|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | | | | | | | | | | |
| **НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ** | | | | | | | | | | | | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
| **КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ** | | | | | | | | | | | | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
| Пояснювальна записка | | | | | | | | | | | | | | | | |
| до бакалаврської роботи | | | | | | | | | | | | | | | | |
|  | | на тему: | | | | | | | | | | | | |  | |
| **«Дослідження шляхів та розробка рекомендацій щодо управління мобільними пристроями за концепцією BYOD в ІС організації»** | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | | Виконав студент 4 курсу, групи БСД-42 | | | | | | | | | |
|  | |  | | | | | спеціальності 125 Кібербезпека | | | | | | | | | |
|  | |  | | | | | освітньо-професійної програми «Інформаційна та | | | | | | | | | |
|  | |  | | | | | кібернетична безпека» | | | | | | | | | |
|  | |  | | | | | (шифр і назва спеціальності) | | | | | | | | | |
|  | |  | | | | | Бондар Б.В. | | | | | | | | | |
|  | |  | | | | | (прізвище та ініціали) | | | | | | | | | |
|  | |  | | | | | Керівник | | Гайдур Г.І. | | | | | | | |
|  | |  | | | | |  | | | | (прізвище та ініціали) | | | | | |
|  | |  | | | | | Рецензент | | |  | | | | | | |
|  | |  | | | | | (прізвище та ініціали) | | | | | | | | | |
|  | |  | | | | | Нормоконтролер | | | | | | Чумак Н.С. | | | |
|  | |  | | | | |  | | | | (прізвище та ініціали) | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | | КИЇВ – 2023 | | | | | | | | | | | | |  | |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | | | | | | | | | | |
| Інститут | | ННІЗІ | | | | |  | | | |  | | | |  | |
| Кафедра | | Інформаційної та кібернетичної безпеки | | | | | | | | | | | | | | |
| Ступінь вищої освіти | | | | Бакалавр | | | | | | |  | | | |  | |
| Спеціальність | | | 125 Кібербезпека | | | | | | | |  | | | |  | |
| Освітньо-професійна програма | | | | | | | Інформаційна та кібернетична безпека | | | | | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | | ЗАТВЕРДЖУЮ | | | | | |
|  | |  | | | | |  | | | | Завідувач кафедри ІКБ | | | | | |
|  | |  | | | | |  | | | |  | | | | Гайдур Г.І. | |
|  | |  | | | | |  | | | | “\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 року | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | | **З А В Д А Н Н Я** | | | | | | | | | | | | |  | |
|  | | **НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ** | | | | | | | | | | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
| Бондару Богдану Васильовичу | | | | | | | | | | | | | | | | |
| (прізвище, ім’я, по батькові) | | | | | | | | | | | | | | | | |
| 1. Тема бакалаврської роботи: | | | | | | «Дослідження шляхів та розробка | | | | | | | | | | | |
| рекомендацій щодо управління мобільними пристроями за концепцією | | | | | | | | | | | | | | | | |
| BYOD в ІС організації» | | | | | | | | | | | | | | | | |
| керівник бакалаврської роботи | | | | | | | Гайдур Галина Іванівна | | | | | | | | | |
|  | |  | | | | | (прізвище, ім’я, по батькові, науковий ступінь, вчене звання) | | | | | | | | | |
| затверджені наказом закладу вищої освіти від «24» лютого 2023 року № 26. | | | | | | | | | | | | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
| 2. Строк подання студентом бакалаврської роботи | | | | | | | | | | | | 25.05.2023 р. | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
| 3. Вихідні дані до бакалаврської роботи | | | | | | | |  | | | | | | |  | |
| центр управління кібербезпекою; | | | | | | | | | | |  | | | |  | |
| рішення BYOD та MobileIron; | | | | | | | | | | | | | | | | |
| наукова та технічна література, експлуатаційна документація, нормативні | | | | | | | | | | | | | | | | |
| документи, міжнародні стандарти. | | | | | | | | | | |  | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
| 4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) | | | | | | | | | | | | | | | | |
| 1. Визначення актуальності потреби підключення та керування мобільними пристроями в ІС організації. | | | | | | | | | | | | | | | | |
| 2. Аналіз методів та засобів підключення та керування мобільними пристроями. | | | | | | | | | | | | | | | | |
| 3. Розроблення рекомендацій щодо застосування методів та засобів політик BYOD в програмі MobileIron. | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | |
| 5. Перелік графічного матеріалу | | | | | | | | | | |  | | | |  | |
| 1. Тема бакалаврської роботи. | | | | | | | | | | | | | | | | |
| 2. Об’єкт, предмет, мета та наукові завдання дослідження. | | | | | | | | | | | | | | | | |
| 3. Результати аналізу проблеми виявлення аномального трафіку у корпоративній мережі. | | | | | | | | | | | | | | | | |
| 4. Результати дослідження методів та засобів підключення та курування мобільними пристроями. | | | | | | | | | | | | | | | | |
| 5. Порядок застосування політик BYOD в програмі MobileIron. | | | | | | | | | | | | | | | | |
| 6. Розроблення рекомендацій щодо застосування методів та засобів політик BYOD в програмі MobileIron. | | | | | | | | | | | | | | | | |
| 7. Висновки за результатами роботи. | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | |
| 6. Дата видачі завдання | | | | | 10.03.2023 р. | | | | | | | | | | | |
|  | |  | | | | |  | | | |  | | | |  | |
|  | | **КАЛЕНДАРНИЙ ПЛАН** | | | | | | | | | | | | |  | |
|  | |  | | | | |  | | | |  | | | |  | |
| №  зп | Назва етапів  бакалаврської роботи | | | | | | | | | | | | | Строк виконання етапів бакалаврської роботи | | Примітка |
| 1. | Визначення актуальності потреби підключення та керування мобільними пристроями в ІС організації. | | | | | | | | | | | | | 30.03.2023 р. | |  |
| 2. | Аналіз наукової та технічної літератури з питань теми бакалаврської роботи. | | | | | | | | | | | | | 06.04.2023 р. | |  |
| 3. | Аналіз методів та засобів підключення та курування мобільними пристроями. | | | | | | | | | | | | | 13.04.2023 р. | |  |
| 4. | Проведення експерименту щодо застосування політик BYOD в програмі MobileIron. | | | | | | | | | | | | | 20.04.2023 р. | |  |
| 5. | Розроблення рекомендацій щодо застосування методів та засобів політик BYOD в програмі MobileIron. | | | | | | | | | | | | | 04.05.2023 р. | |  |
| 6. | Оформлення результатів дослідження. | | | | | | | | | | | | | 16.05.2023 р. | |  |
| 7. | Підготовка доповіді до захисту. | | | | | | | | | | | | | 23.05.2023 р. | |  |
|  | | | | | | | | | | | | | |  | |  |
|  | |  | | | | | Студент | | | | Бондар Б.В. | | | | | |
|  | |  | | | | |  | | | | (підпис) | | | | прізвище та ініціали | |
|  | |  | | | | |  | | | |  | | | |  | |
| Керівник бакалаврської роботи | | | | | | | | | | |  | | | | Гайдур Г.І. | |
|  | |  | | | | |  | | | | (підпис) | | | | прізвище та ініціали | |

**ВІДГУК РЕЦЕНЗЕНТА**

на бакалаврську роботу

студентаБондара Богдана Васильовича

на тему: «Дослідження шляхів та розробка рекомендацій щодо управління мобільними пристроями за концепцією BYOD в ІС організації»

**Актуальність:** Мобільні пристрої в сучасному світі стали невід’ємною частиною нашого життя. Це також не обійшло стороною компанії та бізнес в цілому. У світі зростає попит на фріланс та компанії переходять на віддалену роботу. Таке розпорядження дає позитивний ефект не тільки на продуктивності роботи працівників, а також запобігає витратам на оренду та утримання офісу. Співробітникам це дає змогу менше витрачати часу на дорогу до роботи, що дає змогу більше відпочивати, а також відпадає необхідність витрачати гроші щоб доїхати до офісу.

**Позитивні сторони:**

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми, визначено мета та завдання необхідності в управлінні мобільними пристроями в ІС організації.
2. Досліджено методи та засоби підключення та керування мобільними пристроями.
3. Проведено експеримент щодо застосування політик BYOD в програмі MobileIron.
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 бакалаврської роботи.

**Недоліки:**

В роботі доцільно було привести статистику щодо втрати конфіденційних даних пр використанні мобільних пристроїв в організації.

**Висновок:** Враховуючи відсутність недоліків, бакалаврська робота заслуговує оцінку **Відмінно**, а студент **Бондар Б.В.** – присвоєння кваліфікації *бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека*.

|  |  |  |
| --- | --- | --- |
| Якість роботи | | Підпис рецензента (\_\_\_\_\_\_\_\_\_\_\_\_\_\_)  Підпис засвідчую  Підпис особи, що засвідчує (\_\_\_\_\_\_\_\_\_\_\_\_) |
| Виконано на замовлення підприємства |  |
| Виконано за тематикою НДР |  |
| Виконано з макетом |  |
| Виконано з застосуванням ЕОМ та МПТ | √ |
| Має практичну цінність | √ |
| Проект-частина комплексної теми |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ** | | | | | | | | | |
| **ПОДАННЯ**  **ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ**  **ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ** | | | | | | | | | |
| Направляється студент | | | Бондар Б.В. | | | до захисту бакалаврської роботи | | | |
|  | | | (прізвище та ініціали) | | |  | | | |
| спеціальності 125 Кібербезпека | | | |  | | |  | |  |
| освітньо-професійної програми | | | | Інформаційна та кібернетична безпека | | | | | |
|  |  | | | (шифр і назва спеціальності) | | | | | |
| на тему: | «Дослідження шляхів та розробка рекомендацій щодо управління мобільними пристроями за концепцією BYOD в ІС організації» | | | | | | | | |
| Бакалаврська робота і рецензія додаються. | | | | | | |  | |  |
| Директор інституту | | | |  | | | Савченко В.А. | | |
| (підпис) (прізвище та ініціали) | | | | | | | | | |
|  | |  | |  | | |  | |  |
|  | | **Довідка про успішність** | | | | | | |  |
| Бондар Б.В. | | | | за період навчання в інституті | | | | | |
| (прізвище та ініціали студента) | | | |  | | |  | |  |
| ННІЗІ з 2019 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:  національною шкалою: відмінно \_\_\_\_%, добре \_\_\_\_%, задовільно \_\_\_\_%;  шкалою ECTS: А \_\_\_\_%; В \_\_\_\_%; С \_\_\_\_%; D \_\_\_\_%; Е \_\_\_\_%. | | | | | | | | | |
| Секретар інституту, факультету (відділення) | | | | | | |  | | Берестяна Т.В. |
|  | |  | |  | | | (підпис) | | (прізвище та ініціали) |
|  | | **Висновок керівника бакалаврської роботи** | | | | | | |  |
| Студент ***Бондар Б.В.*** обрав тему роботи, метою якої було розробити рекомендації щодо виявлення аномального трафіку у корпоративній мережі. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Бондар Б.В. показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.  Все це дозволяє оцінити виконану бакалаврську роботу студента Бондара Богдана Васильовича на оцінку **«відмінно»** та присвоїти йому кваліфікацію *бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека*. | | | | | | | | | |
| Керівник бакалаврської роботи | | | | | | |  | | Гайдур Г.І. |
|  | |  | |  | | | (підпис) | | (прізвище та ініціали) |
|  | |  | |  | | | “\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_ 2023 року | | |
|  | | **Висновок кафедри про бакалаврську роботу** | | | | | | |  |
| Бакалаврська робота розглянута. Студент | | | | | Бондар Б.В. | | | | |
|  | |  | |  | (прізвище та ініціали) | | | | |
| допускається до захисту даної бакалаврської роботи в Державній екзаменаційній комісії. | | | | | | | | | |
| Завідувач кафедри Інформаційної та кібернетичної безпеки | | | | | | | |  |  |
| (назва) | | | | | | | | | | |
|  | |  | |  | | |  | | Гайдур Г.І. |
|  | |  | | (підпис) | | | (прізвище та ініціали) | | |
| “\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_ 2023 року | | | |  | | |  | |  |
| **РЕФЕРАТ** | | | | | | | | | |
|  | |  | |  | | |  | |  |
|  | |  | |  | | |  | |  |
| Текстова частина бакалаврської роботи: 59 сторінок, Рисунки, одна таблиця, 10 джерел.  *Об’єкт дослідження* –процес управління мобільними пристроями до інформаційної системи організації.  *Предмет дослідження* – методи та засоби управління мобільними пристроями організації за концепцією BYOD.  *Мета роботи* – розробити рекомендації щодо застосування методів та засобів управління мобільними пристроями організації за концепцією BYOD.  *Методи дослідження* – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, проведення експерименту.  В роботі розглянуто способи та методи підключення та управляння мобільними пристроями в ІС організації. Такі як: Mobile Content Management, Mobile Identity Management, Mobile Device Management, Mobile Application Management, Bring your own device, Choose Your Own Device, Corporate Owned Personally Enabled. Розроблено рекомендації щодо застосування MobileIron в ІС організації  MOBILE IDENTITY MANAGEMENT, MOBILE DEVICE MANAGEMENT, MOBILE APPLICATION MANAGEMENT, BYOD, МОБІЛЬНІ ПРИСТРОЇ, УПРАВЛІННЯ | | | | | | | | | |

ЗМІСТ

[ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 8](#_Toc135814523)

[ВСТУП 9](#_Toc135814524)

[1 АНАЛІЗ УПРАВЛІННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ В ІС ОРГАНІЗАЦІЇ 10](#_Toc135814525)

[**1.1 Роль і місце мобільних пристроїв в ІС організації** 10](#_Toc135814526)

[**1.2 Аналіз загроз щодо користувачів ІС організації** 15](#_Toc135814527)

[**1.3 Аналіз основних методів та засобів управління мобільними пристроями в ІС організації** 22](#_Toc135814528)

[2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ В ІС ОРГАНІЗАЦІЇ 30](#_Toc135814529)

[**2.1 Аналіз концепцій застосування мобільних пристроїв в ІС організації** 30](#_Toc135814530)

[**2.2 Архітектура BYOD** 39](#_Toc135814531)

[**2.3 Функції та складові BYOD** 45](#_Toc135814532)

[3. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО НАЛАШТУВАНЬ РІШЕННЯ BYOD В УПРАВЛІННІ МОБІЛЬНИМИ ПРИСТРОЯМИ 52](#_Toc135814533)

[**3.1 Загальні вимоги та методи програми MobileIron** 52](#_Toc135814534)

[**3.2 Налаштування програми MobileIron** 57](#_Toc135814535)

[**3.3** **Розробка рекомендацій щодо застосування MobileIron в ІС організації** 64](#_Toc135814536)

[ВИСНОВКИ 70](#_Toc135814537)

[ПЕРЕЛІК ПОСИЛАНЬ 71](#_Toc135814538)

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС - Операційна Система

ІС - інформаційна система

МСМ - Mobile Content Management

МІМ - Mobile Identity Management

MDM - Mobile Device Management

MAM - Mobile Application Management

VPN - Virtual Private Network

Wi-Fi - Wireless Fidelity

BYOD - Bring your own device

CYOD - Choose Your Own Device

COPE – Corporate Owned Personally Enabled

SSL - Secure Sockets Layer

TLS- Transport Layer Security

# ВСТУП

*Актуальність дослідження.* Мобільні пристрої в сучасному світі стали невід’ємною частиною нашого життя. Це також не обійшло стороною компанії та бізнес в цілому. У світі зростає попит на фріланс та компанії переходять на віддалену роботу. Таке розпорядження дає позитивний ефект не тільки на продуктивності роботи працівників, а також запобігає витратам на оренду та утримання офісу. Співробітникам це дає змогу менше витрачати часу на дорогу до роботи, що дає змогу більше відпочивати, а також відпадає необхідність витрачати гроші щоб доїхати до офісу.

*Об’єкт дослідження* – процес управління мобільними пристроями до інформаційної системи організації.

*Предмет дослідження* – методи та засоби управління мобільними пристроями організації за концепцією BYOD.

*Мета роботи* – розробити рекомендації щодо застосування методів та засобів управління мобільними пристроями організації за концепцією BYOD.

*Наукові завдання:*

проаналізувати проблему захисту корпоративної інформації;

проаналізувати існуючі методи та засоби підключення мобільних пристроїв до мережі компанії;

дослідити методи та засоби використання методу BYOD при керування мобільними пристроями;

розглянути порядок застосування політик BYOD в програмі MobileIron;

*Методи дослідження* – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, проведення експерименту.

*Практичне значення одержаних результатів* полягає в розробці рекомендацій щодо застосування політик BYOD в програмі MobileIron.

# 1 АНАЛІЗ УПРАВЛІННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ В ІС ОРГАНІЗАЦІЇ

## **1.1 Роль і місце мобільних пристроїв в ІС організації**

Мобільні пристрої, такі як смартфони та планшети та ноутбуки, стали невід'ємною частиною інформаційних систем (ІС) організацій.

Мобільні пристрої стали невід'ємною частиною нашого повсякденного життя, а в бізнес-середовищі вони є необхідним інструментом для роботи в дорозі, на зустрічах, на віддаленому робочому місці тa інших ситуаціях, де доступ до ІС організації потрібен поза межами офісу.

Однією з переваг використання мобільних пристроїв є їх мобільність. Це дозволяє співробітникам працювати в різних місцях та у різний чaс, що підвищує продуктивність та ефективність роботи. Зокрема, мобільні пристрої дозволяють співробітникам виконувати різні завдання, такі як перегляд електронної пошти, доступ до документів, управління проектами та зустрічами, віддалене керування комп'ютерами та інші.

Мобільні пристрої можуть використовуватися для забезпечення комунікації між співробітниками організації. Вони дозволяють взаємодіяти у режимі реального часу, обмінюватися інформацією та здійснювати відео- та аудіоконференції. Це особливо важливо для організацій з великою кількістю віддалених співробітників або тих, що працюють з дому.

Мобільні пристрої в ІС організації забезпечують швидкий та зручний доступ до інформації, можливість роботи в режимі реального часу та забезпечують ефективну комунікацію між співробітниками. Однак, необхідно забезпечувати безпеку даних та захищати мобільні пристрої від загроз, таких як віруси тa хакерські атаки. Також, варто мати політику використання мобільних пристроїв у ІС організації та навчати співробітників правильному використанню цих пристроїв.

