання інших програм.

IoT - концепція, яка описує мережу фізичних пристроїв, оснащених сенсорами, програмним забезпеченням та іншими технологіями для збору, обміну та обробки даних через Інтернет.

ЗМІСТ

ВСТУП

Актуальність теми. Організації все частіше використовують смартфони та планшети як основні робочі інструменти, що створює нові виклики у забезпеченні їхньої безпеки та контролю, тому управління мобільними пристроями стало критично важливим завданням.

Мета і задачі дослідження. Метою даної роботи є аналіз методів та технологій управління мобільними пристроями на основі систем Knox Manage та SOTI MobiControl, а також порівняння їх ефективності для корпоративного використання.

Для досягнення поставленої мети потрібно вирішити наступні завдання:

– Проаналізувати сучасні тенденції використання мобільних пристроїв у бізнес-середовищі.

– Дослідити принципи роботи MDM-систем та їх роль у корпоративній безпеці.

– Провести порівняльний аналіз систем Knox Manage та SOTI MobiControl.

– Визначити основні переваги та недоліки досліджуваних рішень.

Об’єкт дослідження є системи керування корпоративними мобільними пристроями.

Предмет дослідження. Системи керування мобільними пристроями Knox Manage та SOTI MobiControl.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у тому, що отримала подальший розвиток методика керування мобільними пристроями.

Практичне значення одержаних результатів. Проведено дослідження щодо того, як за допомогою різних систем керування мобільними пристроями можна ефективно управляти корпоративними пристроями. В результаті отримано перелік необхідних характеристик та передумов для вибору MDM-системи.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на XIII Міжнародна науково-технічна

конференція молодих учених та студентів «Актуальні задачі сучасних технологій» Тернопільського національного технічного університету імені Івана Пулюя (м. Тернопіль, 2024 р.).

Публікації. Основні результати кваліфікаційної роботи опубліковано у двох працях конференції (Див. додатки А).

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури з 55 найменувань та 1 додатків. Загальний обсяг кваліфікаційної роботи складає 69 сторінки, з них 50 сторінки основного тексту, який містить 20 рисунків та 0 таблиць.

1 ОГЛЯД СИСТЕМ КЕРУВАННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ

1.1 Актуальність теми та мета дослідження

Враховуючи, що організації залучаються до ініціативи цифрової трансформації та адаптуються до динамічних бізнес-вимог, їхні IT-активи зростають, змінюються та постійно переміщуються з одного місця в інше [54]. Замість набору настільних комп'ютерів, підключених до корпоративної мережі, бізнес все більше покладається на мобільні пристрої для ключових бізнес-функцій. Ця тенденція зумовлена кількома різними факторами. Пандемія COVID-19 підштовхнула компанії до віддаленої роботи, що зумовило поширення політики «принеси свій пристрій», яка дозволяє мати доступ до корпоративних ресурсів навіть з особистого пристрою. Щороку компанії збільшують кількість пристроїв, що належать та управляються компаніями. З цим зростанням використання мобільних пристроїв виникає потреба в управлінні та захисті цих пристроїв. Ефективне та масштабоване управління вимагає рішення для управління мобільними пристроями [6].

Управління мобільними пристроями у компаніях стає все більш важливим з огляду на питання безпеки. Велика кількість людей використовують смартфони для доступу до критично важливих даних компанії. Інструменти, які називаються системами управління мобільними пристроями, стають все більш необхідними. Це швидко зростаючий ринок, який стрімко зростає з року в рік. У 2012 році ринкова вартість перевищила 500 мільйонів доларів з більш ніж ста постачальниками програмного забезпечення, тоді як у 2015 році ринкова вартість вже становила 2 мільярди доларів. У 2019 року ринкова вартість MDM була на рівні 3,94 мільярда доларів [1]. Основна мета MDM - захистити корпоративну ресурси, забезпечуючи безпеку та оптимізацію мобільних пристроїв, включаючи смартфони, планшети та інші мобільні пристрої, які підключаються до корпоративних мереж. Окрім підвищення безпеки бізнес-мереж, це також дозволяє співробітникам використовувати свої власні пристрої, а не надані компанією, щоб працювати більш ефективно та продуктивніше [2].

Android наразі є найбільш використовуваною операційною системою на мобільному ринку, як показано на рисунку 1.1.

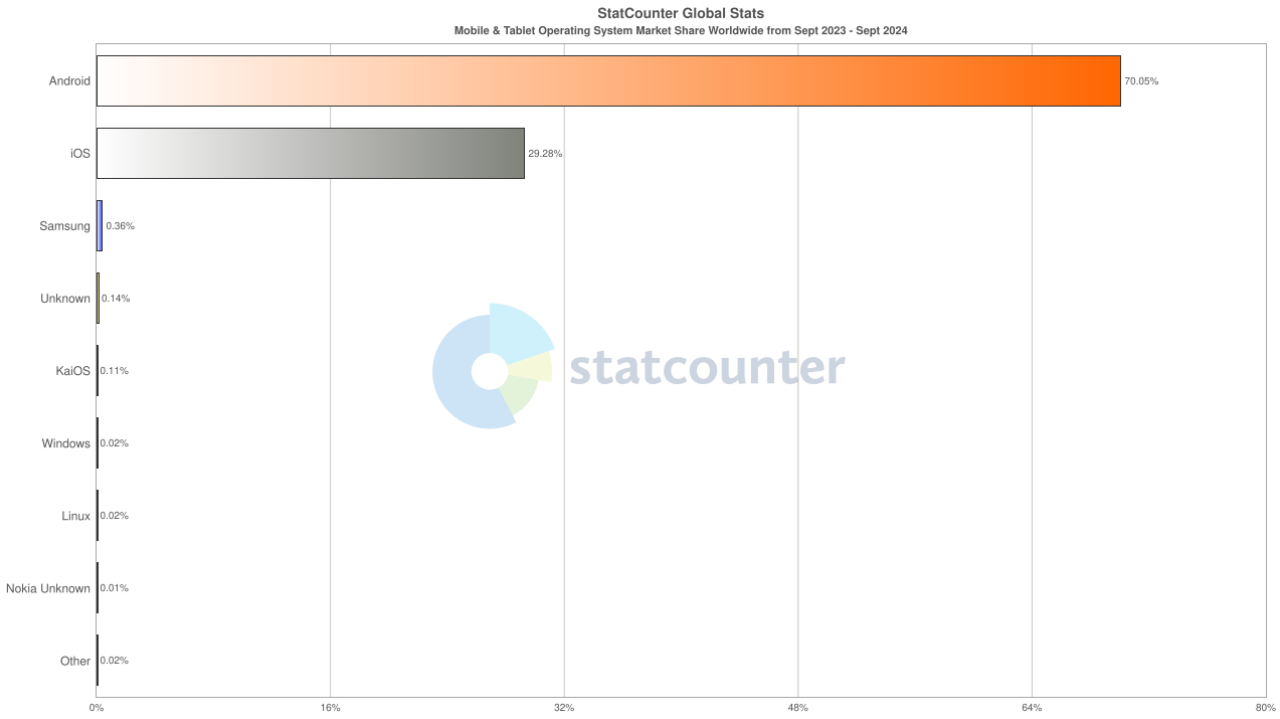

Рисунок 1.1 - Найбільш використовувані операційні системи в мобільних пристроях

Як показують наведені вище статистичні дані, рішення MDM не може зосереджуватися лише на Android, а також повинно пропонувати підтримку інших систем.

Метою дослідження є аналіз основних принципів та підходів до управління мобільними пристроями за допомогою MDM-систем, а також визначення їхньої ролі в сучасній корпоративній інфраструктурі. На основі прикладів систем Knox Manage і SOTI був здійснений порівняльний огляд різних підходів до MDM, що дозволив виявити сильні та слабкі сторони таких рішень і зрозуміти, які функції є критично важливими для організацій різного масштабу.

1.2 Основні поняття та можливості MDM

Системи керування мобільними пристроями являють собою набір технологій і сервісів, що дозволяють організаціям забезпечувати безпеку та контроль за мобільними пристроями, які використовуються їхніми співробітниками. До таких пристроїв належать смартфони, планшети та спеціалізовані комп'ютери, наприклад, термінали збору даних чи мобільні платіжні пристрої. Поняття MDM охоплює широкий спектр інструментів і протоколів. Головною метою цих систем є забезпечення безпечного управління мобільними пристроями, які мають доступ до корпоративної мережі. Водночас важливим аспектом є контроль не стільки за пристроями, скільки за програмами, що на них встановлені [3].

MDM - це рішення, яке використовує програмне забезпечення як компонент для налаштування мобільних пристроїв, захищаючи активи організації, такі як дані чи самі мобільні пристрої. Організації практикують MDM, застосовуючи програмне забезпечення та політики безпеки до мобільних пристроїв і їх використання. Окрім управління кількістю пристроїв і налаштування, рішення MDM захищають корпоративні додатки, дані та вміст пристрою [4].

Мобільні пристрої, незалежно від того, належать вони компанії чи працівнику, відкривають цілком новий набір ризиків для цілісності інформації. Навіть коли дані знаходяться на пристрої, що належить працівнику, організації несуть відповідальність за дотримання їхньої безпеки та цілісності. Існує три області контролю, які слід врахувати при розробці політики:

– Обмежене особисте та ділове використання: Сюди входять програми з білого та чорного списку, а також процеси доступу та аутентифікації.

– Підтримувані пристрої та платформи: Зазвичай підтримуються пристрої Android, iOS та Windows. Пристрої постійно оновлюються, тому важливо забезпечити підтримку різних версій операційної системи. Оскільки мобільні пристрої стають основним робочим інструментом в діловому світі, вони можуть потребувати підтримки.

– Політики/правила: містять інформацію щодо належного використання, правила передачі даних використовуючи безпровідні мережі для повідомлення про втрату пристрою чи порушення політик, а також коли потрібно стерти дані з пристрою або видалити програму.

Політики також окреслюють обов'язки користувача та компанії, брандмауери та програми безпеки, а також обслуговування пристрою. Кожна МДМ система надає ряд інструментів для керування необхідною кількістю пристроїв і захисту інформації на них, також ці інструменти можна налаштувати відповідно до потреб організації [5].

Інструменти для керування мобільними пристроями:

– Інструменти відстежування пристроїв;
– Управління мобільними пристроями;
– Управління безпекою додатків;
– Керування ідентифікаційними даними та доступом;
– Захист пристроїв та мереж.

Розглянемо трішки детальніше, що може кожен із вище перелічених інструментів.

За допомогою інструментів відстежування пристроїв є можливість налаштувати кожен пристрій, який є на балансі підприємства таким чином, щоб він включав GPS-відстеження та інше ПЗ. Це дозволить ІТ-фахівцям підприємства відстежувати, оновлювати та усувати неполадки пристрою в режимі реального часу. Вони також можуть виявляти пристрої з високим ризиком або невідповідними даними розташування та повідомляти про них і навіть віддалено блокувати або стирати дані про пристрій у разі втрати або крадіжки.

ІТ-відділи закуповують, керують і підтримують мобільні пристрої для співробітників, включаючи усунення несправностей функціональних пристроїв. Ці відділи гарантують, що кожен пристрій постачається з необхідними операційними системами та програмами для користувачів компанії, включаючи програми для продуктивності, безпеки та захисту даних, резервного копіювання та відновлення.

Застосування безпеки може включати загортання додатків, при якому IT-адміністратор застосовує функції безпеки або управління до програми. Потім ця програма повторно розгортається як контейнеризована програма. Ці функції безпеки можуть визначати, чи потрібна автентифікація користувача для відкриття програми чи можна копіювати, вставляти або зберігати дані з програми на пристрої і чи може користувач поділитися файлом цієї програми.

Безпечне керування мобільними пристроями вимагає надійного керування ідентифікацією та доступом (IAM). IAM дозволяє підприємству керувати ідентифікаторами користувачів, пов’язаними з пристроєм. Доступ кожного користувача в організації можна повністю регулювати за допомогою таких функцій, як єдиний вхід, багатофакторна автентифікація та рольовий доступ.

Безпека кінцевих пристроїв охоплює всі пристрої, які отримують доступ до корпоративної мережі, включаючи мобільні пристрої та спеціалізовані мобільні пристрої. Вона може включати стандартні інструменти мережевої безпеки, такі як антивірусне програмне забезпечення та контроль доступу до мережі та реагування на інциденти, фільтрація URL-адрес та хмарна безпека [4].

За допомогою цих інструментів можна максимально ефективно уникати проблеми з безпекою та доступом, а також реалізувати гнучке управління мобільними пристроями, що позитивно вплине на продуктивність мобільного сегменту організації [5].

Переваги MDM включають в себе наступне:

– Підвищення продуктивності співробітників;
– Підвищений захист від витоків даних;
– Покращений контроль за мобільними пристроями;
– Зниження витрат на обладнання.

1.3 Можливість керування мобільними пристроями засобами Active Directory

Мобільні пристрої відрізняються від настільних ПК тим, що зазвичай не можуть бути приєднані до домену Active Directory. Коли ПК приєднується до домену Active Directory, створюється обліковий запис комп'ютера як засіб аутентифікації та ідентифікації цього комп'ютера під час його роботи в мережі. Крім того, застосування налаштувань групової політики може забезпечити безпеку ОС комп'ютера, а списки контролю доступу забезпечують механізм контролю доступу до мережевих ресурсів на рівні комп'ютера. Мобільні пристрої є повною протилежністю. Вони не можуть бути приєднані до домену Active Directory і, отже, не має можливості застосувати налаштування групової політики до мобільного пристрою. Раніше одним з найкращих варіантів для забезпечення безпеки мобільних пристроїв, які беруть участь у корпоративній мережі, було використання політик ActiveSync. Вони були вперше представлені в Exchange Server як механізм для надсилання електронної пошти на мобільні пристрої. Згодом Microsoft розширила протокол ActiveSync у спробі дозволити застосування налаштувань безпеки до мобільних пристроїв [7].

Exchange ActiveSync дозволяє користувачам мобільних телефонів отримувати доступ до своєї електронної пошти, календаря, контактів та завдань, а також продовжувати доступ до цієї інформації, коли вони працюють офлайн. Стандартні послуги шифрування додають безпеки мобільному зв'язку з сервером. Exchange ActiveSync включає налаштування шифрування Secure Sockets Layer для зв'язку між сервером Exchange та мобільним пристроєм [8].

ActiveSync став галузевим стандартом для забезпечення синхронізації між Exchange та мобільними пристроями. Кожен великий виробник пристроїв підтримує використання політик ActiveSync як спосіб блокування своїх пристроїв. Однак є кілька проблем, які обмежують ActiveSync як комплексне рішення для безпеки мобільних пристроїв. Перша проблема полягає в тому, що мобільні пристрої підтримують ActiveSync в різному ступені. Політики ActiveSync складаються з набору окремих налаштувань політики. Більшість

мобільних пристроїв, доступних сьогодні, не підтримують всі доступні налаштування політики. Таким чином, адміністраторам не гарантовано, що налаштування політики буде застосовано до кожного пристрою, що використовується в їхній мережі, якщо вони не обмежать доступ до пристроїв, які не повністю підтримують всі налаштування політики (до яких належить більшість типів пристроїв). Інша проблема з використанням ActiveSync для безпеки мобільних пристроїв полягає в тому, що його стало все важче повністю реалізувати. Exchange Server 2013 та Microsoft Office 365 відкривають налаштування політики ActiveSync через політики поштових скриньок мобільних пристроїв. Microsoft робить відносно простим створення політик поштових скриньок мобільних пристроїв, але Центр адміністрування Exchange Server 2013 та Центр адміністрування Exchange Office 365 відкривають лише основні налаштування політики. Це налаштування політики, які використовуються для вимоги пароля та для встановлення атрибутів, пов'язаних з паролем, таких як мінімальна довжина пароля. Є десятки інших налаштувань ActiveSync, доступних, але їх використання потребує Windows PowerShell.

Враховуючи, що мобільні пристрої не мають можливості приєднатися до домену в традиційному сенсі, це ускладнює управління мобільними пристроями. Хоч Microsoft і надає кілька хороших інструментів для управління безпекою пристроїв та контролю доступу до мережевих ресурсів, цього не достатньо для повноцінного керування мобільними пристроями.

