4. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg: National Institute of Standards and Technology, 2020. 59 p. URL: https://doi.org/10.6028/NIST.SP.800-207 (дата звернення: 16.05.2026).

Забезпечення автономності та цілісності даних у мобільних системах управління ремонтними роботами.

УДК 621.395.7 (043.2)

Назар Огінський[1]

Тернопільский національний технічний університет імені Івана Пулюя,
[1]nazar_ohinskyi0706@tntu.edu.ua

Сучасна практика менеджменту в будівництві потребує використання спеціалізованих цифрових інструментів, що гарантують конфіденційність розрахунків та стійкість комерційної інформації до зовнішніх загроз безпеці даних. Проблема ефективного супроводу ремонтних робіт полягає у відсутності зручних інструментів для точних обчислень, а також у ризиках використання хмарних сервісів, що можуть призвести до витоку персональної фінансової інформації [1]. Більшість існуючих рішень вимагають постійної синхронізації, що робить дані вразливими до перехоплення у відкритих мережах.

Метою дослідження є проєктування та розробка автономного мобільного застосунку для автоматизації обчислення площ приміщень та формування кошторисів. Актуальність роботи зумовлена необхідністю мінімізації помилок при ручних розрахунках та потребою у конфіденційному інструменті, який забезпечує повний контроль над даними без залучення сторонніх серверів.

Наукова новизна полягає у розробці моделі автономного функціонування прикладного програмного забезпечення, яка базується на принципах ізоляції фінансових обчислень у локальному середовищі мобільної ОС для мінімізації ризиків перехоплення та витоку комерційної інформації. На відміну від аналогів, запропоновано модель локального збереження даних, яка виключає ризики несанкціоного доступу до інформації у хмарних сховищах.

Для реалізації системи обрано мову Kotlin та фреймворк Jetpack Compose [2]. Програмна архітектура побудована на патерні MVVM, що дозволило ізолювати логіку обчислень від інтерфейсу. Розрахунковий модуль автоматизує визначення необхідних для роботи параметрів об’єкту. Локальне збереження даних реалізовано за допомогою бібліотеки Room на базі SQLite, що гарантує автономність роботи та швидкість доступу до інформації. Цей підхід забезпечує цілісність даних та захист від мережевих загроз, оскільки всі дані обробляються виключно на пристрої [3]. Розроблено каталог робіт, який дозволяє гнучко налаштовувати фінансові параметри проекту в ізольованому середовищі.

Розроблений мобільний застосунок забезпечує автоматизацію основних етапів супроводу ремонтних робіт, поєднуючи зручність інтерфейсу з принципами безпечного збереження даних. Отримані результати підтверджують ефективність локальних баз даних для вирішення прикладних задач будівельної інженерії, гарантуючи приватність фінансових розрахунків.

1. OWASP Mobile Application Security (MAS). URL: https://mas.owasp.org/ (дата звернення: 14.05.2026).
2. Bloch J. Effective Java. 3rd ed. Boston: Addison-Wesley Professional, 2017. 412 p.
3. Griffiths D., Griffiths D. Head First Android Development: A Learner's Guide to Building Android Apps with Kotlin. 3rd ed. Sebastopol: O'Reilly Media, 2021. 930 p.

Змагальні атаки на системи виявлення вторгнень з гібридною архітектурою у мережах IoT

УДК 004.056.5 Ірина Удовик[1], Олександр Кручінін[2], Дмитро Тимофєєв[3]

Національний технічний університет «Дніпровська політехніка»,
[1]udovyk.i.m@nmu.one, [2]kruchinin.o.v@nmu.one, [3]tymofieiev.d.s@nmu.one

Сучасна еволюція цифрової інфраструктури характеризується стрімким поширенням технологій Інтернету речей (IoT) та кіберфізичних систем. Враховуючи динамічність, багатоетапність та адаптивність сучасних кіберзагроз. інтеграція методів машинного навчання (ML) та глибокого навчання (DL) у системи виявлення вторгнень (IDS) стала критичною необхідністю. Однак, в цьому випадку з'являються загрози реалізації змагальних атак (adversarial attacks) на такі IDS.

Метою даної роботи є аналіз можливих змагальних атак на IDS з гібридною архітектурою у мережах IoT.

Однією з найбільш перспективних стратегій захисту є перехід від ізольованого аналізу окремих подій до виявлення кореляційних зв'язків у часі та просторі. Традиційні IDS не враховують, що атаки в середовищах IoT поширюються через логічні взаємини між пристроями та еволюціонують через чіткі темпоральні фази. Застосування гібридних архітектур, що поєднують графові нейронні мережі (GNN) та мережі довгої короткострокової пам'яті (LSTM), дозволяє одночасно фіксувати структурні та часові динаміки атак [1].

Однак ця подвійна природа збільшує поверхню для змагальних атак. Однією із вразливістю GNN є неевклідова природа графових даних, де навіть незначна зміна ваги ребра або атрибута вузла може радикально змінити результат агрегації повідомлень через ітеративний характер навчання. У випадку LSTM вразливість криється в авторегресивній природі моделі, тобто помилка, внесена в один часовий крок, накопичується та спотворює внутрішній стан комірки пам'яті для всіх наступних кроків.

Серед таких змагальних атак можна виділити наступні:

1) Fast Gradient Sign Method (FGSM) – є однією з найбільш фундаментальних атак білої скриньки, яка використовує градієнт функції втрат щодо вхідних даних для швидкої генерації змагальних прикладів. В IoT-мережах FGSM дозволяє зловмиснику маніпулювати статистичними характеристиками пакетів (час між пакетами або розміром вікна), роблячи шкідливий потік невідрізним від нормального для GNN-класифікатора. Це особливо ефективно проти моделей, які не пройшли спеціальне змагальне навчання [2].