Вони забезпечують різноманітні функції, такі як:

* Забезпечення зв'язку: Мобільні пристрої можуть використовуватися для зв'язку між співробітниками організації, які перебувають на різних місцях. Це може бути особливо корисно для компаній з великою кількістю робітників, що працюють на віддаленій роботі або для тих, хто часто подорожує відрядженням.
* Доступ до ІС: Мобільні пристрої можуть дозволити співробітникам організації отримувати доступ до ІС з будь-якого місця з підключенням до Інтернету. Це дозволяє робити роботу з дому або під час подорожей.
* Керування проектами: Мобільні пристрої можуть допомогти співробітникам вести керування проектами та плануванням завдань з будь-якого місця. Додатки для управління проектами можуть дозволити відстежувати прогрес проекту, спілкуватися зі співробітниками та ділитися документами.
* Комунікація з клієнтами: Мобільні пристрої можуть допомогти забезпечити комунікацію з клієнтами організації. Наприклад, можна використовувати текстові повідомлення, електронну пошту або додатки для чату для спілкування з клієнтами та відповіді на їх запити.
* Збір даних: Мобільні пристрої можуть використовуватися для збору даних, що може бути корисним для досліджень та аналізу.
* Моніторинг робочого процесу: Мобільні пристрої можуть використовуватися для моніторингу робочого процесу в реальному часі. Наприклад, виробнича компанія може використовувати мобільні пристрої для моніторингу роботи обладнання, роботи працівників тa збору даних про продуктивність.
* Реклама та маркетинг: Мобільні пристрої можуть використовуватися для реклами та маркетингу продуктів та послуг організації. Наприклад, компанії можуть використовувати рекламні додатки для розсилки рекламних повідомлень та пропозицій.
* Збір зворотного зв'язку: Мобільні пристрої можуть використовуватися для збору зворотного зв'язку від клієнтів, що дозволяє організації збирати відгуки та пропозиції для поліпшення продуктів та послуг.
* Навчання та підтримка співробітників: Мобільні пристрої можуть використовуватися для навчання та підтримки співробітників. Організації можуть створювати навчальні матеріали, які доступні через мобільні додатки, що дозволяє співробітникам отримувати доступ до навчального матеріалу з будь-якого місця.
* Управління документами: Мобільні пристрої можуть використовуватися для управління документами організації. Співробітники можуть відкривати, переглядати та редагувати документи зі своїх мобільних пристроїв, що дозволяє підвищити ефективність та продуктивність роботи організації.
* Моніторинг витрат та фінансів: Мобільні пристрої можуть використовуватися для моніторингу витрат та фінансів організації. Співробітники можуть вносити витрати зі своїх мобільних пристроїв, що дозволяє ефективно відслідковувати витрати та підвищувати контроль над фінансами.
* Підтримка клієнтів: Мобільні пристрої можуть використовуватися для підтримки клієнтів. Наприклад, компанії можуть використовувати спеціальні додатки для спілкування з клієнтами, відповіді на запитання та розв'язання проблем.
* Забезпечення безпеки: Мобільні пристрої можуть використовуватися для забезпечення безпеки організації. Наприклад, можна використовувати мобільні пристрої для контролю доступу до об'єктів або для моніторингу безпеки приміщень.
* Моніторинг конкурентів: Мобільні пристрої можуть використовуватися для моніторингу конкурентів організації. Наприклад, компанії можуть використовувати спеціальні додатки для відстеження діяльності конкурентів та отримання важливої інформації про їх продукти та послуги.
* Віддалений доступ до робочого столу: Мобільні пристрої можуть використовуватися для віддаленого доступу до робочого столу комп'ютера. Це дозволяє співробітникам отримувати доступ до робочого столу з будь-якого місця, що дозволяє підвищити продуктивність та ефективність роботи.
* Підтримка процесів виробництва: Мобільні пристрої можуть використовуватися для підтримки процесів виробництва. Наприклад, співробітники можуть використовувати мобільні пристрої для моніторингу стану обладнання та збору даних про ефективність виробничих процесів.
* Моніторинг та аналітика: Мобільні пристрої можуть використовуватися для моніторингу та аналітики даних. Наприклад, можна використовувати мобільні пристрої для збору даних про клієнтів, аналізу даних та прийняття рішень на основі аналітики.
* Відео конференції: Мобільні пристрої можуть використовуватися для проведення відео конференцій. Це дозволяє співробітникам з різних місць збиратися разом і проводити зустрічі, обговорювати питання та приймати рішення.
* Спрощення комунікації: Мобільні пристрої допомагають спростити комунікацію між співробітниками та клієнтами. Наприклад, можна використовувати мобільні додатки для спілкування через месенджери, електронну пошту та соціальні мережі.
* Підвищення ефективності роботи: Мобільні пристрої дозволяють співробітникам працювати більш ефективно та продуктивно. Наприклад, можна використовувати мобільні пристрої для швидкого доступу до інформації, планування та координації робіт, виконання завдань в режимі реального часу та збільшення швидкості прийняття рішень.
* Віддалене навчання та підтримка: Мобільні пристрої можуть бути використані для віддаленого навчання та підтримки працівників, наприклад, за допомогою відеокурсів, онлайн-семінарів та інших форм навчання.

Можна сказати, що мобільні пристрої мають значний потенціал для підвищення ефективності та продуктивності роботи співробітників організації.

Для ефективного використання мобільних пристроїв у ІС організації також важливо встановлювати стандарти та правила використання таких пристроїв. Це може включати в себе такі аспекти, як правила використання мобільних пристроїв на робочому місці, обмеження доступу до певних типів даних на мобільних пристроях, а також правила використання сховищ на мобільних пристроях для зберігання конфіденційної інформації.

Організація повинна мати відповідну інфраструктуру та технічні засоби для підтримки мобільних пристроїв, таких як програмне забезпечення для управління мобільними пристроями, безпечна Wi-Fi мережа та доступ до хмарних сервісів для зберігання та обміну даними.

Організації повинні використовувати спеціальне програмне забезпечення для управління мобільними пристроями, яке дозволяє керувати правами доступу та налаштуваннями, забезпечує оновлення програм та інші функції для захисту даних.

Для досягнення цих цілей необхідно створювати політики та процедури використання мобільних пристроїв, які включатимуть у себе необхідні заходи безпеки та використання пристроїв згідно зі стандартами та правилами.

Важливо мати політику використання мобільних пристроїв у ІС організації, яка повинна бути офіційно оприлюднена та відома всім співробітникам. Політика повинна включати правила використання мобільних пристроїв, доступ до корпоративних даних, відповідальність за безпеку даних та інші важливі питання.

Навчання співробітників правильному використанню мобільних пристроїв та їх взаємодії з ІС організації також є важливим для ефективного використання мобільних пристроїв.

Додатковою важливою складовою ефективного використання мобільних пристроїв у ІС організації є розуміння використання аналітики даних. Мобільні пристрої збирають велику кількість даних, таких як геолокація, інформація про використання додатків та поведінку користувачів. Ці дані можуть бути використані для аналізу та вдосконалення роботи організації. Наприклад, дані про використання додатків на мобільних пристроях можуть допомогти організації зрозуміти, які додатки користуються найбільшою популярністю серед співробітників, і вдосконалити процеси роботи відповідно до цього.

Також важливо враховувати соціальну відповідальність організації та питання екології при використанні мобільних пристроїв. Зазвичай, мобільні пристрої мають короткий термін експлуатації та потребують заміни через деякий час. Організації повинні розробляти та впроваджувати плани щодо зменшення кількості відходів від старих мобільних пристроїв та їх вторинної переробки.

Отже, мобільні пристрої є невід’ємною частиною ІС організації, яка дозволяє підвищити ефективність та продуктивність роботи співробітників. Однак, для успішного впровадження мобільних пристроїв в ІС організації необхідно дотримуватися політик та процедур щодо захисту даних, навчати співробітників з використання та безпечного зберігання мобільних пристроїв та їх даних. Також необхідно мати добре розроблену стратегію управління мобільними пристроями, щоб забезпечити ефективне використання ресурсів та зменшити ризики пов'язані з їх використанням.

## **1.2 Аналіз загроз щодо користувачів ІС організації**

Аналіз загроз щодо користувачів ІС організації є важливим етапом в забезпеченні безпеки інформаційної системи. Загрози можуть бути різноманітними, включаючи технічні, соціальні та організаційні. В даному випадку, ми розглянемо загрози, пов'язані з користувачами ІС організації.

Однією з основних загроз є недбале ставлення користувачів до безпеки інформації. Недосвідчені або неуважні користувачі можуть надавати доступ до своїх облікових записів, використовувати слабкі паролі або зберігати конфіденційну інформацію на незахищених пристроях. Це може призвести до несанкціонованого доступу до інформації, втрати конфіденційності або пошкодження даних.

Іншою загрозою є зловживання привілеями. Користувачі з повним доступом до системи можуть використовувати свої привілеї для несанкціонованого доступу до інформації або внесення змін у систему. Наприклад, адміністратор мережі може надавати доступ до конфіденційної інформації недостатньо авторизованим особам.

Також, загрозою є крадіжка облікових даних. Хакери можуть використовувати різні методи, щоб отримати доступ до облікових даних користувачів, наприклад, шляхом підміни паролів або перехопленням даних при передачі через мережу. Після отримання цих даних, зловмисники можуть використовувати їх для несанкціонованого доступу до інформації та проведення атак на систему.

Так, соціальна інженерія є ще однією з загроз, які можуть виникнути щодо користувачів ІС організації. Соціальна інженерія - це процес використання маніпуляції людей з метою отримання доступу до конфіденційної інформації або проведення шкідливих дій. Атаки соціальної інженерії можуть бути проведені через електронну пошту, телефон, соціальні мережі або особистий контакт з працівником організації.

Наприклад, зловмисники можуть використовувати соціальні мережі, щоб вивчити інформацію про співробітників організації, їхні інтереси та звички. Після цього вони можуть надіслати шахрайські повідомлення або електронні листи, які містять фішингові посилання або віруси. Якщо співробітник організації натисне на ці посилання та введе свої облікові дані, зловмисники зможуть отримати доступ до їх облікових записів.

Іншим прикладом може бути використання методу "соціальної інженерії через телефон". Зловмисники можуть використовувати телефон для того, щоб надати себе за представника організації, яка потребує негайного доступу до конфіденційної інформації. Якщо співробітник організації не перевірить ідентифікацію особи, яка звернулася до нього за допомогою телефону, зловмисники можуть отримати доступ до цієї інформації.

Оскільки соціальна інженерія залежить від маніпулювання людьми, то неможливо повністю захиститися від таких атак технічними засобами. Тому дуже важливо навчати співробітників організації, як відрізняти правдиву інформацію від шахрайства та інформації з підозрілих джерел. Це можна здійснити шляхом проведення тренінгів та семінарів з кібербезпеки, де співробітникам надається інформація про основні загрози та методи захисту від них.

Щоб запобігти соціальній інженерії, необхідно проводити навчання співробітників організації та забезпечувати їхню свідомість про ризики. Також можна використовувати технології захисту, такі як фільтри спаму та вірусів, а також двофакторну аутентифікацію.

Важливо регулярно проводити аудит безпеки ІС організації та виявляти можливі слабкі місця, які можуть бути використані зловмисниками. Зокрема, важливо перевіряти наявність оновлень та патчів для програмного забезпечення, виявляти та усувати вразливості мережевої інфраструктури та перевіряти права доступу до інформації.

Важливо мати плани невідкладних заходів у разі кібератак, а також регулярно проводити навчання з планування та виконання дій у разі кризових ситуацій.

Також можливими загрозами щодо користувачів ІС організації є кібершпигунство та кібершантаж. Кібершпигунство означає незаконне здобування конфіденційної інформації про організацію з метою отримання переваг у сфері бізнесу або політики. Кібершантаж, з свого боку, означає шахрайство, коли зловмисники здобувають доступ до важливої інформації та вимагають від організації викуп за її повернення.

Для захисту від таких загроз необхідно використовувати захисні технології, такі як антивірусні програми, файрволи та інші засоби захисту. Важливо дотримуватися політик безпеки даних та процедур, що включають у себе зміну паролів, шифрування даних, заборону використання неофіційного програмного забезпечення та інші важливі кроки.

Крім того, загрози для користувачів ІС організації можуть виникати із зовнішніх джерел, таких як зловмисники, що намагаються отримати несанкціонований доступ до системи, шляхом перехоплення трафіку або використання вразливостей системи. Найбільш поширеними видами таких атак є фішинг, злам паролів, злам електронної пошти та соціальна інженерія.

Ще однією загрозою є втрата або крадіжка пристроїв, що містять конфіденційну інформацію. Якщо зловмисники отримають доступ до таких пристроїв, вони можуть зламати захист і отримати доступ до цієї інформації. Тому, користувачам потрібно дотримуватися політик щодо безпеки пристроїв та інформації, таких як налаштування складних паролів, використання шифрування та захисту даних віддаленим знищенням у разі втрати пристроїв.

Загрози щодо користувачів ІС організації є постійними та еволюціонуючими, тому важливо регулярно оновлювати політики безпеки та процедури, навчати співробітників щодо їх виконання та захисту від нових видів атак. Тільки так організація може забезпечити надійний захист своїх ІС та інформації від зловмисних дій.

До загроз для користувачів ІС організації можна віднести і випадки фізичного доступу до комп'ютерів, серверів та інших пристроїв, які містять важливу інформацію. Це може статися через викрадення або втрату пристроїв, несанкціонований доступ до офісів або інших приміщень, де знаходяться комп'ютери та інші пристрої.

Для запобігання таким загрозам необхідно встановлювати фізичні бар'єри доступу до приміщень з комп'ютерами та іншими пристроями, обмежувати фізичний доступ до цих пристроїв та забезпечувати їх безпеку при використанні з боку співробітників.

Також варто зазначити, що загрози щодо користувачів ІС можуть виникнути із зовнішнього середовища, наприклад, через використання незахищеного Wi-Fi або підключення до невідомих пристроїв. У таких випадках можуть бути викрадені особисті дані, паролі, банківські реквізити та інші конфіденційні дані.

Однією з можливостей захисту від зовнішніх загроз є використання ефективних засобів антивірусного захисту, фірмових брандмауерів та інших програм для забезпечення безпеки ІС організації. Також важливо регулярно оновлювати програмне забезпечення та використовувати сильні паролі для доступу до ІС організації.

Усі ці заходи мають на меті зменшити ризик виникнення загроз для користувачів ІС організації та забезпечити безпеку даних та інформаційних ресурсів. Однак, важливо розуміти, що заходи безпеки мають бути постійно оновлюваними та підлаштовуваними до нових загроз, що виникають у сучасному світі.

Додатково, для аналізу загроз щодо користувачів ІС організації можуть бути використані різні методики та підходи, наприклад:

* SWOT-аналіз. Даний підхід дозволяє визначити сильні та слабкі сторони системи, а також можливості та загрози, які можуть впливати на безпеку ІС організації.
* Аналіз історії інцидентів. Цей підхід базується на аналізі історичних даних про попередні інциденти та атаки на ІС організації, які відбувалися в минулому. Це дозволяє виявити типові атаки та проблеми, які можуть з'явитися у майбутньому.
* Аналіз ризиків. Цей підхід дозволяє визначити ризики, які можуть виникнути в ІС організації та виявити їх потенційний вплив на систему.
* Аналіз вразливостей. Даний підхід дозволяє виявити потенційні вразливості в ІС організації та оцінити їх важливість та віддаленість від цілей атакуючого.

Усі ці методи можуть бути використані для аналізу загроз щодо користувачів. ІС організації та розробки стратегій щодо їх запобігання. При цьому важливо враховувати специфіку організації та її ІС, а також нові тенденції та загрози, які з'являються в цій галузі.

Ще одним важливим аспектом є забезпечення доступу до систем ІС організації тільки авторизованим користувачам. Це може бути забезпечено за допомогою різних методів аутентифікації, таких як паролі, біометричні дані або токени.

Проте, багато атак на ІС організації відбуваються через компрометацію аутентифікаційних даних користувачів, таких як паролі. Тому важливо навчати співробітників використовувати складні та унікальні паролі, регулярно змінювати їх та не використовувати один і той же пароль для кількох систем.

Також, необхідно забезпечити захист від шкідливих програм, таких як віруси, троянські програми та інші види зловмисного програмного забезпечення. Це може бути забезпечено за допомогою антивірусного програмного забезпечення та регулярного оновлення програм та операційних систем.

Крім того, важливо забезпечити регулярні бекапи даних, щоб у разі втрати чи пошкодження даних їх можна було відновити. Бекапи повинні бути збережені на захищеному сервері або в хмарному сховищі з адекватними політиками збереження даних.

Відповідно до загальних принципів інформаційної безпеки, захист ІС організації від атак повинен включати такі складові:

* Для забезпечення захисту ІС організації необхідно спочатку *ідентифікувати можливі загрози*, які можуть впливати на безпеку системи. Це може бути здійснене шляхом аналізу попередніх атак, оцінки вразливостей системи та її компонентів, та інших методів.
* Після ідентифікації загроз необхідно *розробити політику безпеки*, яка буде визначати правила та процедури для забезпечення захисту системи. Політика повинна охоплювати такі аспекти, як контроль доступу, захист даних, мережевий захист, захист від вірусів, та інші.
* Після розробки політики безпеки, необхідно *розробити процедури, які забезпечать її виконання*. Ці процедури можуть включати такі елементи, як процедури автентифікації та авторизації, резервне копіювання даних, моніторинг мережі та систем, та інші.
* В разі, якщо інформаційна система була скомпрометована або пошкоджена, необхідно *мати план відновлення*, який дозволить повернути систему до нормального стану. Це може включати резервне копіювання даних, тестування процедур відновлення, та інші елементи.
* Крім технічних засобів захисту, важливо також *навчати співробітників* *організації* правилам та процедурам захисту інформації. Це допоможе зменшити ризик неправильної поведінки співробітників, яка може призвести до компрометації конфіденційної інформації організації.

Навчання співробітників повинно починатися з ознайомлення з політикою безпеки інформації організації та правилами щодо користування ІС. Кожен співробітник має бути свідомим ризиків, пов'язаних з використанням ІС та вміти застосовувати правила забезпечення безпеки інформації у своїй роботі.

Навчання повинно включати освіту співробітників щодо загроз безпеці інформації, які включають в себе такі явища, як фішинг, шпигунство, віруси та інші види атак. Співробітники повинні розуміти, які заходи можуть бути прийняті для запобігання цим загрозам, наприклад, як використовувати антивірусне програмне забезпечення, як забезпечити безпечні паролі, як перевірити автентичність електронної пошти тощо.

Також важливо навчити співробітників організації виявляти підозрілі ситуації, повідомляти про них відповідні служби організації та реагувати на події, пов'язані з інцидентами безпеки. Це також може включати навчання співробітників про те, які дії слід приймати в разі викрадення або втрати пристроїв, які містять конфіденційну інформацію, та як захистити свої пристрої від крадіжки. Співробітники повинні знати, як правильно використовувати паролі та інші засоби аутентифікації, які дозволяють забезпечити доступ лише для авторизованих користувачів. Регулярні навчальні семінари та тренінги можуть допомогти оновити знання співробітників та підвищити їхню обізнаність щодо захисту ІС організації.

На етапі навчання слід розглянути можливі сценарії інцидентів безпеки та визначити ролі та відповідальності співробітників в процесі їх виявлення, реагування та подальшого вирішення. Варто провести практичні тренування та симуляції інцидентів, щоб співробітники могли набути практичного досвіду та навчитися швидко та ефективно реагувати на негативні ситуації.

Також важливо, щоб навчання співробітників з охорони інформації проводилось регулярно, оскільки швидко розвиваються технології та появляються нові загрози. Вони можуть вимагати оновлення знань та навичок. Навчання співробітників щодо захисту ІС повинно бути обов'язковою складовою будь-якої політики безпеки в організації, оскільки вони є першою лінією захисту інформації та можуть значно впливати на успішність заходів щодо її захисту.

На кожному етапі процесу реагування на інцидент необхідно забезпечити координацію дій між всіма відповідальними службами організації та партнерами, які можуть надавати допомогу в такій ситуації. Це включає проведення перевірок систем безпеки, збір та аналіз даних про інцидент, відновлення роботи систем та оцінку наслідків для організації.

## **1.3 Аналіз основних методів та засобів управління мобільними пристроями в ІС організації**

Роль мобільних пристроїв не можливо переоцінити в сучасній ІС організації. Однак, мобільні пристрої також стали об'єктом вразливостей та загроз для ІС організації, що може призвести до втрати конфіденційної інформації, порушення цілісності даних та вірусних атак.

Управління мобільними пристроями в ІС організації означає встановлення та забезпечення безпеки на мобільних пристроях, що використовуються співробітниками організації. Основна мета полягає в тому, щоб запобігти можливості віддаленого доступу до мобільних пристроїв неправомірними особами.

На сьогоднішній день існує безліч різних рішень для керування мобільними пристроями в ІС організації. Деякі з них є комерційними продуктами, які пропонуються провайдерами мобільних послуг або спеціалізованими постачальниками програмного забезпечення, а інші можуть бути розроблені внутрішніми командами ІТ-спеціалістів організації.