1.4 Основні технології та протоколи для керування мобільними пристроями

1.4.1 Open Mobile Alliance Device Management

OMA – це галузева група, до складу якої входять понад 200 операторів мобільного зв'язку, виробників мобільних пристроїв і постачальників програмного забезпечення (включаючи Microsoft). OMA була сформована в 2002 році для створення єдиної групи для управління зростаючою кількістю стандартів мобільних пристроїв, які з'являлися на ринку, включаючи WAP,

Device Management і SyncML. Така множинність груп створювала дублювання роботи, тому зацікавлені галузеві партнери зібралися разом і об'єднали всі ці важливі ініціативи в єдину парасолькову групу. Стандарти OMA допомагають спростити роботу з мобільними пристроями та мережами, створюючи непатентований спосіб зв'язку між технологіями. SyncML і OMA-DM є двома аспектами цього сімейства відкритих протоколів [9].

SyncML — це розмітка на основі XML, яка використовується як основа для більшості протоколів, визначених OMA. Документ SyncML називається повідомленням. Повідомлення має бути добре сформованим XML, але не обов'язково коректним. Це означає, що воно повинно мати однакові відкриті та закриті теги для всіх елементів, лапки навколо всіх атрибутів, а в іншому мати чітку конструкцію, що є важливим для будь-якого XML документа. Незважаючи на те, що існує визначення типу документа SyncML, немає вимоги, щоб відправник або одержувач перевіряли його дотримання. Однією з причин цього є те, що перевірка вимагає додаткової пам'яті та процесорного часу, а мобільним пристроям, як правило, не вистачає обох цих ресурсів. Повідомлення, містить елементи команд, які виконують роботу з конкретними протоколами OMA.

SyncML і OMA-DM не потребують маршрутної прив’язки на відміну від HTTP чи проколу обміну об'єктами. Це робить SyncML і OMA-DM корисними інструментами для бездротового надсилання команд чи повідомлень на пристроїв. Використовуючи SyncML і OMA-DM із сумісним сервером керування пристроями, є можливість надсилати конфігурації на пристрій без використання карти пам'яті, без прив'язки пристрою до модема та без запиту кінцевого користувача про взаємодію, наприклад під час відвідування веб-сайту.[9]

Сесія керування пристроями (DM) складається з серії команд, які обмінюються між сервером DM та клієнтським пристроєм. Сервер надсилає команди, що вказують на операції, які потрібно виконати клієнтським пристроєм. Клієнт відповідає, надсилаючи команди, які містять результати та будь-яку запитувану інформацію про статус. Коротку DM сесію можна підсумувати так: сервер надсилає команду «get» клієнтському пристрою, щоб отримати вміст одного з вузлів дерева управління. Пристрій виконує операцію

та відповідає командою «result», яка містить запитуваний вміст. Сесію DM можна розділити на дві фази: фаза налаштування та фазу управління. Спершу у відповідь на тригерну подію клієнтський пристрій надсилає ініціююче повідомлення на DM сервер. Пристрій і сервер обмінюються необхідною аутентифікацією та інформацією про пристрій. Далі DM сервер контролює процес. Він надсилає команди управління пристрою, а пристрій відповідає. Друга фаза закінчується, коли сервер DM перестає надсилати команди та завершує сесію. Під час типової сесії клієнт DM викликається для зворотного зв'язку з сервером управління. Повідомлення тригера містить ідентифікатор сервера та вказує клієнтському пристрою ініціювати сесію з сервером. Клієнтський пристрій аутентифікує повідомлення тригера та перевіряє, що сервер має право спілкуватися з ним. Пристрій надсилає повідомлення через IP-з'єднання, щоб ініціювати сесію. Це повідомлення містить інформацію про пристрій та облікові дані. Клієнт і сервер здійснюють взаємну аутентифікацію через канал TLS/SSL або в DM додатку [10].

1.4.2 Firmware Over The Air

FOTA, або Firmware Over-The-Air, є революційною технологією, яка дозволяє виробникам пристроїв дистанційно оновлювати прошивку пристроїв бездротовим способом. Завдяки FOTA такі пристрої, як розумні домашні прилади з модулями IoT та стільниковим зв'язком, можуть отримувати останні покращення прошивки безпосередньо по повітрю, усуваючи необхідність у ручних, фізичних оновленнях [52]. Ця можливість бездротового оновлення є критично важливою для підтримки безпеки пристроїв, впровадження нових функцій та виправлення програмних помилок. Процес оновлення FOTA значно зменшує час простою та усуває незручності, пов'язані з підключенням пристроїв до комп'ютерів для покращення програмного забезпечення, роблячи його більш ефективним та зручним для користувачів. Дозволяючи безперебійні бездротові оновлення, FOTA забезпечує, щоб пристрої працювали на останньому програмному забезпеченні, безпосередньо сприяючи їх довговічності та стійкості до загроз безпеці. Це особливо важливо в контексті "оновлення

прошивки", що означає забезпечення постійного покращення та патчування вбудованого програмного забезпечення, яке контролює апаратне забезпечення, щоб захистити його від вразливостей. Для продуктів з модулями IoT та стільниковим зв'язком оновлення OTA (Over-The-Air) є особливо важливими для підтримки ефективності та безпеки пристроїв завдяки своєчасним оновленням прошивки. FOTA відіграє ключову роль в управлінні життєвим циклом розумних пристроїв, активів IoT та мобільних гаджетів, забезпечуючи їх роботу на найсучасніших та найбезпечніших версіях програмного забезпечення [53]. Ця технологія є важливою для покращення користувацького досвіду, підвищення продуктивності пристроїв та захисту від кіберзагроз. У недавніх досягненнях технологія FOTA еволюціонувала, щоб підтримувати інкрементні оновлення, що означає, що лише змінені частини прошивки надсилаються по повітрю, зменшуючи використання даних та прискорюючи процес оновлення. FOTA дозволяє безперебійні бездротові оновлення прошивки, забезпечуючи захист інтернет-підключених пристроїв від майбутніх загроз [11].

Android підтримує оновлення FOTA з Android 1.6 Donut. Дизайн з тих пір був значно оновлений до такої міри, що оновлення проходять безшовно і майже непомітно. Пристрої Android складаються з кількох основних розділів, які містять специфічні файли. Завантажувач завантажується першим, коли пристрій вмикається. Його роль полягає в перевірці цілісності різних розділів і завантаженні ядра в оперативну пам'ять. Оскільки процес завантаження має кілька етапів, існує кілька розділів завантажувача. Розділ /boot складається з ядра Android Linux, а також з ramdisk (на пристроях до запуску Android 13), який є набором скриптів, що визначають порядок, у якому процеси запускаються системою. В розділі /data зберігаються всі дані користувача, такі як встановлені програми, дані програм, медіа (фото, завантаження тощо). Цей розділ очищається, коли пристрій скидається до заводських налаштувань. Розділ /recovery - це міні-операційна система, яка діє як інтерфейс для оновлення інших розділів, поки вони неактивні. На пристроях без підтримки оновлень A/B оновлення FOTA застосовуються через відновлення. Розділ /system містить більшість системних файлів Android, таких як системні програми, системні медіа

(включаючи анімацію завантаження, рінгтони тощо), бібліотеки низького рівня C та фреймворк Android. Розділ /vendor подібний до розділу системи, і він містить специфічні для пристрою системні файли, такі як драйвери користувацького простору (розширення від драйверів ядра) та HAL (шари абстракції апаратного забезпечення). Крім цих, можуть бути й інші розділи, залежно від архітектури пристрою OEM. Оновлення FOTA може оновити один або всі з цих розділів [12].

1.4.3 Zero-touch enrollment

Zero-touch реєстрація - це спрощений процес реєструватися в корпоративних системах керування мобільними пристроями для Android-пристроїв. Під час першого запуску пристрої перевіряють, чи їм було призначено конфігурацію підприємства. Якщо так, пристрій завантажує відповідний додаток контролера політики пристрою, який потім завершує налаштування керованого пристрою. Zero-touch реєстрація пропонує безшовний метод розгортання для корпоративних Android-пристроїв, що робить масштабні розгортання швидкими, простими та безпечними для організацій, IT та співробітників. Zero-touch спрощує налаштування пристроїв онлайн і їх реєстрацію з примусовим управлінням, щоб співробітники могли користуватися мобільними пристроями без додаткового налаштування [13].

Безконтактна реєстрація є методом налаштування для пристроїв Android, який дозволяє IT-адміністраторам розгортати корпоративні пристрої з попередньо налаштованими параметрами. Після активації пристрої автоматично бездротово підключаються до МДМ системи підприємства та отримують раніше заготовлені конфігурації.

Одною з найбільших переваг такої реєстрації пристроїв є набагато менший час розгортання та об’єм трудовитрат в порівнянні з іншими засобами реєстрації пристроїв. Цей метод також підвищує безпеку шляхом забезпечення послідовних конфігурацій та спрощує впровадження для масштабних розгортань. Реєстрація такого типу не призначена для пристроїв, які не були придбані через авторизовані канали, тобто вона застосовується тільки для

пристроїв що були придбані у офіційних постачальників, які можуть занести список ідентифікаторів у різноманітні МДМ системи [15].

Зазвичай для початку налаштування потрібно лише кілька секунд, а для завершення самонастроювання пристрою після ввімкнення та підключення до Інтернету - кілька хвилин.

Реєстрація пристроїв без участі користувача широко застосовується в великих підприємствах, які одночасно реєструють тисячі пристроїв та забезпечують співробітників мобільними терміналами POS, терміналами збору даних, корпоративними мобільними пристроями та іншими пристроями [14].

2 ПОРІВНЯЛЬНИЙ АНАЛІЗ СИСТЕМ КРЕУВАННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ

2.1 Характеристика Samsung Knox

Samsung Knox - це комплексний набір рішень для управління мобільними пристроями, розроблений для захисту пристроїв Samsung від сучасних загроз. Knox надає безпечну та налаштовувану платформу для бізнесу, щоб управляти та контролювати свої мобільні пристрої. Деякі з ключових функцій Samsung Knox включають:

– Knox Platform for Enterprise (KPE): апаратна платформа безпеки, яка забезпечує багаторівневий захист для пристроїв Samsung.

– Knox Mobile Enrollment (KME): хмарна служба, яка спрощує розгортання та налаштування пристроїв Samsung.

– Knox Configure: хмарне рішення, яке дозволяє налаштовувати та конфігурувати пристрої Samsung відповідно до їх специфічних потреб.

– Knox Manage: хмарне рішення MDM, яке дозволяє бізнесу віддалено управляти та захищати пристрої Samsung.

Samsung Knox широко використовується бізнесом у різних галузях, включаючи охорону здоров'я, фінанси та державний сектор. Наприклад, лікарня може використовувати Knox для захисту даних пацієнтів на пристроях Samsung, тоді як банк може використовувати Knox для захисту інформації клієнтів на мобільних пристроях [16].

2.1.1 Історія розвитку Samsung Knox

Samsung Knox було вперше представлено у 2013 році як частину стратегії Samsung з підвищення безпеки своїх мобільних пристроїв. Платформа розроблена спеціально для пристроїв Samsung і є інтегрованою частиною їх операційної системи. Основна ідея Knox — створення багаторівневого захисту, починаючи з апаратного рівня. Платформа постійно вдосконалюється, зокрема

завдяки впровадженню Knox Vault, Knox Manage та інших компонентів, які забезпечують адаптивність системи до сучасних загроз [16].

Samsung увійшла на ринок мобільних підприємств в 2013 році, щоб підтримати тенденцію використання мобільних пристроїв в робочому просторі. Це створило швидко зростаючий попит на бізнес-пристрої як для окремих осіб, так і для організацій. Спочатку Samsung Knox був розроблений як вбудована платформа безпеки, щоб задовольнити основну вимогу мобільного ринку B2B – захист корпоративних даних, навіть під час роботи з мобільними пристроями.

Бізнеси та корпоративні клієнти потребували впевненості в тому, що їх робочі пристрої та дані є під захистом. Це вимагало постійно еволюціонуючих, інноваційних технологій. Samsung хотіла задовольнити цю основну потребу, створивши платформу Knox для підприємств. Вона швидко отримала сертифікації від урядів та експертів з безпеки, які вона досі має.

У 2015 році Samsung Knox повинен був еволюціонувати, щоб відповідати зростаючим вимогам до надійного управління пристроями, розробивши набір хмарних рішень, які використовували можливості платформи Knox. EMM, контроль версій ОС та конфігурація пристроїв були випущені, щоб допомогти адміністраторам IT впоратися з викликами в реальних сценаріях.

Оскільки нові потреби B2B2C стали на перший план, Samsung розширила свій асортимент продукції, щоб охопити більше випадків використання, таких як ребрендинг/кастомізація пристроїв та захист від шахрайства/викрадення. Все це досягається завдяки таким функціям, як інтелект активів, тригери політики на основі події, мінімізовані етапи реєстрації та віддалене усунення неполадок [17].

До сьогоднішнього дня компанія продовжує еволюціонувати, щоб забезпечити спрощений досвід як єдина бізнес-платформа.

2.1.2 Особливості платформи Samsung Knox

Платформа Knox пропонує найкращу в своєму класі апаратну безпеку, управління політиками та можливості дотримання вимог, які перевищують стандартні функції, поширені на сучасному ринку мобільних пристроїв.

Платформа Knox є показником сильної стратегії мобільної безпеки, що підтримує широкий спектр пристроїв Samsung.

Завдяки системам EMM, IT-адміністратори можуть використовувати веб-консоль для централізованого управління віддаленими пристроями по повітрю. IT-адміністратори можуть всебічно контролювати пристрої Samsung Knox, легко керуючи функціями пристроїв [18].

Samsung Knox використовує апаратний рівень як основу захисту мобільних пристроїв, забезпечуючи високий рівень цього захисту через кілька ключових технологій:

– Root of Trust. Шкідливе програмне забезпечення продовжує вдосконалюватися в складності, намагаючись випередити розвиваючі засоби захисту мобільних пристроїв. Тому створили надійний стек Root of Trust, який мінімізує ризики, виявляє віруси та захищає чутливу інформацію [20]. Root of Trust це серія суворих перевірок, що починаються на апаратному рівні, а не на програмному. Ця функція ускладнює вплив шкідливого ПЗ на пристрій, оскільки ідентифікує сам вірус на апаратному рівні, що дозволяє ефективніше застосовувати забезпечення на програмному рівні [19].

– Система Knox Vault від Samsung є еволюцією апаратної безпеки, яку Samsung розвиває в смартфонах Galaxy протягом багатьох років. Knox Vault розширює захист, який пропонує TrustZone, середовище довіреного виконання (TEE), яке було впроваджено Samsung для захисту критичних даних, таких як паролі, біометричні дані та криптографічні ключі. У той час як TrustZone працює поряд з Android на основному процесорі додатків, Knox Vault функціонує абсолютно незалежно від основного процесора [21].

– Trusted Boot ідентифікує та розрізняє несанкціоновані та застарілі файли завантажувача перед тим, як вони зможуть отримати доступ до мобільного пристрою. Якщо виявлено несанкціоновану або застарілу версію компонента, встановлюється запобіжник від підробки. Після встановлення запобіжника критичні робочі програми та дані в контейнері робочого профілю назавжди шифруються та стають недоступними, оскільки цілісність пристрою більше не гарантується або не перевіряється [22].

До програмних механізмів безпеки входять:

– Runtime Kernel Protection (RKP). Захист ядра є центральним елементом безпеки пристроїв та захисту даних підприємств. Коли зловмисники знаходять вразливості в програмному забезпеченні, вони часто підвищують привілеї та компрометують ядро операційної системи. Компрометоване ядро може призвести до витоку чутливих даних і навіть дозволити віддалений моніторинг і контроль над ураженим пристроєм. RKP використовує монітор безпеки в ізольованому середовищі виконання. Запуск в ізольованому середовищі виконання зазвичай надає здатність механізму безпеки бачити в ядро та моніторити активність під час виконання. RKP використовує запатентовані технології для контролю управління пам'яттю пристрою та перехоплюючи і перевіряючи критичні дії ядра перед їх виконанням [23].;

– Sensitive Data Protection (SDP). Samsung створила Захист чутливих даних (SDP), що вирішує проблему витоку даних при втраті пристрою. Платформа Knox захищає дані користувача на пристрої за допомогою шифрування даних. Дані залишаються зашифрованими на диску і можуть бути розшифровані лише тоді, коли пристрій увімкнено [55]. Крім того, надається механізм, який дозволяє за бажанням позначати дані як важливі, які потім не можуть бути розшифровані, поки пристрій знаходиться в заблокованому стані [24].

