ЗАХИЩЕНИЙ МЕСЕНДЖЕР ІЗ ЛОКАЛЬНИМ ЗБЕРІГАННЯМ КРИПТОГРАФІЧНИХ КЛЮЧІВ НА КЛІЄНТСЬКОМУ ПРИСТРОЇ

Федюшин О.І., Корсун А.Д.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних комунікаційних системах безпека даних значною мірою залежить не лише від алгоритмів шифрування, а насамперед від способу зберігання та керування криптографічними ключами. Більшість популярних месенджерів покладаються на серверну інфраструктуру для управління ключами, що створює ризики компрометації через витік даних, зловмисний доступ або помилки конфігурації. Проблема централізованого зберігання ключів є одним із ключових викликів у сфері захисту інформації.

Метою даної роботи є розроблення архітектури підсистеми локального зберігання криптографічних ключів у межах захищеного месенджера, де ключі користувача ніколи не покидають меж клієнтського пристрою. Запропонований підхід використовує вбудовані системні сховища: Windows DPAPI, macOS Keychain, Android Keystore та Linux Secret Service – для створення уніфікованого інтерфейсу керування ключами (Key Storage API) [1, 2]. **Предметом дослідження** є архітектура, алгоритми і засоби захисту локального зберігання ключів у клієнтських застосунках, а об'єктом – процеси безпечного управління криптографічними ключами у середовищах користувацьких пристроїв. У роботі проведено дослідження механізмів апаратно-захищеного зберігання, алгоритмів zeroization, шифрування резервних копій ключів із використанням PBKDF2 та Argon2id, а також методів ізоляції ключового матеріалу від додатків і процесів операційної системи. Розроблений модуль інтегровано у клієнтський застосунок на базі Electron/React, що забезпечує взаємодію з бекендом (Spring Boot, PostgreSQL, WebSocket) без передачі ключів через мережу. Проведено статичний і динамічний аналіз безпеки (SAST, DAST) та ручне пентестування, які підтвердили надійність реалізації і відсутність витоків секретного матеріалу під час роботи програми. Отримані результати можуть бути використані для створення систем безпечного зберігання криптографічних даних у застосунках нового покоління, що дотримуються принципу «Zero Trust», коли користувач повністю контролює свої ключі та доступ до них [3].

Список літератури

1. Marlinspike M., Perrin T. The Signal Protocol (X3DH and Double Ratchet) Technical Overview. – Open Whisper Systems, 2016.

2. NIST SP 800-57. Recommendation for Key Management. – Part 1: General. – National Institute of Standards and Technology, 2020.

3. Moskvin, K., & Sievierinov, O. (2025). Zero Trust Architecture in Corporate Cybersecurity Systems // Computer and Information Systems and Technologies Kharkiv, September 2024. P. - 54-55.