Деякі з основних методів та засобів управління мобільними пристроями в ІС організації:

* *Mobile Content Management (МСМ)* – метод, який використовується для керування та захисту даних на мобільних пристроях. МСМ дозволяє адміністраторам ІТ-системи контролювати доступ до даних, захищати їх та керувати політиками безпеки відносно даних, що зберігаються на мобільних пристроях;
* *Mobile Identity Management (МІМ)* - використовується для керування ідентифікацією та автентифікації;
* *Mobile Device Management (MDM)* - системи управління мобільними пристроями, які дозволяють керувати даними та налаштуваннями на мобільних пристроях з центрального сервера. MDM може включати в себе такі функції, як керування додатками, контроль доступу, шифрування даних, встановлення політик безпеки тощо **(Рис. 1.1. );**

****

**Рис.1.1 Функції управління мобільними пристроями**

MDM забезпечує централізоване управління мобільними пристроями, зокрема дозволяє:

* віддалено налаштовувати та керувати настройками мобільних пристроїв;
* встановлювати та оновлювати програмне забезпечення на мобільних пристроях;
* визначати політики безпеки для мобільних пристроїв (наприклад, вимагати використання паролів або шифрування даних);
* віддалено вимагати видалення даних з пристроїв у разі втрати або крадіжки;
* віддалено заблоковувати пристрої в разі неправильних спроб входу.

Застосування MDM дозволяє знизити ризики витоку конфіденційної інформації та збільшити ефективність роботи співробітників з мобільними пристроями, зменшуючи витрати на обслуговування та підтримку цих пристроїв.

MDM може бути встановлений на мобільні пристрої через спеціальні програми, які надають відповідні можливості для організацій, або на рівні операційної системи самого пристрою.

Використання MDM може бути особливо важливим для компаній, які працюють з конфіденційною інформацією або зберігають важливі дані на мобільних пристроях. Такі компанії можуть застосовувати MDM для забезпечення безпеки своїх даних та контролю над доступом до них, а також для зменшення ризику втрати або крадіжки мобільних пристроїв.

Окрім того, MDM може бути корисним для управління та підтримки мобільних пристроїв у великих організаціях, де є багато співробітників, які використовують мобільні пристрої. За допомогою MDM, адміністратори можуть забезпечити належну підтримку та обслуговування мобільних пристроїв, встановлювати та оновлювати програмне забезпечення та додатки, а також забезпечувати належну безпеку пристроїв та даних, які на них зберігаються.

Зазвичай, MDM може включати в себе такі функції, як налаштування Wi-Fi, VPN, мобільного доступу до даних, збір аналітики використання пристроїв та додатків, встановлення правил використання пристроїв, оновлення та установку програмного забезпечення, контроль доступу до даних та інші функції.

MDM також може бути корисним для забезпечення відповідності з різними нормативними актами та стандартами безпеки, такими як HIPAA, PCI DSS, GDPR, і багатьма іншими. Це особливо важливо для компаній, які мають справу з конфіденційною медичною інформацією, фінансовими даними та іншими чутливими даними, що підлягають захисту.

MDM може допомогти зменшити втрату часу та збільшити продуктивність співробітників, забезпечивши їм доступ до важливих даних та інструментів на мобільних пристроях. За допомогою MDM, співробітники можуть віддалено отримувати необхідну інформацію, виконувати свої робочі завдання та спілкуватися з колегами, навіть якщо вони знаходяться за межами офісу.

Проте, варто зазначити, що MDM може викликати певні проблеми відносно приватності та захисту особистої інформації користувачів мобільних пристроїв. Таким чином, важливо, щоб при використанні MDM, організації дотримувалися вимог законодавства з приводу захисту особистої інформації та забезпечували належний рівень конфіденційності даних користувачів.

* *Mobile Application Management (MAM)* - системи управління додатками, які дозволяють керувати встановленими на мобільних пристроях додатками. МАМ може включати в себе такі функції, як контроль доступу до додатків, керування політиками безпеки, контроль доступу до даних, керування конфігурацією та оновленнями програмного забезпечення, а також віддалене видалення даних з пристроїв у випадку їх втрати або крадіжки.

Поширена помилкова думка, що керування мобільними пристроями (MDM) і керування мобільними додатками (MAM) подібні. MDM і MAM є двома найпоширенішими рішеннями для безпечного використання смартфонів і планшетів. Незважаючи на те, що вони служать різним цілям, деякі їхні функції збігаються, і все більше постачальників об’єднують дві технології в одне рішення (Рис. 1.2).

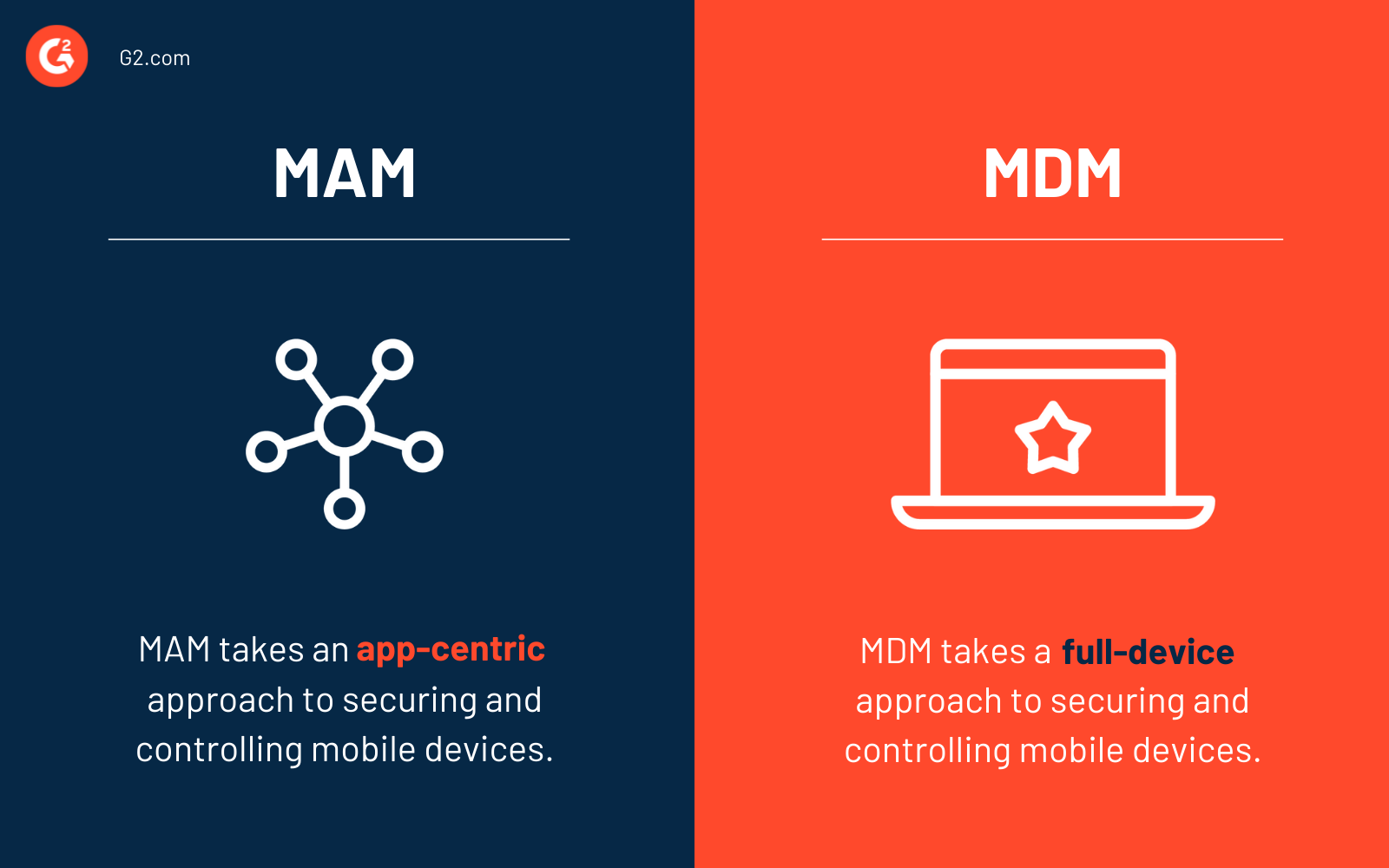
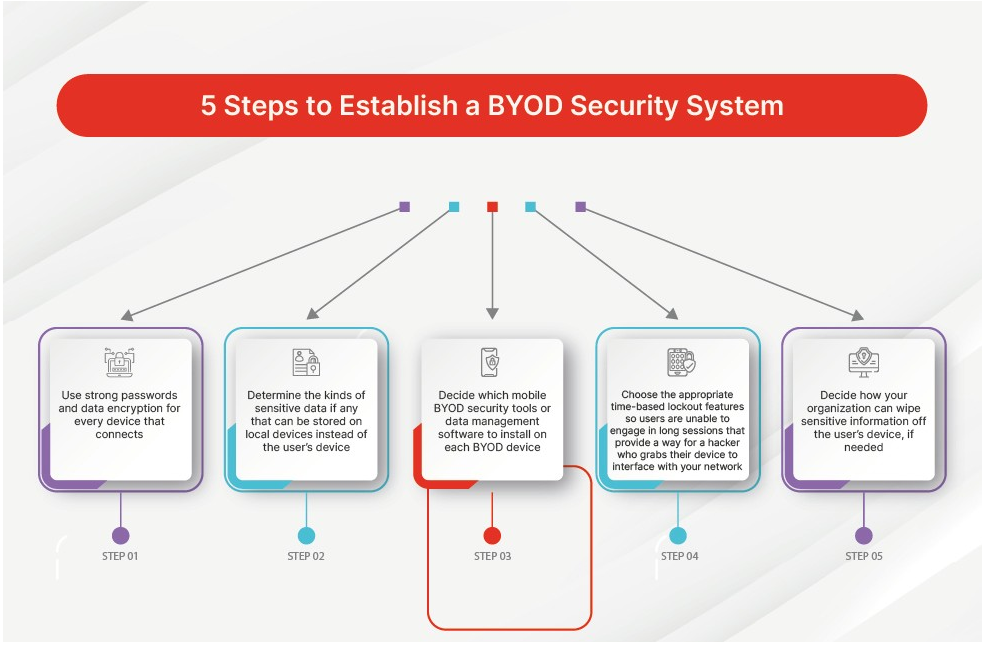


Рис. 1.2 Різниця MAM і MDM

Одним з методів управління мобільними пристроями є політика Bring Your Own Device (BYOD). Цей підхід дозволяє співробітникам використовувати свої власні мобільні пристрої для роботи в організації. При цьому важливо розробити політику безпеки, щоб забезпечити захист корпоративної інформації на пристроях співробітників. Це може включати в себе встановлення захисного програмного забезпечення на пристрої, вимогу до паролів, обмеження доступу до деяких додатків та інші заходи.

**Рис. 1.3. Кроки налаштування захисту в BYOD**

Інший метод управління мобільними пристроями - це використання корпоративних пристроїв. Такі пристрої можуть бути використані для роботи виключно в організації та керуватись МАМ-системою. Такий підхід дає більший контроль над мобільними пристроями, оскільки можна заборонити використання небезпечних додатків, вимагати від співробітників встановлення певних захисних програм і так далі.

Важливою складовою управління мобільними пристроями є відстеження та контроль за їх використанням. Для цього можуть бути використані різні засоби, такі як моніторинг трафіку, логування подій та аудиту. Важливо також мати можливість віддаленого керування пристроями, наприклад, вимагати пароль для розблокування, встановлювати та відключати додатки, відправляти сповіщення

Додатково до контролю доступу та керування політиками безпеки, МАМ може надавати інші корисні функції, такі як:

* Керування даними: МАМ може керувати даними на мобільних пристроях, включаючи шифрування даних, віддалене видалення даних, а також контроль доступу до даних.
* Керування конфігурацією: МАМ може забезпечити стандартизацію налаштувань пристроїв, додатків та інших параметрів, що дозволяє забезпечити однакову конфігурацію на всіх пристроях в організації.
* Моніторинг: МАМ може надавати можливість моніторити та аналізувати активність мобільних пристроїв у реальному часі. Це дозволяє виявляти та вирішувати проблеми з безпекою раніше, ніж вони стануть критичними.
* Віддалене управління: МАМ може забезпечити можливість віддаленого управління мобільними пристроями, включаючи віддалене управління налаштуваннями, програмами та даними. Це дозволяє зменшити час та зусилля, необхідні для управління мобільними пристроями.
* Розгортання додатків: МАМ може допомогти в розгортанні додатків на мобільних пристроях, забезпечуючи стандартизацію та безпеку додатків, що використовуються в організації.

МАМ є важливим інструментом для забезпечення безпеки та ефективного управління мобільними пристроями в організації. Вона дозволяє контролювати та захищати дані, зменшувати ризик безпеки та забезпечувати стандарти безпеки на мобільних пристроях. МАМ також може бути використана для керування налаштуваннями пристроїв та додатків, управління оновленнями програмного забезпечення та віддаленого видалення даних в разі втрати або крадіжки пристрою.

Однією з основних функцій МАМ є контроль доступу до додатків. Завдяки цьому функціоналу, МАМ дозволяє адміністраторам забезпечити, що лише відповідальні працівники мають доступ до конфіденційних даних та додатків. Це забезпечує високий рівень захисту від зловживань та несанкціонованого доступу до даних.

Крім того, МАМ дозволяє адміністраторам керувати політиками безпеки на пристроях. Завдяки цьому функціоналу, можна створювати та виконувати політики, що дозволяють захистити дані на пристроях від несанкціонованого доступу, втрати або крадіжки.

Додатково, МАМ може бути використана для управління налаштуваннями пристроїв та додатків. Адміністратори можуть контролювати та налаштовувати параметри пристроїв та додатків, щоб забезпечити відповідність політик безпеки та вимогам організації.

МАМ дозволяє адміністраторам керувати оновленнями програмного забезпечення на пристроях, щоб забезпечити актуальність захисних механізмів та протоколів безпеки. Це допомагає уникнути ризику вразливостей та забезпечує високий рівень захисту даних.

Нарешті, МАМ може бути використана для віддаленого видалення даних в разі втрати або крадіжки мобільного пристрою. Це важлива функція для забезпечення безпеки даних в ІС організації, особливо у випадку, коли мобільні пристрої містять конфіденційну інформацію, таку як логіни та паролі, фінансові дані або персональну інформацію клієнтів.

Управління мобільними пристроями за допомогою МАМ є важливим елементом забезпечення безпеки даних в ІС організації. Він дозволяє контролювати доступ до додатків та даних, встановлювати політики безпеки, захищати пристрої від загроз та віддалено видаляти дані у випадку крадіжки або втрати. Ретельний аналіз методів та засобів управління мобільними пристроями допоможе організації забезпечити безпеку даних та зменшити ризик їх втрати чи небезпечного використання.

Важливо також зазначити, що вибір МАМ повинен бути зроблений з урахуванням потреб організації та її інфраструктури. Деякі МАМ можуть мати обмеження щодо типу та кількості підтримуваних пристроїв, а також щодо функцій, які вони надають. Організації повинні ретельно проаналізувати свої потреби та зробити вибір МАМ, який найкраще відповідає їх вимогам.

Крім вибору МАМ, важливо також враховувати інші аспекти управління мобільними пристроями, такі як політики безпеки, процедури управління ризиками та навчання співробітників. Ці аспекти взаємодіють з МАМ та взаємно залежні один від одного, тому важливо забезпечити їх розуміння та виконання для забезпечення безпеки мобільних пристроїв та даних організації.

Також, віддалене видалення даних може бути корисним у випадку втрати пристрою або в разі, якщо співробітник покинув організацію. Завдяки МАМ, адміністратор може здійснювати віддалене видалення конфіденційної інформації, щоб зменшити ризик її витоку або використання недобросовісними особами.

Нарешті, МАМ може забезпечувати відповідність організації з різними регуляторними та законодавчими вимогами, пов'язаними з захистом даних, збереженням архівів, аудитом тощо. Вона може надавати адміністраторам звіти про використання додатків та пристроїв, що дозволяє контролювати та забезпечувати відповідність з інформаційно-безпечними стандартами.

Узагалі, МАМ може допомогти організації забезпечити безпеку та ефективність роботи з мобільними пристроями, зменшити ризик витоку конфіденційної інформації та забезпечити відповідність з регуляторними вимогами.

Зазначена функція МАМ є важливою для захисту конфіденційної інформації та виключення можливості несанкціонованого доступу до неї у разі втрати чи крадіжки мобільного пристрою. МАМ дозволяє виконувати інвентаризацію мобільних пристроїв, що є важливою складовою управління ІС організації. За допомогою інвентаризації можна відстежувати кількість мобільних пристроїв у використанні, оновлювати програмне забезпечення та забезпечувати належний захист даних на них.

Використання МАМ дозволяє забезпечити дотримання стандартів безпеки у ІС організації, що може бути вимогою регуляторів або клієнтів. Застосування МАМ дозволяє контролювати доступ до додатків та обмежувати можливості співробітників щодо використання мобільних пристроїв у робочому середовищі. Це забезпечує зниження ризику неправомірного використання даних та можливості зламу ІС організації через мобільні пристрої.

Узагалі, використання МАМ є важливою складовою управління мобільними пристроями в ІС організації. Це дозволяє забезпечити безпеку даних та дотримання стандартів, зменшити ризик інцидентів безпеки та відповідальність ІС організації в цілому.

# 2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ В ІС ОРГАНІЗАЦІЇ

## **2.1 Аналіз концепцій управління мобільними пристроями в ІС організації**

Застосування мобільних пристроїв в інформаційній системі (ІС) організації є актуальною та важливою темою. Концепції застосування мобільних пристроїв в ІС організації можуть відрізнятися залежно від цілей, потреб та можливостей організації.

Однією з головних концепцій застосування мобільних пристроїв в ІС організації є забезпечення мобільності працівників та збільшення продуктивності роботи. Мобільні пристрої, такі як смартфони та планшети, дозволяють працівникам працювати з будь-якого місця та в будь-який час, що забезпечує збільшення продуктивності та ефективності роботи.

Іншою концепцією є забезпечення зв’язку між працівниками та забезпечення більш швидкого та ефективного обміну інформацією. Мобільні пристрої можуть бути використані для спілкування з колегами, замовниками та партнерами з будь-якого місця та в будь-який час, що дозволяє забезпечити більш швидкий та ефективний обмін інформацією.

Також концепцією застосування мобільних пристроїв в ІС організації є забезпечення більш зручного та швидкого доступу до даних та інформації. Мобільні пристрої можуть бути використані для доступу до електронної пошти, документів, звітів та інших ресурсів організації з будь-якого місця та в будь-який час.аппри

Іншою концепцією є Choose Your Own Device (CYOD) (укр. «Обери свій пристрій»), яка дозволяє організаціям надавати працівникам вибір з обмеженого переліку затверджених мобільних пристроїв, які відповідають вимогам організації з точки зору безпеки та сумісності. Ця стратегія дозволяє зберігати контроль над пристроями, які використовуються працівниками, та зменшує ризик втрати або порушення безпеки даних. Однак, CY BERCOM зазначає, що відділенням технологій ІТ повинні бути виконані попередні дослідження та тестування перед тим, як будь-який новий пристрій або програмне забезпечення буде дозволено використовувати в організації. Слід враховувати витрати на управління та підтримку мобільних пристроїв у системі безпеки ІС.

Інша концепція застосування мобільних пристроїв в ІС організації полягає у використанні технології "Bring Your Own Device" (BYOD). BYOD дозволяє працівникам використовувати свої власні мобільні пристрої в робочих цілях, забезпечуючи при цьому робочий контекст та рівень безпеки відповідно до політики безпеки організації.

