ОГЛЯД ТА АНАЛІЗ ЕФЕКТИВНОСТІ АНТИВІРУСНИХ АЛГОРИТМІВ ДЛЯ МОБІЛЬНИХ ОПЕРАЦІЙНИХ СИСТЕМ

Керівник курсової роботи
старший викладач
Кирієнко О.В

Виконала
студентка 3 року навчання
Голянська Т.С

АКТУАЛЬНІСТЬ ТЕМИ

- Мобільні пристрої = центр персональних даних
- Широке використання у фінансах, бізнесі, спілкуванні
- Мета атак — саме мобільні ОС
- Загрози стають складнішими → стандартного захисту вже недостатньо
- Потрібен глибокий аналіз ефективності антивірусних алгоритмів

МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

Мета: проаналізувати ефективність антивірусних алгоритмів у захисті мобільних ОС

Об'єкт: системи та технології кіберзахисту мобільних платформ

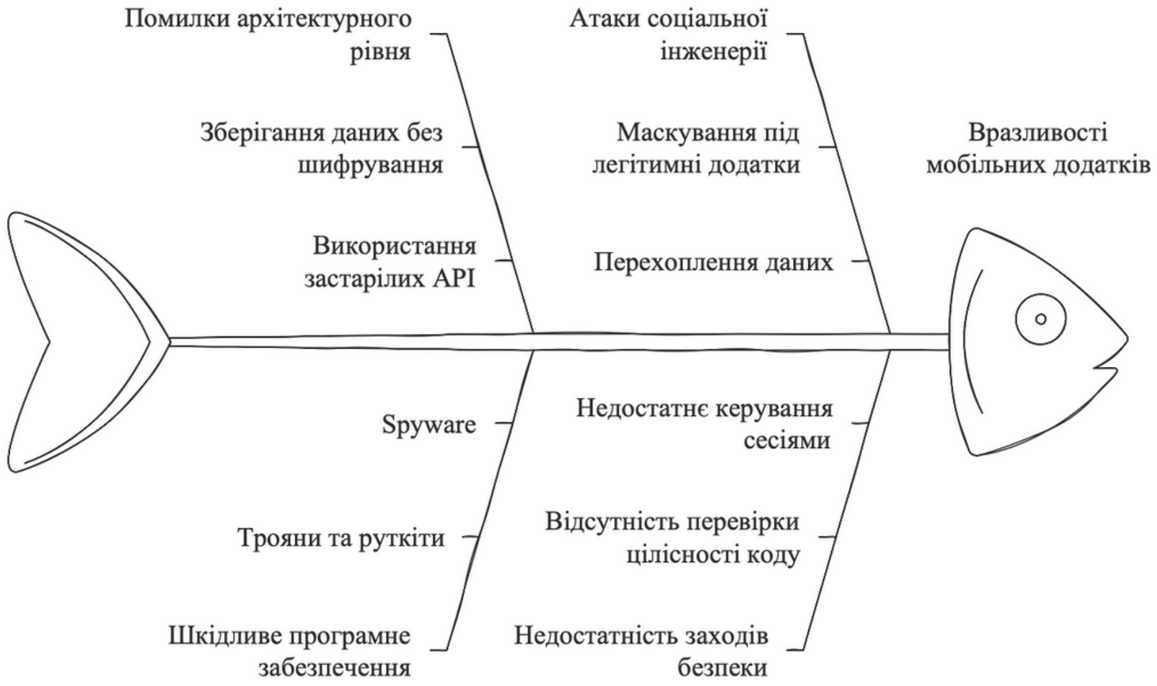
Предмет: методи виявлення та нейтралізації мобільного шкідливого ПЗ

Завдання:

- класифікувати загрози
- оцінити ефективність алгоритмів
- надати рекомендації

ТЕОРЕТИЧНІ ОСНОВИ АНТИВІРУСНИХ АЛГОРИТМІВ І МОБІЛЬНИХ ЗАГРОЗ

Аналіз мобільних загроз



Цикл безпеки мобільних додатків

ОСОБЛИВОСТІ МОБІЛЬНИХ ОПЕРАЦІЙНИХ СИСТЕМ У КОНТЕКСТІ ЗАХИСТУ

Таблиця 2.1 – Порівняльна характеристика механізмів безпеки в ОС Android та iOS

Аспект	Android	iOS
Архітектура	Відкрита платформа, заснована на ядрі Linux, що дозволяє модифікацію коду виробниками та розробниками. Це забезпечує гнучкість, але може створювати потенційні ризики безпеки.	Закрита екосистема, розроблена Apple, з обмеженим доступом до вихідного коду. Це дозволяє Apple підтримувати суворий контроль над безпекою та якістю додатків.
Модель безпеки	Використовує модель безпеки, засновану на дозволах, де користувачі повинні надавати додаткам доступ до певних функцій або даних. Ця система може бути вразливою, якщо користувачі неуважно надають дозволи.	Застосовує суворіший підхід до безпеки, зосереджуючись на ізоляції додатків та контролі доступу до даних. Кожен додаток працює в "пісочниці", що обмежує його можливості взаємодії з іншими додатками та системою в цілому.
Управління додатками	Дозволяє встановлення додатків з різних джерел, включаючи сторонні магазини додатків, що може підвищити ризик встановлення шкідливого ПЗ.	Обмежує встановлення додатків лише через офіційний App Store, де всі додатки проходять ретельну перевірку перед публікацією, що знижує ймовірність поширення шкідливого ПЗ.
Оновлення безпеки	Оновлення безпеки залежать від виробників пристроїв та операторів зв'язку, що може призводити до затримок у впровадженні критичних оновлень.	Apple контролює процес оновлення, забезпечуючи швидке та одночасне розповсюдження оновлень безпеки для всіх підтримуваних пристроїв.

ОГЛЯД СУЧАСНИХ АНТИВІРУСНИХ РІШЕНЬ ДЛЯ МОБІЛЬНИХ ОПЕРАЦІЙНИХ СИСТЕМ

Багаторівневі підходи – ключ до ефективного захисту:

- Сигнатурний аналіз — швидкий, але неефективний проти нових загроз
- Евристика — виявляє підозрілу поведінку без бази підписів
- Статистичний метод — фіксує аномалії мережевого трафіку
- Поведінковий аналіз — відстежує дії програм у реальному часі

ПРОВЕДЕНО:
порівняльний аналіз антивірусних алгоритмів у мобільних продуктах
аналіз компаній-лідерів на ринку мобільної кібербезпеки
аналіз ефективності антивірусного захисту мобільних операційних систем

РЕЗУЛЬТАТИ

У ході виконання курсової роботи «Огляд та аналіз ефективності антивірусних алгоритмів для мобільних операційних систем» було виконано наступні завдання:

1. Проаналізовано основні типи загроз для мобільних пристроїв, зокрема шкідливе ПЗ (трояни, руткіти, шпигунське ПЗ) та методи соціальної інженерії.
2. Досліджено архітектуру безпеки мобільних операційних систем Android та iOS, визначено ключові особливості їх захисту та вразливості.
3. Розглянуто сучасні антивірусні алгоритми: сигнатурний, евристичний, статистичний і поведінковий аналіз; проведено їх порівняння за критеріями ефективності, адаптивності та впливу на продуктивність.
4. Встановлено, що найефективніший захист забезпечується шляхом поєднання кількох підходів до виявлення загроз, що дозволяє підвищити стійкість мобільних систем до сучасних атак.

ДЯКУЮ ЗА УВАГУ