ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНОЛОГІЯ УПРАВЛІННЯ КОРПОРАТИВНИМИ МОБІЛЬНИМИ ПРИСТРОЯМИ ТА ЇХ ЗАХИСТУ НА БАЗІ РІШЕННЯ MICROSOFT INTUNE»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

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

Виконав: здобувач(ка) вищої освіти групи БСДМ-63
Дорош Сергій
(ПРІЗВИЩЕ, Ім'я)

Керівник: Собчук Андрій
Доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___”_____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дорошу Сергію Валерійовичу
(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи:
«Технологія управління корпоративними мобільними пристроями та їх захисту на базі рішення Microsoft Intune»
керівник кваліфікаційної роботи: Собчук Андрій, доцент
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «» р. .

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
інформаційна система організації;
технологія управління корпоративними мобільними пристроями та їх захисту на базі рішення Microsoft Intune;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз необхідності контролю доступу до мережі на основі застосування політик пристроїв і користувачів корпоративних мереж.
2. Методи та засоби управління мережевим доступом організацій.

3. Розроблення варіанта технологія управління корпоративними мобільними пристроями та їх захисту на базі рішення Microsoft Intune

5. Перелік ілюстративного матеріалу:
Презентація PowerPoint

6. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Дослідження актуальності проблеми управління привілеями в інформаційній системі організації	19.10.2023 р.	
2.	Аналіз наукової та технічної літератури за темою кваліфікаційної роботи.	22.10.2023 р.	
3.	Аналіз необхідності контролю доступу до мобільних пристроїв на основі застосування політик пристроїв і	27.10. 2023р.	
4.	Методи та засоби управління мережевим доступом організацій	03.11.2023 р.	
5.	Розроблення варіанта технологія управління корпоративними мобільними пристроями та їх захисту на базі рішення Microsoft Intune	15.11.2023 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	26.11.2023 р.	
7.	Підготовка доповіді до захисту.	15.12.2023 р.	

Здобувач(ка) вищої освіти _____ Сергій ДОРОШ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Андрій СОБЧУК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня магістра

Направляється здобувач Дорош С.В до захисту кваліфікаційної роботи
(прізвище та ініціали)

За спеціальністю 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія управління корпоративними мобільними пристроями та їх захисту на базі рішення Microsoft Intune».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

Висновок керівника кваліфікаційної роботи

Керівник кваліфікаційної роботи _____ Андрій СОБЧУК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*
"____" _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач(ка) Дорош Сергій. допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача Дороша Сергія
на тему: «Технологія управління корпоративними мобільними пристроями та їх захисту на базі рішення Microsoft Intune».

Актуальність:

Дослідження актуальності технології управління корпоративними мобільними пристроями та їх захисту на базі Microsoft Intune відображає важливість розуміння сучасних викликів і можливостей, що стоять перед сучасними бізнесами.

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми забезпечення контролю керування мобільними пристроями в інфраструктурі .
2. Досліджено методи та засоби керування мобільними пристроями.
3. Запропоновано варіант технології керування на базі технології Microsoft Intune.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У кваліфікаційній роботі доцільно було б більш детально описати різні групи користувачів мобільних пристроїв у організації.
2. Запропонований варіант варіант технології управління доступом до мережі організації на базі рішення Microsoft Intune доцільно було б показати на прикладі конкретного підприємства.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «» здобувач **ДОРОШ Сергій** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент:
д.т.н., професор _____ _____
підпис *Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи и на здобуття освітнього ступеня магістра: 62 сторіноки, 6 рисунків, 1 таблиці, 9 джерел.

Об'єкт дослідження – процес контролю доступу мобільних пристроїв до інфраструктури підприємства.

Предмет дослідження – технологія контролю мобільними пристроями на базі рішення Microsoft Intune .

Мета роботи – розробити варіант розгортання технології контролю за мобільними пристроями на базі рішення Microsoft Intune для інформаційної системи організації та рекомендації щодо застосування технології

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу контролю доступу до мережі на базі рішення Microsoft Intune.

В роботі проведено аналіз проблеми контролю доступу до мережі на основі застосування політик пристроїв і користувачів корпоративних мереж. Проаналізовано існуючі технології контролю доступу до мережі організації.

Досліджено методи та засоби управління доступом до мережі організацій.

Запропоновано варіант технології управління доступом та керування пристроями на базі рішення Microsoft Intune. Визначено призначення, основні функції та склад компонентів даної технології.

На основі проведених досліджень, в роботі розроблено варіант впровадження на базі рішення Microsoft Intune для різної кількості користувачів організації

Галузь використання – кібербезпека інфраструктури компанії.

ABSTRACT

The text part of the qualification work and for obtaining the master's degree: 63 pages, 3 figures, 1 table, 8 sources.

Object of research - is the process of controlling the access of mobile devices to the enterprise infrastructure.

Subject of research - is mobile device control technology based on the Microsoft Intune solution.

The purpose of the work is to develop an option for deploying mobile device control technology based on the Microsoft Intune solution for the organization’s information system and recommendations for using the technology

Research methods – study of the literature on this topic, analysis of operating documentation, international standards and their comparison, modeling of the network access control process based on the Microsoft Intune solution.

The paper analyzes the problem of network access control based on the application of policies of devices and users of corporate networks. Existing access control technologies to the organization's network were analyzed.

The methods and means of managing access to the network of organizations have been studied.

A version of access control technology and device management based on the Microsoft Intune solution is offered. The purpose, main functions and composition of the components of this technology are defined.

On the basis of the conducted research, the paper developed an implementation option based on the Microsoft Intune solution for a different number of users of the organization

The field of use is cyber security of the company's infrastructure.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

MDM - Mobile Device Managed

MAM - Mobile Application Management

ADD - Azure Active Directory

BYOD - Bring Your Own Device

VPN - Virtual Private Network

SDK - Software Developer Kit

EMM – Enterprise Mobile Management

ВСТУП

Актуальність дослідження. Дослідження актуальності технології управління корпоративними мобільними пристроями та їх захисту на базі Microsoft Intune відображає важливість розуміння сучасних викликів і можливостей, що стоять перед сучасними бізнесами.

З поглибленням використання мобільних пристроїв у корпоративному середовищі зростає не лише кількість, а й різноманітність загроз для безпеки даних. Підприємства потребують ефективних та надійних засобів управління цими пристроями, а також захисту конфіденційної інформації.

Дослідження в цій області дозволяє краще розуміти переваги та можливості, які надає Microsoft Intune, його потенціал у забезпеченні безпеки даних та управлінні корпоративними пристроями. Також воно сприяє виявленню найкращих практик у впровадженні цієї технології, адаптації до змін у бізнес-середовищі та вирішенню проблем, пов'язаних з безпекою даних.

Враховуючи швидкі темпи зростання та розвитку цифрових технологій, дослідження у цій області є критично важливим для бізнесу будь-якої масштабності, щоб забезпечити ефективність роботи та захист конфіденційної інформації в умовах постійних змін і загроз безпеці.

Об’єкт дослідження – процес контролю доступу мобільних пристроїв до інфраструктури підприємства

Предмет дослідження – технологія контролю мобільними пристоями на базі рішення Microsoft Intune

Мета роботи – розробити варіант розгортання технології контролю за мобільними пристроями на базі рішення Microsoft Intune для інформаційної системи організації та рекомендації щодо застосування технології.

Наукові завдання:

- провести аналіз питання щодо необхідності контролю доступу до додатків організації;
- проаналізувати основні загрози інформаційній системі організації;
- проаналізувати продукти представлені на ринку України
- розробити варіант з тест-кейсами для імплеметації рішення в інфраструктуру

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу контролю доступу до мережі на базі рішення Microsoft Intune.

1 АНАЛІЗ НЕОБХІДНОСТІ ВПРОВАДЖЕННЯ В ІНФРАСТУРКТУРУ СИСТЕМИ УПРАВЛІННЯ КОРПОРАТИВНИМИ ПРИСТРОЯМИ

1.1. Оцінка потреб корпорації в управлінні мобільними пристроями

Розглядаючи проблематику оцінки потреб корпорації в управлінні мобільними пристроями, розглянемо кілька ключових аспектів та можливі проблеми, які можуть виникнути:

Різноманітність пристроїв та операційних систем:

Корпорації зазвичай стикаються з широким спектром мобільних пристроїв різних виробників, моделей та операційних систем, таких як Android, iOS, Windows та інші. Кожна з цих платформ має свої особливості, вимоги до безпеки та різні методи управління:

- Різноманітність моделей: Компанії можуть мати велику кількість моделей мобільних пристроїв, що вимагає врахування різниць у характеристиках та можливостях кожної моделі при розробці стратегій управління.
- Операційні системи: Крім різноманітності моделей, різні операційні системи (iOS, Android, Windows) потребують індивідуального підходу до управління, оскільки вони мають власні протоколи безпеки та оновлення.
- Сумісність інфраструктури: Різноманітність може створювати виклики у впровадженні єдиної інфраструктури для управління цими пристроями.
- Стандартизація управління: Неможливість встановлення єдиної системи управління через різні операційні системи може ускладнити стандартизацію процесів.

Стратегії вирішення:

- Використання MDM/EMM: Використання систем управління мобільними пристроями (MDM/EMM) може допомогти забезпечити централізоване керування різноманітними пристроями та операційними системами.

- Стандартизація політик безпеки: Розробка стандартів безпеки, які можуть застосовуватися на різних операційних системах, дозволить забезпечити єдність заходів безпеки [1].

1. Безпека даних та загрози:

Однією з найбільших та найбільш актуальних проблем при управлінні мобільними пристроями є забезпечення безпеки конфіденційної інформації, яка може бути збережена на цих пристроях. Загрози безпеці включають втрату пристроїв, крадіжку інформації, атаки з метою отримання доступу до корпоративних даних та інші:

- Проблемою є можливість втрати або крадіжки мобільних пристроїв, які можуть призвести до доступу до конфіденційної інформації.
- Атаки з метою отримання доступу: Кіберзлочинці можуть намагатися отримати доступ до даних через віруси, фішингові атаки або використання слабкостей безпеки.
- Втрата чи витік конфіденційної інформації може мати серйозні наслідки для компанії та клієнтів.
- Неоднорідність заходів безпеки: Різні операційні системи та моделі пристроїв можуть вимагати різних заходів для забезпечення безпеки, що ускладнює розробку єдиної стратегії.
- Використання шифрування та аутентифікації: Застосування шифрування даних на пристроях та багаторівневої аутентифікації може допомогти уникнути несанкціонованого доступу.

5. Управління та підтримка пристроїв:

Підтримка та оновлення мобільних пристроїв для великої кількості співробітників може стати складною. Потрібна чітка стратегія оновлення операційних систем, програмного забезпечення та підтримки для різних моделей пристроїв.

6. Неоднорідність потреб різних відділів/підрозділів:

Різні відділи можуть мати власні потреби у функціональності мобільних пристроїв. Наприклад, вимоги маркетингу можуть відрізнятися від потреб фінансового відділу, що вимагає індивідуальних стратегій управління.