За концепцією BYOD, працівники можуть мати доступ до обмеженої інформації ІС організації на своїх особистих мобільних пристроях, а також використовувати програмне забезпечення, яке їм зручно. Організації можуть забезпечити безпеку даних та захист ІС, встановивши політику BYOD та дотримуючись її призначення. Вона може включати вимоги щодо паролів та шифрування, рівні доступу до інформації ІС, вимоги до програмного забезпечення та ін.

Однак, застосування BYOD в ІС організації має свої ризики, такі як втрата чи крадіжка мобільних пристроїв працівників, збільшення витрат на підтримку та безпеку, а також ризик втрати конфіденційності та цілісності даних через неналежну конфігурацію та належне захист мобільних пристроїв. Ці ризики можуть бути зменшені за допомогою ретельної підготовки та імплементації політики BYOD.

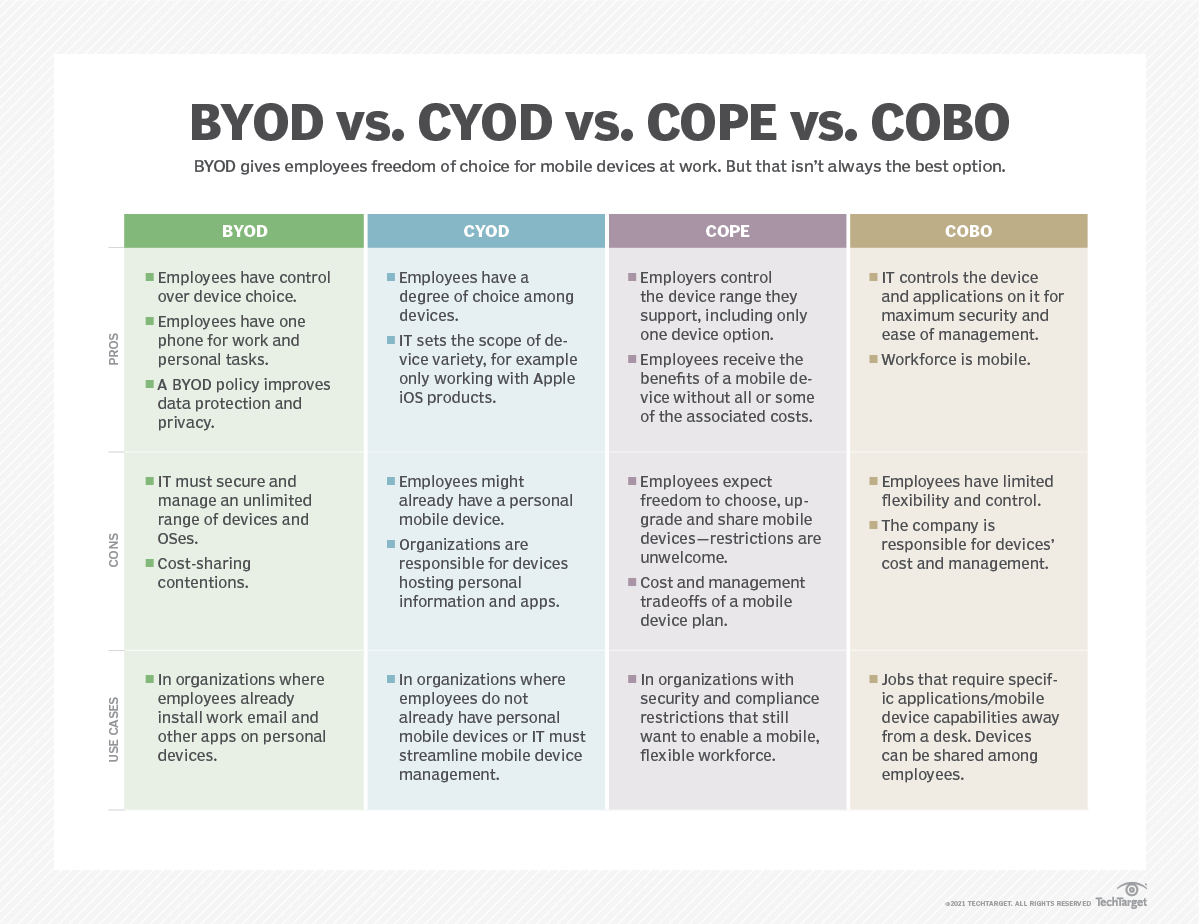
Одним із варіантів впровадження BYOD може бути використання контейнерів на мобільних пристроях. Контейнер - це ізольоване середовище на мобільному пристрої, в якому зберігаються корпоративні дані та додатки. Це дозволяє зберігати корпоративні дані відокремлено від особистих даних працівників, забезпечуючи при цьому достатній рівень захисту та безпеки.

Для забезпечення безпеки та контролю над пристроями, які використовуються в BYOD, можуть бути використані різні засоби управління мобільними пристроями, такі як Mobile Device Management (MDM), Mobile Application Management (MAM) та Mobile Content Management (MCM). Ці засоби дозволяють керувати доступом до корпоративних даних та додатків на мобільних пристроях, контролювати політики безпеки та налаштування, та забезпечувати віддалену підтримку пристроїв.

Важливо також регулярно оцінювати ефективність використання BYOD в організації та робити необхідні зміни для забезпечення максимального рівня безпеки та продуктивності працівників.

Одним зі способів зменшення ризиків при застосуванні BYOD є встановлення політики безпеки, яка включає в себе вимоги щодо налаштування та підтримки безпеки мобільних пристроїв працівників. Така політика може включати в себе вимогу до встановлення антивірусного програмного забезпечення, зашифрованого зберігання даних, вимогу до використання складних паролів та вимогу до регулярної зміни паролів.

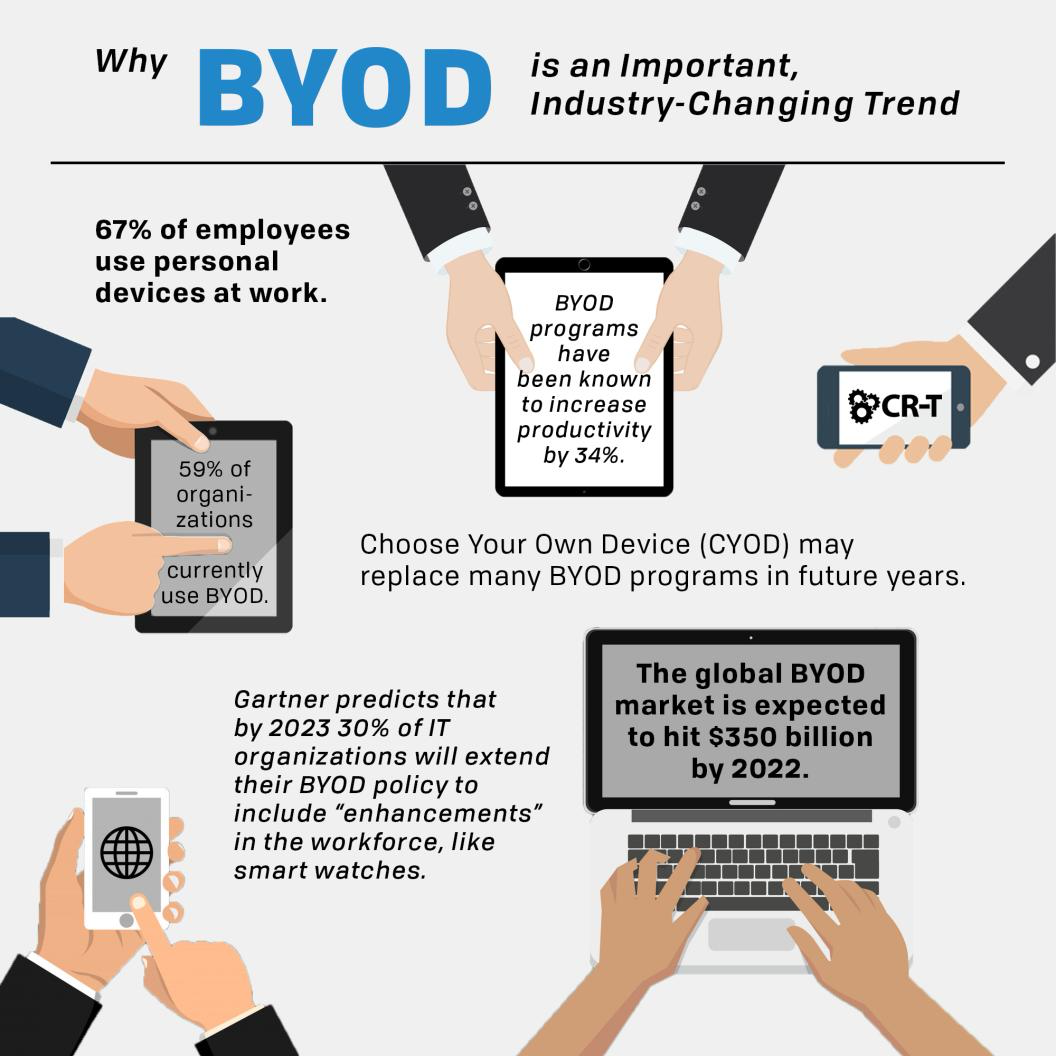
Крім того, організації можуть використовувати різні технології для забезпечення безпеки при застосуванні BYOD, такі як мобільні застосунки для контролю доступу до даних та зниження ризику втрати даних, віртуальні приватні мережі (VPN) для захищеного з'єднання пристроїв до корпоративних мереж, та віддалене керування пристроями.



**Рис. 2.1. Різниця в методах управління**

Окрім BYOD, існує і концепція Corporate-Owned Personally-Enabled (COPE), яка передбачає володіння організацією мобільними пристроями, але дозволяє працівникам використовувати ці пристрої для особистих потреб. COPE дозволяє організації забезпечити більший контроль та безпеку, але також потребує значних витрат на придбання та підтримку мобільних пристроїв.

У будь-якому випадку, аналіз концепцій застосування мобільних пристроїв в ІС організації є важливим етапом розробки стратегії безпеки та вибору оптимального підходу до управління мобільними пристроями. При цьому необхідно враховувати різні фактори, такі як тип діяльності організації, розмір та склад організації, кількість працівників та їх потреби у мобільних пристроях, а також рівень конфіденційності та цінності даних, які обробляються та зберігаються в ІС організації.



**Рис. 2.2. Важливість BYOD**

Якщо організація вирішує використовувати BYOD, то необхідно розробити політику безпеки, яка б включала в себе правила використання мобільних пристроїв працівниками, умови використання корпоративних даних на особистих пристроях, вимоги до безпеки та захисту даних на мобільних пристроях та інші аспекти безпеки (Рис.2.2).

Для забезпечення безпеки використання мобільних пристроїв у BYOD моделі, можуть бути використані різні технології, такі як мобільні застосунки для забезпечення безпеки, віртуальні приватні мережі (VPN), мобільні системи управління (MDM), контроль доступу до даних, шифрування даних та інші заходи.

У разі використання корпоративних мобільних пристроїв, організація може використовувати ті ж технології безпеки, що і для BYOD, однак контроль над пристроями та захист даних будуть забезпечуватися централізовано.

Аналіз концепцій застосування мобільних пристроїв в ІС організації показує, що обидві моделі мають свої переваги та ризики, тому вибір моделі залежить від конкретних умов та потреб організації. В будь-якому випадку, безпека даних та пристроїв повинна бути на високому рівні, а для цього необхідно використовувати сучасні технології. Так, для забезпечення безпеки даних та пристроїв необхідно використовувати сучасні технології. Одним з головних інструментів, які можна використовувати для захисту від кібератак та збереження безпеки даних в ІС організації, є криптографія. Криптографія - це наука про забезпечення безпеки комунікації та захисту інформації від несанкціонованого доступу.

Для захисту від кібератак та збереження безпеки даних можна використовувати різні криптографічні методи, такі як симетричне та асиметричне шифрування, хеш-функції, електронний підпис тощо. Симетричне шифрування використовує один ключ для шифрування та дешифрування даних, тоді як асиметричне шифрування використовує два ключі: публічний та приватний. Публічний ключ використовується для шифрування даних, а приватний ключ - для їх розшифрування.

Хеш-функції використовуються для створення унікального ідентифікатора даних, який можна використовувати для перевірки цілісності даних. Електронний підпис - це механізм захисту від підробки документів та інших електронних даних шляхом використання криптографічного ключа та алгоритмів.

Окрім криптографії, для забезпечення безпеки даних та пристроїв в ІС організації можна використовувати різні заходи захисту, такі як багатофакторна аутентифікація, контроль доступу, моніторинг мережі та пристроїв, захист від вірусів та інших шкідливих програм. Багатофакторна аутентифікація вимагає від користувача не тільки пароль, але й інші форми ідентифікації, наприклад, відбиток пальця або обличчя, що забезпечує більш високий рівень захисту від несанкціонованого доступу.

Контроль доступу може бути реалізований за допомогою політик доступу, які встановлюють, які користувачі мають доступ до яких даних та ресурсів. Також можна використовувати різні рівні доступу до даних, залежно від потреб користувача та ролі в організації.

Моніторинг мережі та пристроїв дозволяє вчасно виявляти можливі загрози безпеці та кібератаки. Можуть використовуватися різні засоби моніторингу, наприклад, системи виявлення вторгнень (IDS) та системи запобігання вторгнень (IPS), які реагують на загрози та спрямовують їх на аналіз та блокування.

Захист від вірусів та інших шкідливих програм може бути забезпечений за допомогою антивірусного програмного забезпечення та фаєрволів. Антивірусні програми аналізують файлову систему та поштові скриньки на наявність вірусів та інших шкідливих програм. Фаєрволи контролюють мережевий трафік та блокують небезпечні з'єднання.

Можна використовувати різні техніки шифрування даних, що забезпечує їх конфіденційність та цілісність. Наприклад, шифрування дискових просторів, шифрування файлів та шифрування з'єднань можуть бути використані для забезпечення безпеки даних.

Для забезпечення безпеки в ІС організації необхідно приділяти увагу всім аспектам, що стосуються інформаційної безпеки та захисту даних. Окрім технічних заходів, необхідно також забезпечувати належний рівень культури безпеки серед працівників та розробляти політики та процедури безпеки даних.

Для підвищення рівня культури безпеки в ІС організації необхідно проводити навчання та тренінги з питань інформаційної безпеки для всіх працівників організації. Вони повинні знати, як поводитись з конфіденційною інформацією та даними, як захищати свої пристрої та робочі місця від кібератак, які практики є безпечними при роботі з електронною поштою та соціальними мережами.

Крім того, необхідно розробляти політики та процедури безпеки даних, які б забезпечували належний рівень захисту інформації. Ці документи повинні містити вимоги до захисту даних та пристроїв, правила використання паролів, правила зберігання та передачі даних, вимоги до програмного забезпечення та апаратного забезпечення, процедури резервного копіювання даних, правила використання BYOD та інші важливі аспекти.

Для забезпечення безпеки в ІС організації також важливо здійснювати постійний моніторинг мережі та пристроїв, а також аналізувати дані, які збираються, для виявлення можливих загроз та ризиків. Також необхідно проводити регулярні навчання та тренінги для працівників з питань безпеки даних та пристроїв, щоб вони могли вчасно виявляти можливі загрози та діяти відповідно до встановлених процедур.

Важливим етапом у забезпеченні безпеки в ІС організації є також виконання аудиту безпеки, який дозволяє перевірити виконання встановлених вимог та процедур забезпечення безпеки та виявити можливі проблеми та недоліки. Аудит безпеки повинен проводитись регулярно та включати в себе оцінку рівня захисту даних та пристроїв, аналіз можливих загроз та ризиків, перевірку виконання процедур та встановлених вимог.

Забезпечення безпеки даних та пристроїв в ІС організації є важливим етапом у забезпеченні успішної та безпечної діяльності. Для цього необхідно використовувати сучасні технології та методи захисту, встановлювати відповідні вимоги та процедури, проводити регулярний моніторинг та аудит безпеки, а також забезпечувати постійне навчання та тренінги працівників з питань безпеки даних та пристроїв.

Важливим аспектом забезпечення безпеки є постійне оновлення програмного забезпечення та оперативної системи на мобільних пристроях, встановлення антивірусного програмного забезпечення та захисту від шкідливих програм. Також необхідно встановлювати заходи з контролю доступу до даних та пристроїв, забезпечувати шифрування та захист від несанкціонованого доступу.

Крім технічних заходів, необхідно враховувати і культурні та поведінкові аспекти забезпечення безпеки. Програма навчання працівників повинна включати освіту про загрози безпеці даних, рекомендації щодо безпечної поведінки в мережі та правила безпечного використання мобільних пристроїв.

Навчання працівників повинно включати інструктаж щодо безпечного використання мобільних пристроїв, таких як не встановлювати програмне забезпечення з ненадійних джерел, не натискати на посилання від невідомих відправників, не використовувати прості паролі та не зберігати паролі на мобільному пристрої.

Забезпечення безпеки даних та пристроїв в ІС організації є комплексним процесом, який потребує поєднання технічних та поведінкових заходів. Забезпечення безпеки даних та пристроїв допомагає зменшити ризики витоку інформації, крадіжки та порушення цілісності даних, а також збільшити довіру та надійність діяльності організації.

Важливо враховувати, що забезпечення безпеки не може бути повністю гарантоване, і існує завжди ризик інциденту. Тому важливо мати готовість до реагування на можливі інциденти та мати плани невідкладних заходів. Наприклад, план евакуації в разі пожежі, план відновлення після кібератаки або план взаємодії з правоохоронними органами в разі порушення безпеки даних.

Також, важливо відзначити, що забезпечення безпеки даних та пристроїв повинно бути постійним і динамічним процесом. Технології та загрози постійно розвиваються, тому важливо регулярно оновлювати заходи захисту та навчати працівників новим методам та технологіям.

Загалом, забезпечення безпеки даних та пристроїв в ІС організації є складним та важливим процесом, який потребує комплексного підходу. Необхідно поєднувати технологічні заходи захисту з встановленням відповідних процедур та правил, проводити регулярний моніторинг та аудит безпеки, а також навчати та тренувати працівників з питань безпеки даних та пристроїв. Тільки так можна забезпечити успішну та безпечну діяльність організації.

Крім того, важливо проводити регулярні оновлення програмного забезпечення, щоб забезпечити відповідність до сучасних стандартів безпеки та уникнути вразливостей. Також необхідно встановлювати захист на рівні мережі та додатків, а не тільки на рівні пристроїв, що дозволяє

Окрім технічних заходів, важливо також враховувати аспекти культури безпеки та забезпечити участь всіх працівників у процесі забезпечення безпеки даних та пристроїв. Необхідно проводити навчання та тренінги з питань безпеки, робити акцент на відповідальність кожного працівника за захист даних та пристроїв, а також забезпечувати систему звітності та відповідальності за порушення правил безпеки.

Забезпечення безпеки даних та пристроїв в ІС організації є важливим та складним завданням, яке вимагає поєднання технічних та культурних аспектів. Дотримання вимог безпеки дозволить забезпечити захист від ризиків втрати та порушення безпеки даних, зберігати довіру клієнтів та забезпечувати успішну та безпечну діяльність організації.

Також важливим етапом забезпечення безпеки в ІС організації є встановлення та впровадження процедур резервного копіювання даних. Це дозволяє забезпечити можливість відновлення даних у випадку їх втрати або пошкодження.

Додатковою мірою захисту може стати використання облікових записів з обмеженими правами доступу, що дозволяє обмежити доступ до конфіденційних даних лише необхідним працівникам.