– DualDAR (Dual Data-at-Rest Encryption). Knox DualDAR захищає всі дані профілю роботи на пристроях з двома різними рівнями шифрування. Це рішення також захищає дані, обмежуючи додатки від запису або збереження даних у незашифрованому просторі на пристрої. Внутрішні та зовнішні шари безпеки DualDAR є незалежними та захищають всю інформацію, що зберігається в робочому профілі, коли пристрій вимкнений [25].

Платформа Samsung Knox демонструє високий рівень безпеки, застосовуючи інструменти як апаратної, так і програмної безпеки, що дає одну з найбільш захищених платформ сьогодення.

2.1.3 Інструменти платформи Samsung Knox

Samsung Knox — це інтегрована платформа безпеки та набір рішень для управління мобільними пристроями, розроблені компанією Samsung. Вона забезпечує високий рівень захисту даних і надає можливості для ефективного управління пристроями в корпоративному середовищі.

2.1.3.1 Knox Manage

Knox Manage - це потужне хмарне рішення, розроблене для управління пристроями Android, iOS, ChromeOS, macOS або Windows. З більш ніж 300 доступними політиками можна безпечно налаштовувати, управляти та віддалено відстежувати всі корпоративні пристрої [26].

Knox Manage — це інструмент для централізованого управління мобільними пристроями в корпоративному середовищі. Він забезпечує комплексний контроль, дозволяючи в реальному часі відстежувати місцезнаходження пристроїв, перевіряти статус відповідності політикам і швидко реагувати на загрози. Платформа підтримує багатокористувацьке налаштування через функції масового додавання і автоматизації, включаючи кіоск-режим із кастомізованими застосунками та віджетами [51].

Knox Manage дозволяє застосовувати політики для різних сценаріїв, використовувати віддалену підтримку Knox Remote Support для швидкого вирішення проблем, а також оптимізувати оновлення ОС завдяки E-FOTA. Інтеграція з Android Enterprise та Knox API забезпечує гнучкість і ефективність управління. Рішення підтримує шифрування AES-256, двофакторну автентифікацію, завантаження та безпечну дистрибуцію контенту через CDN, а також масову реєстрацію пристроїв за допомогою Knox Mobile Enrollment (KME) та Automated Device Enrollment (ADE). Завдяки функціям аудиту адміністратори можуть відстежувати системні події, політики, порушення відповідності та проводити відповідні заходи.

Додатково, Knox Manage дозволяє запускати пристрої з увімкненою функцією Direct Boot, забезпечуючи їх готовність до роботи ще до розблокування користувачем. Це робить систему оптимальним вибором для

компаній, які потребують безпечного та ефективного управління пристроями [27].

2.1.3.2 Knox Configure

Knox Configure - це хмарний сервіс, який надає підприємствам можливість налаштовувати та автоматизувати реєстрацію пристроїв Samsung, придбаних у авторизованих постачальників Samsung.

Використовуючи веб-консоль, можна створювати профілі з налаштуваннями пристроїв, обмеженнями, додатками та іншим контентом, який буде розгорнуто на групах пристроїв. Після успішної реєстрації пристроїв у підприємстві ви отримуєте профілі пристроїв через Wi-Fi або мобільні дані. Рисунок 2.1 ілюструє процес розгортання.

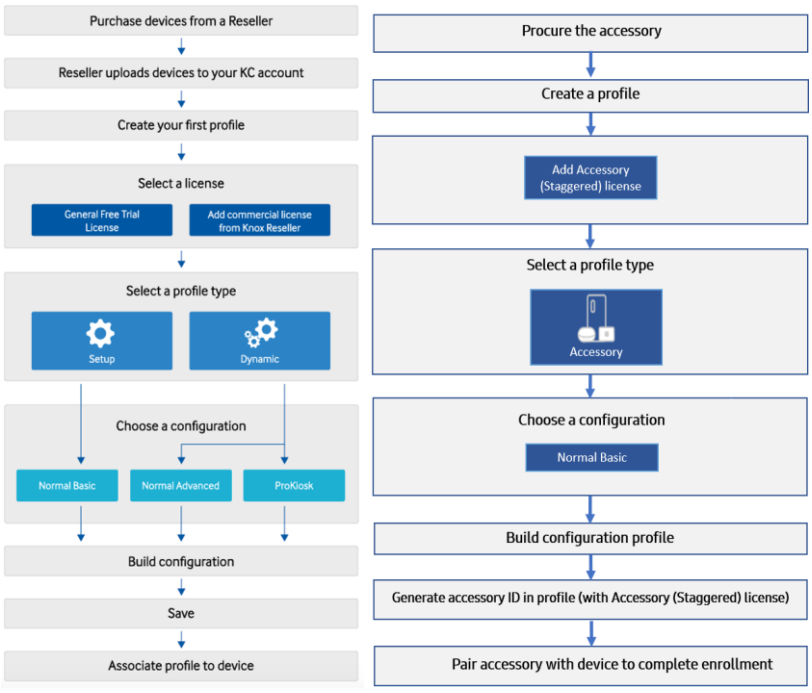

Рисунок 2.1 – Процес введення пристрою в систему та присвоєння йому профілю

Після налаштування профілю його можна призначити конкретним пристроям, зареєстрованим у Knox Configure. Призначення профілю пристрою є останнім етапом у процесі налаштування, хоча пристрої можуть бути заблоковані операторами та посередниками після розгортання [28].

2.1.3.3 Knox Asset Intelligence

Аналітика на основі даних Knox Asset Intelligence допомагає покращити управління, продуктивність та життєвий цикл пристроїв. З Knox Asset Intelligence з'являється можливість налаштувати панель управління з віджетами даних, щоб допомогти прогнозувати та запобігати проблемам на передньому краї, які найбільше важливі для компанії.

Переваги використання Knox Asset Intelligence:

– Глибоке та всебічне відстеження даних — дозволяє контролювати програми, заряд батареї, мережу та дані про місцезнаходження пристроїв компанії, щоб забезпечити їхню продуктивність та готовність до використання.

– Підсумки даних — дозволяє отримувати щоденні підсумки значущих бізнес-висновків з легкими у використанні, гнучкими та повністю налаштовуваними панелями приладів.

– Діагностика та усунення неполадок — дозволяє отримувати повну характеристику станів пристроїв за допомогою детальних звітів про дані.

Щоб використовувати Knox Asset Intelligence, необхідно: пристрої з відповідною версією, пристрої повинні бути повністю керованими або корпоративними із робочим профілем, обліковий запис Samsung Knox;,дійсна ліцензія Knox Suite або Knox Asset Intelligence [29].

2.1.3.4 Knox Guard

Knox Guard — це хмарний сервіс, який дозволяє захищати пристрої, корпоративні активи та платіжні плани від шахрайства та крадіжок. З Knox Guard можна віддалено керувати, надсилати повідомлення та, якщо це необхідно, блокувати пристрої Samsung, щоб зменшити фінансові ризики організації та продажі пристроїв на чорному ринку.

Knox Guard надає можливість встановлювати детальні обмеження на пристрої, такі як увімкнення/вимкнення певних SIM-карт, блокування пристрою, коли він не був в мережі протягом визначеного періоду часу, надсилання нагадувань про прострочені платежі та багато іншого.

Knox Guard пропонує ключові функції для управління пристроями, включаючи відправку повідомлень (зокрема повноекранних), нагадування з миготінням, блокування пристроїв, видалення пристроїв із системи після виконання певних умов, а також реєстрацію авторизованих посередників для перевірки права власності. Knox Guard також дозволяє створювати ролі для адміністраторів, управляти політиками для налаштувань за замовчуванням, повідомлень і блокування, забезпечуючи ефективне управління корпоративними пристроями [30].

2.2 Характеристика SOTI

SOTI є провідним постачальником рішень для управління мобільними пристроями та інтернетом речей, які допомагають бізнесу оптимізувати свої операції та підвищувати їхню продуктивність. Флагманський продукт SOTI ONE є комплексним набором рішень MDM, до якого входять:

– SOTI MobiControl: потужне рішення MDM, яке дозволяє бізнесу управляти та захищати мобільні пристрої, програми та контент.

– SOTI Assist: рішення для віддаленої підтримки, яке дозволяє IT-командам усувати неполадки та вирішувати проблеми на мобільних пристроях.

– SOTI Snap: платформа швидкої розробки додатків, яка допомагає бізнесу швидко створювати та впроваджувати власні мобільні програми.

SOTI користуються довірою бізнесу всіх розмірів, від малих стартапів до великих підприємств. Наприклад, логістична компанія може використовувати SOTI MobiControl для відстеження та управління своїм парком мобільних пристроїв, тоді як роздрібна мережа може використовувати SOTI Snap для створення власних мобільних додатків для своїх співробітників [16].

2.2.1 Історія розвитку SOTI

Заснована у 1995 році, компанія SOTI виникла завдяки візіонерським ідеям її засновника та генерального директора Карла Родрігеса. Його прагнення спростити процес управління мобільними пристроями стало основою для

створення рішень, які значно випереджали свій час. На момент заснування смартфони ще не були широко поширеними, але SOTI вже передбачала зростання важливості мобільних технологій у бізнесі. Компанія стала піонером у галузі управління мобільністю, пропонуючи рішення, які допомогли тисячам організацій ефективно використовувати мобільні пристрої для досягнення бізнес-цілей.

Перший продукт компанії, «SOTI Pocket Controller», швидко завоював популярність на міжнародному ринку. Цей програмний продукт дозволяв ефективно управляти мобільними пристроями, зокрема їхнім інтерфейсом, забезпечуючи гнучкість та зручність використання. Успіх Pocket Controller став основою для створення більш комплексного рішення — «SOTI MobiControl», яке зараз є флагманським продуктом компанії. MobiControl забезпечує управління мобільністю підприємств (EMM), дозволяючи організаціям контролювати пристрої, додатки, дані та контент [31].

У 2017 році SOTI зробила ще один великий крок у своєму розвитку, запустивши платформу «SOTI ONE» — інтегрований набір інструментів для управління мобільними та IoT-рішеннями. Ця платформа покликана зменшити витрати, скоротити простої та спростити роботу з критично важливими для бізнесу технологіями. Завдяки цьому підходу SOTI утвердила себе як світовий лідер у сфері управління мобільними та IoT технологіями [32].

На сьогодні SOTI обслуговує понад 17 000 корпоративних клієнтів у більш ніж 170 країнах світу. Компанія має широкий портфель інноваційних продуктів, які допомагають організаціям захищати дані, оптимізувати процеси та максимізувати рентабельність інвестицій у мобільні технології. Її рішення підтримують різноманітні платформи та пристрої, що робить їх універсальними для бізнесу різних масштабів. SOTI пройшла шлях від стартапу, що складався з однієї людини, до глобального гравця з більш ніж 1200 співробітниками. Головний офіс компанії розташований у Міссісазі, Канада, а її мережа включає 12 регіональних офісів у таких країнах, як Велика Британія, Ірландія, Швеція, Індія, Австралія та Японія. У планах компанії — подальше розширення на нові ринки, щоб ще краще відповідати потребам своїх клієнтів [31].

SOTI не лише продовжує інвестувати в дослідження та розвиток, а й адаптується до швидкозмінних умов ринку, впроваджуючи новітні технології для створення найкращих рішень у галузі мобільності та IoT.

2.2.2 Особливості платформи SOTI

Платформа SOTI дозволяє IT-адміністраторам централізовано керувати пристроями через веб-консоль, спрощуючи виконання рутинних завдань, таких як впровадження політик, моніторинг продуктивності та забезпечення безпеки. Завдяки інструментам віддаленого управління, аналітиці в реальному часі та налаштуванню кіоск-режимів, SOTI MobiControl забезпечує безперебійну роботу пристроїв та підвищує ефективність бізнесу в таких галузях, як логістика, рітейл, медицина та виробництво [33].

Це рішення стало еталоном у сфері мобільного управління, пропонуючи гнучкість, універсальність та передові засоби забезпечення безпеки, які відповідають найвищим вимогам сучасних підприємств.

Основні особливості, що відрізняють SOTI від інших МДМ систем:

– Indoor Location. Функція Indoor Location використовує позиціонування за допомогою Wi-Fi для визначення поточного місцезнаходження пристроїв у визначеній області та того, де вони були протягом часу. Indoor Location дозволяє аналізувати дані з пристроїв, включаючи силу сигналу, стан батареї та використання ЦП [34]. Щоб отримувати точні оновлення позиції пристроїв у приміщенні, потрібно стабільне підключення до мережі Wi-Fi. Карта приміщення може бути вже надана або є можливість завантажити її з локального комп'ютера чи створити карту приміщення, використовуючи SOTI XSight Design Studio [35].

– Команди-скрипти. SOTI MobiControl дозволяє надсилати скрипти на пристрої для виконання серії команд. Скрипти доставляються на пристрої шляхом ініціювання з'єднання з SOTI MobiControl або за допомогою SMS. Скрипти підтримують пристрої Android Plus, Linux, Windows Desktop Classic та Windows Mobile/CE, хоча лише пристрої Windows Desktop Classic та Windows Mobile/CE можуть отримувати та виконувати їх за допомогою SMS. SOTI

MobiControl має кілька попередньо визначених скриптів, готових до використання, таких як активація з'єднання, показ повідомлення та очищення пристрою. Можна використовувати один з попередньо визначених скриптів SOTI MobiControl або створити власний скрипт [36].

– Підтримка спеціалізованих пристроїв. SOTI виділяється своєю здатністю підтримувати широкий спектр пристроїв, включаючи не лише сучасні смартфони та планшети, але й спеціалізоване обладнання та застарілі платформи. Платформа інтегрується з такими пристроями, як сканери штрих-кодів, промислові мобільні термінали та принтери, що часто використовуються у логістиці, продажах та інших галузях. Завдяки партнерству з провідними виробниками, такими як Zebra, Honeywell та Panasonic, SOTI пропонує доступ до розширених функцій пристроїв, включаючи детальну діагностику, управління батареєю та оновлення прошивки [37]. Крім того, SOTI підтримує застарілі операційні системи, зокрема Windows Mobile і Windows CE, що дозволяє компаніям поступово модернізувати обладнання без втрати функціональності чи додаткових витрат [38].

2.2.3 Інструменти платформи SOTI

SOTI пропонує комплексну платформу для управління мобільними пристроями та корпоративними процесами, яка складається з декількох інтегрованих рішень. Кожен інструмент цієї екосистеми спрямований на вирішення специфічних завдань, від централізованого управління пристроями до розробки мобільних додатків та управління IoT-обладнанням. Унікальною перевагою платформи є її здатність адаптуватися до різних бізнес-середовищ, забезпечуючи безпеку, масштабованість та простоту використання.

Ці інструменти працюють разом, створюючи універсальне рішення для бізнесу, яке дозволяє компаніям швидко реагувати на виклики сучасного ринку. Опис кожного компонента платформи SOTI демонструє, як вона допомагає підприємствам ефективно керувати своїми мобільними активами, мінімізувати операційні витрати та оптимізувати робочі процеси.

2.2.3.1 SOTI MobiControl

SOTI MobiControl — це рішення Enterprise Mobility Management (EMM), яке дає видимість і контроль над тим, де знаходяться критично важливі для бізнесу мобільні пристрої, що вони роблять, як вони працюють і з якими ризиками безпеки вони стикаються. Це рішення EMM, розроблене для будь-якого пристрою, будь-якого форм-фактора, будь-якої операційної системи і будь-яких вимог бізнесу [39].

SOTI MobiControl працює на платформах Android, Windows CE/Windows Mobile, Windows Desktop, Apple iOS та Linux. Також підтримує широкий спектр пристроїв, включно з промисловими моделями, наприклад Zebra чи Honeywell та споживчими смартфонами від Sony, Samsung, Motorola тощо.

Система забезпечує ефективні інструменти для віддаленої підтримки, включно з повним дистанційним управлінням пристроями. Адміністратори можуть робити скріншоти, записувати відео, отримувати доступ до файлів і запускати програми на пристроях. До функцій безпеки належать захист від несанкціонованого доступу, кіоск-режим (наприклад, режим однієї програми), блокування екрану із використанням HTML-шаблонів та можливість автоматичного блокування пристрою під час руху (наприклад, для водіїв транспортних засобів).