Вимоги до додатків та програмного забезпечення: Наприклад, відділ маркетингу може вимагати специфічних додатків для аналізу даних, тоді як фінансовий відділ може бажати доступ до фінансових програм. Потреби в безпеці та доступі до даних. Різні відділи можуть мати різні рівні важливості безпеки та доступу до певних даних. Врахування різниці у потребах різних відділів при розробці універсальної стратегії управління мобільними пристроями. Різні відділи можуть вимагати використання різних моделей пристроїв або операційних систем, що може ускладнити стандартизацію. Важливо активно співпрацювати з представниками різних відділів, щоб зрозуміти їхні потреби та вимоги.

7. Забезпечення відповідності та політики безпеки:

Потреба в визначенні та узгодженні стратегії управління корпоративними мобільними пристроями виникає через велику різноманітність вимог до безпеки та функціональності. Різні структурні підрозділи компанії можуть мати відмінні потреби у забезпеченні безпеки даних, доступі до програм та інших можливостей на мобільних пристроях. Необхідно збалансувати ці вимоги та розробити стратегію, що задовольняє потреби всіх відділів, а також враховує різноманітність моделей та операційних систем. Узгодження такої стратегії вимагає тісної співпраці між IT-відділом, керівництвом компанії та представниками різних підрозділів для визначення пріоритетів, розробки єдиної політики безпеки та управління, що враховує потреби всіх структурних підрозділів компанії. Такий підхід дозволяє створити універсальні стратегії, що покращують безпеку, ефективність та спрощують управління мобільними пристроями в корпоративному середовищі.

8. Вплив на продуктивність та робочі процеси:

Однією з ключових проблем при впровадженні технологій управління корпоративними мобільними пристроями є необхідність відповідності до регулятивних стандартів та політик безпеки. Компанії повинні дотримуватися законодавчих вимог, які стосуються збереження та обробки конфіденційної інформації, особливо на мобільних пристроях. Це включає в себе захист особистих даних співробітників та клієнтів, відповідність стандартам безпеки (наприклад, GDPR, HIPAA, PCI DSS) та інші регуляторні вимоги. Успішне впровадження стратегій управління мобільними пристроями вимагає ретельного аналізу законодавства, розробки політик безпеки, які враховують ці вимоги, і постійного моніторингу для забезпечення відповідності. Створення і ефективне виконання політик, що відповідають регулятивним стандартам, стає важливим елементом успішного та безпечного управління корпоративними мобільними пристроями.

9. Необхідність визначення та узгодження стратегії управління:

Необхідність визначення та узгодження стратегії управління корпоративними мобільними пристроями випливає з потреби створення консистентного та ефективного середовища для їхнього управління в рамках організації. Ця стратегія повинна охоплювати не лише аспекти безпеки та технічного аспекту, а й враховувати індивідуальні потреби відділів, забезпечуючи їм необхідні інструменти для ефективної роботи. Ключовим елементом є співпраця між відділами технологій, безпеки та керівництвом компанії, щоб збалансувати вимоги до безпеки даних та робочої продуктивності. Такий підхід дозволяє створити єдину стратегію, що відповідає потребам всієї організації, покращуючи ефективність управління мобільними пристроями та забезпечуючи співвідношення між безпекою та зручністю використання.

1.2. Аналіз загроз безпеці у корпоративному середовищі пов’язаних з використанням мобільних пристроїв

Використання мобільних пристроїв у корпоративних середовищах є невід'ємною частиною сучасного бізнесу, проте це також створює потенційні загрози для безпеки даних і інфраструктури компанії. Однією з головних загроз є втрата чи крадіжка мобільних пристроїв, яка може призвести до витоку конфіденційної інформації. Втрата контролю над такими пристроями може викликати доступ до корпоративних даних та вразливості у безпеці.

Фішингові атаки та використання шкідливих програм також становлять значні ризики. Злоумисники можуть використовувати різноманітні соціальні інженерні методи для отримання доступу до чутливих даних, шляхом спроб отримати важливу інформацію через маніпуляцію користувачів.

Використання відкритих або ненадійних мереж Wi-Fi також може стати причиною загроз. Це може призвести до несанкціонованого доступу до пристроїв та інформації, що зберігається на них.

Крім того, існує ризик від використання ненадійних додатків або програм, які можуть містити шкідливий код або несанкціонований доступ до даних. Це може призвести до витоку конфіденційних даних чи порушення безпеки компанії.

Аналіз цих загроз дозволяє розробляти комплексні стратегії безпеки, які включають в себе застосування шифрування даних, управління доступом до інформації, регулярні оновлення програмного забезпечення та навчання персоналу щодо практик безпечного використання мобільних пристроїв. Тільки поєднання технологій та освіти забезпечить найвищий рівень захисту в умовах постійно зростаючих кіберзагроз. [2]

1.3 Визначення переваг впровадження системи MDM

Управління мобільними пристроями (MDM) в корпоративному середовищі відіграє важливу роль у забезпеченні безпеки та ефективності використання цих пристроїв. Враховуючи різноманітність моделей, операційних систем, а також різний рівень безпеки та доступу до програм, MDM надає єдиний, централізований механізм управління, що дозволяє керувати та моніторити мобільні пристрої з використанням спеціалізованих інструментів.

Одна з ключових переваг - це забезпечення безпеки даних. Встановлення єдиної політики безпеки на всіх пристроях, використання шифрування, можливість віддаленого видалення даних в разі втрати пристрою або ризику несанкціонованого доступу, дозволяють знизити ризики втрати чутливої інформації.

MDM також сприяє автоматизації ряду процесів. Це охоплює встановлення програм, надання дозволів, розгортання оновлень та віддалену підтримку. Це допомагає спростити та прискорити багато аспектів адміністрування мобільних пристроїв [3].

Уніфікованість і стандартизація - ще одна перевага MDM. Впровадження єдиної політики управління пристроями забезпечує єдність у робочому середовищі. Це допомагає знизити ризики помилок та забезпечити спільні стандарти використання [4].

Додатково, MDM дозволяє відстежувати вартість пристроїв, їхню продуктивність та стан, що сприяє плануванню обслуговування та більш ефективному управлінню цими ресурсами.

Впровадження MDM в компанію сприяє покращенню безпеки, ефективності та контролю над мобільними пристроями, що в свою чергу забезпечує підвищення продуктивності та зниження ризиків для бізнесу.

1.4 Технологія управління корпоративними мобільними пристроями: визначення, функції та ключові аспекти.

Технологія управління корпоративними мобільними пристроями (Mobile Device Management - MDM) є комплексною системою, спрямованою на централізоване керування та контроль над мобільними пристроями, які використовуються в організації. Вона стала необхідною у зв'язку зі зростанням числа різноманітних пристроїв (смартфони, планшети, ноутбуки) в бізнес-середовищі, що потребують управління та захисту.

Функції MDM охоплюють широкий спектр можливостей. По-перше, це централізований контроль за налаштуваннями, політиками та доступом до пристроїв. Адміністратор може встановлювати, моніторити та оновлювати програми, налаштовувати параметри безпеки, а також надавати доступ до корпоративних ресурсів.

Ключовою функцією є також захист конфіденційної інформації. MDM надає засоби шифрування даних, віддаленого видалення інформації в разі втрати пристрою, а також встановлення політик безпеки, що зменшують ризики витоку інформації чи несанкціонованого доступу.

Ключові аспекти включають уніфікацію та стандартизацію налаштувань. Це означає, що незалежно від типу пристрою чи операційної системи, MDM дозволяє створити єдину систему управління та застосувати її для всіх пристроїв.

Технологія управління корпоративними мобільними пристроями стала невід'ємною складовою сучасного бізнесу, що дозволяє підвищити безпеку, ефективність та контроль над пристроями, які використовуються в корпоративному середовищі.

2 АРХІТЕКТУРА ТА ФУННКЦІОНАЛ MICROSOFT INTUNE

2.1. Детальний розбір компонентів та їх функціоналу

1. Intune - це компонент рішення Enterprise Mobility + Security (EMS), який управляє мобільними пристроями і додатками. Intune тісно інтегрується з іншими компонентами EMS, такими як Azure Active Directory (Azure AD), для керування посвідченнями та контролю доступу, а також з Azure Information Protection для захисту даних. При використанні разом з Office 365 ваші співробітники можуть ефективно працювати на всіх пристроях з одночасним захистом даних організації.

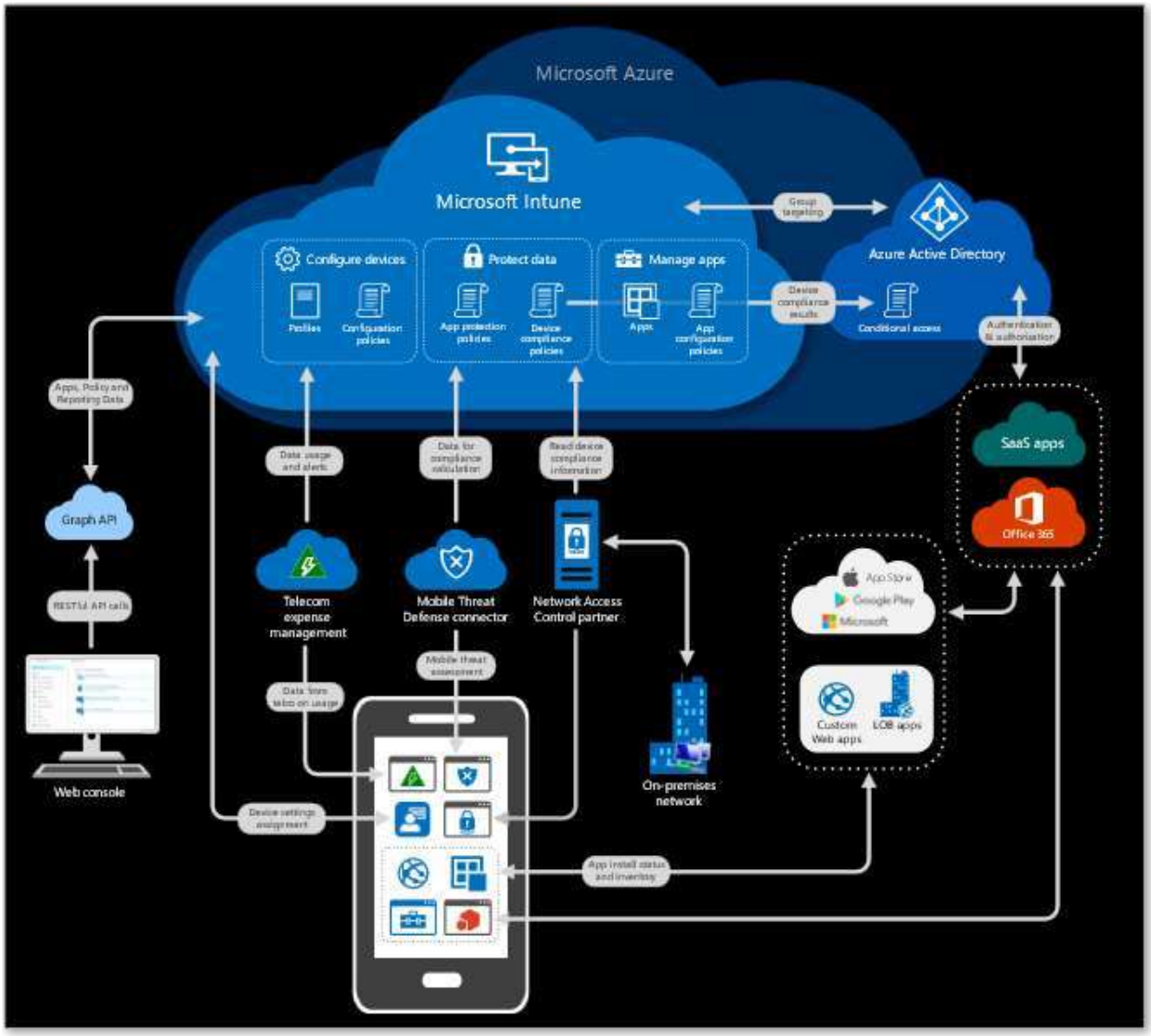

Рисунок 2.1 Схема архітектури Intune

Управління пристроями Intune використовує протоколи або API, доступні в операційних системах мобільних пристроїв. Вона включає такі завдання, як:

Реєстрація пристроїв в системі управління, щоб IT-відділ мав відомостями про пристрої, здійснюють доступ до корпоративних службам:

- Налаштування пристроїв, щоб забезпечити їх відповідність стандартам по працездатності і безпеки організації.
- Надання сертифікатів і профілів Wi-Fi і VPN для доступу до корпоративних службам.
- Оцінка відповідності пристроїв корпоративним стандартам і ведення відповідних звітів.
- Видалення корпоративних даних з керованих пристроїв. Вважають, що контроль доступу до корпоративних даних є функцією управління пристроями. Але ці можливості не надаються мобільною операційною системою. За це відповідає постачальник посвідчень. У нашому випадку постачальником посвідчень є Azure Active Directory (Azure AD) - система управління ідентифікацією та доступом корпорації Майкрософт. Intune інтегрується з Azure AD, щоб підтримувати широкий набір сценаріїв контролю доступу.

Наприклад, можна зажадати, щоб мобільний пристрій відповідало корпоративним стандартам, визначеним у Intune, перш ніж воно зможе отримати доступ до корпоративної службі, такий як Exchange. Аналогічним чином можна прив'язати корпоративну службу до певного набору мобільних додатків. Наприклад, можна дозволити доступ до Exchange Online тільки з Outlook або Outlook Mobile.

Коли говориться про управління додатками, то мають на увазі такі завдання:

- призначення мобільних додатків співробітникам;
- настройку додатків за допомогою стандартних налаштувань, які

- використовуються при запуску додатки;
- управління використанням корпоративних даних і загальним
- доступом до них в мобільних додатках;
- видалення корпоративних даних з мобільних додатків;
- оновлення додатків.
- звіти по інвентаризації мобільних додатків;
- відстеження використання мобільних додатків.

Коли говориться про конфігурацію програми та Intune, ми маємо на увазі конкретні технології, наприклад конфігурація керованого застосування в iOS або в Android. Поняття управління мобільними додатками (MAM), позначається як кожна з цих можливостей окремо, так і певне їх поєднання. Наприклад, користувачі часто не відрізняють концепцію конфігурації програми від концепції захисту корпоративних даних в мобільних додатках. Це викликано тим, що деякі мобільні додатки містять параметри для настройки функцій забезпечення безпеки даних.

При використанні Intune з іншими службами в EMS для мобільних додатків організації можна забезпечити значно вищий рівень безпеки, ніж той, який дозволяє реалізувати мобільна операційна система і конфігурація мобільних додатків. Додаток, кероване з допомогою EMS, має доступ до великого набору засобів захисту мобільних додатків і даних, включаючи наступне:

- Єдиний вхід.
- Багатофакторна перевірка справжності
- Умовний доступ для додатка - дозвольте доступ, якщо
- мобільний додаток містить корпоративні дані
- Ізоляція корпоративних даних від особистих даних всередині однієї програми.
- Політика захисту програми (ПІН-код, шифрування, елемент
- "зберегти як", буфер обміну і т.д.).

- Очищення корпоративних даних з мобільного додатка.

Забезпечення безпеки додатків є частиною управління додатками і в Intune, коли говориться про безпеку мобільного додатка, мається на увазі наступне:

- Зберігання особистих відомостей окремо від корпоративних.
- Обмеження дій, які користувачі можуть виконувати з
- корпоративною інформацією, наприклад: копіювання,
- вирізання та вставка, збереження і перегляд.
- Видалення корпоративних даних з мобільних додатків, яке
- також називають вибіркової або корпоративним очищенням.

Одним із способів забезпечення безпеки мобільних додатків в

Intune є функція політики захисту додатків. Політика захисту додатків використовує посвідчення Azure AD, щоб ізолювати корпоративні дані від особистих даних. Для відомостей, доступ до яких здійснюється даних за допомогою корпоративних облікових даних, застосовуються додаткові заходи захисту.

Наприклад, при вході на пристрій за допомогою корпоративних облікових даних користувач отримує доступ до даних, які недоступні при використанні особистого посвідчення. При використанні корпоративних даних політики захисту додатків контролюють їх збереження і спільне використання. Аналогічні засоби захисту не застосовуються, коли доступ до даних здійснюється з допомогою особистого посвідчення користувача. Таким чином, IT-відділ може керувати корпоративними даними, і кінцевий користувач зберігає контроль над своїми особистими даними, які залишаються конфіденційними.

Більшість рішень для управління корпоративною мобільністю підтримує основні технології мобільних пристроїв і мобільних додатків.

Зазвичай вони нерозривно пов'язані з пристроєм, який реєструється в рішенні управління мобільними пристроями (MDM) організації. Intune підтримує такі сценарії, а також підтримує безліч сценаріїв "без реєстрації".

Рівень впровадження сценаріїв "без реєстрації" в різних організаціях різний. У деяких організаціях вони є основним стандартом або дозволені для додаткових пристроїв, таких як особисті планшети. В інших вони взагалі не підтримуються. Навіть в останньому випадку, коли організації потрібно реєструвати всі пристрої співробітників в системі MDM, сценарії "без реєстрації" зазвичай підтримуються для підрядників, постачальників та інших пристроїв, що представляють певні виключення.

Технологію "без реєстрації" Intune можна використовувати навіть на зареєстрованих пристроях. Наприклад, пристрої, зареєстровані в MDM, можуть мати засоби захисту, що надаються мобільною операційною системою. Захист від відкриття - це функція iOS, яка забороняє відкривати документи в додатках, наприклад Outlook, в інших додатках, наприклад Word, якщо обидва додатки не перебувають під управлінням провайдера управління мобільними пристроями. Крім того, IT-відділ може застосувати до керованим за допомогою EMS мобільних додатків політику захисту додатків, щоб управляти функціями "зберегти як" або надати багатофакторну перевірку справжності.

Яку б позицію організація не займала по відношенню до зареєстрованих і незареєстрованим мобільних пристроїв і додатків, Intune в складі EMS володіє засобами, які допоможуть підвищити ефективність роботи співробітників і захистити корпоративні дані.

Потреби в мобільності підприємства стрімко змінюються, і підхід Microsoft до задоволення їх іноді може відрізнятися від інших рішень на ринку. Найкращий спосіб узгодити ваші бізнес-цілі полягає в тому, щоб представити те, що ви хочете

досягти, у вигляді сценаріїв, які необхідно реалізувати для ваших співробітників, партнерів і IT-відділів.

В роботі розглядалося шість найбільш поширених сценаріїв для використання Intune.

Більшість стратегій мобільності підприємства починаються з плану надання співробітникам безпечного доступу до електронної пошти з мобільних пристроїв, підключених до Інтернету. Багато організацій досі мають локальні дані та сервери застосунків, наприклад, Microsoft Exchange, розміщені в корпоративній мережі.

Intune надає інтегрований умовний доступ рішення для Exchange Server, який гарантує, що доступ до електронної пошти доступний тільки через мобільні пристрої, зареєстровані в Intune. Не потрібно розгортати інші шлюзові комп'ютери в корпоративній мережі.

Крім того, Intune дозволяє надавати мобільні додатки з безпечним доступом до локальних даних, таких як сервер додатків. Зазвичай, для керування доступом у поєднанні зі стандартним шлюзом VPN або проксі-сервером у мережі периметра використовувати керовані сертифікати Intune.

У цих випадках єдиним способом доступу до корпоративних даних є реєстрація пристрою в системі управління. Після реєстрації пристроїв система керування гарантує, що пристрої відповідають політиці перед наданням їм доступу до корпоративних даних. Крім того, ви можете використовувати інструмент упаковки додатків в Intune для забезпечення того, щоб корпоративні дані будуть залишаються в бізнес- додатках і не будуть передані споживачу додатків або послуг.

Захист корпоративних даних (e-mail, документи, миттєві повідомлення, контакти) в хмарному сервісі Office 365 не дає жодних труднощів для вас або ваших користувачів.

Intune є інтегроване рішення умовного доступу, яке гарантує, що користувачі, додатки та пристрої можуть отримати доступ до даних Office 365, лише якщо вони відповідати вимогам щодо відповідності організації :

- пройшли багатофакторну автентифікацію,
- зареєстровані з Intune,
- використовують керовану програму,
- мають підтримувану версію ОС,
- мають пристрій PIN-код пристрою,
- мають низький ризик профілю користувача.

Часто при розгортанні Office 365 можна налаштувати обов'язкову реєстрацію пристрою в системі керування, якщо бажано використовувати корпоративні додатки, сертифікати, Wi-Fi та конфігурації VPN, які є типовими для організації.

Але якщо користувачеві просто потрібен доступ до корпоративної електронної пошти і документів, як це часто буває у випадку з особистими пристроями, можна зажадати, щоб він використовував додатки Office для мобільних пристроїв до яких застосовані політики захисту додатків на порталі, а реєстрацію пристрою можна не виконувати.

У будь-якому випадку дані Office 365 будуть захищені встановленими вами політиками.

Концепція " приноси свій пристрій " (BYOD) продовжує набирати популярність в організаціях як спосіб зменшити апаратні витрати або запропонувати співробітникам широкий спектр інструментів для мобільних робіт. Сьогодні є майже кожен персональний телефон, так навіщо виконувати іншу? Основна проблема завжди була переконати співробітників зареєструвати свої персональні пристрої в системі управління через побоювання, що IT-фахівці зможуть переглядати дані на них і виконувати інші дії.

Якщо реєстрація пристрою не відповідає, Intune пропонує альтернативний підхід до BYOD, що дозволяє легко керувати застосунками корпоративних даних. Intune захищає корпоративні дані, навіть якщо заявка використовується для доступу як корпоративних, так і персональних даних, як і у випадку з офісом для мобільних додатків.

Адміністратор повинен настроїти доступ до Office 365 лише з Office для мобільних пристроїв і встановлення політик для застосунків, які захищають дані за допомогою шифрування та PIN коду. Ці політики захисту додатків запобігають втраті даних у некерованих додатках і розташуваннях зберігання, як всередині, так і зовні таких програм.