Також необхідно забезпечити захист пристроїв та даних від фізичного доступу. Для цього можна використовувати різноманітні засоби захисту, такі як паролі, смарт-карти, біометричні системи ідентифікації та інші.

Важливим аспектом забезпечення безпеки даних та пристроїв є встановлення процедур виявлення та реагування на інциденти безпеки. Це дозволяє швидко виявляти та вирішувати проблеми безпеки, що можуть виникнути у майбутньому.

Узагалі, забезпечення безпеки даних та пристроїв в ІС організації є важливим етапом у забезпеченні її стійкості та надійності. Для цього необхідно використовувати сучасні технології та методи захисту, встановлювати відповідні вимоги та процедури, проводити регулярний моніторинг та аудит безпеки, а також забезпечувати постійне навчання та тренінги працівників з питань безпеки даних та пристроїв.

Також, важливо забезпечити регулярне оновлення програмного забезпечення та патчів безпеки, щоб уникнути вразливостей та атак на систему. Необхідно мати план аварійного відновлення та резервне копіювання даних, щоб у разі катастрофи або випадку втрати даних було можливо відновити роботу системи.

Нарешті, слід пам'ятати, що забезпечення безпеки даних та пристроїв в ІС організації є процесом, який потребує постійної уваги та підтримки. Навчання та тренінги працівників з питань безпеки даних та пристроїв повинні проводитися регулярно, а плани та процедури безпеки повинні оновлюватися відповідно до змін у технологіях та загрозах безпеки.

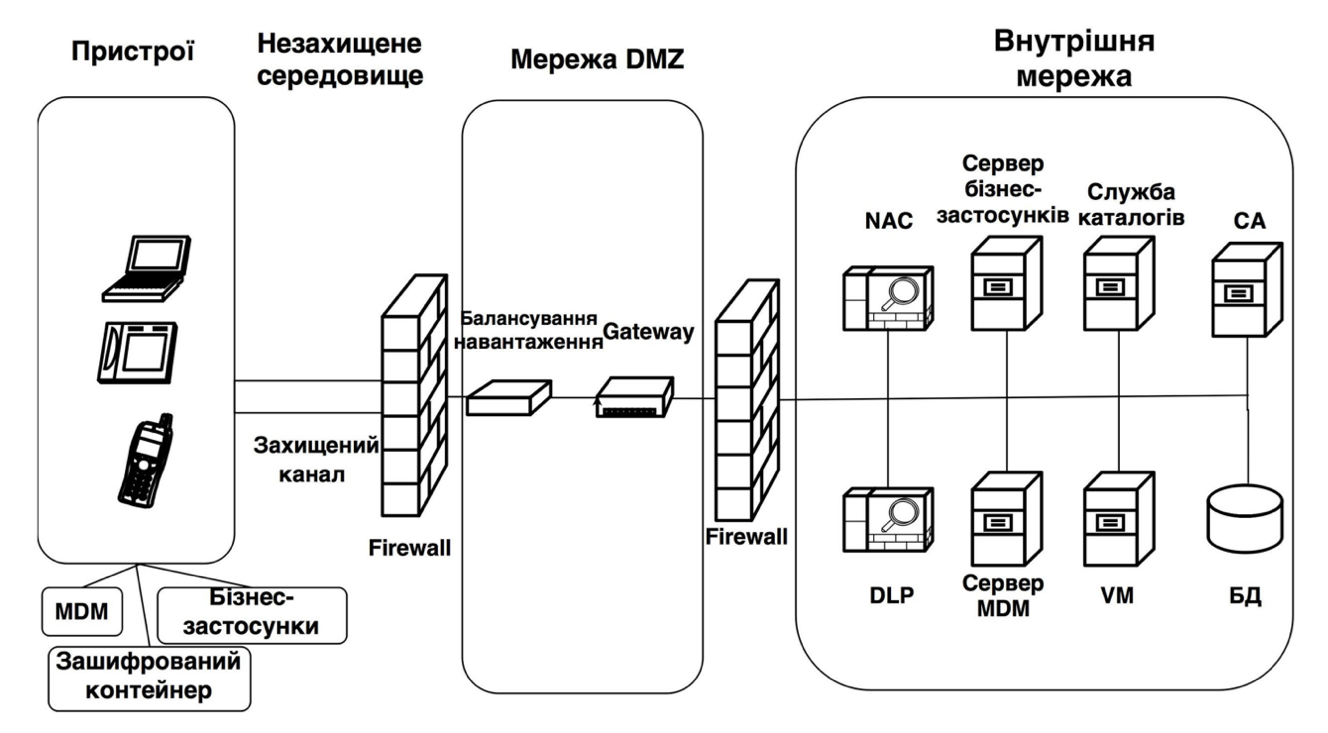
В цілому, забезпечення безпеки даних та пристроїв в ІС організації є складним процесом, але це необхідно для забезпечення успішної та безпечної діяльності організації.

## **2.2 Архітектура BYOD**

Архітектура BYOD (Bring Your Own Device) - це підхід до управління комп'ютерною мережею, в якому дозволяється працювати з власними персональними пристроями працівників (таких як ноутбуки, планшети, смартфони тощо) в офісному середовищі. Замість того, щоб видавати працівникам спеціальні пристрої для роботи, компанії дозволяють працівникам використовувати власні пристрої для доступу до корпоративної мережі, даних та додатків.

Основна ідея застосування BYOD полягає в забезпеченні максимальної гнучкості та зручності працівників. Працівники можуть використовувати пристрої, з якими вони звикли працювати, та не потребують додаткового часу для навчання використання нових пристроїв. Це дозволяє працювати з будь-якого місця та в будь-який час, що забезпечує більшу продуктивність та ефективність роботи.

Проте, використання BYOD вимагає певної архітектури мережі та системи безпеки, щоб забезпечити надійність, безпеку та конфіденційність даних, що обмінюються між користувачами та корпоративною мережею.

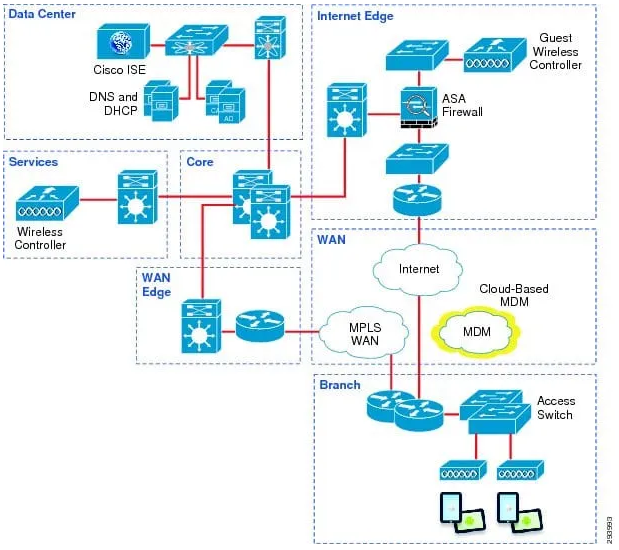


**Рис. 2.3. Архітектура MDM**

Основними компонентами архітектури BYOD є:

* MDM – система, що застосовується для керування локальними додатками на пристроях, виконання віддаленого видалення даних, забезпечення надійного захисту паролем пристрою та шифрування даних.
* Мобільні користувачі можуть використовувати велику кількість незахищених мобільних додатків, які завантажуються з незахищених джерел. MDM повинна відрізняти захищене корпоративне середовище бізнес-додатків, які обмінюються конфіденційною інформацією, від незахищеного середовища застосунків, призначених для особистих потреб користувачів, що працюють з власними даними. Необхідно забезпечити умови, при яких додатки, що призначені для користувачів, не матимуть доступу до захищеного середовища.
* захищений контейнер, в якому зберігаються дані за допомогою безпечного шифрування. Локальні кеші електронної пошти, переглянуті веб-сторінки та дані з будь-яких мобільних додатків підлягають захисту. У разі потреби може бути реалізована аутентифікація, шифрування та вибіркове видалення захищених даних, не торкаючись персональні дані, які також зберігаються на BYOD пристрої.
* Для забезпечення безпечної передачі даних створюється захищений канал, який може бути реалізований за допомогою VPN-підключень до корпоративної мережі або шляхом шифрування окремих додатків (наприклад, електронної пошти або доступу до веб-сайтів через HTTPS).
* Network Access Control - це стратегія управління доступом до корпоративної пошти, додатків, контенту та веб-трафіку, яка враховує дії користувача та налаштування їх BYOD-пристроїв. Доступ користувача до ресурсів визначається в залежності від того, наскільки добре він відповідає корпоративним стандартам безпеки, які включають в себе налаштування його пристрою. Оскільки користувачі можуть змінювати налаштування безпеки на своїх пристроях, автоматична оцінка довіри до підключеного BYOD-пристрою є важливим завданням. На основі рівня довіри визначається доступ до ресурсів корпоративної мережі.
* За допомогою Служби Каталогiв доступ до даних вiртуального робочого середовища забезпечується лише пiсля того, як користувач авторизується за допомогою свого облiкового запису в доменi Служби Каталогiв. Для забезпечення безпеки передачi даних використовується захищений канал, який вимагає сувору аутентифiкацiю користувача та пристрою.
* VM – це вiртуальна реалiзацiя системи, яка надає користувачам робоче середовище, в якому можуть бути опублiкованi i доступнi необхiднi для роботи програми та данi.
* DLP є інтегрованою системою у віртуальному робочому середовищі, що запобігає витоку даних. Вона забезпечує контроль доступних каналів передачі даних в конкретному віртуальному середовищі, таких як електронна пошта, веб-сайти, месенджери, канал друку та переслані на віртуальне середовище локальні USB-пристрої, щоб запобігти витоку даних з пристрою BYOD. Компоненти DLP-системи виконують пошук та класифікацію інформації, що захищається за встановленими критеріями. SIEM формує єдине вікно для адміністратора безпеки, в якому зведені дані про виявлені файли, які підлягають захисту, спроби доступу до них, а також пов'язана (корельована) технологічна інформація, що надходить від ОС, СУБД, мережевого обладнання та інших джерел, щоб сформувати повну картину стану ІБ в організації.
* Мережева інфраструктура: мережа повинна забезпечувати доступ користувачів до корпоративної мережі та даних за допомогою їх власних пристроїв. Для цього, мережа повинна бути налаштована на роботу з різними типами пристроїв та операційних систем, що використовуються користувачами.
* Системи безпеки: BYOD може представляти загрозу для безпеки мережі та даних компанії, тому важливо забезпечити надійну систему безпеки. Основні компоненти системи безпеки включають в себе:
* Політики безпеки: компанії повинні мати чіткі політики, які регулюють використання BYOD, зокрема, управління дозволами на доступ до даних, захист від вірусів та зловмисного програмного забезпечення, налаштування паролів та віддаленого видалення даних у разі втрати або крадіжки пристрою.
* Аутентифікація та авторизація: користувачі повинні бути аутентифіковані та авторизовані для доступу до корпоративної мережі та даних.
* Шифрування даних: дані, що передаються між пристроями та мережею, повинні бути шифровані, щоб забезпечити їх конфіденційність та захист від несанкціонованого доступу.
* Захист від вірусів та зловмисного програмного забезпечення: пристрої, які підключаються до корпоративної мережі, повинні бути захищені від вірусів та зловмисного програмного забезпечення.
* Управління пристроями: компанії повинні мати систему управління пристроями, яка дозволяє забезпечити безпеку та конфіденційність даних, що обмінюються між користувачами та мережею.
* Система управління пристроями може включати в себе:
* Реєстрацію та авторизацію пристроїв: користувачі повинні реєструвати свої пристрої для підключення до корпоративної мережі та даних.
* Віддалене управління пристроями: компанії повинні мати можливість віддаленого управління пристроями для захисту від крадіжки, втрати або несанкціонованого доступу до даних. Це може включати в себе віддалене видалення даних, заборону доступу до корпоративних даних та встановлення політик безпеки на пристроях.
* Моніторинг пристроїв: система управління повинна забезпечувати моніторинг пристроїв, щоб виявляти будь-які підозрілі дії та заходити на захист даних.
* Віддалене оновлення програмного забезпечення: система управління повинна забезпечувати можливість оновлення програмного забезпечення пристроїв, щоб захистити їх від нових загроз та вразливостей.
* Підтримка та сервісне обслуговування: компанії повинні забезпечити підтримку та сервісне обслуговування для пристроїв, які підключаються до корпоративної мережі. Це може включати в себе підтримку з налаштування, відновлення пристроїв та допомогу у віддаленому управлінні пристроями.
* Бізнес-процеси: BYOD може змінювати бізнес-процеси компанії та впливати на її організацію. Компанії повинні розробляти нові бізнес-процеси, які враховують використання BYOD та забезпечують ефективність та безпеку використання пристроїв.
* Успішна реалізація BYOD-стратегії потребує ретельного планування та розробки архітектури, яка забезпечує безпеку даних та високу ефективність використання пристроїв користувачів.
* Проте, важливо зазначити, що BYOD також має свої ризики та виклики, які повинні бути враховані при розробці стратегії. Основні ризики пов'язані з безпекою даних, несумісністю пристроїв та програмного забезпечення, втратою контролю над даними та викликами з приводу підтримки та сервісного обслуговування.
* Отже, при реалізації стратегії BYOD компанії повинні враховувати як переваги, так і ризики, та розробляти архітектуру, яка забезпечує ефективне та безпечне використання пристроїв користувачів.

Для успішної реалізації стратегії BYOD компанії повинні мати високу ступінь контролю та управління над пристроями, які використовуються працівниками. Для цього можуть використовуватися різноманітні інструменти, такі як мобільні пристрої керування (Mobile Device Management, MDM), мобільні пристрої аудиту (Mobile Device Audit, MDA) та інші.



**Рис. 2.4. Структура MDM системи**

Крім того, компанії повинні розробити чітку політику BYOD та документацію, яка описує вимоги до пристроїв, програмного забезпечення та безпеки даних. Також потрібно надати працівникам достатню кількість навчальних матеріалів та семінарів, щоб вони могли розуміти політику BYOD та свої обов'язки.

Узагальнюючи, архітектура BYOD - це комплексна система, яка дозволяє працівникам використовувати власні пристрої для роботи в офісі, що забезпечує більшу свободу та гнучкість роботи, а також знижує витрати компаній на придбання пристроїв. Однак, реалізація BYOD-стратегії повинна бути обдуманою та ретельно спланованою, щоб забезпечити безпеку даних та ефективність роботи працівників.

BYOD - це тенденція, яка набуває все більшої популярності, тому варто розглянути її переваги та недоліки, щоб вирішити, чи вона відповідає потребам конкретної компанії. Якщо компанія розробляє стратегію BYOD, то їй слід ретельно продумати всі аспекти реалізації, включаючи політику безпеки даних, вимоги до пристроїв та програмного забезпечення, процедури управління пристроями, навчання працівників та інші фактори.

Також слід пам'ятати, що BYOD не є універсальним рішенням для всіх компаній, оскільки вона може не відповідати певним секторам ринку чи індустрій. Наприклад, у деяких виробничих компаніях або компаніях з високими стандартами безпеки даних може бути складніше реалізувати BYOD-стратегію, тому їм може бути краще залишитися при традиційному підході до використання пристроїв.

Отже, архітектура BYOD може бути корисною для компаній, якщо вона ретельно продумана та розроблена з урахуванням всіх вимог щодо безпеки даних та високої ефективності роботи працівників.

## **2.3 Функції та складові BYOD**

BYOD (Bring Your Own Device) - це стратегія використання робочих пристроїв, яка передбачає, що працівники можуть використовувати власні пристрої для роботи. Оскільки BYOD стає все популярнішою, компанії повинні розуміти функції та складові цієї стратегії, щоб ретельно продумати та розробити свою власну BYOD-стратегію.

Основні функції BYOD:

* BYOD дозволяє працівникам працювати з будь-якого місця та будь-якого пристрою, що дозволяє збільшити продуктивність та ефективність роботи;
* замість того, щоб компанії купували пристрої для кожного працівника, вони можуть дозволити працівникам використовувати свої власні пристрої, що може допомогти знизити витрати на обладнання та підтримку;
* працівники більш задоволені, коли можуть використовувати свої власні пристрої для роботи, оскільки вони можуть працювати з тими пристроями, які вони знають та відчувають зручними;
* використання BYOD може збільшити ризик порушення безпеки даних, проте застосування відповідних політик та процедур забезпечує високий рівень безпеки даних.

Основні складові BYOD наведені у таблиці 2.1.

Таблиця 2.1.

**Складові Bring Your Own Device (BYOD)**

|  |  |
| --- | --- |
| Програмне забезпечення для моніторингу та управління | для безпеки даних та високої ефективності роботи працівників, компанії повинні мати програмне забезпечення, що дозволяє моніторити та управляти пристроями. |
| Політики безпеки | компанії повинні встановити політики безпеки, які дозволяють забезпечити безпеку даних та мережі компанії. Ці політики повинні визначати, які типи пристроїв можуть бути використані для роботи, які додатки можуть бути встановлені, які типи даних можуть бути доступні на пристроях працівників та інші важливі правила. |
| Засоби аутентифікації | для забезпечення безпеки даних, компанії повинні мати систему аутентифікації, яка дозволяє перевіряти ідентифікацію працівників, які намагаються отримати доступ до робочих даних на своїх пристроях. |
| Система управління пристроями | система управління пристроями дозволяє компаніям контролювати та керувати пристроями, що використовуються працівниками для роботи. Це може включати віддалене встановлення програмного забезпечення, оновлення безпеки та зміну політик безпеки. |
| Бездротові мережі | для забезпечення доступу до мережі компанії з будь-якого місця, компанії повинні мати бездротові мережі, що дозволяють працівникам підключатися до мережі зі своїх власних пристроїв. |
| Додатки для роботи | компанії повинні мати додатки для роботи, які дозволяють працівникам доступ до робочих даних та ресурсів з їхніх власних пристроїв. Ці додатки повинні бути безпечними та захищеними від зловмисних атак. |
| Підтримка та навчання | компанії повинні забезпечувати підтримку та навчання працівників з питань використання робочих даних на їхніх власних пристроях. |
| Моніторинг | компанії повинні мати механізми моніторингу, які дозволяють виявляти та запобігати зловмисним діям та інцидентам в області безпеки даних та мережі. |
| Інтеграція з іншими системами | BYOD повинна бути інтегрована з іншими системами компанії, такими як системи електронної пошти, системи зберігання даних та системи відеоконференцій, щоб забезпечити повну інтеграцію та доступ до робочих ресурсів з будь-якого місця та пристрою. |
| Політика відповідальності | компанії повинні мати політику відповідальності, що регулює використання BYOD працівниками. Ця політика повинна включати правила використання пристроїв, доступу до робочих даних та інформації, а також відповідальність за порушення правил. |

BYOD - це архітектура, яка дозволяє працівникам використовувати свої особисті пристрої для роботи та доступу до робочих ресурсів. Для того, щоб забезпечити безпеку даних та мережі компанії, необхідно мати встановлені політики безпеки, системи аутентифікації, управління пристроями, бездротові мережі, додатки для роботи, підтримку та навчання працівників, механізми моніторингу, інтеграцію з іншими системами та політику відповідальності.

Для того, щоб забезпечити успішну імплементацію BYOD в компанії, необхідно провести детальний аналіз її потреб та можливостей. Доцільно провести пілотний проект з декількох працівників, щоб випробувати технології та процеси та виявити можливі недоліки.

Наступним кроком є створення політики BYOD, яка повинна бути чіткою та зрозумілою для всіх працівників компанії. Політика повинна містити правила використання особистих пристроїв, вимоги до безпеки та конфіденційності даних, процедури відключення пристроїв та роботи з даними у випадку втрати пристроїв, вимоги до сторонніх додатків та багато іншого.