SOTI MobiControl дозволяє автоматично налаштовувати мережеві з’єднання, зокрема Wi-Fi, 4G/5G та VPN. Механізми захисту від крадіжок включають примусове встановлення паролів, шифрування пристроїв, блокування доступу до скидання до заводських налаштувань тощо. Крім цього, MobiControl дозволяє управляти сертифікатами, забезпечуючи їх автоматичне оновлення без участі користувачів.

Серед функцій також є можливість визначати геозони для пристроїв. Наприклад, якщо пристрій покидає задану територію (будівлю, вулицю чи місто), до нього можуть застосовуватися певні політики. Програми та файли легко встановлюються і оновлюються віддалено за допомогою пакетів, створених у MobiControl Package Studio. Крім того, система підтримує віддалене оновлення операційної системи, наприклад, для пристроїв Zebra LifeGuard.

Синхронізація файлів між мобільними пристроями та корпоративною мережею здійснюється швидко й безпечно. Налаштування пристроїв можна формувати у вигляді профілів, які автоматично застосовуються або видаляються залежно від заданих умов чи належності пристрою до певних груп.

Процес підключення пристроїв до системи максимально спрощений: можна використовувати QR-коди, Zebra StageNow чи Honeywell Enterprise Provisioner. MobiControl має сертифікат Android Enterprise Recommended і підтримує інтеграцію з Google Workspace та Managed Google Play. Пристрої можна налаштувати як повністю керовані або створити та управляти лише робочим профілем, відокремлюючи його від особистих даних користувача.

Для пристроїв, що не підтримують Android Enterprise, доступний режим «Android Classic» із використанням спеціальних агентів SOTI, адаптованих для понад 170 виробників мобільних пристроїв. MobiControl також забезпечує безпечний доступ до корпоративних документів через SOTI Hub, який підтримує WebDAV, SharePoint, Box, OneDrive тощо. Крім цього, SOTI Surf дозволяє налаштувати безпечний веб-браузер відповідно до корпоративних вимог.

Інтерфейс системи простий у використанні, доступний через веб браузер і підтримує створення статичних і динамічних груп пристроїв. Додатково передбачена функція перетягування пристроїв між групами. Для інтеграції та автоматизації завдань можна використовувати JavaScript і власну мову скриптів SOTI.

Таким чином, MobiControl – це комплексне рішення для управління мобільними пристроями, яке забезпечує високу безпеку, гнучкість і зручність у роботі для сучасних підприємств [40].

2.2.3.2 SOTI XSight

SOTI XSight - це рішення для діагностичної інтелектуальної підтримки, яке надає організаціям інструменти, необхідні для ефективного усунення проблем з мобільними пристроями швидше. SOTI XSight забезпечує візуалізацію в реальному часі аналітичних даних, щоб допомогти приймати рішення на основі отриманих даних [41].

SOTI XSight містить ряд потужних інструментів для аналізу даних з мобільних пристроїв. Система Smart Battery Dashboard, використовуючи дані про кількість циклів заряджання та розряджання, температуру та інші параметри, прогнозує можливий вихід батареї з ладу. Вона також дає рекомендації щодо своєчасної заміни батарей, запобігаючи ситуаціям, коли мобільні пристрої стають непридатними для роботи через несправні акумулятори. Крім того, функція дозволяє виявляти батареї, які не витримують повної робочої зміни. Наразі ця функція підтримується батареями PowerPrecision та PowerPrecision+ від Zebra, а також вибраними моделями від Panasonic і Bluebird.

Функція App Dashboards надає інформацію про додатки, які споживають найбільше мобільних даних, розряджають батарею чи займають надмірну кількість пам’яті. Це дозволяє виявляти найбільш критично важливі додатки, а також ті, які можуть бути видалені для оптимізації ресурсів пристроїв.

Інструмент Cellular Coverage Dashboards візуалізує мапи покриття мобільного зв’язку із зазначенням сили сигналу. Ця інформація допомагає оцінити якість мобільного покриття в певних зонах і визначити, чи відповідає воно вимогам роботи [42].

SOTI XSight Live View, перший інструмент такого роду, об’єднує бізнес-дані та дані про пристрої, дозволяючи організаціям візуалізувати свої операції в режимі реального часу на карті або в списку для цілісного перегляду. Організації можуть використовувати Live View Map для візуалізації пристроїв і бізнес-даних під час руху пристроїв у режимі реального часу. Перегляд списку допомагає візуалізувати ті самі дані з пристроїв, які знаходяться в приміщенні. Пристрої відображаються з даними (такими як рівень заряду акумулятора та потужність сигналу), бізнес-даними (такими як рівень запасів і стан доставки) та будь-якими іншими показниками, які потрібно контролювати компанії [41].

SOTI XSight не лише підвищує продуктивність пристроїв, а й дозволяє бізнесу приймати обґрунтовані рішення на основі актуальних даних, що сприяє підвищенню оперативності, зменшенню витрат і вдосконаленню загального рівня обслуговування.

2.2.3.3 SOTI Connect

SOTI Connect - це система для комплексного управління IoT-пристроями, особливо мобільними та промисловими принтерами.

Система для управління корпоративними пристроями пропонує універсальне рішення, яке дозволяє працювати з пристроями від різних виробників незалежно від їх моделі. Завдяки цьому забезпечується зручне управління пристроями таких виробників, як Zebra, Honeywell, Sato, Brother, Epson, Toshiba та інші. Це зменшує складність налаштувань і дозволяє керувати різними пристроях за допомогою єдиних команд.

Однією з ключових переваг є оптимізація процесу впровадження принтерів. Їх можна доставляти безпосередньо на кінцеві локації, де пристрої автоматично виявляються, додаються до системи, налаштовуються і групуються відповідно до фізичного розташування. Система дозволяє точно відстежувати кількість принтерів у мережі, суттєво знижуючи час на налаштування та виключаючи ризик людської помилки.

Функціонал значно зменшує витрати на обслуговування і ремонт принтерів. Використовуючи зібрані дані, наприклад, стан пристрою, рівень використання, стан друкарської головки чи рівень заряду батареї, адміністратори можуть своєчасно діагностувати й вирішувати проблеми дистанційно. Також система попереджає про можливі несправності, завчасно сповіщаючи IT-відділ про потенційно проблемні пристрої.

Інвентаризація пристроїв стала ще простішою завдяки автоматичному відстеженню й оновленню інформації про місцезнаходження принтерів. Якщо пристрій переміщується, його група в системі змінюється автоматично. Усі дані представлені в уніфікованому вигляді, незалежно від виробника, і включають такі параметри, як рівень батареї, швидкість друку, температура друкарської головки, використання пам’яті та інші показники.

Для зручності управління створений інструмент Visualization Design Studio, який дозволяє легко налаштовувати інтерфейс відображення даних. Адміністратори можуть створювати індивідуальні панелі, які включають властивості принтера, графіки та необхідні дії для вирішення проблем.

Система також підтримує функції самодіагностики. Принтери автоматично повідомляють про виявлені проблеми, що значно прискорює їх усунення. Окрему увагу приділено безпеці: система перевіряє відповідність принтерів заданим політикам і автоматично позначає ті, що не відповідають вимогам. Віддалене встановлення оновлень програмного забезпечення та зміна небезпечних паролів дозволяють запобігти несанкціонованому доступу. Додатково передбачена функція віддаленої установки Wi-Fi сертифікатів, що дозволяє зручно оновлювати налаштування мережі [43].

Загалом, система забезпечує централізоване, надійне та ефективне управління корпоративними пристроями та принтерами, зменшує витрати на їх обслуговування і гарантує високий рівень безпеки.

2.3 Підсумки порівняльного аналізу систем Samsung Knox та SOTI

Системи Samsung Knox та SOTI займають важливе місце серед інструментів для управління мобільними пристроями, але їх функціональні можливості та підхід до реалізації суттєво різняться.

Samsung Knox відзначається високим рівнем інтеграції з пристроями Samsung. Такий підхід дозволяє максимально ефективно використовувати як апаратні, так і програмні можливості цих пристроїв. Knox забезпечує багаторівневий захист даних, що робить його надійним рішенням для організацій, де безпека є пріоритетом, наприклад, у фінансовій сфері або державному секторі. Крім того, такі модулі, як Knox Guard, дають можливість дистанційного блокування пристроїв у разі їхньої втрати чи неналежного використання. Проте основним обмеженням системи є її орієнтованість на пристрої Samsung, що може створювати труднощі для компаній із різнотипним парком техніки.

На відміну від Knox, платформа SOTI розроблена для роботи з різноманітними пристроями, незалежно від їхнього виробника чи операційної системи. Вона підтримує Android, iOS, Windows, а також IoT-пристрої, що робить її універсальним рішенням для компаній з різноплановими потребами.

Наприклад, логістичні чи виробничі підприємства, які використовують пристрої різних брендів, можуть повною мірою оцінити можливості SOTI. Зокрема, SOTI MobiControl дозволяє централізовано налаштовувати пристрої, забезпечувати їх оновлення та здійснювати моніторинг у реальному часі. Окрім цього, модуль SOTI XSight пропонує розширені можливості аналітики та виявлення проблем. Проте вартість ліцензій на рішення SOTI зазвичай є вищою порівняно з Samsung Knox, що може стати вагомим фактором при виборі платформи.

Цінове порівняння двох систем показує, що Samsung Knox є більш доступним варіантом. Ліцензії, наприклад, на Knox Manage, коштують від $2 до $4 на місяць за пристрій [44]. У свою чергу, вартість використання SOTI MobiControl стартує від $4 і може сягати $7 на місяць за один пристрій [45]. Для компаній із великим парком техніки навіть така різниця у вартості може мати значення.

У підсумку, вибір між Samsung Knox та SOTI значною мірою залежить від специфіки потреб організації. Samsung Knox буде оптимальним вибором для компаній, які активно використовують пристрої Samsung та мають підвищені вимоги до безпеки. Натомість SOTI стане чудовим рішенням для компаній із різноманітними пристроями, що потребують універсальної та масштабованої платформи для їхнього управління.

3 ПРАКТИЧНЕ ДОСЛІДЖЕННЯ МДМ СИСТЕМ НА ПРИКЛАДІ KNOX MANAGE ТА SOTI MOBICONTROL

3.1 Огляд веб-консолі Knox Manage та SOTI MobiControl

Knox Manage та SOTI MobiControl дають змогу адміністраторам управляти мобільними пристроями за допомогою веб-конснолі. Це дозволяє не прив’язуватися до конкретного робочого місця чи програмного забезпечення і мати доступ до MDM систем майже з будь якого пристрою.

Початкова сторінка консолі Knox Manage, що зображена на рисунку 3.1 показує статистичні дані по кількості пристроїв, користувачів, профілів та багато іншого.

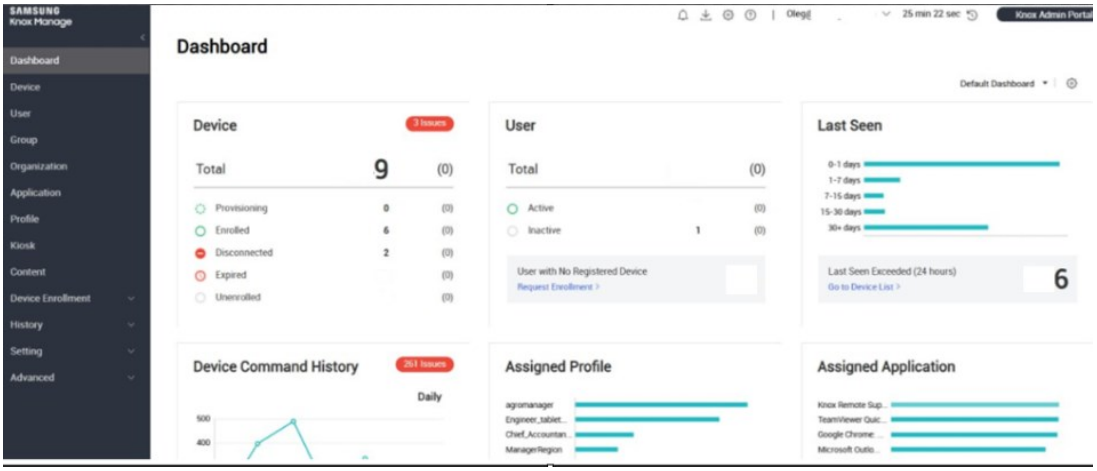

Рисунок 3.1 – Початкова сторінка консолі Knox Manage

За допомогою бокової панелі можна переходити в основні розділи системи, такі як: пристрої, користувачі, групи, організації, програми та профілі. Загалом взаємозв’язок між компонентами зображений на рисунку 3.2.

Рисунок 3.2 – Взаємозв’язок компонентів системи Knox manage

Як можна побачити з рисунку основним елементом є група (організація), до якої прив’язуються: користувач, профіль та політика доступних додатків. Це основні елементи, які потрібні для налаштування початкового середовища керування мобільними пристроями. Також до групи можна прив’язати політику нових файлів та в профіль додати режим обмеженого відображення – кіоск режим.

Всі пристрої в системі повинні мати користувача, а користувач в свою чергу повинен мати присвоєну групу. І саме за допомогою групи присвоюються профілі обмежень та доступні для завантаження робочі додатки пристрою. Також групи виконують функцію впорядкування, тобто можуть розділяти пристрої в компанії. В залежності від посади, кожен прошарок працівників можна розділити на окремі групи, таким чином кожен користувач отримує необхідні обмеження, додатки та оновлення, які йому необхідні відповідно до профілю посади. Це дозволяє гнучко управляти мобільними пристроями та чітко їх ділити за необхідності.

Веб-консоль SOTI MobiControl зустрічає більш комплексним меню, зверху знаходяться графіки, які показують різноманітність вендорів мобільних пристроїв, версії операційних систем та інші дані. Нижче знаходиться список всіх наявних пристроїв в MDM системі. А в боковій панелі знаходяться деревоподібна схема із групами, де знаходяться самі пристрої (див. рисунок 3.3).

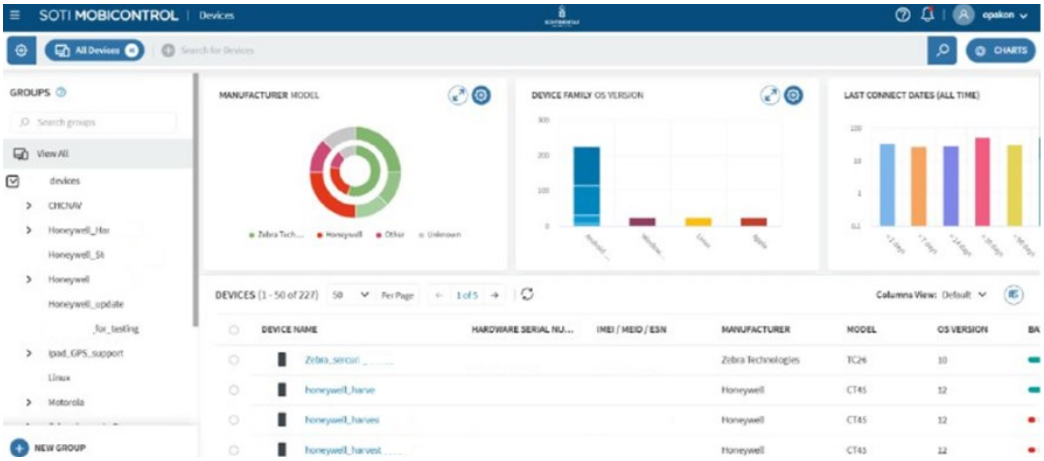

Рисунок 3.3 – Початкова сторінка SOTI MobiControl

Групи в SOTI MobiControl відіграють ту саму роль що і групи в Samsung Knox, тобто є вмістилищем не тільки для пристроїв, а й профілів та політик. Єдине що відрізняє, це те що пристрій можна напряму помістити у відповідну папку, без необхідності залучати ще користувача.

За допомогою бокового меню, можна потрапити в налаштування профілю та політик (див. рисунок 3.4).

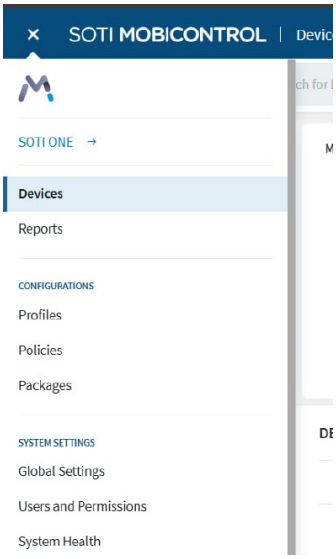

Рисунок 3.4 – Бокове меню SOTI MobiControl

В цьому вікні також є можливість переходу до налаштувань самої системи та до управління користувачами та доступами.