Наприклад, вони можуть заборонити користувачу копіювати текст з підприємства на особистий профіль електронної пошти, навіть якщо профіль налаштовано в Outlook Mobile. Аналогічні конфігурації можуть бути розгорнуті в інші послуги та програми, які необхідні для BYOD користувачів.

Сьогодні багато співробітників є мобільними, тому ефективність мобільних пристроїв надзвичайно важлива для підвищення конкурентоспроможності. Ці співробітники вимагають безшовних доступ до всіх корпоративних додатків і даних у будь-який час і з будь- якої точки. Треба і забезпечити безпеку ваших корпоративних даних і знизити витрати на адміністрування.

Intune пропонує масові підготовки та управління рішення, що інтегрується з основними платформами підприємства для управління пристроями, представленими на ринку, в тому числі Apple пристрій реєстрації та мобільний пристрій безпеки платформи Samsung Knox. Централізоване створення конфігурацій пристроїв з використанням Intune дозволяє значно автоматизувати підготовку корпоративних пристроїв.

Іноді співробітникам потрібно використовувати пристрої, додатки або браузери, якими ви не можете управляти, наприклад загальнодоступні комп'ютери на торгових виставках або в вестибюлях готелів.

Чи слід дозволяти співробітникам доступ до корпоративної електронної пошти з таких пристроїв? При використанні Intune дозволяється доступ до електронної пошти тільки з пристроїв, якими керує ваша організація. Так забезпечується надійна перевірка справжності співробітників і гарантуєтеся, що вони не залишать корпоративні дані на ненадійному комп'ютері В організаціях, що підтримують BYOD, дуже поширене управління мобільними додатками (MAM) без використання управління мобільними пристроями (MDM). Можливо надати користувачам можливість доступу до електронної пошти зі служби Outlook Mobile (яка підтримує функції захисту MAM), розгорнувши політику умовного доступу в Exchange Online. Існують такі причини для управління тільки додатками на особистих пристроях:

Зручність роботи користувачів. При реєстрації в системі MDM виводиться безліч попереджень, які є обов'язковими відповідно до вимог платформи. В результаті користувач може відмовитися від доступу до електронної пошти з особистого пристрою. В системі MAM попереджень набагато менше - користувач бачить лише одне спливаюче вікно з повідомленням про те, що функції захисту MAM включені.

Відповідність вимогам. У деяких організаціях діють політики, які пред'являють більш низькі вимоги до можливостей управління особистими пристроями. Наприклад, система MAM дозволяє видаляти тільки корпоративні дані з додатків, в той час як система MDM дозволяє видаляти всі дані з пристроїв управління пристроєм і управління додатками

За допомогою умовного доступу можна надати користувачам можливість реєструвати свої пристрої або використовувати керовані програми, такі як Outlook Mobile. В обох випадках можна налаштовувати і інші умови:

- хто саме намагається отримати доступ;
- чи є розташування довіреною або недовірених;
- рівень ризику при вході
- платформа пристрою

В таблиці 2.1 наведено порівняння цих сервісів по протидії загрозам

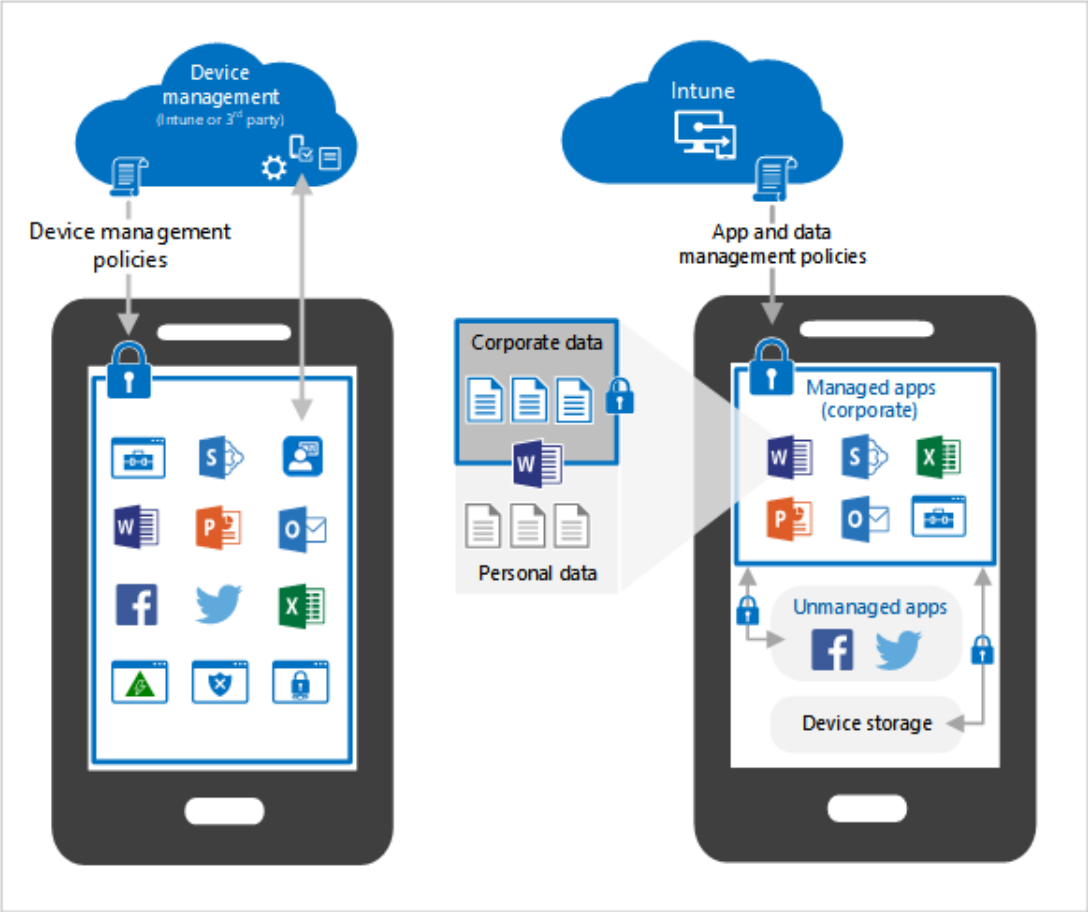

Рисунок 2.2 Схема взаємодії Intune

Таблиця 2.1

Загроза	Стосується MDM	Стосується MAM
Несанкціонований доступ до даних	Вимагати членства в групі	Вимагати членства в групі
Несанкціонований доступ до даних	Вимагати реєстрації пристрою	Вимагати використання захищеного програми
Несанкціонований доступ до даних	Вимагати конкретне розташування	Вимагати конкретне розташування
Компрометація облікових записів користувачів	Вимагати багатофакторну аутентифікацію	Вимагати багатофакторну аутентифікацію
Компрометація облікових записів користувачів	Блокування користувачів з високим рівнем ризику	Блокування користувачів з високим рівнем ризику
Компрометація облікових записів користувачів	ПИН-код пристрою	ПИН-код пристрою
Компрометація пристрою або додатку	Вимагати відповідні вимоги до пристрою	Перевірка зняття захисту при запуску додатку
Компрометація пристрою або додатку	Шифрування даних на пристрої	Шифрування даних додатку

Управління мобільними додатками (MAM) в Intune - це набір функцій управління, що дозволяють публікувати, відправляти, налаштовувати, захищати, відстежувати і оновлювати мобільні додатки для користувачів.

MAM захищає корпоративні дані в самому додатку. За допомогою MAM без реєстрації ви можете керувати робочими або навчальними програмами, які містять конфіденційні дані, практично з будь-якого пристрою, включаючи особисті пристрої в рамках сценарію BYOD. Intune MAM дозволяє управляти багатьма бізнес-додатками, включаючи програми Microsoft Office.

Intune MAM підтримує дві конфігурації:

- Intune MDM і MAM. IT-адміністратори можуть керувати програмами тільки за допомогою MAM і політик захисту додатків на пристроях, зареєстрованих з використанням управління мобільними пристроями Intune (MDM). Для управління додатками за допомогою MDM і MAM слід використовувати консоль Intune, яку можна знайти на порталі Azure за адресою https://portal.azure.com.
- MAM без реєстрації пристрою. MAM без реєстрації пристрою (MAM-WE) дозволяє IT-адміністраторам керувати програмами за допомогою MAM і політик захисту додатків на пристроях, які не зареєстровані з використанням Intune MDM. Це означає, що додатками можна управляти в Intune на пристроях, зареєстрованих з використанням сторонніх постачальників EMM. Для управління додатками за допомогою MAM слід використовувати консоль Intune, яку можна знайти на порталі Azure. Крім того, додатками можна управляти в Intune на пристроях, зареєстрованих з використанням сторонніх постачальників EMM (Enterprise Mobility Management) або зовсім не зареєстрованих в MDM. [5]

2.2. Переваги використання Microsoft Intune у корпоративних середовищах

Microsoft Intune надає корпоративним середовищам безліч переваг. Ця плаформа спрощує управління пристроями та даними, забезпечує безпеку та підвищує продуктивність.

1. Управління різноманітністю пристроїв:

- Intune підтримує різні типи пристроїв, включаючи ПК, ноутбуки, смартфони, планшети та IoT-пристрої.
- Це забезпечує можливість управляти різними платформами та операційними системами, такими як Windows, macOS, iOS, Android та інші, у єдиному інтерфейсі.
- Спрощена установка та конфігурація:
- Intune дозволяє швидко налаштовувати нові пристрої та включати їх до корпоративної мережі з мінімальними зусиллями.
- Адміністратори можуть легко надавати доступ до ресурсів та конфігурувати пристрої згідно з корпоративними стандартами безпеки.

2. Управління застосунками:

- Платформа дозволяє адміністраторам ефективно керувати застосунками на пристроях користувачів, встановлюючи, оновлюючи та видаляючи їх віддалено.
- Це дає можливість обмежувати доступ до певних програм відповідно до корпоративних політик та безпеки.

3. Безпека даних:

- Intune надає інструменти для шифрування даних на пристроях та віддаленого видалення інформації у разі втрати пристрою або порушення безпеки.
- Це допомагає уникнути витоку конфіденційної інформації та зберігає дані під контролем організації.

4. Управління оновленнями та патчами:

- Адміністратори можуть керувати оновленнями операційних систем та програмного забезпечення на пристроях з метою уникнення вразливостей та забезпечення стабільності роботи.

- Це дозволяє забезпечити безпеку та актуальність програмного забезпечення на всіх пристроях у мережі.

5. Аналітика та звітність:

- Intune забезпечує збір та аналіз даних про використання пристроїв та застосунків.
- Це дозволяє адміністраторам рішень щодо оптимізації інфраструктури, підвищення продуктивності та забезпечення безпеки.

