Багаторівневий захист мобільного застосунку

УДК 004.056.5:004.9

Любомир Боценюк

Ужгородський національний університет, liubomyr.botseniuk@uzhnu.edu.ua

Сьогодні смартфон фактично став персональним сховищем конфіденційної інформації: від фото й листування до банківських застосунків та приватних фінансових нотаток. Саме тому захист даних на телефоні є не менш важливим, ніж захист у мережі. Реальні ризики часто виникають у повсякденних ситуаціях: підглядання через плече, випадковий скріншот, запис екрана, залишений застосунок у перемикачі останніх програм або короткочасний доступ до пристрою без власника. Навіть якщо застосунок працює офлайн і не передає дані на сервер, загроза витоку не зникає — вона просто зміщується на локальне зберігання та поведінку інтерфейсу.

У межах проєкту створено мобільний офлайновий фінансовий застосунок для обліку та керування коштами. Він дозволяє створювати кілька гаманців, задавати назву, валюту та суму, додавати курс обміну й одразу бачити перерахунок у гривні. Застосунок підраховує загальний баланс по всіх гаманцях, підтримує редагування й видалення записів, зміну порядку гаманців, а також має режим приватності: суми можна швидко замаскувати або контрольовано відображати — окремо по кожному гаманцю чи одразу для всіх.

Захист реалізований за принципом багаторівневості (defense-in-depth), коли безпека не зводиться до одного механізму, а розподіляється на кілька незалежних шарів.

Перший рівень — автентифікація доступу: вхід через PIN-код і, за потреби, біометрію (Face ID/Touch ID) з коректною обробкою сценаріїв, коли користувач просто скасовує біометричну перевірку.

Другий рівень — захист від підбору коду: ліміт невдалих спроб і прогресивне блокування (1 секунда → 2 → 5 → 10 → 30…), що робить атаки типу brute-force практично неефективними, при цьому користувач бачить прозорий таймер блокування.

Третій рівень — контроль сесії: автоматичне блокування при неактивності та під час повернення застосунку з фону, щоб фінансова інформація не залишилася відкритою без нагляду.

Четвертий рівень — захист від витоку через інтерфейс: заборона скріншотів і запису екрана, а також захист мініатюр у перемикачі застосунків там, де це підтримується платформою.

Окремо важливий базовий принцип — безпечне зберігання: чутливі дані та ключі доступу зберігаються в захищеному сховищі пристрою в зашифрованому форматі, щоб навіть у разі доступу до файлів вони не читалися у відкритому вигляді.

Додатковим напрямом у межах проєкту став модуль Face ID, який розширює класичну ідею «пустити / не пустити». У більшості застосунків біометрія — це бінарна перевірка: користувач пройшов автентифікацію і отримав доступ. У запропонованому рішенні підхід інший: Face ID виступає інструментом ідентифікації, тобто дозволяє не просто підтвердити факт входу, а визначити,

хто саме зайшов у систему. Це дає можливість прив'язувати сесію до конкретної особи, а також застосовувати розмежування доступу залежно від ролі. Концепція працює так: під час реєстрації для користувача створюється локальний профіль з ідентифікатором та роллю, а під час входу здійснюється біометричне розпізнавання, яке визначає належність до одного із зареєстрованих профілів. Після успішної ідентифікації система може надавати різні рівні доступу до функцій і даних. Таким чином, біометрія перетворюється на основу керування правами, а не лише на зручний «замок» для входу.

Логічним продовженням розвитку застосунку є поглиблення цього механізму: розширення системи ролей і політик доступу, додавання сценаріїв «підвищеного підтвердження» для критичних дій (повторна ідентифікація), а також гнучке налаштування правил приватності під конкретного користувача. Перспективними є й режими спільного використання одного пристрою кількома людьми, ведення безпечного локального журналу подій (без фінансових деталей, але з фіксацією фактів входу/виходу) та посилення захисту локального зберігання і резервних копій, щоб навіть у разі компрометації середовища дані залишалися недоступними без ключів і підтвердження особи.

У підсумку багаторівневий підхід дозволяє зробити офлайновий фінансовий застосунок не лише зручним, а й стійким до типових реальних загроз. Він поєднує механізми операційної системи, продуману логіку доступу та приватність інтерфейсу користувача (UI), формуючи просте правило: навіть якщо один бар'єр не спрацює, інші шари все одно зменшать ризик витоку та несанкціонованого доступу.

Безпека транспортної інфраструктури України в умовах повномасштабної війни як пріоритетне завдання Державної спеціальної служби транспорту

УДК 656.078:351.862 (477)

Володимир Будз[1], Сергій Костиря[2], Станіслав Шумлянський[3]

Науково-дослідний центр Державної спеціальної служби транспорту,
[1]budzwolodymyr@gmail.com, [2]kostyrya81@gmail.com,
[3]s.shumlianskyi@dsst.gov.ua

Критична інфраструктура (КІ) забезпечує повноцінне функціонування суспільства. До неї належать енергетичні мережі, транспортні вузли, зв'язок, системи водопостачання, охорона здоров'я, банківська система, оборонна промисловість, а також інформаційні технології, в умовах війни вона стає головною мішенню для ворога [1, с. 75]. Руйнування транспортної інфраструктури разом з іншими діями ворога створили безпрецедентні труднощі для національної економіки [2, с. 167], а безпека транспортних маршрутів є одним із ключових викликів для логістичної діяльності в умовах війни [2, с. 168]. Зокрема, за даними СБУ, на кінець січня 2026 року було нейтралізовано понад 14 тисяч масштабних кібератак на Україну за час повномасштабного вторгнення [3]. В умовах повномасштабної російсько-української війни захист КІ України набуває стратегічного значення, оскільки