3.2 Налаштування інфрастуктури систем

Налаштування інфраструктури є важливим етапом для забезпечення ефективного управління мобільними пристроями. У випадку Knox Manage та SOTI MobiControl це стосується створення профілів, груп пристроїв і роботи з програмами. Ці елементи утворюють основу для налаштування системи під потреби компанії.

3.2.1 Налаштування групи пристроїв

Щоб перейти до створення чи налаштування групи в Knox Manage потрібно перейти на вкладку «Group», зображено на рисунку 3.5.

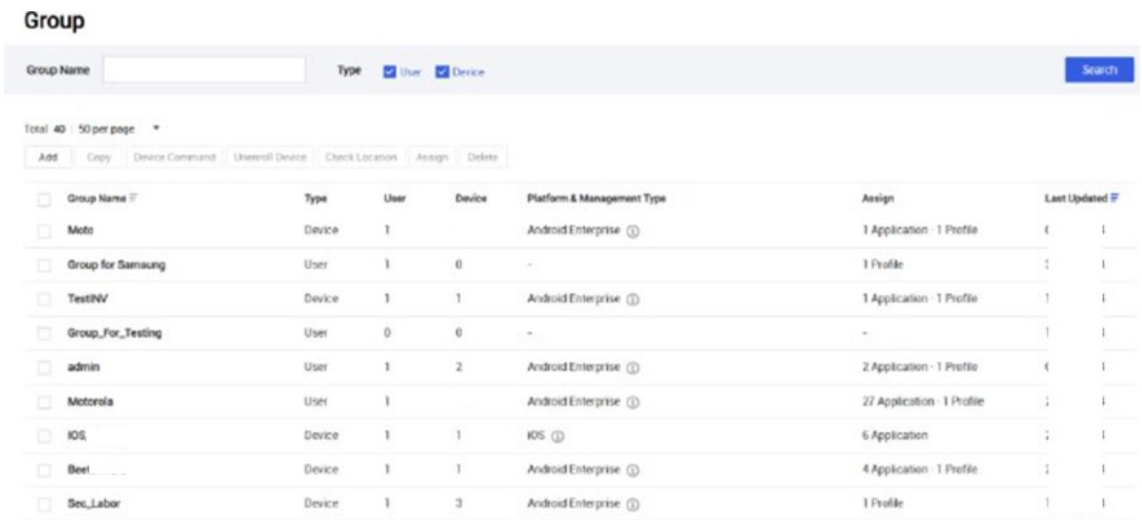

Рисунок 3.5 – Групи в Knox Manage

На цій вкладці є список всіх створених груп їх можна модифікувати або створити нову за допомогою кнопки «Add». На рисунку 3.6 зображено процес створення нової групи пристроїв.

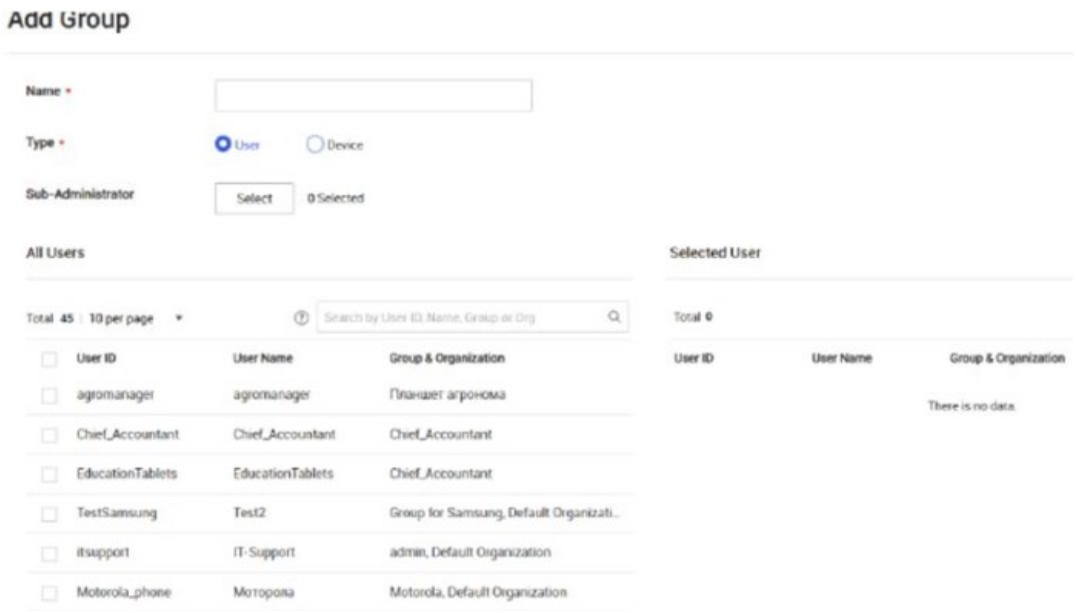

Рисунок 3.6 – Створення нової групи пристроїв в Knox Manage

Щоб створити нову групу достатньо вписати її назву та вказати для чого вона призначена: для ряду користувачів чи для конкретних пристроїв.

В SOTI MobiControl створення нової групи відбувається набагато швидше, на початковому вікні в лівому нижньому кутку натискаємо кнопку «New Group» (див. рисунок 3.7).

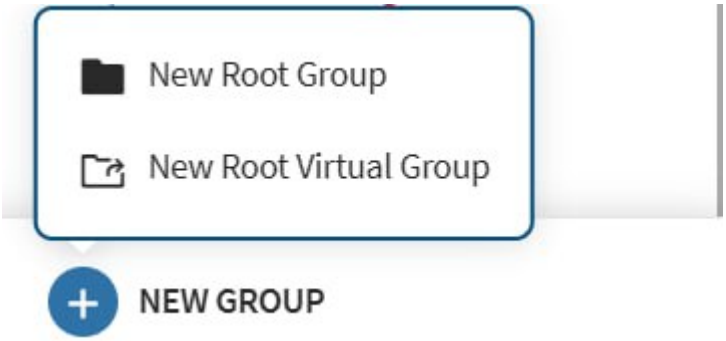

Рисунок 3.7 - Створення нової групи пристроїв в SOTI MobiControl

Далі потрібно вибрати тип групи, звичайна чи віртуальна, віртуальні групи дозволяють групувати пристрої з різних груп пристроїв разом, не переміщуючи їх із їхніх «реальних» груп пристроїв, по суті створюючи посилання для кожного пристрою у віртуальній групі. В наступному вікні ввівши назву, можна створити групу.

3.2.2 Налаштування профілю пристроїв

Профілі в Knox Manage розташовані у вкладці «Profile». На рисунку 3.8 зображено сторінку із всіма профілями в системі, також тут можна створювати нові профілі та редагувати вже наявні.

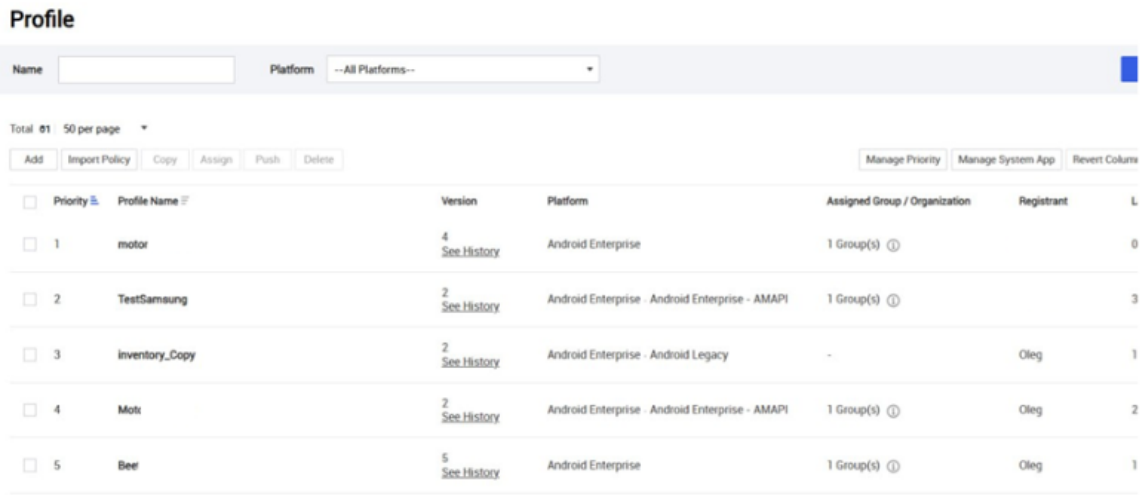

Рисунок 3.8 – Перелік профілів Knox Manage

За допомогою кнопки «Add» є можливість створити новий профіль. Після того як задати назву профіля і його платформу з’являється список політик безпеки, який зображено на рисунку 3.9.

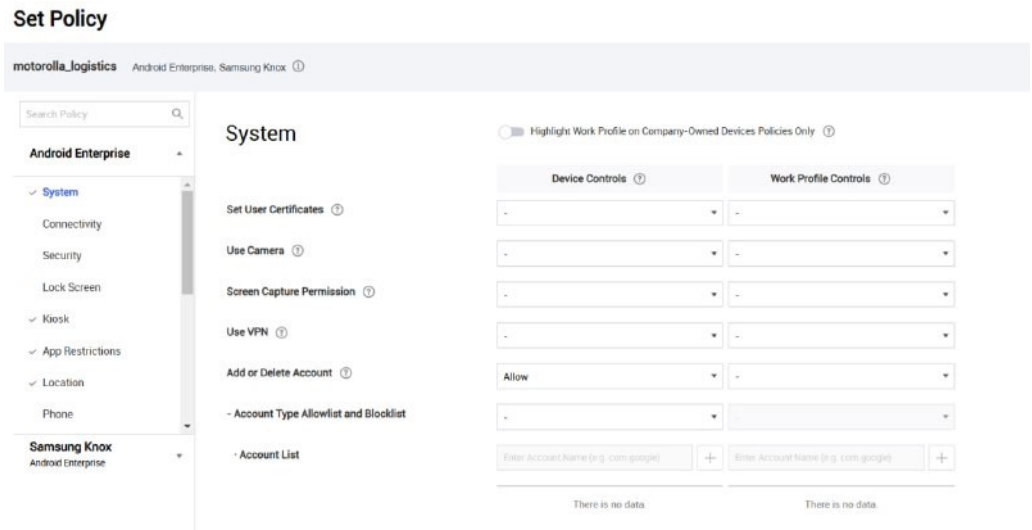

Рисунок 3.9 – Політики безпеки Knox Manage

За допомогою цих політик можна детально та гнучко налаштувати дозволи та обмеження пристрою, для якого буде застосовуватись новостворена політика.

Наприклад можна обмежити використання VPN чи Bluetooth або навпаки увімкнути і заборонити вимикати користувачу, за такою логікою працюють більшість політик безпеки. Також окремо слід виділити політику збору геолокації пристрою, в ній можна налаштувати наскільки часто слід оновлювати дані про розташування пристрою. За необхідністю можна призначити режим обмеженого відображення, кіоск режим.

Аналогічно профілі розташовані і в SOTI MobiControl, тож розглянемо детальніше процес створення нового профілю. Як зображено на рисунку 3.10 спершу потрібно вибрати платформу та тип профілю. В SOTI MobiControl є доступні три типи профілів: повністю керований, персональний з робочою областю та робочий з персональною областю.

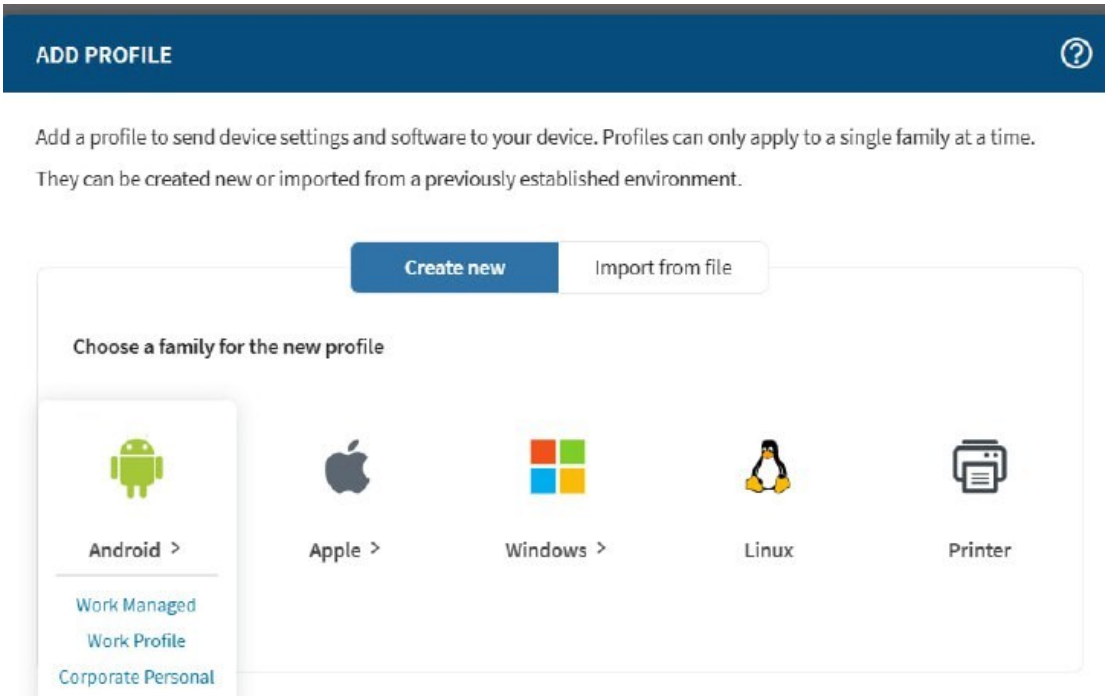

Рисунок 3.10 – Створення профілю в SOTI Mobicontrol

В наступному вікні задаємо назву профілю і в другій вкладці можна вибрати які політики безпеки будуть застосовуватися в профілі (див. рисунок 3.11).

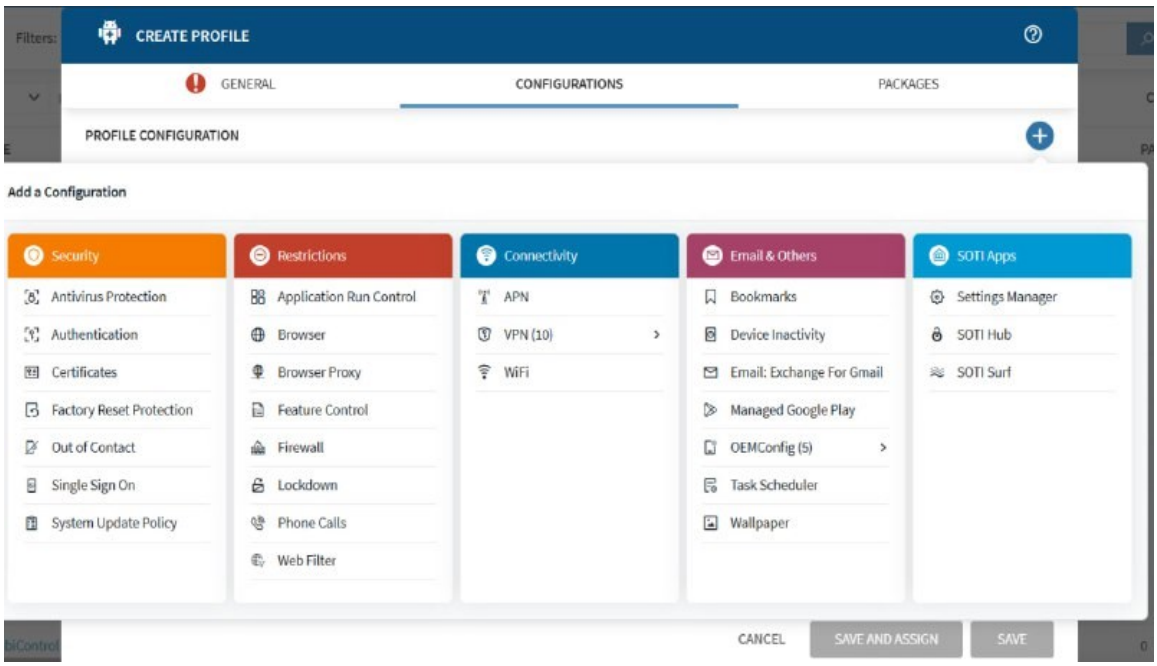

Рисунок 3.11 - Політики безпеки SOTI Mobicontrol

Функції політик безпеки Soti MobiControl аналогічно працюють як і політики Knox Manage, хіба що їхнє відображення подається більш структуровано і зрозуміло. Серед них варто виділити «OEMConfig», вона відкриває більш гнучке налаштування пристроїв таких як: Zebra, Honeywell, Samsung та інші. Це дозволяє мати доступ до ширших налаштувань вищевказаних пристроїв.