6. Хмарна інтеграція та сумісність:

- Intune легко інтегрується з іншими хмарними сервісами Microsoft, такими як Azure Active Directory, що дозволяє створювати єдине та злагоджене робоче середовище для корпоративного користувача.
- Ці переваги Intune роблять його потужним інструментом для організацій, які прагнуть ефективно управляти пристроями, забезпечити безпеку даних та підвищити продуктивність у корпоративному середовищі.
- отримувати цінну інформацію для прийняття

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ УПАРВІЛІННЯ ПРИСТРОЯМИ MDM MICROSOFT INTUNE

3.1 Впровадження та використання Microsoft Intune в корпоративних середовищах

Існує три підходи до вирішення питання про управління пристроями:

- Першій підхід, для управління всіма аспектами пристроїв можна використовувати всі вбудовані можливості Intune. Цей варіант називається управлінням мобільними пристроями (MDM). У цьому випадку користувачі реєструють свої пристрої і взаємодіють з Intune за допомогою сертифікатів. IT-адміністратор може відправляти додатки на пристрої, обмежувати пристрою певної операційної системою, блокувати особисті пристрої та багато іншого. Якщо пристрій буде втрачено або вкрадено, з нього можна видалити всі дані.
- Другий підхід полягає в управлінні додатками на пристроях. Такийваріант називається управління мобільними додатками (MAM). У цьому випадку користувачі звертаються до ресурсів організації зі своїх особистих пристроїв. При запуску цієї програми, наприклад електронної пошти або SharePoint, користувачам пропонується пройти додаткову перевірку справжності. якщо пристрій буде втрачено або вкрадено, з нього можна видалити всі дані організації.
- Третій підхід полягає в використанні як в управлінні мобільними пристроями так і в управління мобільними додатками.
- Політики захисту додатків - це правила, які забезпечують захист корпоративних даних (Включаючи ті, які зберігаються в керованих додатках). Політика може бути або правилом, яке застосовується, коли користувач намагається отримати доступ або перемістити корпоративні дані, або набором дій, які заборонено виконувати або які відслідковуються, коли користувач працює з додатком.

Згідно завдання дипломної роботи були визначені вимоги до керованих додатків Intune в разі використання політик захисту додатків:

- У користувача повинна бути обліковий запис Azure Active Directory (AAD).
- У користувача повинна бути ліцензію Microsoft Intune, призначену його облікового запису Azure Active Directory.
- Користувач повинен бути включений в групу безпеки, на яку поширюється політика захисту додатків. Ця ж політика захисту додатків повинна поширюватися і на певне використовуваним додатком.
- Політики захисту додатків треба створювати і розгортати в консолі Intune на порталі Azure.
- Користувач повинен увійти в додаток, використовуючи свій обліковий запис AAD.
- На пристрої користувача має бути встановлено мобільний додаток Outlook.
- У користувача повинні бути поштова скринька Office 365 Exchange Online і ліцензія, пов'язана з обліковим записом Azure Active Directory

Підтримка множинної ідентифікації дозволяє пакету SDK для додатків Intune застосовувати політики захисту додатків тільки до робочої або навчальної облікового запису, що використовується для входу в додаток. Якщо вхід в додаток виконаний за допомогою особистий обліковий запис, дані залишаться без змін.

Підтримка множинної ідентифікації забезпечує загальнодоступний випуск додатків для корпоративного та особистого користування включаючи додатки Office з функціями захисту додатків Intune для корпоративних облікових записів.

Так як в Outlook реалізовано об'єднане подання повідомлень електронної пошти (особистих і корпоративних), додаток Outlook при запуску запитує PIN-код Intune.

Персональний ідентифікаційний номер (ПІН-код) - це секретний код, який використовується для перевірки прав користувача на доступ до корпоративних даних в додатку.

Intune запитує PIN-код для додатка, коли користувач намагається отримати доступ до корпоративних даних. У додатках з підтримкою множинної ідентифікації (включаючи Word, Excel і PowerPoint) користувач повинен вводити ПІН-код при спробі відкрити корпоративний документ або файл. У додатках, що використовують єдину ідентифікацію (включаючи бізнес-додатки, керовані за допомогою інструменту упаковки для додатків Intune), ПІН код потрібно вводити при запуску, так як пакет SDK для додатків Intune завжди обробляє всі дані в додатку як корпоративні.

IT-адміністратор може визначити параметр "Перевіряти вимоги доступу повторно через (Хв) "в налаштуваннях політики захисту програми Intune за допомогою консолі адміністрування Intune. Цей параметр визначає період часу, через який виконується перевірка вимоги та надають допуск на пристрої, після чого знову з'являється вікні керування з ПІН-кодом.

Для зручності ПІН-код є загальним для додатків одного видавця. В iOS один ПІН-код використовується в усіх програмах одного видавця. В Android один ПІН-код використовується у всіх додатках.

Поведінка «Перевіряти вимоги доступу повторно через (хв)" після перезавантаження пристрою.» Таймер ПІН-коду відстежує кількість хвилин бездіяльності, що визначає час для наступного відображення ПІН-коду програми Intune. В iOS перезавантаження пристрою не зачіпає таймер ПІН-коду. Тому перезавантаження пристрою не впливає на кількість хвилин, яке користувач був неактивним в додатку iOS з діючою політикою щодо ПІН-кодів Intune. В Android таймер ПІН-коду скидається при перезавантаженні пристрою.

Тому після перезавантаження пристрою додатки Android з діючою політикою в відношенні ПІН-кодів Intune, найімовірніше, запросять ПІН-код додатка незалежно відзначення параметра "Перевіряти вимоги доступу повторно через (хв)".

Для пристроїв iOS, навіть якщо ПІН-код є загальним для додатків різних видавців, запит з'явиться знову при досягненні значення «Ще раз перевірити вимоги доступу через (хв)» для додатки, у якого немає основного фокуса введення. Наприклад, у користувача є додаток A видавця X і додаток B видавця Y, і ці два додатки спільно використовують один і той же ПІН-код.

Користувач працює з додатком A (на передньому плані); додаток B знаходиться в згорнутому стані. Після досягнення значення «Ще раз перевірити вимоги доступу через (хв)», коли користувач перейде до додатка B, буде потрібно ввести ПІН-код.

Робота ПІН-коду Intune заснована на таймері бездіяльності (тобто значення параметра "Перевіряти вимоги доступу повторно через (хв) ". Таким чином, функція ПІН-коду Intune є незалежною від запитів ПІН- коду вбудованих додатків для Outlook і OneDrive, які часто за замовчуванням прив'язані до запуску додатка. Якщо користувач одночасно отримує обидва запиту на введення ПІН-коду, PIN-код Intune повинен мати пріоритет.

ПІН-код надає доступ до корпоративних даних тільки користувачам з відповідними повноваженнями. Отже, щоб налаштувати або скинути ПІН-код для додатка Intune, користувач повинен увійти з використанням своєї робочої або навчальної облікового запису. Ця перевірка справжності обробляється Azure Active Directory за допомогою безпечного обміну маркерами і не є прозорою для пакета SDK для додатків Intune. З міркувань безпеки рекомендується шифрувати корпоративні або навчальні дані. Шифрування пов'язане з ПІН-кодом для застосування; це окрема політика захисту додатків.

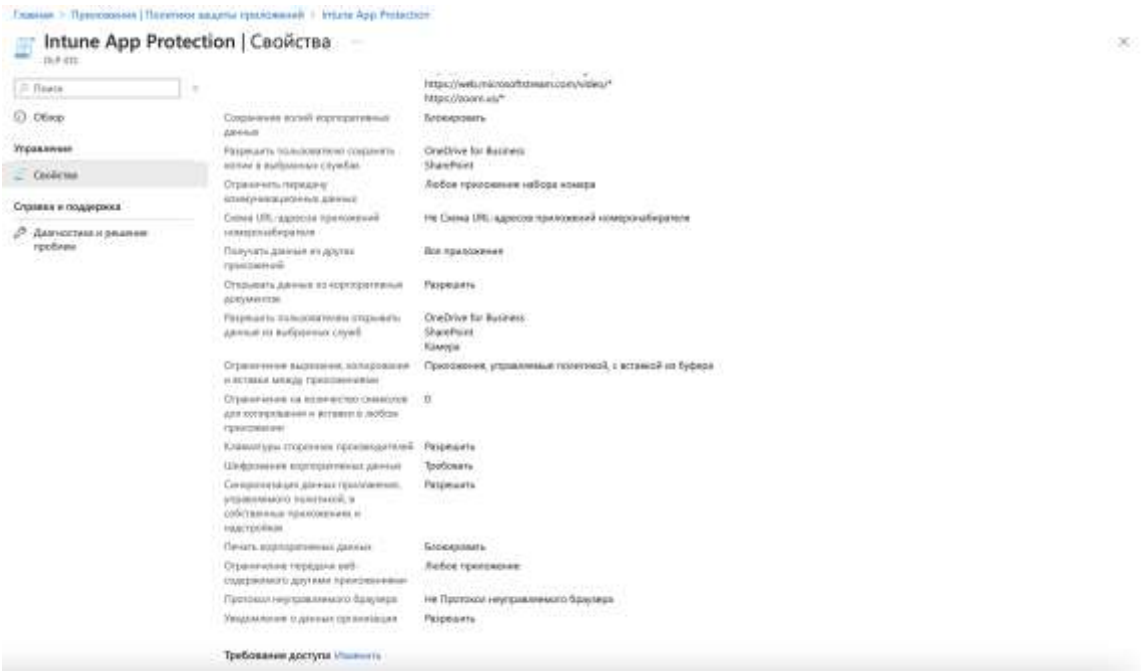

Рисунок 3.1 – Політика захисту додатків

Шифрування даних додатків

ІТ-адміністратори повинні розгорнути політику захисту додатків, відповідно до якої дані додатки повинні шифруватися. В рамках політики ІТ-адміністратор також може визначити, коли зміст має бути зашифровано.

Відповідно до політики захисту додатків, визначеної ІТ- адміністратором, шифруються тільки ті дані, які відзначені як корпоративні. Дані вважаються корпоративними, якщо вони створені в корпоративному розташуванні. При роботі з додатками Office в Intune корпоративними вважаються такі розташування:

- електронна пошта (Exchange) або хмарне сховище (додаток OneDrive з обліковим записом OneDrive для бізнесу).
- У бізнес-додатках, керованих за допомогою інструменту упаковки для додатків Intune, всі дані вважаються корпоративними.

Intune може очищати дані додатків трьома способами: повне очищення пристрою, вибіркова очистка для управління мобільними пристроями і вибіркова

очищення для управління мобільними додатками. Додаткові відомості про віддалену очищення для MDM см. В статті Видалення пристроїв шляхом очищення або припинення використання.

Панель моніторингу управління пристроями - це централізоване засіб для виконання завдань для мобільних пристроїв та управління ними.

На цій панелі моніторингу знаходяться служби, що використовуються для управління пристроями, включаючи Intune і Azure Active Directory, а також для управління клієнтськими додатками.