При розгортанні BYOD в компанії також варто розглянути можливість використання різних інструментів для захисту даних, наприклад, шифрування, контролю доступу, моніторингу мережі та пристроїв, а також використання віртуальних рішень для забезпечення безпеки.

Нарешті, компанії повинні мати механізми підтримки працівників, які використовують BYOD, та надавати їм навчання та інструкції з використання технологій BYOD та вимог безпеки даних.

BYOD є корисною архітектурою, яка дозволяє працівникам використовувати свої особисті пристрої для роботи та доступу до робочих ресурсів, але при цьому необхідно виконувати вимоги безпеки та контролю. Розгортання BYOD повинно бути попередньо ретельно продумано, а також включати в себе пілотний проект, створення політики безпеки та забезпечення механізмів підтримки для працівників. Компанії повинні забезпечити регулярне навчання та інструктажі з використання технологій BYOD та вимог безпеки даних для всіх працівників, які мають намір використовувати свої особисті пристрої для роботи.

Одним з головних переваг BYOD є зменшення витрат компанії на закупівлю та підтримку обладнання, а також збільшення продуктивності працівників за рахунок зручного доступу до робочих ресурсів. BYOD дозволяє працівникам працювати з будь-якого місця та у зручний для них час, що поліпшує їх робочі умови та підвищує їх задоволеність роботою.

Однак, BYOD також має свої недоліки. Наприклад, компанії можуть стикнутися з проблемами з безпекою даних та конфіденційністю, якщо не будуть вжиті заходи для контролю доступу до ресурсів та даних. Наявність різних типів пристроїв може вимагати додаткових зусиль для забезпечення сумісності та підтримки різноманітних операційних систем та додатків.

У будь-якому випадку, вирішення використання BYOD повинно бути ретельно продумано і реалізовано з урахуванням всіх можливих наслідків та ризиків.

Одним із важливих складових BYOD є політика безпеки даних. Компанії повинні розробити чітку політику забезпечення безпеки даних, щоб уникнути можливих загроз безпеці при використанні особистих пристроїв працівниками. Ця політика може включати такі пункти, як:

* Встановлення вимог до паролів та захисту доступу до пристроїв;
* Вимога до використання антивірусного та антишпигунського програмного забезпечення на пристроях;
* Обмеження доступу до робочих даних та ресурсів;
* Встановлення вимог до зберігання та передачі конфіденційної інформації;
* Правила використання мережі та доступу до неї.

Крім того, компанії повинні забезпечити підтримку для працівників, які використовують BYOD, шляхом надання їм можливості доступу до робочих даних та ресурсів з їхніх особистих пристроїв. Це може включати встановлення спеціального програмного забезпечення, яке дозволить працівникам віддалено підключатися до робочих серверів та ресурсів, а також забезпечення підтримки для різних типів операційних систем та пристроїв.

Важливо надавати працівникам інформацію та навчати їх про правила використання BYOD та вимог безпеки даних. Це може включати організацію спеціальних тренінгів, надання інструкцій та розробку матеріалів, які допоможуть працівникам зрозуміти потенційні загрози та ризики, пов'язані з використанням особистих пристроїв для роботи.

Узагальнюючи, BYOD може бути вигідним рішенням для компаній, які хочуть зменшити витрат

Узагальнюючи, BYOD може бути вигідним рішенням для компаній, які хочуть зменшити витрати на придбання та управління обладнанням, підвищити продуктивність та ефективність працівників, та забезпечити більш гнучкі умови роботи. Однак, для успішного впровадження BYOD в компанії, необхідно ретельно планувати та розробляти стратегію та політику безпеки даних, а також забезпечувати підтримку та навчання працівників.

Окрім цього, при використанні BYOD виникає ризик витоку конфіденційної інформації та порушення правил безпеки даних, тому важливо мати механізми контролю та моніторингу використання особистих пристроїв працівниками. Також важливо розглядати різні варіанти BYOD та вибирати той, який найкраще відповідає потребам конкретної компанії.

Загалом, BYOD є цікавим та перспективним рішенням для компаній, які шукають нові способи забезпечення ефективної та гнучкої роботи своїх працівників. Однак, впровадження BYOD повинно бути ретельно сплановане та реалізоване з урахуванням вимог безпеки даних та підтримки працівників.

BYOD може також допомогти компаніям забезпечувати більш гнучкі умови роботи, що може знизити витрати на працівників та збільшити їх задоволеність роботою. Наприклад, працівникам можуть дозволяти працювати з будь-якого місця, коли це їм зручно, що знижує витрати на оренду та обслуговування офісного приміщення.

BYOD може допомогти компаніям підвищити продуктивність працівників, оскільки вони можуть використовувати свої особисті пристрої, які вони вже знають та вміють використовувати ефективно. Це може також збільшити задоволеність працівників роботою та знизити ризик втрати талантів через незадоволеність умовами роботи.

Нарешті, BYOD може знизити витрати на придбання та управління обладнанням для компанії, оскільки працівники використовують свої власні пристрої. Це може знизити витрати на придбання нових комп'ютерів, ноутбуків та інших пристроїв, а також зменшити витрати на їх обслуговування та підтримку.

Узагальнюючи, BYOD може бути вигідним рішенням для компаній, які шукають нові способи забезпечення ефективної та гнучкої роботи своїх працівників та зниження витрат на обладнання. Проте, при впровадженні BYOD необхідно дотримуватись вимог безпеки даних та розробляти стратегію, яка відповідає потребам конкретної компанії.

# 3. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО НАЛАШТУВАНЬ РІШЕННЯ BYOD В УПРАВЛІННІ МОБІЛЬНИМИ ПРИСТРОЯМИ

## **3.1 Загальні вимоги та методи програми MobileIron**

MobileIron - це платформа для управління мобільними пристроями, що дозволяє організаціям забезпечувати безпеку, простоту та контроль над різними типами мобільних пристроїв та застосунків.

Для того, щоб користуватися функціями цієї платформи, необхідно виконувати деякі загальні вимоги.

Перш ніж налаштовувати MobileIron Threat Defense, виконайте такі попередні умови:

* Налаштуйте MobileIron Core для керування пристроями.
* Отримайте ліцензію MTD.
* Отримайте облікові дані клієнта Threat Management Console.
* Відкрити вхідний порт 8883 із консолі керування загрозами до ядра.

Клієнти, які використовують списки керування доступом порталу для білих списків IP-адрес, щоб дозволити з’єднання від консолі керування загрозами до свого ядра для портів 443 або 8883, можуть використовувати цю інформацію: MobileIron Threat Defense Management zConsole вимагає оновлення правил брандмауера, щоб уникнути переривання обслуговування.

MobileIron підтримує такі ОС як iOS, Android, BlackBerry та Windows. Проте, перед тим, як використовувати MobileIron, необхідно переконатися, що мобільні пристрої які будуть використовуватися, *підтримуються платформою і мають підтримку останніх версій операційних систем.* Це дозволяє забезпечити безпеку за допомогою оновлення та підтримки новіших версій програмного забезпечення.Також для забезпечення повної функціональності системи потрібно встановити на кожен мобільний пристрій додаток MobileIron.

Треба *мати пристрої з підтримкою Enterprise*. Це означає, що пристрій має бути придбаний виробником з підтримкою Enterprise та мати вбудовані функції безпеки.

Програма потребує *постійного з'єднання з Інтернетом* для оновлення списку дозволених додатків та збереження даних про пристрої.

Необхідно *встановити MobileIron Core* - центральну частину системи, яка забезпечує керування всіма пристроями та додатками. Вона може бути встановлена як фізичний апарат або віртуальна машина. Крім того, також необхідно *встановити інші компоненти*, такі як MobileIron Sentry, MobileIron Access та MobileIron Tunnel.

Для використання потрібно *мати* *діючу ліцензію*, яка дозволить використовувати всі функції платформи. Ліцензія може бути придбана від MobileIron або від одного з його партнерів.

MobileIron потребує *підключення до джерела даних*, таких як Active Directory або LDAP для автоматичного створення облікових записів користувачів та керування доступом до ресурсів.

Необхідно *дотримуватись вимог безпеки даних*. MobileIron надає різні функції безпеки, такі як шифрування даних, контроль доступ. Але окрім забезпечення захисту даних та керування мобільними пристроями, MobileIron також потребує *наявності захищеного з'єднання* для забезпечення безпеки даних та зменшення ризику їх втрати.

Від користувачів потребується *встановлення автентифікаційних даних*, таких як ім'я користувача та пароль. Це дозволяє переконатися, що пристрій користується дозволеним користувачем і забезпечує безпеку доступу до даних інформації, що зберігається на пристрої.

MobileIron може вимагати *встановлення додаткового програмного забезпечення* на підключених пристроях для забезпечення додаткової безпеки. Це може включати антивірусне програмне забезпечення або додаткові захисні рішення.

Також *платформа може встановлювати обмеження* на використання деяких функцій на підключених пристроях. Наприклад, можуть бути заборонені певні додатки або функції, які можуть представляти ризик для безпеки даних.

Додатково, MobileIron вимагає *встановлення на пристрої користувача спеціальної програми - Mobile@Work*. Ця програма дає користувачам доступ до корпоративних ресурсів, таких як електронна пошта, календар, контакти, документи, через захищену блокову область на їхньому пристрої.

Mobile@Work забезпечує розділення особистих даних користувача і корпоративних даних, що покращує безпеку даних.

Дає можливість IТ-адміністраторам віддалено керувати налаштуваннями та політиками безпеки на мобільних пристроях співробітників. Вони можуть віддалено встановлювати, оновлювати та видаляти додатки, керувати налаштуваннями безпеки, надавати доступ до корпоративних ресурсів і контролювати використання пристроїв.

Дозволяє підприємствам контролювати встановлені додатки на мобільних пристроях співробітників. Адміністратори можуть забороняти або дозволяти встановлення певних додатків, встановлювати оновлення, керувати ліцензіями та моніторити використання додатків.

Однією з важливих складових вимог MobileIron є також підтримка пристроєм протоколу SSL (Secure Sockets Layer) або TLS (Transport Layer Security) для захисту передачі даних через мережу.

Загальні вимоги MobileIron забезпечують безпеку даних корпорації та допомагають уникнути можливих загроз для їх безпеки. Ці вимоги можуть залежати від конкретних потреб компанії, але загалом, вони допомагають забезпечити безпеку пристроїв і даних в BYOD середовищі.

MobileIron є платформою для управління мобільними пристроями та захисту корпоративних даних. Вона надає широкий спектр функцій та методів для ефективного управління мобільними пристроями, додатками та безпекою. Основні методи, які використовуються в програмі MobileIron, включають наступне:

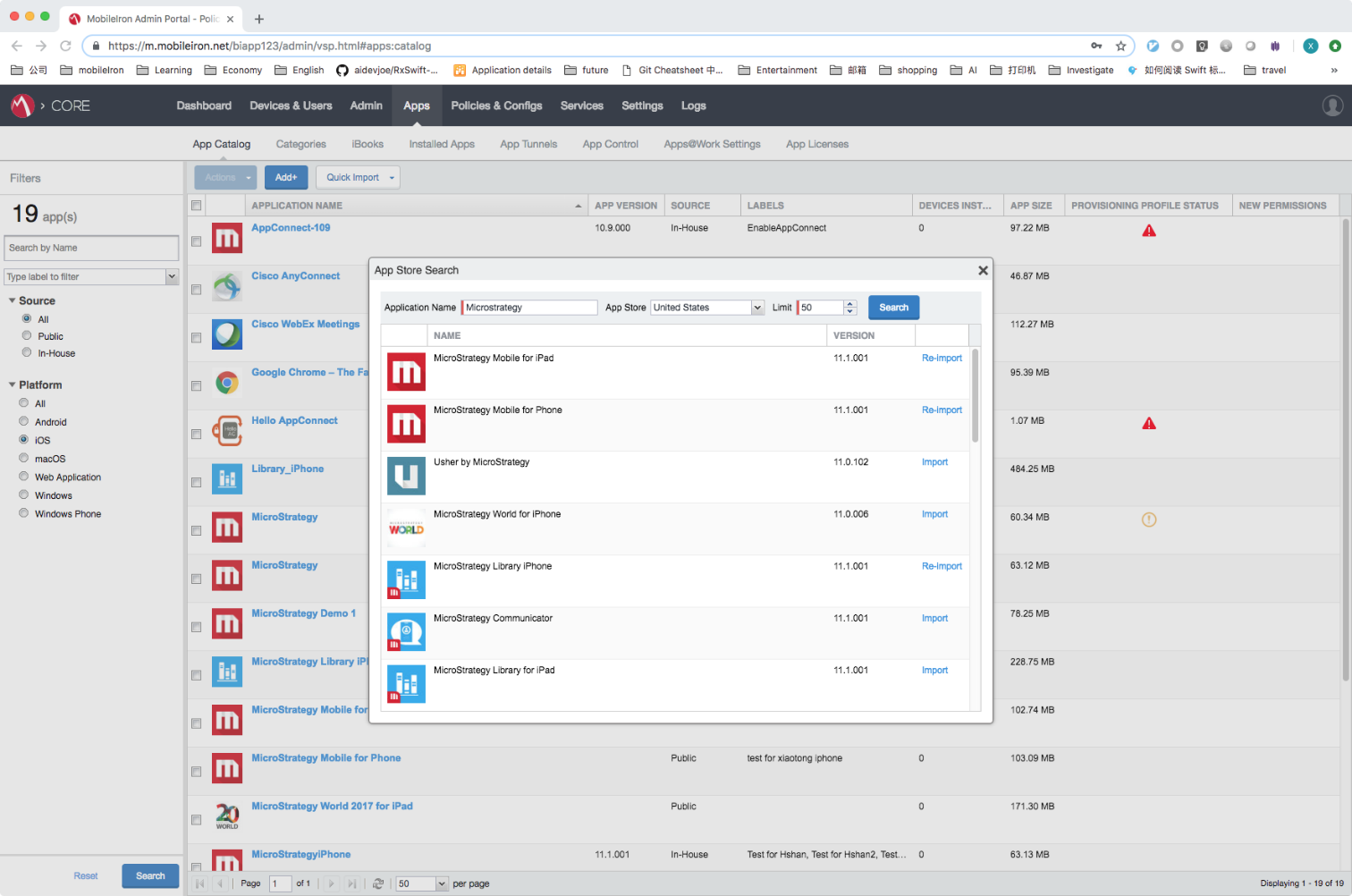
1. Управління пристроями (Mobile Device Management, MDM): Цей метод дозволяє організаціям повністю контролювати мобільні пристрої, які використовуються співробітниками. За допомогою MDM, адміністратори можуть віддалено налаштовувати, керувати та моніторити пристрої з центральної консолі. Вони можуть вимагати реєстрацію пристроїв, встановлювати політики безпеки, надавати віддалену підтримку, відстежувати стан батареї та мережі, блокувати або видаляти дані в разі втрати або крадіжки пристрою, а також встановлювати та оновлювати додатки на пристроях.
2. Управління програмами (Mobile Application Management, MAM): Цей метод дозволяє організаціям керувати додатками, які встановлені на мобільних пристроях. Він надає можливість встановлювати, оновлювати та видаляти додатки, контролювати доступ до певних додатків, встановлювати політики безпеки для додатків, контролювати права доступу та шифрувати дані, що стосуються додатків.
3. Управління контентом (Mobile Content Management, MCM): Цей метод дозволяє організаціям контролювати доступ до корпоративного контенту на мобільних пристроях. Він дозволяє співробітникам отримувати доступ до корпоративних файлів та документів, зберігати їх на пристроях і синхронізувати з центральним сервером. Можуть застосовуватись політики безпеки, такі як шифрування даних, віддалене видалення контенту у разі втрати пристрою та обмеження можливостей копіювання або передачі файлів.
4. Безпека та захист даних: MobileIron надає різноманітні функції безпеки для захисту корпоративних даних на мобільних пристроях. Включаються можливості шифрування даних, встановлення політик паролів та блокування пристроїв, виявлення та запобігання вторгнень, контроль за використанням небезпечних додатків, віддалене видалення даних у разі втрати пристрою, аутентифікація та управління правами доступу.
5. Автоматизація та інтеграція: MobileIron може інтегруватись з іншими системами управління, такими як системи ідентифікації користувачів (Identity and Access Management) та системи управління доступом (Access Management). Це дозволяє автоматизувати процеси реєстрації, управління правами доступу та інші рутинні операції, спрощуючи адміністрування та забезпечуючи єдиноцентровий контроль.
6. Управління програмами та додатками: MobileIron дозволяє організаціям управляти програмами та додатками на мобільних пристроях, включаючи можливість створювати список дозволених та заборонених додатків, контролювати доступ до них, встановлювати оновлення та інші функції. Також можливе віддалене видалення додатків з пристроїв.
7. Моніторинг та аналітика: MobileIron надає засоби моніторингу та аналітики використання мобільних пристроїв, що дозволяє організаціям контролювати та аналізувати різноманітні показники, такі як кількість пристроїв, кількість трафіку, використання додатків та інші. Це дозволяє покращити ефективність та забезпечити безпеку мобільного середовища.
8. Підтримка різноманітних платформ: MobileIron підтримує різноманітні платформи, такі як iOS, Android, Windows та інші, що дозволяє організаціям використовувати програму на різних мобільних пристроях та операційних системах.
9. Розгортання в хмарі: MobileIron може бути розгорнутий в хмарі, що дозволяє організаціям забезпечувати управління мобільними пристроями та безпеку даних без необхідності використовувати власні сервери та програмне забезпечення.
10. Підтримка BYOD: MobileIron дозволяє організаціям підтримувати модель Bring Your Own Device (BYOD), що дозволяє співробітникам використовувати власні мобільні пристрої для роботи, забезпечуючи при цьому контроль, безпеку та розділення корпоративних та особистих даних.
11. Управління політиками безпеки: MobileIron дозволяє організаціям встановлювати та керувати політиками безпеки на мобільних пристроях. Це включає в себе вимоги до паролів, шифрування даних, віддалене видалення даних у разі втрати пристрою, вимкнення функцій, таких як камера чи Bluetooth, та інші параметри безпеки.
12. Розподілене управління: MobileIron надає можливість розподіленого управління, що дозволяє декентралізованою команді адміністраторів керувати мобільними пристроями та політиками безпеки. Це особливо корисно для організацій з розподіленою структурою або філіалами в різних регіонах.
13. Інтеграція з корпоративними ресурсами: MobileIron може бути інтегрований з корпоративними ресурсами, такими як пошта, календарі, дисків, файлові сервери та інші. Це дозволяє співробітникам зручно отримувати доступ до корпоративних даних та спілкуватися з колегами безпосередньо з мобільних пристроїв.
14. Управління мобільними пристроями через API: MobileIron надає API, що дозволяє інтегрувати його функціональність з іншими системами та додатками. Це дозволяє створювати власні рішення та розширювати можливості MobileIron у відповідності до конкретних потреб організації.
15. Моніторинг стану пристроїв: MobileIron забезпечує можливість моніторити стан мобільних пристроїв, включаючи інформацію про версії операційної системи, доступність оновлень, стан батареї та інші технічні показники. Це допомагає адміністраторам виявляти проблеми та забезпечувати оптимальну працездатність пристроїв.

Ці методи MobileIron дозволяють організаціям максимально ефективно управляти мобільними пристроями, забезпечувати безпеку та виконувати специфічні вимоги своєї ділової діяльності.

Узагальнюючи, методи MobileIron дійсно дозволяють компаніям забезпечити безпеку даних та пристроїв в BYOD середовищі, що може бути дуже важливим для захисту конфіденційної інформації та запобігання порушенням безпеки даних. Завдяки можливості встановлювати правила та обмеження щодо доступу до даних та можливості віддаленого керування пристроями, компанії можуть забезпечити контроль над використанням пристроїв та даних ними.