Профілі в MDM системах Knox Manage та SOTI MobiControl слугують шаблоном, який визначає, як саме має працювати пристрій у рамках вимог компанії. Вони є основним інструментом, який дозволяє централізовано адаптувати пристрої до потреб компанії, враховуючи їхній тип, функціональність та роль у корпоративній інфраструктурі.

3.2.3 Налаштування політик

Окрім політик безпеки є ще політики доступних програм та файлів завантаження. За їхньою допомогою можна обмежувати доступні додатки користувачам або відкривати доступ до закритих корпоративних додатків чи даних.

В Knox Manage є окреме вікно «Application», де зберігаються всі доступні додатки. Щоб добавити новий додаток потрібно вибрати для якої платформи пристроїв він призначений та його джерело (див. рисунок 3.12).

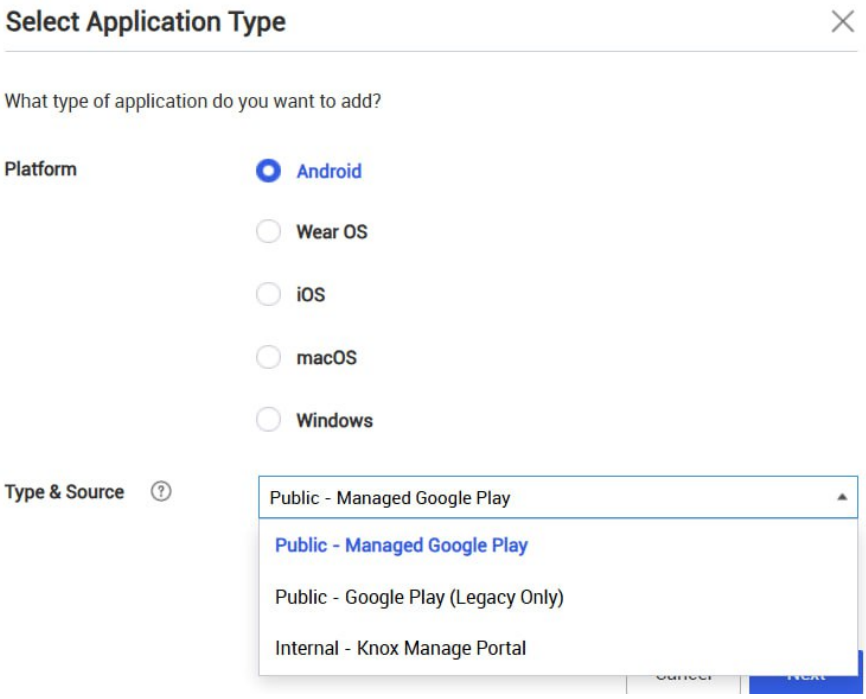

Рисунок 3.12 – Додавання нового додатку в Knox Manage

За платформу взято Android, оскільки це найпопулярніша ОС серед мобільних пристроїв. Є два типи джерел завантаження нових додатків: з Google Play Market та із apk файлу. Використовуючи перший тип можна добавити в список додатків програми із Play Market, по суті тут доступні всі ті самі додатки що може кожен завантажити. А за допомогою другого типу можна добавити додаток напряму із файлу apk, що може бути корисним для корпоративних додатків, які не опубліковані на загал.

Після того як необхідний додаток з’явився в загальному списку, його потрібно присвоїти відповідній групі. На рисунку 3.13 зображено процес додавання вибраного додатка у групу.

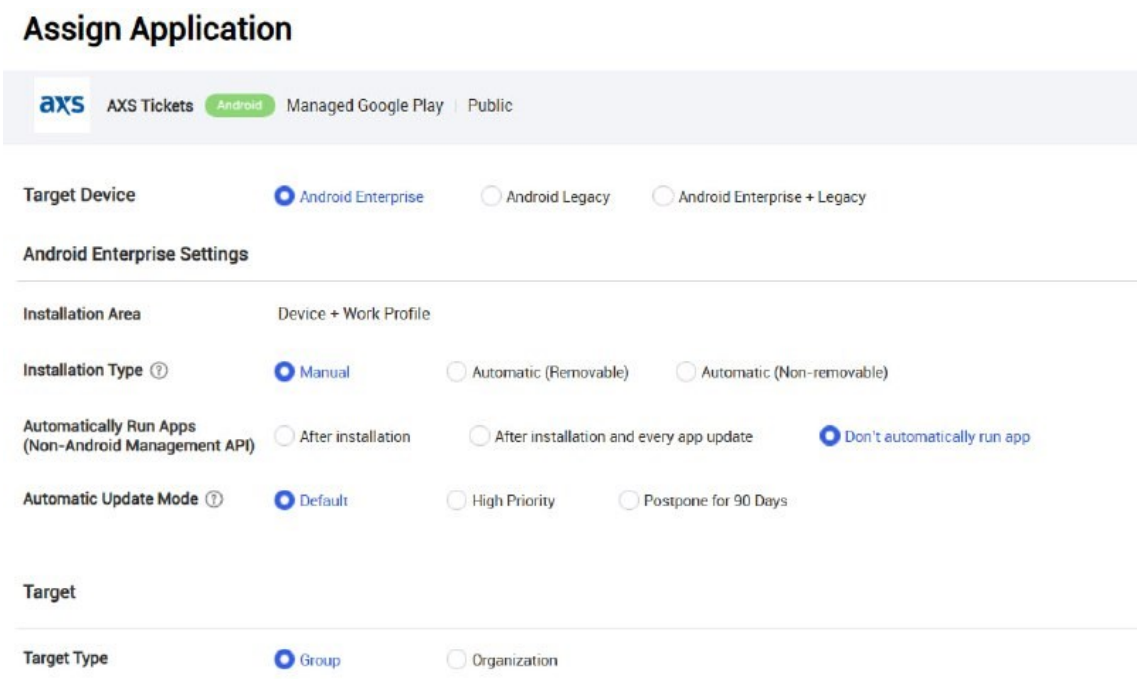

Рисунок 3.13 – Присвоєння додатка групі в Knox Manage

Тут можна задати налаштування додатку: ручне чи автоматичне завантаження, автозапуск та пріоритетність оновлення.

В SOTI MobiControl ця політика реалізована майже аналогічно, але є одна відмінність. Тут не можна потрапити в загальний список доступних додатків, замість цього є сторінка із різними політиками програм, тобто можна створити перелік необхідних додатків і вже цей перелік присвоювати відповідним групам, що є кращим рішенням, якщо необхідно присвоїти декільком групам список базових корпоративних додатків.

3.3 Процес заведення нових пристроїв в систему

Щоб керувати пристроями, адміністратору потрібно спершу їх додати в MDM систему. Існує багато способів завести пристрій в систему: за допомогою посилання, додатку, використовуючи QR-код. Але нижче розглянемо два абсолютно різних способи і умови для їхнього використання.

Оскільки Knox Manage це MDM система яка спеціалізується на пристроях Samsung, в неї є можливість завести пристрій Samsung із необхідним профілем ще до того як його дістануть із коробки. Це все відбувається за допомогою

Samsung Knox Admin Portal, на цьому порталі зберігаються дані про всі пристрої Samsung в системі(див. рисунок 3.14).

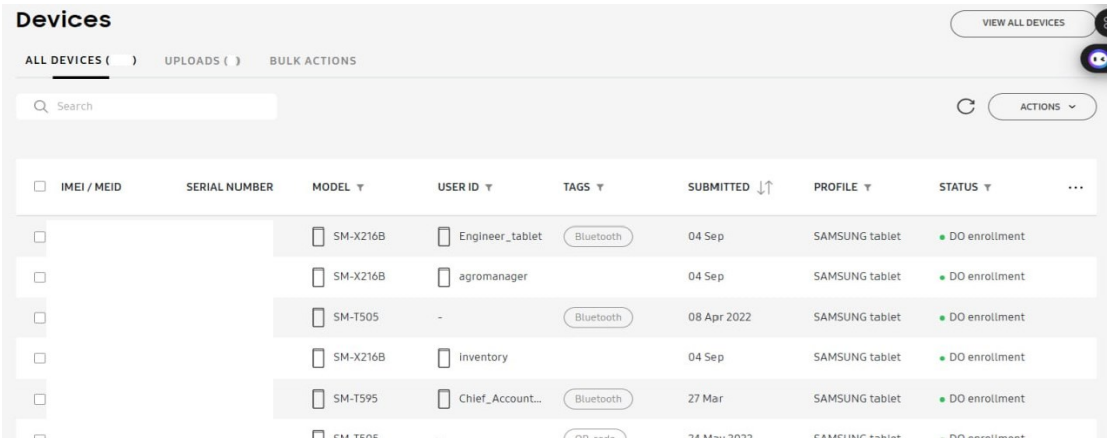

Рисунок 3.14 – Перелік пристроїв в Samsung Knox Admin Portal

Сюди пристрої може завести постачальник або адміністратор за допомогою мобільного застосунку Knox Deployment. Як вище було зазначено, для того щоб пристрою призначити потрібну групу спершу треба створити відповідного користувача. На рисунку 3.15 показано процес створення користувача.

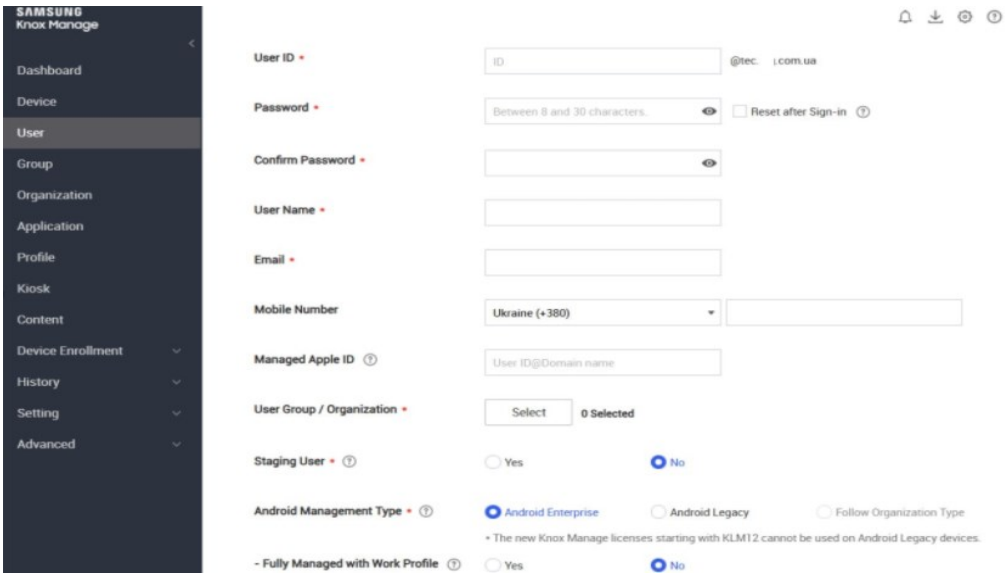

Рисунок 3.15 – Створення нового користувачка в Knox Manage

Користувач в Knox Manage може бути як конкретним співробітником компанії, так і сервісним користувачем для працівників конкретної посади або

відділу, тобто багато пристроїв можуть мати одного користувача. При створенні нового користувача потрібно задати: логін, пароль, назву, поштову скриньку і групу. Коли необхідний користувач є, то його можна призначити відповідному пристрою через Samsung Knox Admin Portal, таким чином разом із користувачем призначається відповідна група, а отже також профіль та політики (див. рисунок 3.16).

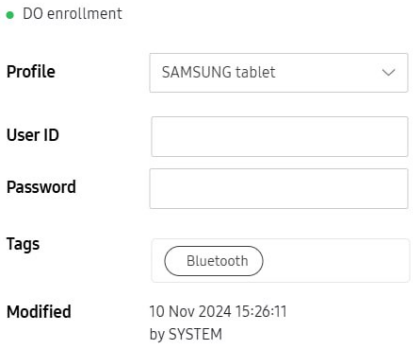

Рисунок 3.16 – Картка пристрою в Samsung Knox Admin Portal

Тепер при першому увімкнені пристрою буде відбуватися перевірка Knox на наявність реєстрації пристрою в Samsung Knox Admin Portal і після успішної перевірки завантажується агент та підтягується призначений користувач, група та профіль.

SOTI MobiControl використовує політику зарахування для додавання нового пристрою в систему. При створенні нової політики потрібно ввести її назву, далі вибрати тип профілю. Рисунок 3.17 зображує третій етап створення політики зарахування.

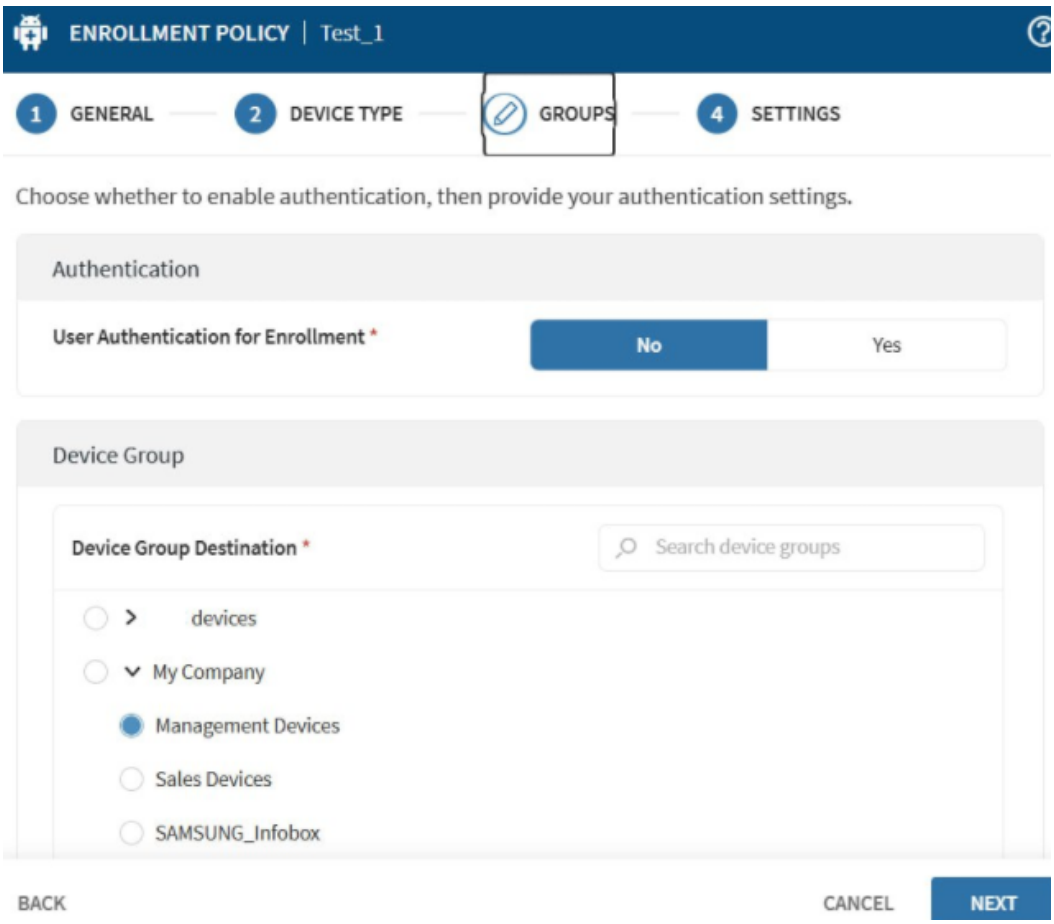

Рисунок 3.17 – Присвоєння політики групі в SOTI Mobicontrol

Окрім того що на цьому етапі потрібно присвоїти групу, також є можливість задати чи для заведення пристрою потрібна аутентифікація паролем. Зважаючи на те, що в SOTI MobiControl не має такої складової інфраструктури як користувачі, як в Knox Manage, тут можна включити додаткову перевірку, щоб обмежити доступ до системи чужим пристроям.