На панелі моніторингу "Управління пристроями" можна виконувати такі завдання:

- Реєстрація пристроїв
- Завдання відповідності пристрою вимогам
- Управління пристроями
- Управління додатками
- управління ролями
- Управління оновленнями програмного забезпечення
- Керування користувачами
- Управління групами і членами
- Усунення проблем

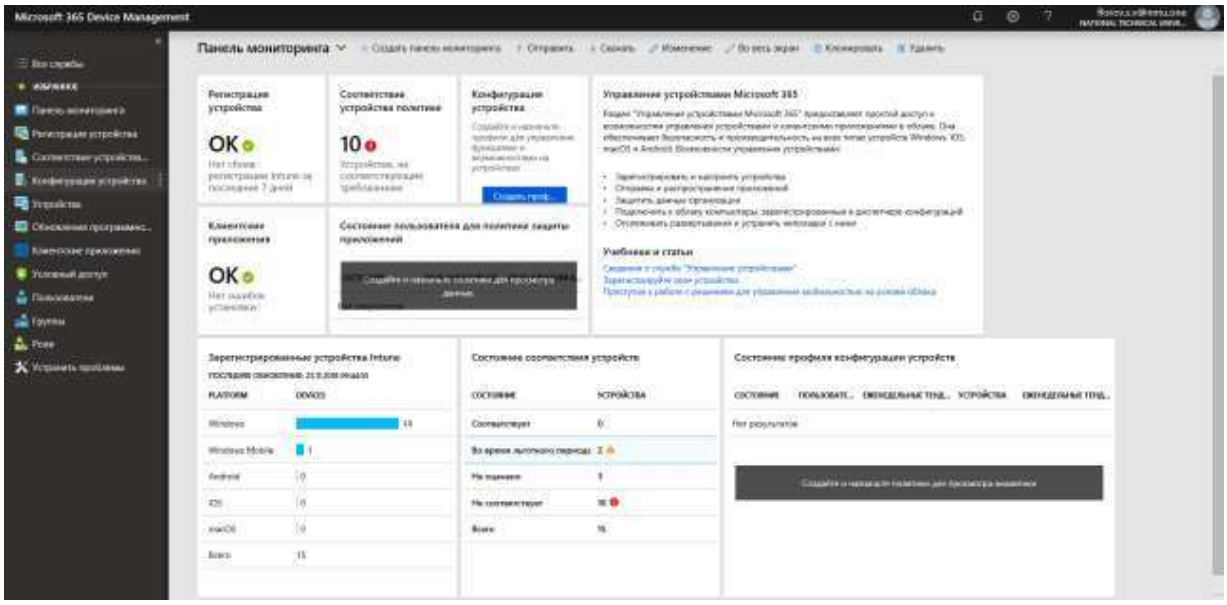

Рисунок 3.1.1 Панель моніторингу "Управління пристроями"

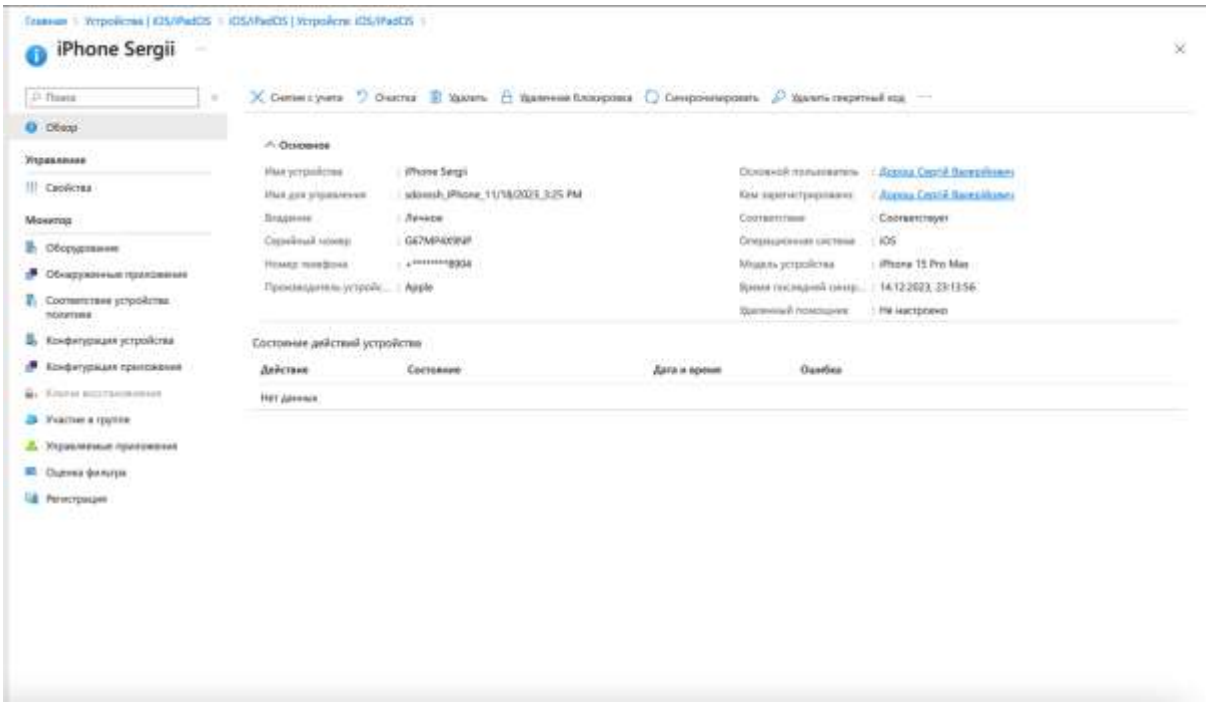

Рисунок 3.1.2 – Зареєсстрований пристрій в системи MDM Intune

Рекомендації щодо плану впровадження Microsoft Intune

Згідно з завданням роботи було розроблено план впровадження установки і настройки Intune

Необхідні умови розгортання Intune:

- Підписка на Enterprise Mobility + Security (EMS) / Intune
- Підписка Office 365 (для додатків Office і додатків під управлінням політики захисту додатків)
- Сертифікат APNs Apple для включення управління платформою пристроїв iOS) Azure AD Connect для синхронізації служби каталогів
- Локальний з'єднувач Intune для Exchange забезпечує умовний доступ для локальної організації Exchange, якщо це необхідно) Intune
- Certificate Connector (для розгортання сертифіката SCEP, якщо це необхідно)

Згідно best practice визначено 13 окремих задач по розгортанню Intune:

Задача 1. Необхідно оформити підписку на або Intune.

Необхідно зверніться до корпорації Майкрософт або службу облікових записів Майкрософт і повідоміть, про бажання придбати Intune.

Задача 2. Підписатися на Office 365.

Вона необхідна в тому випадку, якщо ви плануєте використовувати Exchange Online і управляти мобільними додатками Office за допомогою політик захисту додатків. Якщо у організації немає такої підписки, треба звернутися до корпорації Майкрософт або служби технічної підтримки облікових записів Майкрософт.

Задача 3. Додавання груп користувачів в Azure AD

Залежно вимог і сценаріїв використання Intune може знадобитися додавання користувачів або груп безпеки в Active Directory або Azure Active Directory треба переглянути поточних користувачів і групи безпеки в Active Directory або Azure Active Directory і визначте, повністю чи вони відповідають вашим потребам організації. Нових користувачів і групи безпеки треба додавати в Active Directory і синхронізувати з Azure Active Directory за допомогою Azure AD Connect

Задача 4. Призначення користувальницьких ліцензій Intune і Office 365 Всім користувачам, яких торкнеться розгортання Intune і Office 365, необхідно призначити ліцензію. Призначити ліцензії Intune і Office 365 можна на порталі Центру адміністрування Office 365.

Задача 5. Розгортання центру управління мобільними пристроями в Intune.

Перед початком установки, настройки, реєстрації пристроїв і управління ними за допомогою Intune слід задати Intune в якості центру управління пристроями.

Задача 6. Підключення платформи пристрою.

За замовчуванням більшість платформ пристроїв, крім пристроїв Apple (iOS і Mac), включені. Перш ніж можна буде реєструвати пристрої iOS в Intune і управляти ними, потрібно включити цю платформу пристроїв. Для цього необхідно створити сертифікат MDM Push і додати його в Intune.

Задача 7. Додавання і та розгортання політик умов Intune підтримує політики умов. Додайте потрібні політики умов і поверніть його в цільових групах з урахуванням вимог і варіантів використання для розгортання Intune.

Задача 8. Додавання і та розгортання політик зміни конфігурації Intune підтримує два типи політик конфігурації - загальні і настроюються. Додайте потрібні політики

конфігурації і поверніть його в цільових групах з урахуванням вимог і варіантів використання для розгортання Intune.

Задача 9. Додавання і та розгортання профілів ресурсів Intune підтримує профілі електронної пошти, Wi-Fi і VPN. Додайте потрібні профілі і поверніть його в цільових групах з урахуванням вимог і варіантів використання для розгортання Intune.

Задача 10. Додавання і та розгортання додатків.

Intune підтримує розгортання веб-додатків, бізнес-додатків і додатків, опублікованих в магазині. Крім того, додатками з інтегрованим пакетом SDK Intune можна управляти, зіставивши їх з політиками захисту додатків. Додайте потрібні програми і поверніть його в цільових групах з урахуванням вимог і варіантів використання для розгортання Intune.

Задача 11. Додавання і розгортання політик відповідності Intune, підтримує політики відповідності. Додайте потрібні політики відповідності і поверніть його в цільових групах з урахуванням вимог і варіантів використання для розгортання Intune.

Задача 12. Включення політик умовного доступу.

Intune підтримує умовний доступ до Exchange Online і локальної організації Exchange, SharePoint Online, Skype для бізнесу Online і Dynamics CRM Online. Необхідно увімкнути і налаштуйте потрібні політики умовного доступу з урахуванням вимог і варіантів використання для розгортання Intune.

Задача 13. Реєстрація пристроїв.

Intune підтримує платформи настільних і мобільних пристроїв Windows, iOS, Mac OS, Android. Зареєструйте потрібні платформи мобільних пристроїв з урахуванням вимог і варіантів використання для розгортання Intune. [6]

Рекомендації налаштування параметрів обмежень для Android пристроїв в Intune

Загальні параметри:

- Копіювання і вставка між робочим і особистим профілями. контролює операції копіювання і вставки між робочими й особистими додатками. Треба вибрати «Блокувати», щоб заблокувати. Треба вибрати «Не налаштовано», щоб відключити блокування.
- Спільне використання даних між робочим і особистим профілем. використовується, щоб дозволити або заборонити обмін даними між додатками роботи та дозвілля профілів. Цей параметр керує доступними в додатках діями загального доступу, наприклад параметром Загальний доступ в додатку браузера Chrome. Цей параметр не застосовується до операцій копіювання і вставки в буфері обміну. На відміну від параметрів політики захисту додатків, параметри обмеженого використання пристроїв управляються на порталі Intune і використовують розділ робочого профілю Android для ізоляції керованих додатків. Треба вибрати один з наступних типів:
- Обмеження загального доступу. Це поведінка для спільного використання за замовчуванням на пристрої, який залежить від використовуваної версії Android. За замовчуванням можна передавати дані з особистого профілю в робочий. Крім того, за замовчуванням заборонено передавати дані з робочого профілю в особистий. Цей параметр дозволяє запобігти витік даних з робочого профілю в особистий. На пристроях під управлінням версії 6.0 або новішої версії Google не блокує передачу даних з особистого профілю в робочий.
- Додатки в робочому профілі можуть обробити запит на загальний доступ з особистого профілю. Використовується, щоб включити вбудовану функцію в Android, що дозволяє передавати дані з особистого профілю в робочий. Коли ця функція включена, запит на загальний доступ, ініційований з програми особистого профілю, зможе обмінюватися даними з додатками робочого

профілю. Цей параметр представляє поведінка за умовчанням для пристроїв Android під керуванням більш ранніх версій, ніж 6.0.