## **3.2 Налаштування програми MobileIron**

Як використовувати Mobile Iron за допомогою AppConfig.

Перейдіть в Додатки → Каталог додатків, імпортуйте внутрішній додаток за допомогою кнопки Додати+ або додайте додаток з магазину додатків за допомогою швидкого імпорту.

**Рис. 3.1. Панель програми**

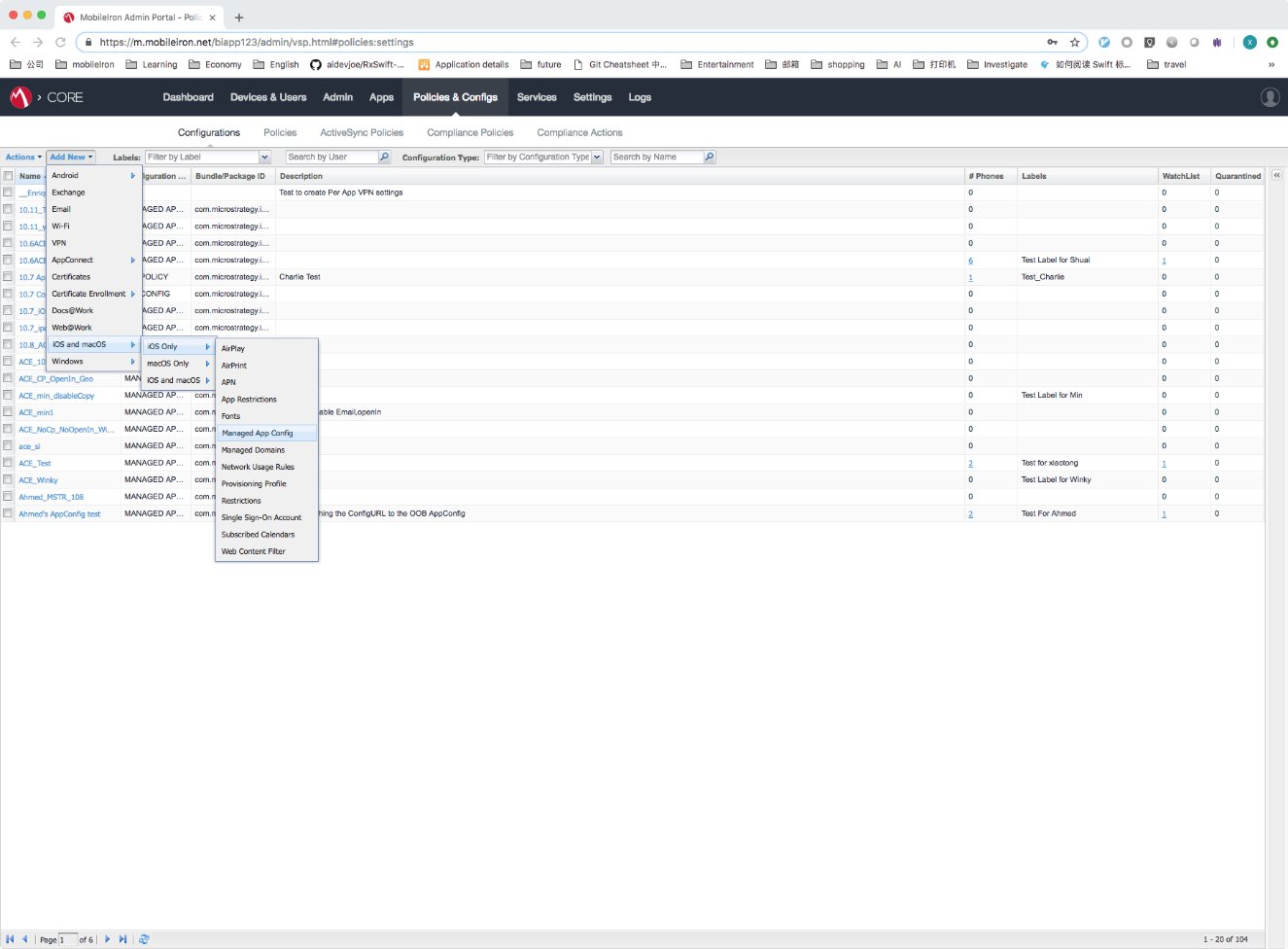
Застосуйте мітку до цієї програми, ця мітка також повинна бути застосована до вашого пристрою, інакше ви не зможете знайти програму в Apps@Work.

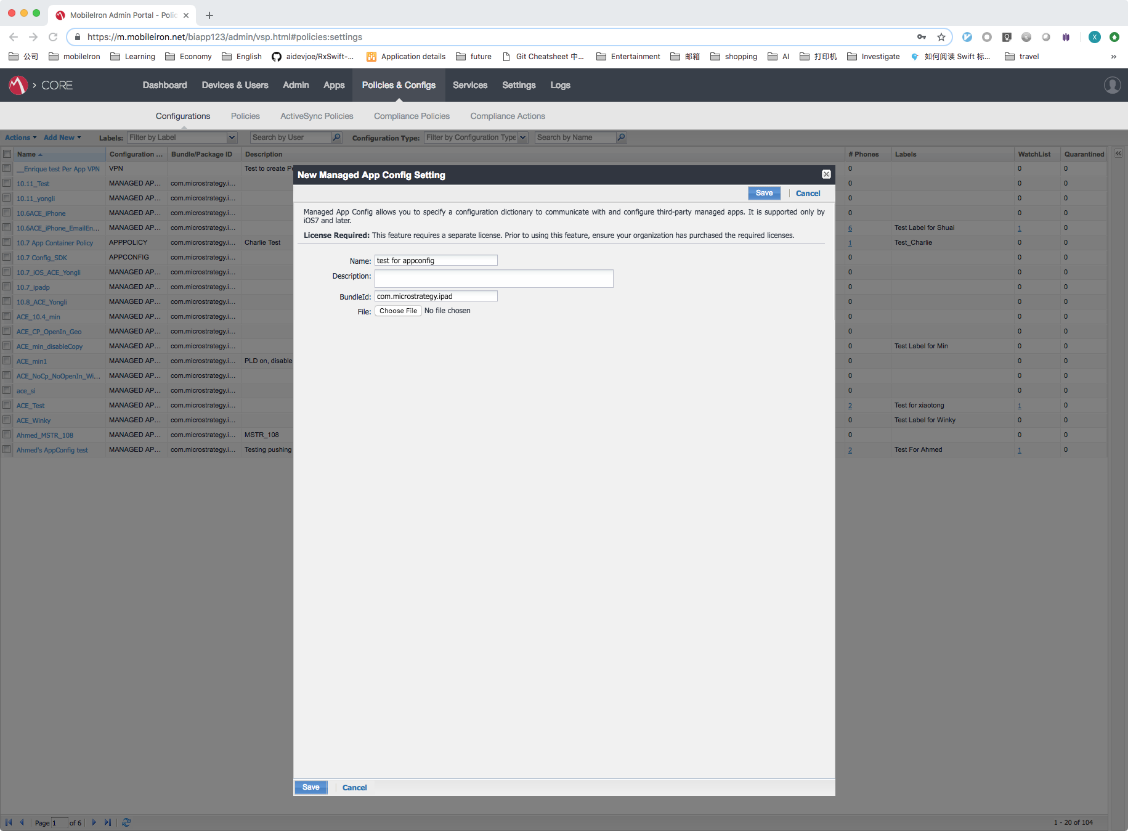
Створення конфігурації програми

Існує 2 способи створення конфігурації програми (ACE). Один з них - застарілий спосіб з використанням конфігурації програми, керованої mobileIron. Інший - метод каталогу додатків.

Застарілий спосіб

Увійдіть в Mobile Iron Core, перейдіть в "Конфігурації та політики" -> "Конфігурації". Додайте конфігурацію типу "Managed App Config", дайте їй назву і завантажте файл списку властивостей. Цей файл списку властивостей має містити потрібні вам конфігурації.

Застосуйте цю конфігурацію з міткою, яку ви застосували до вашого пристрою та програми.

Р**ис. 3.2. Панель програми**

**Рис. 3.3 Панель програми**

Ось приклад файлу plist:

<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN""https://www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">

<dict>

<key>DisableSaveToPhotos</key>

<true/>

<key>DisableLocationServices</key>

<false/>

<key>DisableCameraAccess</key>

<false/>

<key>DisablePrint</key>

<true/>

<key>DisableOpenIn</key>

<false/>

<key>DisableEmail</key>

<false/>

<key>DisableCopyPaste</key>

<true/>

<key>ConfigurationURL</key>

<string>mstr://?url=http%3A%2F%2F10.197.32.63%3A8080%2FMicroStrategyMobile%2Fservlet%2FtaskProc%3FtaskId%3DgetMobileConfiguration%26taskEnv%3Dxml%26taskContentType%3Dxmlanf%26configurationID%3Db6071730-53c8-4e6c-821a-444c3ba1409d&amp;authMode=1&amp;dt=2</string>

<key>EnableDataLossPrevention</key>

<true/>

</dict>

</plist>

Примітка: Якщо ви використовуєте файл xml, то посилання на конфігурацію має бути змінено. Після копіювання згенерованого посилання на мобільну конфігурацію зі сторінки мобільного адміністратора, користувачеві потрібно замінити "&" на "&amp;", як у прикладі вище.

Метод каталогу додатків

Ось короткий вступ до методу каталогу додатків mobileIron:

Підприємства використовують послуги Enterprise Mobility Management (EMM) для управління мобільними пристроями, включаючи додатки та контент на цих пристроях. OneTouch спрощує придбання, пошук, розгортання, конфігурацію, зворотній зв'язок і прийняття ваших програм корпоративними клієнтами. Конфігурація керованих програм за допомогою методу каталогу програм використовує вбудовані можливості iOS для керованих програм і конфігурації керованих програм. Керовані програми - це програми, які розповсюджуються та управляються за допомогою служби EMM.

Конфігурація керованих програм за допомогою методу каталогу програм:

Дозволяє вашій програмі автоматично отримувати від служби EMM параметри конфігурації за замовчуванням, щоб користувачі пристроїв могли негайно почати користуватися програмою.

Надає адміністраторам підприємства простий графічний інтерфейс користувача для налаштування вашого додатку відповідно до їхніх потреб, якщо стандартних налаштувань конфігурації недостатньо.

Дозволяє вашому додатку отримати параметр конфігурації, який визначає версію налаштувань, отриманих від служби EMM. Налаштування версії дозволяє кожній версії програми коректно обробляти різні версії налаштувань конфігурації.

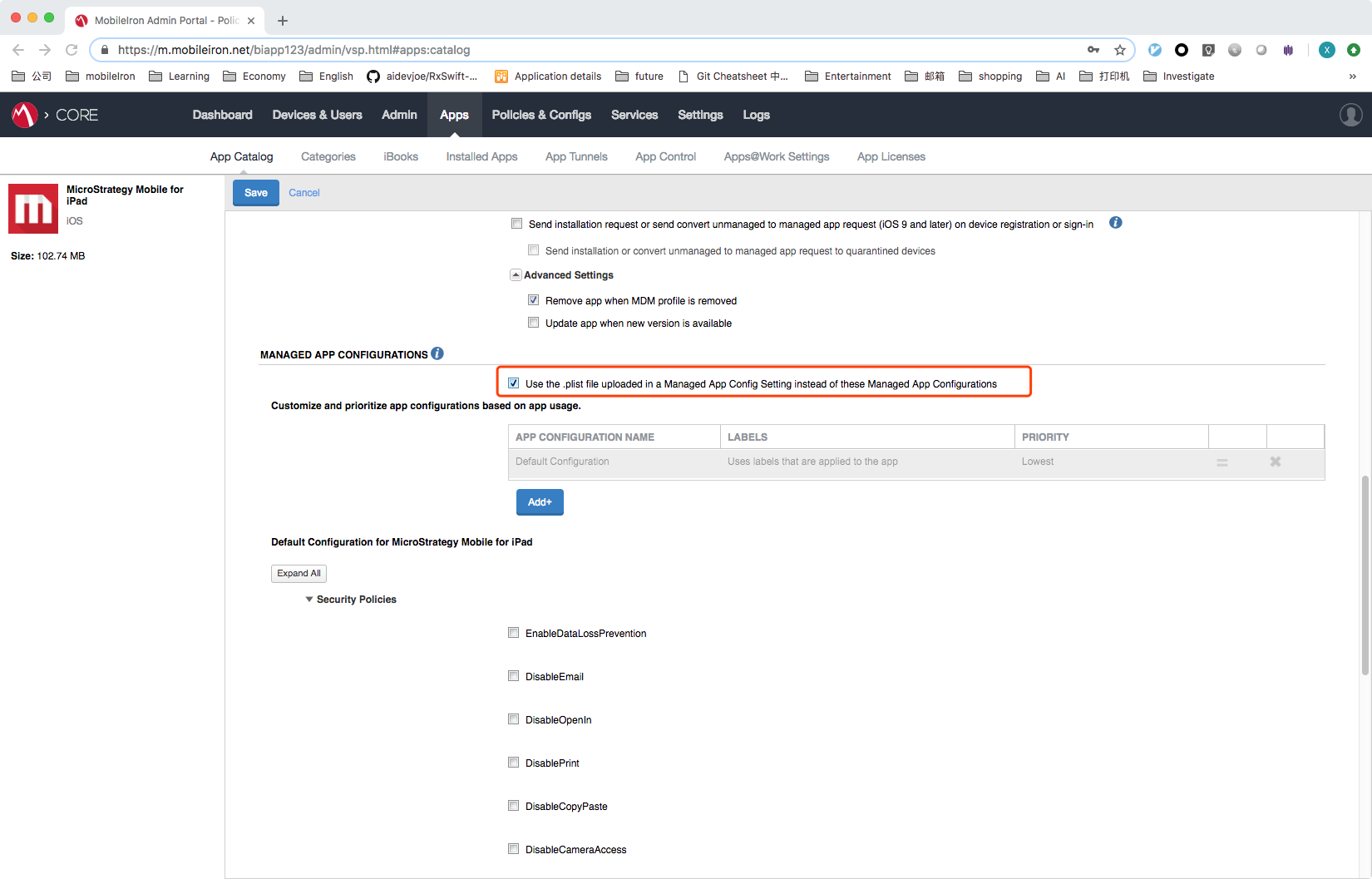
Для керованої конфігурації програми через каталог програм розробник програми створює файл .xml за допомогою цього http://appconfig.org/appconfigspeccreator/ і надає його MobileIron.

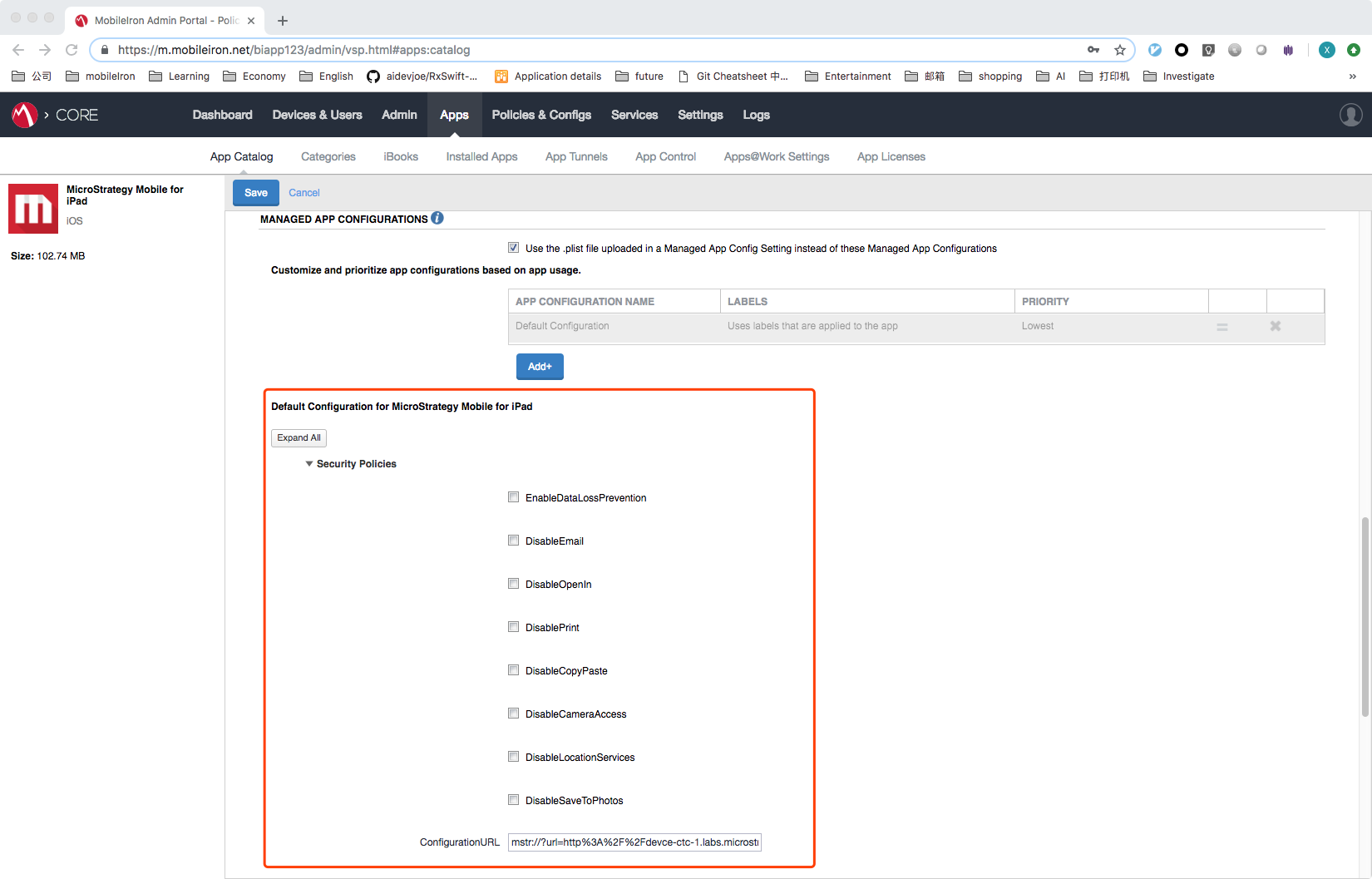
Зараз ми надіслали один файл .xml до MobileIron, і MobileIron завантажив його вручну.