На наступному етапі потрібно прописати логіку автонумерації пристроїв, з якими назвами та порядковими номерами вони будуть відображатися в системі, в Knox Manage цю роботу виконує користувач, тобто в системі відображається назва яку задали при створенні користувача і згенерований порядковий номер. Також на четвертому етапі початкові налаштування пов’язані із заведенням пристрою в систему (див. рисунок 3.18).

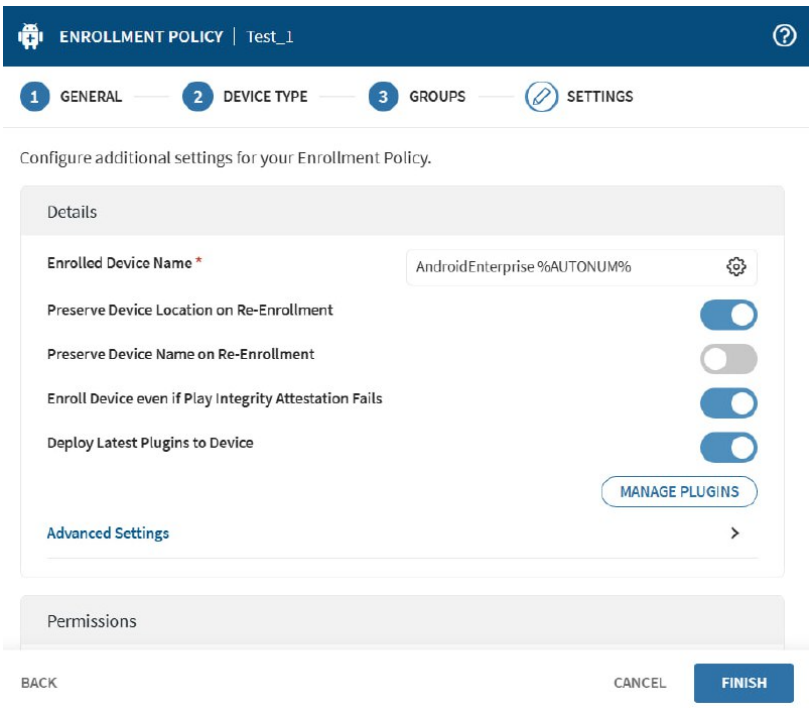

Рисунок 3.18 – Налаштування заведення пристроїв в SOTI MobiControl

Після створення політики зарахування, на основі ID політики генерується QR-код. На пристрої за допомогою сканера зчитується код і відбувається завантаження агенту та заведення пристрою в систему.

3.4 Інструменти управління пристроями

Коли є вже сформований парк мобільних пристроїв, адміністраторам потрібно ними керувати. Knox Manage і SOTI MobiControl мають ряд інструментів, які дозволяють ефективно управляти пристроями. Основні команди для керування мобільними пристроями:

– Віддалене підключення. Дозволяє дистанційно підключитись до пристрою;

– Перезавантаження. Дозволяє віддалено викликати перезавантаження пристрою;

– Геолокація пристрою. Дозволяє отримати поточну локацію мобільного пристрою та історію його переміщення, кількість записів залежить від налаштування політики;

– Керування додатками. Дозволяє запускати, видаляти та очищувати дані вибраних додатків.

Крім команд також присутня картка пристрою, що може надати базову інформацію про пристрій, таку як: серійний номер, mac-адресу, кількість вільного місця накопичувача, стан батареї та багато іншого. Це може стати в нагоді при вирішенні щоденних проблем, наприклад якщо пристрій має проблеми з підключенням до мережі Wi-fi, можна отримати ip або mac-адресу, що дозволить дослідити проблему зі сторони мережевого обладнання.

Слід виділити можливість в SOTI MobiControl створювати власні команди за допомогою скриптів. Використовуючи засоби Java script чи PowerShell можна наприклад увімкнути режим розробника, вимкнути автооберт екрану, від’єднатись від мобільної мережі і ще багато чого іншого. Також можна побудувати багатошаровий скрипт, який буде виконувати зразу декілька дій, що може бути надзвичайно корисним.

3.5 Підсумки дослідження систем Knox Manage та SOTI MobiControl

Порівнявши основні функції та особливості систем керування мобільними пристроями Knox Manage та SOTI MobiControl, можна зробити низку важливих висновків. Обидві системи є надійними рішеннями у сфері Mobile Device Management, проте вони орієнтовані на різні задачі та мають свої сильні сторони.

Knox Manage — це спеціалізована платформа, створена для роботи з пристроями Samsung. Її основна перевага — глибока інтеграція з екосистемою Samsung, що дозволяє максимально використовувати всі функції цих пристроїв. Завдяки цьому Knox Manage забезпечує високий рівень безпеки та простоту у налаштуванні. Веб-консоль цієї системи розроблена таким чином, щоб навіть користувачі без великого досвіду могли швидко розібратися з її інтерфейсом. Це робить Knox Manage ідеальним вибором для компаній, де важливо мінімізувати

час, витрачений на навчання адміністраторів. Серед основних можливостей системи можна виділити просте налаштування політик безпеки, управління конфігураціями пристроїв, а також функції захисту даних.

З іншого боку, SOTI MobiControl позиціонується як універсальне рішення для компаній, які працюють із пристроями різних виробників та платформ. Ця система забезпечує високу гнучкість і масштабованість, що робить її привабливою для великих організацій з широким спектром мобільних пристроїв. Веб-консоль SOTI MobiControl має розширений функціонал, зокрема можливість детального налаштування політик, управління застосунками та моніторингу стану пристроїв у реальному часі. Проте інтерфейс системи може здаватися складнішим для нових користувачів, що потребує більше часу на навчання. Водночас досвідчені адміністратори оцінять розширені можливості кастомізації й глибокий рівень контролю над пристроями.

Knox Manage найкраще підходить для невеликих і середніх компаній, які прагнуть швидко й ефективно налаштувати свої пристрої з акцентом на безпеку. Ця система є оптимальною для організацій, де більшість пристроїв — Samsung. Натомість SOTI MobiControl більше орієнтована на компанії з великою кількістю різнорідних пристроїв, які працюють на різних операційних системах.

Таким чином, вибір між Knox Manage та SOTI MobiControl залежить від конкретних потреб компанії. Якщо головний акцент робиться на безпеці пристроїв Samsung, швидкому розгортанні та простоті управління, то Knox Manage стане найкращим рішенням. Якщо ж організація потребує підтримки різних платформ, розширених інструментів моніторингу та детальних налаштувань, доцільніше обрати SOTI MobiControl. Обидві системи є сучасними інструментами для управління мобільними пристроями та добре справляються зі своїми задачами. Проте їхні сильні сторони варто оцінювати, виходячи з пріоритетів компанії та кількості пристроїв, що потребують управління.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Механізми мінімізації впливу іонізуючих випромінювань на працівників підприємств

Радіаційний захист — це система заходів, спрямованих на зменшення впливу іонізуючого випромінювання на людину. Основними завданнями радіаційного захисту є зниження рівня опромінення до безпечного та використання спеціальних споруд, що послаблюють інтенсивність випромінювання. Основна мета радіаційного захисту — забезпечити безпеку як працівників, які мають контакт із джерелами випромінювання, так і тих, хто взагалі не взаємодіє з ними, шляхом зменшення доз опромінення до допустимих меж. Проблема радіаційного захисту почала актуалізуватися після відкриття рентгенівських променів і радіоактивності. На початку XX століття зусилля були спрямовані на захист медичного персоналу, який працював із радіоактивними матеріалами. З розвитком ядерних технологій виникла потреба у захисті працівників ядерних підприємств та створенні ефективного захисту для ядерних реакторів. Сучасні підходи також враховують захист біосфери, включаючи безпечне захоронення радіоактивних відходів [46].

Розрізняють два основних види радіаційного впливу: зовнішнє опромінення, яке викликане джерелами випромінювання, що знаходяться поза тілом людини, та внутрішнє опромінення, спричинене радіонуклідами, що потрапляють в організм через їжу, воду, повітря або шкіру. Іонізуюча радіація поділяється на природну (фонову), яка виникає через випромінювання космосу та природних радіоактивних елементів у довкіллі, та штучну, що виникає внаслідок діяльності людини (медичні процедури, робота АЕС, ядерні випробування тощо). Вплив радіації на клітини організму може призводити до мутацій, змін у процесі ділення клітин, їхньої загибелі, розвитку ракових утворень і генетичних аномалій. Дослідження показують, що при опроміненні в білках можуть утворюватися аномальні амінокислоти, що порушують обмін

речовин. Особливу загрозу становлять генетичні мутації, які можуть передаватися майбутнім поколінням. Водночас природна радіація в невеликих дозах є одним із чинників еволюції, викликаючи 1–6% спонтанних мутацій [47].

Джерела іонізуючого випромінювання поділяються на такі групи: джерела для індивідуального опромінення, що впливають на окремих осіб або невеликі групи; джерела аварійного опромінення, які можуть викликати масове опромінення або радіоактивне забруднення довкілля; джерела майбутніх загроз, пов'язані з природними катастрофами або ненавмисним втручанням людини; та джерела для медичних процедур, таких як радіотерапія та радіодіагностика.

Захист від α-випромінювання є порівняно нескладним завданням через короткий пробіг α-частинок. Достатньо знаходитися на відстані понад 10 см від джерела та використовувати засоби індивідуального захисту, як-от одяг і рукавиці. Для захисту персоналу від β-випромінювання операції з β-радіонуклідами проводяться за екраном або в захисних шафах, а також розраховується товщина захисного екрану з урахуванням гальмівного випромінювання. Найбільш ефективними матеріалами для захисту від γ-випромінювання є свинець, залізо, бетон, вода та свинцеве скло. Рідше використовуються важкі метали, такі як вісмут чи тантал [46].

Ефективний радіаційний захист — це поєднання технічних, організаційних і правових заходів. Систематичний моніторинг, застосування сучасних матеріалів і технологій, а також підвищення обізнаності працівників допомагають мінімізувати ризики впливу іонізуючого випромінювання на людину.

4.2 Моделі оповіщення населення в умовах надзвичайних ситуацій техногенного та природного походження

Коли трапляються аварії або надзвичайні ситуації, які загрожують безпеці людей, важливо мати дієву систему оповіщення. Це дозволяє швидко попередити населення про можливу небезпеку. В Україні, з її великою кількістю заводів та природних об'єктів, організація системи оповіщення є дуже важливою. Системи

оповіщення класифікуються за кількома моделями: загальнодержавна, територіальна та об'єктова. Загальнодержавна система охоплює всю країну та базується на використанні державних мереж зв'язку, таких як телефонні, телеграфні, радіо та телевізійні мережі. Територіальні системи створюються на рівні областей, міст чи районів і координуються місцевими органами влади. Об'єктові системи діють на рівні окремих підприємств чи установ і забезпечують оперативне оповіщення працівників у разі небезпеки [48].

Для сповіщення використовують різні засоби. Наприклад, електросирени, які розміщують на важливих об'єктах, автоматично або вручну передають сигнал тривоги. Вони мають радіус дії від 3 до 5 км залежно від моделі. Крім того, для оповіщення використовують гудки підприємств і транспортних засобів. У невеликих районах або вночі можуть застосовуватися ручні сирени, мегафони та пересувні звукові станції.

Особливе місце займає сигнал «УВАГА ВСІМ!». Його подають для привернення уваги людей і повідомлення про небезпеку. Почувши цей сигнал, потрібно:

– Увімкнути радіо або телебачення, щоб дізнатися інформацію про ситуацію і рекомендації.
– Слухати повідомлення про аварію чи іншу надзвичайну ситуацію.
– Розповісти про це сусідам, щоб більше людей знали про небезпеку.
– Виконувати інструкції, які надають служби цивільного захисту.

Ефективна система оповіщення та правильні дії громадян можуть врятувати життя і зменшити збитки. Наприклад, якщо трапляється пожежа чи хімічна аварія, спеціальні сигнали або повідомлення допомагають зрозуміти, що робити. Важливо залишити небезпечну зону та виконувати інструкції служб. Зв'язок також грає важливу роль у цивільному захисті. Він організовується відповідно до рішень начальників цивільного захисту. Для цього використовують державні та відомчі мережі зв'язку. Державна мережа забезпечує більшу частину зв'язку й включає телефонні, телеграфні, поштові та радіомережі. Відомча мережа охоплює зв'язок у різних галузях, наприклад, у транспорті чи енергетиці. Для обміну інформацією використовуються

адміністративний, диспетчерський і технологічний зв'язок. У надзвичайних ситуаціях цей зв'язок працює через спеціальні мережі та радіостанції, які можуть бути стаціонарними або переносними. Це дозволяє швидко передавати повідомлення навіть у складних умовах. Стаціонарні системи зазвичай встановлюють на стратегічних об’єктах, тоді як переносні пристрої використовуються для оперативного реагування [50].

Оповіщення організовується на різних рівнях: загальнодержавному, територіальному та об'єктовому. Електросирени, як-от «С-40» чи «С-28», встановлюються на будівлях і підприємствах для передавання сигналів на велику відстань. «С-40», наприклад, забезпечує озвучення території в радіусі 300–700 м залежно від рівня шумів і висоти встановлення. Також використовуються сучасні супутникові системи та пейджери для передачі інформації. Інноваційні технології, такі як мобільні додатки, допомагають швидше поширювати інформацію серед населення [49].

Таким чином, наявність сучасних систем оповіщення та правильна організація зв'язку є важливими для захисту населення в разі небезпеки. Від оперативності таких систем залежить не тільки безпека людей, але й успішність дій у надзвичайних ситуаціях.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи магістра було проведено дослідження сучасних систем управління мобільними пристроями в корпоративному середовищі.

У першому розділі розглянуто актуальність теми та тенденції цифрової трансформації бізнесу, що обумовлюють зростання потреби у мобільних пристроях. Проаналізовано виклики та ризики, пов'язані з їх використанням, а також визначено необхідність впровадження систем управління мобільними пристроями для забезпечення безпеки та контролю.

У другому розділі представлено теоретичні аспекти систем управління мобільними пристроями, зокрема описано принципи роботи MDM-рішень, їх основні функціональні можливості та роль у корпоративній інфраструктурі. Було досліджено методи захисту даних, а також можливості моніторингу та адміністрування мобільних пристроїв.

У третьому розділі проведено порівняльний аналіз систем Knox Manage та SOTI MobiControl. Проаналізовано функціональні можливості обох рішень, їх переваги та недоліки для корпоративного використання. В результаті дослідження встановлено, що система SOTI MobiControl є більш гнучкою для великих підприємств завдяки розширеним можливостям налаштування та інтеграції, тоді як Knox Manage забезпечує високу безпеку і оптимальне управління для пристроїв Samsung.

У четвертому розділі «Охорона праці та безпека в надзвичайних ситуаціях» проаналізовано механізми впливу іонізуючих випромінювань на працівників підприємств. Описано моделі оповіщення населення в умовах надзвичайних ситуацій техногенного та природного походження.

ПЕРЕЛІК ДЖЕРЕЛ

1. Analysis of a cloud-based mobile device management solution on android phones: technological and organizational aspects. [Електронний ресурс] – Режим доступу: https://link.springer.com/article/10.1007/s42452-019-1819-z#Fig1 (дата звернення: 16.11.2024).

2. Mobile Device Management. [Електронний ресурс] – Режим доступу: https://www.fortinet.com/resources/cyberglossary/mobile-device-management (дата звернення: 16.11.2024).

3. Що таке Mobile Device Management і чи потрібен він вашій компанії? [Електронний ресурс] – Режим доступу: https://wiseit.com.ua/shho-take-mobile-device-management-i-chi-potriben-vin-vashij-kompaniyi/ (дата звернення16.11.2024).

4. Mobile Device Management. [Електронний ресурс] – Режим доступу: https://www.ibm.com/topics/mobile-device-management (дата звернення: 16.11.2024).

5. Work from Anywhere – But Only If You Have Strong Mobile Device Management. [Електронний ресурс] – Режим доступу: https://www.smartsheet.com/mobile-device-management (дата звернення: 16.11.2024).

6. Mobile device management guide: comprehensive insights. [Електронний ресурс] – Режим доступу: https://preyproject.com/blog/what-is-mobile-device-management-the-complete-guide (дата звернення: 16.11.2024).