- Дозволити загальний доступ за межами кордонів. Дозволяє загальний доступ через кордони робочого профілю в обох напрямках. При виборі цього параметра додатки в робочому профілі можуть обмінюватися даними з некерованими додатками особистого профілю. Цей параметр дозволяє обмін даних між додатками в робочому профілі та додатками в некерованою частині пристрою. Тому використовувати його потрібно з обережністю.
- Повідомлення для робочого профілю, коли пристрій заблоковано. Використовується, щоб дозволити або заборонити додаткам в робочому профілі відображати дані в повідомленнях при якщо пристрій було заблоковано.
- Дозволи зі стандартними програмами. Задає політику дозволів за замовчуванням для всіх додатків в робочому профілі.
- Пристроїв з робочим профілем Android з ОС Android версії 6.0 або більш пізньої. Якщо включити цей параметр, деякі пристрої Bluetooth можуть отримати дозвіл кешувати робочі контакти при першому підключенні. У разі відключення цієї політики після початкового зв'язування або синхронізації робочі контакти можуть бути не видалені з пристрою Bluetooth.
- Screen capture (Знімок екрану). Блокування створення знімків екрану в робочому профілі пристрою, а також заборона показу вмісту на пристроях відображення, у яких немає безпечного виведення відео.
- Display work contact caller-id in personal profile (Відображати ВД дзвонить, який є робочим контактом, в особистому профілі). Якщо цей параметр включений (не налаштований), відомості про абонента, який є робочим контактом, відображаються в особистому профілі. якщо цей параметр заблокований, номер абонента, який є робочим контактом, не відображається в особистому профілі. Застосовується до ОС Android 6.0 і пізніших версій.
- Camera (Камера). Блокування камери в робочому профілі пристрою. На роботу камери в особистому профілі цей параметр не впливає.

Пароль робочого профілю.

- Вимагати пароль робочого профілю. Застосовується до Android 7.0 і пізніших версій з включеним робочим профілем. Визначення політики секретного коду, яка застосовується тільки до додатків в робочому профілі. За замовчуванням кінцевий користувач може або використовувати два окремо визначаються ПІН-коду, або об'єднати два ПІН-коду в один, при цьому буде використовуватися більш складний ПІН-код.
- Мінімальна довжина пароля. Введіть мінімальну кількість символів, яке повинно бути в паролі користувача (4-16).
- Максимальний час бездіяльності (в хвилинах), після закінчення якого робочий профіль блокується. Виберіть час, який повинен пройти до блокування робочого профілю. За закінчення цього часу для отримання доступу користувачеві необхідно буде заново ввести свої облікові дані.
- Число невдалих спроб входу перед очищенням пристрою. Введіть кількість спроб введення невірного пароля, перш ніж робочий профіль буде видалений з пристрою.
- Закінчення терміну дії пароля (днів). Введіть число днів до зміни пароля користувача (від 1-255).
- Заборонити використання попередніх паролів. Введіть кількість спроб введення нових паролів, перш ніж можна буде використовувати повторно старий пароль (від 1-24).

Розблокування за допомогою відбитків пальців. Забороняє користувачу використовувати сканер відбитків пальців, щоб розблокувати пристрій. Smart Lock і інші довірені агенти. Управляє функцією Smart Lock на сумісних пристроях. Ця функція телефону, яку іноді називають довіреною агентом, дозволяє відключати або обходити пароль робочого профілю, коли пристрій знаходиться в надійному розташуванні. Наприклад, можна обходити пароль робочого профілю,

якщо пристрій підключається до певного пристрою Bluetooth. Використовуйте цей параметр, щоб заборонити користувачам налаштовувати функцію Smart Lock.

Пароль пристрою:

Мінімальна довжина пароля. Введіть мінімальну кількість символів, яке повинно бути в паролі користувача (4-14). Максимальний час бездіяльності (в хвилинах), після закінчення якого екран блокується.

Виберіть час, який повинен пройти до автоматичного блокування неактивного пристрою. Число невдалих спроб входу перед очищенням пристрою. Введіть кількість спроб введення невірного пароля, перш ніж всі дані будуть видалені з пристрою.

Закінчення терміну дії пароля (днів). Введіть число днів до зміни пароля користувача (від 1-255). Необхідний тип пароля. Виберіть тип пароля, який повинен бути заданий для пристрою. Оберіть один з наступних типів:

Пристрій за замовчуванням. Біометричний з низьким рівнем безпеки обов'язкове:

- Принаймні числа, Числовий комплекс.
- Повторювані або послідовні числа, наприклад "1111" або "1234", не допускаються.

Принаймні літери, Принаймні букви і цифри Принаймні цифри, букви і символи:

- Заборонити використання попередніх паролів. Введіть кількість спроб введення нових паролів, перш ніж можна буде використовувати повторно старий пароль (від 1-24).
- Розблокування за допомогою відбитків пальців. Забороняє користувачу використовувати сканер відбитків пальців, щоб розблокувати пристрій.

- Smart Lock і інші довірені агенти. Управляє функцією Smart Lock на сумісних пристроях. Ця функція телефону, яку також називають довіреною агентом, дозволяє відключати або обходити пароль блокування екрану пристрою, коли пристрій знаходиться в надійному розташуванні. Наприклад, можна обходити пароль робочого профілю, якщо пристрій підключається до певного пристрою Bluetooth або знаходиться поруч з NFC-тегом. Використовуйте цей параметр, щоб заборонити користувачам налаштовувати функцію Smart Lock.

Підключення до мережі:

Параметр Always-on VPN (Постійна мережу VPN). Треба вибрати «Увімкнути», щоб клієнт VPN автоматично підключався і перепідключатися до цієї мережі VPN. При перезапуску або розблокуванні пристрою, а також при зміні бездротової мережі VPN- підключення не буде розірвано або буде відразу ж відновлено. Треба вибрати «Не налаштовано Операцію», щоб відключити постійну мережу VPN для всіх клієнтів VPN.

Клієнти VPN. Необхідно вибрати клієнт VPN, який підтримує AlwaysOn. В наявності є таке:

- CiscoAnyConnect
- F5Access
- PaloAltoNetworksGlobalProtect
- Pulse Secure

3.2. Порівняння Microsoft Intune з іншими системами управління мобільними пристроями

Дивлячись на пропозиції вендорів, на українському ринку які представлені то можемо виділити 6 основних гравців – це Microsoft, IBM, Citrix, Mobileiron, airvatch від VMWare, та Google зі своїм продуктом MDM, який нещодавно був доданий до функціоналу GWS. Проаналізувавши даних вендорів, можемо сказати що в кожно своя особливість, та свій піхід під задачі. Згідно проведеного аналізу інфраструктури компанії, можемо аналізувати яке рішення підходить. Найкращим для звичайних компаній вважаю, є Microsoft Intune, та Google зі своїм GWS. Дані рішення заточені під Enterprise, тому модулі MDM йдуть в базових ліцензія в якій доступні і інші системи. Тобто це повноцінний бандл для компаній, які хочуть будувати свої корпоративні системи з безппекою [7].

Інші рішення є більш дорого вартісними 81-151 долар за одного користувача, на місяць, тоді як Google і Microsoft пропонують вартість близько 12-18 доларів за одного користувача, і це не тільки функціонал MDM.

Рисунок 3.2.1 Порівняння функціоналу

3.3 Розроблення рекомендацій щодо застосування та впроовадження систем Microsoft Intune

Для впровадження Microsoft Intune в організацію важливо систематично пройти кілька етапів. Почніть з ретельного аналізу поточних потреб та інфраструктури, визначте обсяг впровадження та розробіть стратегію міграції. Налаштуйте Intune, створіть політики безпеки та управління пристроями, і проведіть тестування для перевірки ефективності. Після успішних тестів поступово розгортайте систему на виробничих середовищах, забезпечте навчання персоналу і відповідне підтримку. Важливо постійно моніторити та оцінювати роботу Intune, адаптувати політики та надавати оновлення для забезпечення відповідності потребам вашої компанії. [8]

Для впровадження системи необхідно провести тестування функціоналу та пошагово налаштувати дані пункти:

Перегляд підтримуваних конфігурацій
Початок роботи з конфігураціями, що підтримуються.

Перш ніж розпочати налаштування Microsoft Intune, виконайте такі дії:

Ознайомтеся з платформами пристроїв та операційними системами, які підтримуються Intune.

Перевірте, які веб-браузери підтримуються під час доступу до Intune за допомогою служби адміністрування Microsoft Intune.

Ознайомтеся з вимогами щодо пропускної здатності мережі для встановлення та оновлення за допомогою Intune.

Додаткові відомості та відомості про потрібні відомості перед початком роботи див. у розділі Підтримувані конфігурації.

Початок роботи з зареєструватися або увійти до Intune:

Увійдіть до Центру адміністрування Microsoft Intune.

Перед реєстрацією в Intune перевірте, чи немає у вас облікового запису Microsoft Online Services, угоди Enterprise або аналогічної угоди корпоративного ліцензування. Угода про корпоративне ліцензування Майкрософт або підписка на інші хмарні служби Майкрософт, такі як Microsoft 365, зазвичай включає робочий або навчальний обліковий запис.

Якщо у вас уже є робочий або навчальний обліковий запис, увійдіть до системи за допомогою цього облікового запису та додайте Intune до вашої передплати. Якщо ж ні, зареєструйте новий обліковий запис для використання Intune у вашій організації.

Налаштування особистого доменного імені для клієнта Intune:

Початок роботи з налаштуванням особистого доменного імені для клієнта Intune

Коли ваша організація реєструється для отримання Microsoft Intune, ви отримаєте початкове доменне ім'я, розміщене в Azure Active Directory (Azure AD), яке виглядає як your-domain.onmicrosoft.com.

Суфікс onmicrosoft.com призначається всім обліковим записам, доданим до передплати.

У разі потреби можна налаштувати особистий домен організації в Intune, наприклад contoso.com. Якщо ви не додаєте обліковий запис домену, наприклад, contoso.onmicrosoft.com можна використовувати.

Налаштуйте реєстрацію DNS, щоб підключити доменне ім'я вашої компанії за допомогою Intune. При цьому користувачі отримують знайомий домен під час підключення до Intune та використання ресурсів.

Якщо ви просто оцінюєте Intune за допомогою безкоштовної пробної версії, цей крок можна пропустити.

Якщо ви переходите на Microsoft 365 з підписки Office 365, можливо, ваш домен вже знаходиться в Azure AD. Intune використовує той самий Azure AD і може використовувати існуючий домен.

Початок роботи з додаванням користувачів до Intune:

Користувачі зберігаються в Azure AD, яка також входить до складу Microsoft 365. Azure AD керує доступом до ресурсів та перевіряє справжність користувачів. Ви можете додати користувачів або підключити Active Directory для синхронізації з Intune. Цей крок є обов'язковим , якщо ваші пристрої не є пристроями кіоску без користувачів.