Після цього перейдіть на сторінку конфігурації програми → КЕРОВАНІ КОНФІГУРАЦІЇ ПРОГРАМИ

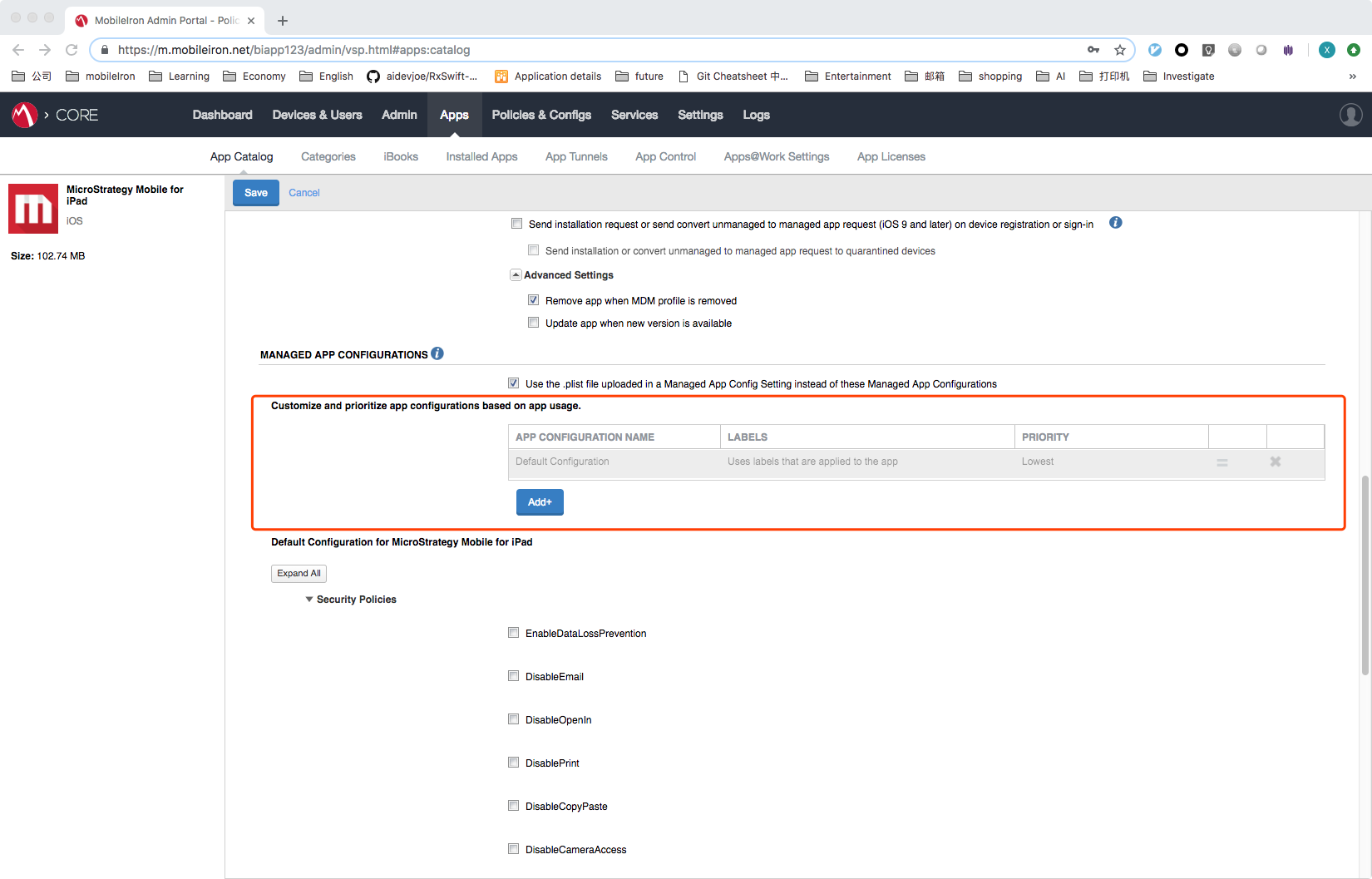
У цьому розділі буде 3 частини:

1. Якщо ви все ще хочете використовувати застарілий спосіб, який використовує .plist, вручну поставте галочку і застосуйте мітку конфігурації керованої програми, яку ви створили в попередньому розділі, до цієї програми. Застарілий спосіб буде працювати (Рис. 3.4).

 **Рис. 3.4. Панель програми**

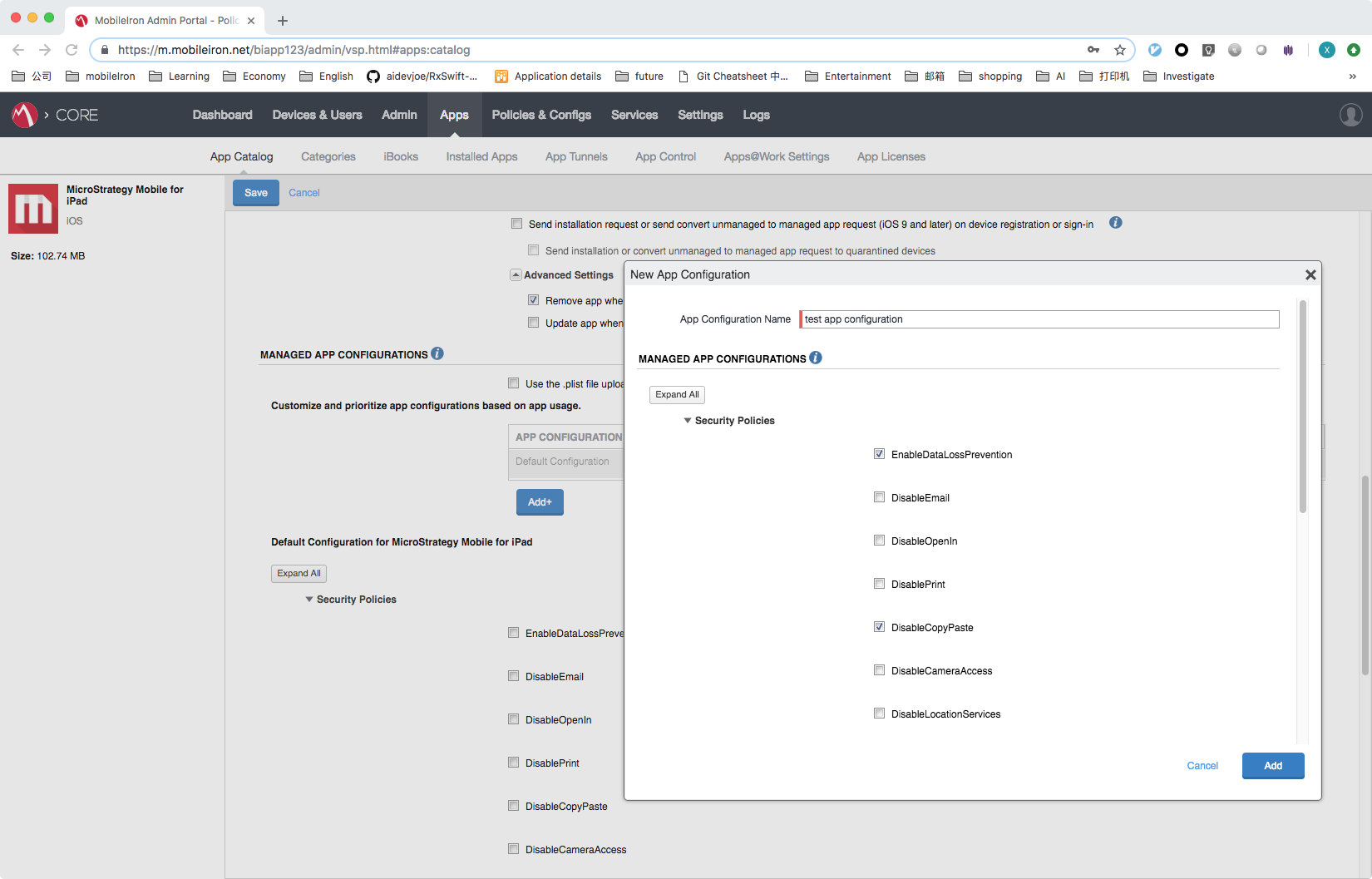
2. Якщо ви хочете використовувати цей метод каталогу програм, просто позначте потрібні пункти, за замовчуванням він буде працювати (Рис. 3.5; 3.6).

Р**ис. 3.5. Панель програми**



**Рис. 3.6. Панель програми**

3. Якщо ви хочете використовувати нову конфігурацію програми, але не хочете змінювати конфігурацію за замовчуванням. Створіть нову конфігурацію, і вона замінить конфігурацію за замовчуванням (Рис. 3.7).

 **Рис. 3.7. Створення нової конфігурації**

## **3.3** **Розробка рекомендацій щодо застосування MobileIron в ІС організації**

Застосування MobileIron в інформаційній системі організації може забезпечити надійний рівень захисту даних та пристроїв в середовищі BYOD. Однак, для максимальної ефективності та успішного впровадження, необхідно дотримуватись деяких рекомендацій:

Перед впровадженням MobileIron необхідно провести аудит інформаційної безпеки організації, щоб визначити можливі ризики та забезпечити відповідність інфраструктури компанії вимогам MobileIron.

Необхідно дотримуватись певних правил:

* Дотримуватись рекомендацій виробника щодо розгортання та конфігурування MobileIron. Необхідно виконати всі необхідні налаштування та належно налаштувати параметри безпеки.
* Забезпечити підтримку та навчання користувачів щодо використання MobileIron. Користувачам необхідно пояснити, як працювати з системою та як дотримуватись правил і політик безпеки.
* Встановити відповідну політику безпеки, яка містить вимоги щодо використання пристроїв та даних. Політика повинна бути доступна для всіх користувачів та регулярно оновлюватись.
* Регулярно оновлювати програмне забезпечення та забезпечувати належний рівень захисту від шкідливих програм та вірусів.
* Регулярно перевіряти систему на наявність вразливостей та проводити аналіз журналів безпеки.
* Забезпечити належну фізичну та логічну захищеність серверів, на яких розгорнута система MobileIron.
* Забезпечити належне навчання співробітників щодо використання MobileIron.

Важливо, щоб усі працівники, які користуються BYOD, були належно навчені використовувати MobileIron. Навчання повинно охоплювати теми, такі як:

* Як налагодити доступ до корпоративних даних на особистих пристроях;
* Як встановити та налаштувати MobileIron на особистих пристроях;
* Як використовувати MobileIron для безпечної роботи з корпоративними даними;
* Як поводитися у разі втрати чи крадіжки особистого пристрою.

Навчання може проводитися в формі інструкцій, відеоуроків або тренінгів. Найкраще, якщо навчання буде регулярним, оскільки нові методи та інструменти можуть з'являтися з часом, а потреби співробітників можуть змінюватися.

Регулярно перевіряти стан безпеки пристроїв та даних.

MobileIron надає засоби для моніторингу стану безпеки пристроїв та даних в BYOD середовищі. Важливо регулярно перевіряти ці показники та здійснювати необхідні заходи для вирішення виявлених проблем.

Зокрема, можна регулярно проводити такі перевірки:

* Моніторинг відповідності політик безпеки на особистих пристроях;
* Аналіз журналів активності на пристроях для виявлення підозрілих дій;
* Перевірка наявності оновлень програмного забезпечення на особистих пристроях;
* Перевірка наявності оновлень MobileIron та інших компонентів інфраструктури BYOD.

Ці перевірки допоможуть вчасно виявляти потенційні проблеми та зменшувати ризики для безпеки даних та пристроїв в BY OD середовищі. Для ефективної інтеграції MobileIron у ІС організації рекомендується виконати наступні кроки:

1. Перед впровадженням MobileIron необхідно ретельно проаналізувати вимоги і потреби організації щодо захисту даних та пристроїв в BYOD середовищі. Важливо врахувати розмір організації, кількість працівників, типи даних, які потрібно захищати, та інші фактори.
2. Перед встановленням MobileIron на пристрої працівників необхідно провести належні навчання щодо правил користування пристроями в BYOD середовищі та належної забезпечення безпеки даних.
3. При встановленні MobileIron на пристрої працівників необхідно встановити правила щодо дозволення чи заборони використання певних додатків чи сервісів. Також рекомендується встановлювати перевірки на наявність шкідливих програм.
4. Потрібно створити політики безпеки, які б детально описували правила використання MobileIron та пристроїв в BYOD середовищі. Ці політики повинні бути обов'язковими для всіх працівників.
5. Після встановлення MobileIron необхідно здійснювати регулярну перевірку стану безпеки даних та пристроїв в BYOD середовищі. Для цього можна використовувати різні інструменти, такі як аудит безпеки, перевірки на віруси та шкідливі програми, контроль використання додатків та інше.
6. Рекомендується створити технічну підтримку для працівників, які користуються MobileIron. Така підтримка допоможе вирішувати. Для ефективної і безпечної роботи з MobileIron у ІС організації можуть бути корисними наступні рекомендації:
7. Забезпечити достатню підтримку технічних засобів та персоналу: використання MobileIron вимагає наявності спеціалістів, які зможуть встановити, налаштувати та підтримувати систему. Необхідно мати сучасні технічні засоби, що відповідають вимогам системи.
8. Налагодити правильну ідентифікацію користувачів: до MobileIron можуть бути підключені різні пристрої та користувачі з різними правами доступу. Однак, щоб забезпечити безпеку даних, необхідно встановити чіткі правила ідентифікації та аутентифікації користувачів.
9. Забезпечити регулярне оновлення програмного забезпечення: оновлення програмного забезпечення важливо для забезпечення безпеки даних та пристроїв. MobileIron регулярно випускає оновлення, які включають в себе нові функції та покращення безпеки. Тому, необхідно вчасно встановлювати ці оновлення.
10. Захистити пристрої від шкідливих програм: в BYOD середовищі існує ризик зараження пристроїв користувачів шкідливими програмами. Для зменшення цього ризику можна встановлювати антивірусне програмне забезпечення та вимагати від користувачів дотримуватися правил безпеки.
11. Визначити правила користування BYOD: заздалегідь встановити правила користування BYOD, включаючи правила використання пристроїв, програмного забезпечення та доступу до даних. Це допоможе уникнути можливих конфлікт Для уникнення можливих конфліктів при впровадженні MobileIron в інформаційну систему організації, можна дотримуватися декількох рекомендацій:
12. Провести аудит існуючої ІС організації, визначити її слабкі місця та підготуватися до впровадження MobileIron. Ретельний аналіз діючої ІС дозволить виявити можливі ризики та проблеми, які можуть виникнути під час впровадження нової системи.
13. Визначити потреби організації щодо MobileIron та підібрати оптимальний пакет послуг. Важливо ретельно оцінити потреби організації та вибрати оптимальний пакет послуг MobileIron, який найкраще задовольнить вимоги безпеки та функціональності.
14. Запровадити MobileIron етапами. Рекомендується запроваджувати MobileIron етапами, починаючи з найменш критичних ділянок ІС, щоб зменшити можливі ризики та помилки.
15. Провести навчання користувачів. Важливо навчати користувачів використовувати MobileIron та дотримуватися правил безпеки в BYOD середовищі.
16. Проводити регулярні перевірки безпеки. Регулярні перевірки безпеки дозволять вчасно виявляти потенційні проблеми та зменшувати ризики для безпеки даних та пристроїв в BYOD середовищі.
17. Дотримання цих рекомендацій допоможе уникнути можливих конфліктів та забезпечити безпеку даних та пристроїв в BYOD середовищі під час впровадження MobileIron в інформаційну систему організації.

Також рекомендується провести навчання користувачів з питань безпеки даних і правильного використання пристроїв під час роботи в BYOD середовищі. Це може включати навчання щодо правил використання паролів, відповідального зберігання та обміну конфіденційною інформацією, запобігання іншим загрозам безпеці, таким як фішингові атаки та шкідливі програми.

Крім того, для забезпечення безпеки даних рекомендується регулярно виконувати резервне копіювання даних на пристроях користувачів та забезпечувати шифрування для збереження конфіденційної інформації в разі втрати або крадіжки пристрою.

Загалом, використання MobileIron може допомогти забезпечити безпеку даних та пристроїв в BYOD середовищі в організації. Однак, для ефективного застосування цієї системи, необхідно ретельно планувати і виконувати відповідні заходи безпеки, проводити регулярну перевірку системи та навчання користувачів з питань безпеки даних.

# ВИСНОВКИ

В роботі встановлено зміст проблеми, визначено мета та завдання управління мобільними пристроями в корпоративній мережі. управління мобільними пристроями в корпоративній мережі є критично важливим завданням для забезпечення продуктивності. Проблема виникає через те, що можливий виток даних. Хакерські атаки можуть надходити з різних джерел, таких як мережеві атаки, фішинг і ненавмисні помилки співробітників, і може мати серйозні наслідки, такі як крадіжка даних, компрометація системи і порушення бізнес-операцій. Тому проблема управління мобільними пристроями та їх захист в корпоративній мережі є критично важливою і потребує постійної уваги та вдосконалення.

Проведено аналіз існуючих методів та засобів управління мобільними пристроями у корпоративній мережі. Існує кілька інструментів, які можна використовувати для управління мобільними пристроями в корпоративній мережі. Це можуть бути BYOD - Bring your own device, CYOD - Choose Your Own Device, COPE – Corporate Owned Personally Enabled.

Визначено основні функції та можливості рішення BYOD в програмі MobileIlron. MobileIlron призначений для постійного відстеження записів потоків у корпоративній мережі, щоб виявляти несанкціонований доступ.

На основі досліджень в роботі проведено експеримент щодо застосування методів та засобів управління мобільними пристроями у корпоративній мережі на базі MobileIlron. Необхідно підкреслити, що додаток MobileIlron використовує алгоритми BYOD.

Розроблено рекомендації фахівцям з кібербезпеки щодо застосування методів та засобів управління мобільними пристроями у корпоративній мережі.

Отже, дотримуючись цих загальних рекомендацій щодо застосування методів та засобів управління мобільними пристроями у корпоративній мережі, організації зможуть краще використовувати мобільні пристрої та захищати їх від кіберзагроз.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Mobile Device Manager Plus [Електронний ресурс] Режим доступу: <https://www.manageengine.com/mobile-device-management/?network=g&device=c&keyword=mdm&campaignid=14672304178&creative=546370934353&matchtype=e&adposition=&placement=&adgroup=130276228227&targetid=kwd-61128886&gclid=CjwKCAjwpayjBhAnEiwA-7ena9X5BlUOzk7OILw40ZFni1NkXBmMmepDg6CfWtn2CTmyRsQmVJFZLxoCvDIQAvD_BwE>
2. What is mobile device management (MDM) [Електронний ресурс] Режим доступу: <https://www.ibm.com/topics/mobile-device-management>
3. Olsen G. MDM vs. MAM: What are the key differences [Електронний ресурс] Режим доступу: <https://www.techtarget.com/searchsecurity/feature/MDM-vs-MAM-Comparing-enterprise-mobile-security-management-options>
4. The Difference Between MDM, MAM, and MIM Електронний ресурс] Режим доступу: <https://cmitsolutions.com/blog/the-difference-between-mdm-mam-and-mim/>
5. BYOD Management Software & Solutions | MDM for BYOD. [Електронний ресурс] Режим доступу: <https://www.manageengine.com/mobile-device-management/bring-your-own-device-byod-management.html?network=g&device=c&keyword=byod&campaignid=14672304178&creative=611599034627&matchtype=e&adposition=&placement=&adgroup=135013364614&targetid=kwd-3789137331&gclid=CjwKCAjwpayjBhAnEiwA-7ena4gCi8K_OMhEh1YnqNlTyNP7ZWdTwymFMdlI7rXxhl2mfotmkwW0ZhoCMAsQAvD_BwE>
6. What is BYOD? | IBM [Електронний ресурс] Режим доступу: <https://www.ibm.com/topics/byod>
7. MobileIron: A Leader in UEM & Zero Trust Security [Електронний ресурс] Режим доступу: <https://www.ivanti.com/en-au/company/history/mobileiron>
8. Home Realm Discovery [Електронний ресурс] Режим доступу: <https://adfs.mobileiron.com/adfs/ls/?wtrealm=https%3A%2F%2Fhome.mobileiron.com&wctx=WsFedOwinState%3Dn66I9KhBVzilvdhY_75ZaQJjZO0u2yHUfiWpuGSj_812mwWwC7V5pq8y8GRNYhHu7xgI118IuZ7sBZY1YdgdColuSjC-StAJ_KOLaxIVnWfCdeyy4vU4eC8uhqYfF3zi&wa=wsignin1.0>
9. Contributor T. What is CYOD (choose your own device) [Електронний ресурс] Режим доступу: <https://www.techtarget.com/searchmobilecomputing/definition/CYOD-choose-your-own-device#:~:text=CYOD%20(choose%20your%20own%20device)%20is%20an%20employee%20provisioning%20model,a%20limited%20number%20of%20options>.
10. CYOD? COPE? BYOD? [Електронний ресурс] Режим доступу: <https://habr.com/ru/articles/442890/>