7. Manage Mobile Devices and Policies in Active Directory. [Електронний ресурс] – Режим доступу: https://redmondmag.com/Articles/2015/02/01/Manage-Mobile-Devices.aspx?Page=1 (дата звернення: 16.11.2024).

8. Exchange ActiveSync in Exchange Server. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/exchange/clients/exchange-activesync/exchange-activesync?view=exchserver-2019&redirectedfrom=MSDN (дата звернення: 17.11.2024).

9. Mobile Device Provisioning with SyncML. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/archive/msdn-magazine/2009/february/going-places-mobile-device-provisioning-with-syncml (дата звернення: 17.11.2024).

10. OMA DM Protocol Support. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/windows/client-management/oma-dm-protocol-support (дата звернення: 17.11.2024).

11. The Ultimate Guide to FOTA. [Електронний ресурс] – Режим доступу: https://www.cavliwireless.com/blog/nerdiest-of-things/fota-why-update-firmware-over-the-air.html (дата звернення: 17.11.2024).

12. How Firmware Over the Air (FOTA) Updates Work on Android. [Електронний ресурс] – Режим доступу: https://www.esper.io/blog/firmware-over-the-air-fota-updates-on-android (дата звернення: 17.11.2024).

13. Zero-touch enrollment for IT admins. [Електронний ресурс] – Режим доступу: https://support.google.com/work/android/answer/7514005?hl=en&ref_topic=13623761&sjid=7743794633608972254-EU#zippy=%2Cget-started%2Caccessing-the-portal%2Cconfigurations%2Cdevices (дата звернення: 17.11.2024).

14. The Definitive Guide to EMM Device Enrollment: Exploring Android Zero-Touch and Other Enrollment Methods. [Електронний ресурс] – Режим доступу: https://socialmobile.com/the-definitive-guide-to-emm-device-enrollment-exploring-android-zero-touch-and-other-enrollment-methods/ (дата звернення: 17.11.2024).

15. Enroll your Android Enterprise dedicated, fully managed, or corporate-owned with work profile devices. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/mem/intune/enrollment/android-dedicated-devices-fully-managed-enroll (дата звернення: 17.11.2024).

16. Samsung Knox vs. SOTI: An Indian IT Manager's Perspective on the Ultimate MDM Showdown. [Електронний ресурс] – Режим доступу: https://siriusstar.in/mobility-solutions-blogs?view=1&view_row_id=1710944&view_w_id=2153470&view_p_id=1234507 (дата звернення: 17.11.2024).

17. Samsung Knox Solutions for Device Customization. [Електронний ресурс] – Режим доступу: https://www.samsungknox.com/en/solutions/device-customization (дата звернення: 18.11.2024).

18. Samsung Knox for Android. [Електронний ресурс] – Режим доступу: https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/the-samsung-knox-platform/ (дата звернення: 18.11.2024).

19. Core Platform Security: Root of Trust. [Електронний ресурс] – Режим доступу: https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/root-of-trust/ (дата звернення: 18.11.2024).

20. Trusted Root in Samsung Mobile Devices. [Електронний ресурс] – Режим доступу: https://insights.samsung.com/2018/01/26/starting-from-scratch-trusted-root-in-samsung-mobile-devices/ (дата звернення: 18.11.2024).

21. Knox Vault Security. [Електронний ресурс] – Режим доступу: https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/knox-vault/ (дата звернення: 18.11.2024).

22. Trusted Boot Overview. [Електронний ресурс] – Режим доступу: https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/trusted-boot/ (дата звернення: 18.11.2024).

23. Real-Time Kernel Protection. [Електронний ресурс] – Режим доступу: https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/real-time-kernel-protection/ (дата звернення: 18.11.2024).

24. Sensitive Data Protection. [Електронний ресурс] – Режим доступу: https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/sensitive-data-protection/ (дата звернення: 18.11.2024).

25. DualDAR Encryption. [Електронний ресурс] – Режим доступу: https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/app-and-data-protection/dualdar-encryption/ (дата звернення: 18.11.2024).

26. Knox Manage. [Електронний ресурс] – Режим доступу: https://docs.samsungknox.com/admin/knox-manage/introduction/about-knox-manage/ (дата звернення: 18.11.2024).

27. Features and Key Strengths of Knox Manage. [Електронний ресурс] – Режим доступу: https://docs.samsungknox.com/admin/knox-manage/introduction/features-and-key-strengths/ (дата звернення: 18.11.2024).

28. Knox Configure Overview. [Електронний ресурс] – Режим доступу: https://docs.samsungknox.com/admin/knox-configure/ (дата звернення: 18.11.2024).

29. Knox Asset Intelligence. [Електронний ресурс] – Режим доступу: https://docs.samsungknox.com/admin/knox-asset-intelligence/ (дата звернення: 18.11.2024).

30. Knox Guard Overview. [Електронний ресурс] – Режим доступу: https://docs.samsungknox.com/admin/knox-guard/ (дата звернення: 18.11.2024).

31. SOTI One Platform Analysis. [Електронний ресурс] – Режим доступу: https://soti.net/media/4267/202101-brochure-hr-hiring-emea-a4.pdf#page=7.23 (дата звернення: 18.11.2024).

32. Analyzing the SOTI One Platform. [Електронний ресурс] – Режим доступу: https://soti.net/resources/analyzing-the-soti-one-platform/ (дата звернення: 20.11.2024).

33. SOTI MobiControl Review. [Електронний ресурс] – Режим доступу: https://www.techradar.com/reviews/soti-mobicontrol-mdm (дата звернення: 20.11.2024).

34. Using Indoor Location with SOTI XSight. [Електронний ресурс] – Режим доступу: https://www.soti.net/sotixsight/help/v2025.0/en/live_view/indoor_location/using_indoor_location.html (дата звернення: 20.11.2024).

35. Adding Indoor Location with SOTI XSight. [Електронний ресурс] – Режим доступу: https://www.soti.net/sotixsight/help/v2025.0/en/live_view/indoor_location/adding_an_indoor_location.html (дата звернення: 20.11.2024).

36. Device Policies in SOTI MobiControl. [Електронний ресурс] – Режим доступу: https://soti.net/resources/help/mobicontrol/en/device_policies/ (дата звернення: 20.11.2024).

37. Honeywell and SOTI Partnership Brings Security, Remote Management to One Million Industrial Mobile Devices. [Електронний ресурс] – Режим доступу: https://www.honeywell.com/us/en/press/2023/12/honeywell-and-soti-partnership-brings-security-remote-management-to-one-million-industrial-mobile-devices (дата звернення: 20.11.2024).

38. SOTI Continues to Support Windows Mobile and Windows CE Devices. [Електронний ресурс] – Режим доступу: https://soti.net/resources/blog/2023/soti-continues-to-support-windows-mobile-and/ (дата звернення: 20.11.2024).

39. SOTI MobiControl Help. [Електронний ресурс] – Режим доступу: https://www.soti.net/mc/help/v14.0/en/start.html (дата звернення: 20.11.2024).

40. SOTI MobiControl. [Електронний ресурс] – Режим доступу: https://mobilitysolutions.cz/eng/products/soti-en/soti-mobicontrol (дата звернення: 20.11.2024).

41. Diagnostic Intelligence to Minimize Downtime and Maximize Your Return On Investment. [Електронний ресурс] – Режим доступу: https://www.soti.net/xsight (дата звернення: 20.11.2024).

42. SOTI XSight. [Електронний ресурс] – Режим доступу: https://mobilitysolutions.cz/eng/products/soti-en/soti-xsight-en (дата звернення: 20.11.2024).

43. SOTI Connect. [Електронний ресурс] – Режим доступу: https://mobilitysolutions.cz/eng/products/soti-en/soti-connect-en (дата звернення: 20.11.2024).

44. Knox Manage License. [Електронний ресурс] – Режим доступу: https://www.samsung.com/us/business/software/knox/knox-manage/knox-manage-1-year-license-mi-kxkmswwc210/ (дата звернення: 20.11.2024).

45. SOTI MobiControl pricing plan. [Електронний ресурс] – Режим доступу: https://www.capterra.com/p/133554/Soti-MobiControl/pricing/ (дата звернення: 20.11.2024).

46. Христич О.В. Матеріали спеціального призначення захисту від іонізуючого випромінювання конспект лекцій. Харків НУЦЗ України, 2022. 21 с.

47. Про захист людини від впливу іонізуючого випромінювання. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/15/98-вр#Text (дата звернення: 20.11.2024).

48. Оповіщення при надзвичайних ситуаціях, ситуаціях техногенного та природного характеру. [Електронний ресурс] – Режим доступу: https://ts.kiev.ua/opovishchennia-pry-nadzvychainykh-sytuatsiiakh-sytuatsiiakh-tekhnohennoho-ta-pryrodnoho-kharakteru/ (дата звернення: 20.11.2024).

49. Організація управління, оповіщення і зв'язку в районі надзвичайної ситуації. [Електронний ресурс] – Режим доступу: https://virt.ldubgd.edu.ua/mod/page/view.php?id=1857 (дата звернення: 20.11.2024).

50. Надзвичайні ситуації та їх класифікація. [Електронний ресурс] – Режим доступу: https://osvita.ua/vnz/reports/bjd/22895/ (дата звернення: 20.11.2024).

51. Слободян П.С., Небесний Р.М. "Актуальність проблем оцінювання якості програмного забезпечення". ТНТУ. 2018. 232–233 с.

52. Pankiv, N., Kunanets, O., Artemenko, N., Veretennikova, N., and Nebesnyi, R., "Project of an Intelligent Recommender System for Parking Vehicles in Smart Cities," Proceedings of the 2021 IEEE 16th International Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine, 2021, pp. 419-422.

53. Duda O., Kochan V., Kunanets N., Matsiuk O., Pasichnyk V., Sachenko A., Pytlenko T. Data processing in IoT for smart city systems. Metz, France, 18–21 September 2019; Volume 1, pp. 96–99.

54. Strutynska I., Kozbur H., Dmytrotsa L., Sorokivska O., Melnyk L. Influence of Digital Technology on Roadmap Development for Digital Business Transformation. Ceske Budejovice : Ternopil National Economic University and University of South Bohemia, 2019. P. 333–337

55. Barannik V. V., Karpinski M. P., Tverdokhleb V. V., Barannik D. V., Himenko V. V., Aleksander M. The technology of the video stream intensity controlling based on the bit-planes recombination. 2018. P. 25-28.

ДОДАТКИ

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Наукове товариство ім. Т.Шевченка

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник
тез доповідей

XIII Міжнародної науково-практичної конференції молодих учених та студентів
11-12 грудня 2024 року

УКРАЇНА
ТЕРНОПІЛЬ – 2024

Матеріали XIII Міжнародної науково-практичної конференції молодих учених та студентів
«АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ» – Тернопіль, 11-12 грудня 2024 року

УДК 004.62

О.Д. Пакон, Р.М. Небесний, доктор філософії
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНАЛІЗ ЕФЕКТИВНОСТІ ВПРОВАДЖЕННЯ MDM СИСТЕМ ДЛЯ КОРПОРАТИВНОГО СЕРЕДОВИЩА

O. D. Pakon, R.M. Nebesnyi Ph.D

ANALYSIS OF THE EFFICIENCY OF THE IMPLEMENTATION OF MDM SYSTEMS FOR THE CORPORATE ENVIRONMENT

За останнє десятиліття мобільні та портативні пристрої стали основою бізнес-стратегії будь-якої організації, адже вони суттєво підвищують мобільність, ефективність та гнучкість робочих процесів. Управління мобільними пристроями (MDM) відіграє ключову роль у цьому процесі, допомагаючи організаціям впроваджувати, забезпечувати безпеку, моніторити, інтегрувати та управляти такими пристроями, як смартфони, ноутбуки, планшети, а також іншими IoT-пристроями [1].

У 2023 році понад 70% підприємств відзначили значні покращення продуктивності завдяки впровадженню рішень для управління мобільними пристроями. Ця статистика яскраво ілюструє, наскільки важливими стали MDM-системи для ефективної організації робочих процесів у цифрову епоху. Компанії, які все більше покладаються на мобільні пристрої для виконання щоденних операцій, стикаються з необхідністю забезпечення їх ефективного, безпечного та безперебійного функціонування. MDM-рішення забезпечують централізовану платформу для управління флотом пристроїв, дозволяючи автоматизувати такі завдання, як застосування оновлень програмного забезпечення, встановлення патчів безпеки та впровадження змін у політиках доступу. Завдяки цьому значно зменшуються час і зусилля, необхідні для ручного втручання, а IT-команди можуть більше зосередитися на стратегічних завданнях, таких як інновації та масштабування систем.

Крім того, автоматизовані процеси, що пропонуються MDM-системами, знижують ризик людських помилок, що сприяє більш стабільній та безпечній роботі пристроїв. Інструменти MDM також забезпечують доступу до інформації про стан пристроїв, рівень їх продуктивності та використання, що дозволяє оперативно реагувати на проблеми та оптимізувати робочі процеси.

Таким чином, завдяки можливостям, які надають сучасні MDM-рішення, підприємства можуть підтримувати безперебійну діяльність, забезпечуючи високу продуктивність і надійність своїх мобільних інфраструктур, навіть у процесі адаптації до нових викликів і технологій [2].

Література

1. Mobile Device Management (MDM) in Organizations, Diksha Barthwal. 2016. – Режим доступу до ресурсу:https://www.researchgate.net/publication/305380830_Mobile_Device_Management_MDM_in_Organizations.

2. How Mobile Device Management (MDM) Revolutionizes Employee Productivity– Режим доступу до ресурсу: https://bestructured.com/how-mobile-device-management-mdm-revolutionizes-employee-productivity/

Матеріали XIII Міжнародної науково-практичної конференції молодих учених та студентів «АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ» – Тернопіль, 11-12 грудня 2024 року

УДК 004.62

О.Д. Пакон, Р.М. Небесний, доктор філософії.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОСНОВНІ ВИКЛИКИ ДЛЯ СИСТЕМ КЕРУВАННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ

O. D. Pakon, R.M. Nebesnyi, Ph.D

MAIN CHALLENGES FOR MOBILE DEVICE MANAGEMENT SYSTEMS

Значні проблеми, які мобільні пристрої створюють для будь-якого бізнесу, надзвичайно поширені, але все одно їх потрібно вирішувати. Якщо залишити напризволяще, деякі з цих проблем можуть перетворитися на досить серйозні вразливості.

Керування мобільними пристроями (MDM) може стикатися з певними проблемами, які організації повинні вирішити. Серед поширених проблем керування мобільними пристроями:

- Безпека. За своєю природою мобільні пристрої можуть становити ризик для будь-якої компанії. Це пояснюється тим, що вони в основному використовують інформацію за межі системи та інфраструктури робочого місця, що потенційно може призвести до витоку важливої інформації;
- Принеси свій власний пристрій (BYOD). Програми BYOD дозволяють співробітникам використовувати власні пристрої на роботі. Хоча це може принести переваги продуктивності, воно також пов'язане з низкою власних проблем: ризики безпеки, проблеми сумісності, вразливість до атак і зловмисного програмного забезпечення, відсутність керування/контролю пристрою;
- Втрата пристрою. Мобільні пристрої неймовірно вразливі до втрати чи викрадення, що несе серйозні наслідки для бізнесу [1].
- Сумісність додатків. Забезпечення сумісності додатків може бути складним завданням, особливо коли компанія має справу з великою кількістю пристроїв із різноманітними вимогами до додатків. Рішення MDM повинні пропонувати надійні можливості керування програмами, щоб оптимізувати розгортання, оновлення та видалення програм.
- Різноманітність пристроїв. Велика різноманітність мобільних пристроїв і операційних систем може стати проблемою в управлінні та підтримці різнорідних середовищ пристроїв. Організаціям може знадобитися забезпечити сумісність із кількома моделями пристроїв, платформами та версіями ОС, що може вимагати додаткових зусиль і ресурсів [2].

Більшість сучасних МДМ систем успішно справляються з цими викликами, в тому числі Samsung Knox та Soti Mobicontrol, які розглядаються у роботі.

Література

1. Common Mobile Device Management (MDM) Challenges and How to Solve Them 2024. –Режим доступу до ресурсу: https://www.burstfire.net/blog/common-mdm-challenges-and-how-to-solve-them
2. What are the challenges of mobile device management?– Режим доступу до ресурсу: https://www.quora.com/What-are-the-challenges-of-mobile-device-management