Кожен співробітник вашої організації потребує облікового запису користувача, перш ніж вони зможуть увійти до системи та отримати доступ до Microsoft Intune. Щоб створити облікові записи користувачів, можна додати користувачів до Intune. Після додавання ви можете надавати дозволи та призначати ліцензії користувачам. Потім можна призначати користувачам різні типи політик, щоб допомогти і захистити їх.

Адміністратор може додавати користувачів окремо або Intune. Для додавання користувачів до Intune необхідно бути адміністратором (глобальним, ліцензійним або адміністратором користувачів). Якщо ви налаштували Intune за допомогою безкоштовної пробної версії, ви є глобальним адміністратором.

Початок роботи з додаванням груп до Intune:

Додавання груп для призначення програм, параметрів та інших ресурсів.

Intune використовує групи Azure Active Directory (Azure AD) для організації пристроїв та користувачів та управління ними. Як адміністратор Intune ви можете налаштовувати групи відповідно до потреб вашої організації. Наприклад, можна створити групи для організації користувачів або пристроїв з географічного розташування, відділу або характеристик обладнання. Крім того, групи можна використовувати для керування завданнями у великому масштабі. Наприклад, можна задати політики для багатьох користувачів або розгорнути програми на наборі пристроїв на основі груп.

Intune доступна в різних підписках, у тому числі як автономна служба. Визначте ліцензовані служби, необхідні для вашої організації, і продовжуйте призначати кожному користувачеві ліцензію на Intune, перш ніж користувачі зможуть зареєструвати свої пристрої в Intune. Визначення потреб у ліцензії
Microsoft Intune доступний для різних розмірів і потреб організації, від простого використання інтерфейсу управління для навчальних закладів і малого бізнесу до більш складних функцій, необхідних корпоративним клієнтам. Адміністратору має бути призначено ліцензію на адміністрування Intune (якщо ви не обрали дозвіл неліцензованих адміністраторів).

Початок роботи з призначенням ліцензій користувачам. Незалежно від того, чи ви додали користувачів по одному або відразу всім користувачам, необхідно призначити кожному користувачеві ліцензію на Intune, перш ніж користувачі зможуть зареєструвати свої пристрої в Intune. Безкоштовна пробна версія Microsoft Intune надає 25 Intune ліцензій. Список ліцензій див. у розділі Ліцензії, які включають Intune. Надайте користувачам дозвіл на використання Intune. Для доступу до служби потрібна ліцензія Intune для кожного користувача або пристрою без користувача.

Ви можете надати адміністраторам доступ до Microsoft Intune без ліцензії на Intune. Ця можливість відноситься до будь-яких адміністраторів, у тому числі до адміністраторів Intune, глобальних адміністраторів, адміністраторів Azure AD і т.д.

Управління ролями та надання дозволів адміністратора для Intune:
Після додавання користувачів до клієнта Intune рекомендується створити команду адміністрування.

Microsoft Intune включає набір ролей адміністратора, які можна призначити користувачам в організації за допомогою центру адміністрування Microsoft Intune. Кожній ролі адміністратора відповідають поширені бізнес-функції, і вона надає користувачам організації дозволу виконання певних завдань у Центрах адміністрування.

Керування доступом на основі ролей (RBAC) допомагає керувати доступом користувачів до ресурсів вашої організації та виконання операцій з цими ресурсами.

Призначаючи ролі користувачам Intune, можна обмежити їхні права перегляду та зміни.

Можна використовувати вбудовані та користувацькі ролі. Вбудовані ролі призначені для найпоширеніших сценаріїв Intune. Ви можете створювати власні настроювані ролі з точним набором необхідних дозволів

Ви можете використовувати управління доступом на основі ролей і теги область, щоб переконатися, що правильні адміністратори мають правильний доступ до потрібних об'єктів Intune і їх видимість. Ролі визначають, які адміністратори мають доступ до якихось об'єктів.

Налаштування центру керування мобільними пристроями:
Налаштування повноважень управління мобільними пристроями (MDM) визначає спосо б управління пристроями. За промовчанням безкоштовна пробна версія Intune задає для центру MDM значення Intune. IT-адміністратор повинен встановити MDM, щоб користувачі могли реєструвати пристрої для керування. Налаштувавши центр MDM, можна розпочати реєстрацію пристроїв.

Якщо ви змінюєте клієнт для підтримки Intune, необхідно змінити конфігурацію центру MDM.

За допомогою програм Корпоративного порталу, веб-сайту "Корпоративний портал" та програми Intune для Android користувачі можуть отримувати доступ до корпоративних даних та виконувати стандартні завдання. Стандартним завданням, крім іншого, вважається реєстрація пристроїв, встановлення програм та пошук відомостей (наприклад, для отримання допомоги IT-відділу).
Початок роботи з налаштуванням корпоративного порталу

Налаштуйте Корпоративний портал Intune, які користувачі використовують для реєстрації пристроїв та інсталяції програм. Ці параметри відображаються у програмі "Корпоративний портал" та на веб-сайті Корпоративного порталу. Ви також можете налаштувати програму Корпоративний портал таким чином, щоб вона була включена до відомостей про вашу організацію [9].

Після налаштування даних пунктів необхідно провести тесутвання функціонал, щоб пітвердити працезданість даного продукту для вашої організації, та виявиги гепи, які можуть виникати при вже поточній інфраструктурі. Наприклад місконфігурація з MFA іншого вендору і тд.

Можна пересвідчиитись, скаласти та пройти по тест кейси, які найкраще зможуть оцінити працездатність :

Конфігурація:

- Заборона створення контейнера або запис корпоративних даних на знімні носії
- Оновлення корпоративних політик без підключення до корпоративної мережі. Політики прилітають через інтернет
- Контроль установлюваних у контейнер додатків
- Заборона збереження даних поза контейнером
- Можливість створення та розповсюдження політик для груп пристроїв, окремо для кожного пристрою
- Налаштування контролю копіювання даних в/з корпконтейнера через синхронізацію з ББ(Великим Братом) і копіювання власне контейнера.
- Налаштування інформування про події ІБ
- Можливість блокування корпоративного контейнера за відсутності підтвердження оновлення політик більш певної кількості днів

Безпека:

- Поділ персональних даних на особистому пристрої від корпоративних

- Встановлення лише узгодженого ПЗ у корпоративний контейнер
- Спільне використання персональних та корпоративних додатків
- Оновлення корпоративних додатків лише з джерела, зазначеного у політках
- Контроль встановлення додатків у корпоративний контейнер

- Видалення даних лише з корпоративного контейнера у разі звільнення працівника, втрати або крадіжки пристрою при першому підключенні до Інтернету
- Видалення даних по команді з консолі управління з персонального контейнера та корпоративного контейнера (повне очищення пристрою без підключення до корпоративної мережі) при першому підключенні до Інтернету у разі втрати або крадіжки пристрою.
- Очищення корпоративних даних під час звільнення співробітника. Автоматизація та інтеграція з кадровою системою банку.
- Додаткова автентифікація при доступі до корпоративного контейнера з додатками та даними
- 10 Можливість двофакторної аутентифікації при доаступі до контейнера
- Можливість керування доступом пристроїв на основі сертифікатів. У разі блокування пристрою вимкнення доступу до контейнера
- Заборона використання контейнера на рутированном пристрої як під час реєстрації пристрою, так і в процесі роботи з контейнером на вже зареєстрованому пристрої
- Очищення контейнера у разі не валиного видалення агента МДМ
- Обов'язкове шифрування даних у корпоративному контейнері та в персональній частині пристрою криптостійкими алгоритмами шифрування.
- Контроль створення резервних копій контейнера та/або пристрою
- Контроль створення скріншотів
- Інтеграція з RMS та DLP

- Можливість на регулярній основі синхронізації корпоративних даних із сховищем у локальній мережі на випадок втрати чи крадіжки пристрою чи звільнення співробітника.

Після проходження даних кейсів, ми на практиці можемо пересвідчитись про працездатність, та виявленні гепи подати на вендора для усунення, або надання рекомендацій щодо інших варіацій налаштувати той функціонал який необхідний.

ВИСНОВОК ДО 3 РОЗДІЛУ

У практичній реалізації системи управління пристроями MDM, такою як Microsoft Intune, важливо враховувати конкретні потреби та характеристики вашої організації. Ця система надає широкі можливості для управління різними типами пристроїв та застосунками, а також забезпечує високий рівень безпеки та інтеграції з іншими сервісами Microsoft.

При впровадженні Intune важливо провести аудит існуючих потреб організації, розробити стратегію міграції та налагодити систему відповідно до цих вимог. Виконання тестів перед розгортанням на виробничих середовищах та надання належної підтримки та навчання персоналу є так само важливими кроками. Оцінка ефективності системи та її постійне удосконалення згідно зі змінами в потребах компанії також мають ключове значення для успішної реалізації Microsoft Intune.

ВИСНОВОК

Захист та управління корпоративними мобільними пристроями стає важливішим аспектом сучасного бізнесу. Розвиток технологій та збільшення використання мобільних пристроїв у робочих цілях ставлять під загрозу безпеку корпоративних даних. Тут входить в роль технологія управління пристроями (MDM), така як Microsoft Intune, що пропонує не лише управління, а й захист від потенційних загроз.

Intune надає компаніям інструменти для керування пристроями, додатками та даними, що забезпечує більшу контрольованість та безпеку корпоративного середовища. Ця система дозволяє створювати та впроваджувати політики безпеки, включаючи обмеження доступу, шифрування даних, віддалене видалення та моніторинг пристроїв.

Успішна імплементація Intune в організацію забезпечує не лише захист конфіденційної інформації, а й підвищує продуктивність, спрощує управління пристроями та зменшує ризики зв'язані з використанням корпоративних даних на особистих пристроях.

Це дає можливість компаніям ефективно пристосовуватися до швидкозмінюваного технологічного середовища й бути впевненим у захищеності своїх активів. Функціонал Microsoft Intune повністю задовольняє всі базові потреби бізнесу, та можна налаштовувати згідно доступного ліцензування, а також гнучкості роботи і пункту ціна-якість. Що і робить цей продукт одним з лідерів ринку ,та найкращим для імплементації, якщо інфраструктура побудована на хмарній основі Microsoft

ПЕРЕЛІК ПОСИЛАНЬ

1. Що таке MDM/EMM. URL: https://uk.theastrologypage.com/enterprise-marketing-management
2. Захист даних в корпоративному середовищі. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-data-security
3. Переваги рішень MDM. URL: https://ts2.space/uk/мобільний-пристрій-управління-mdm/
4. Політики керування MDM. URL: https://ts2.space/uk/мобільний-пристрій-управління-mdm/
5. Документація Microsoft: Налаштування Microsoft Intune. URL: https://learn.microsoft.com/ru-ru/mem/intune/fundamentals/deployment-plan-setup
6. Етапи розгортання Microsoft Intune. URL: https://learn.microsoft.com/ru-ru/mem/intune/fundamentals/get-started-with-intune
7. VMware Що таке керування мобільними пристроями – www.vmware.com/topics/glossary/content/mobile-device-management.html
8. SourceForge: порівняльна діаграма. URL: sourceforge.net /software/compare/Amazon-WorkMail-vs-Google-Workspace-vs-SharePoint/
9. Computerworld: Управління мобільними пристроями. URL: https://www.computerworld.com/category/mobile-device-management/

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)