Короткий огляд методів захисту та шифрування інформації на мобільних пристроях з операційними системами *Android* та *iOS*

Юрій Божко

старший судовий експерт сектору комп'ютерно-технічних телекомунікаційних досліджень та досліджень у сфері інформаційних технологій, Сумський науково-дослідний експертно-криміналістичний центр Міністерства внутрішніх справ України, м. Суми, Україна, e-mail: yuriybozhko93job@gmail.com

Розглянуто основні методи захисту та шифрування інформації на мобільних пристроях під керуванням операційних систем Android та iOS. Наведено приклади реалізації методів захисту та шифрування.

Ключові слова: *Android; iOS; цифрова криміналістика; захист; FDE; FBE; шифрування; аутентифікація; цифрові докази; мобільні пристрої.*

A Brief Overview of the Methods of Protection and Encryption of Information on Mobile Devices With Operating Systems Android and Ios

Yurii Bozhko

This paper deals with basic methods of protection and encryption of information on mobile devices under the management of Android and iOS operating systems. Examples of implementation of protection and encryption methods are given.

Keywords: *Android; iOS; digital forensics; protection; FDE; FBE; encryption; authentication; digital evidence; mobile devices.*

Сучасними мобільними пристроями (смартфони, планшети) користуються не тільки як засобами зв'язку. Вони можуть містити великі обсяги інформації про власника (користувача), що може мати важливе значення під час розслідування правопорушень. Сьогодні такі пристрої мають різні механізми захисту, які базуються на поєднанні апаратних та програмних технологій. Розуміння того, як працює захист та шифрування, може допомогти у вилученні та розшифруванні інформації.

До основних механізмів захисту можуть належати методи аутентифікації користувача на пристрої, наприклад, цифровий PIN-код, символьний пароль, графічний ключ та біометричні методи (відбиток пальця, розпізнавання обличчя).

Разом з методами аутентифікації, застосовується шифрування даних, яке реалізується переважно двома типами: повнодискове шифрування (Full Disk Encryption, FDE) та шифрування окремих файлів (File-Based Encryption, FBE).

Full Disk Encryption (FDE). За цього підходу весь уміст блокового пристрою шифрується одним ключем. Після розблокування пристрою цей ключ розшифровується та надає доступ до всього вмісту. У Android FDE він реалізовувався за допомогою

підсистеми ядра Linux dm-crypt. У старіших версіях Android шифрування виконувалося із застосуванням AES-128 у режимі CBC з ESSIV:SHA256. Пізніше, починаючи з Android 7.0, FDE було поступово замінене на FBE. В iOS застосовувалось повнодискове шифрування (FDE) починаючи з iPhone 3GS (2009 р.). Усі дані в пам'яті шифрувалися апаратно за допомогою унікального ключа пристрою (UID key), убудованого в процесор.

File-Based Encryption (FBE). За цього підходу кожен файл або група файлів шифруються окремими ключами. Це дає змогу більш гнучко керувати доступом: наприклад, частина файлів може бути доступна ще до авторизації користувача, інші — тільки після введення облікових даних користувача. В Android FBE працює у зв'язці з технологією Direct Boot (починаючи з версії Android 7.0) і поділяє дані на два простори Device-Encrypted (DE), де файли доступні одразу після завантаження системи. Це можуть бути системні журнали, службові дані тощо. Credential-Encrypted (CE) файли стають доступними лише після введення користувачем авторизаційних даних.

З технічної позиції FBE реалізується за допомогою інструментів ядра Linux, наприклад fscrypt, і підтримується файловими системами ext4 та f2fs. За замовчуванням уміст файлів шифрується за допомогою AES-256 у режимі XTS, а імена файлів AES-256 — у режимі CBC-CTS. Ключами керує Volume Daemon (vold) у деяких реалізаціях у взаємодії з апаратними модулями Keymaster або StrongBox. Ключі зберігаються в зашифрованому вигляді на диску, за винятком тимчасового ключа Per-Boot, який узагалі не зберігається.

У системі iOS застосовується модель Data Protection classes. Кожному файлу призначається клас захисту (NSFileProtection), який визначає, коли ключ стає доступним (наприклад, лише після розблокування пристрою або тільки під час активного користування файлом). Апаратне шифрування підтримується окремим апаратним модулем Secure Enclave, убудованим у процесори серії A7 і новіші. Ключі, пов'язані з UID пристроєм та авторизаційними даними користувача, зберігаються у так званом keybag, які своєю чергою зашифровані ключами класів (class keys). Кожен файл шифрується AES-256, а його ключ зашифрований class key тим самим алгоритмом. Class keys зберігаються у system keybag, зашифрованому унікальним UID Key та похідним ключем від пароля користувача (PBKDF2-SHA256).

Окрім методів шифрування, важливим є розуміння станів, у яких може перебувати пристрій.

BFU (Before First Unlock) — стан після ввімкнення, але до першого розблокування користувачем. У цьому стані ключі, пов'язані з обліковими даними користувача, ще не завантажені в пам'ять. На iOS більшість файлів перебувають у класі Complete Protection та залишаються зашифрованими. В Android з FBE в цей момент доступна лише DE-зона.

AFU (After first unlock) — стан після першого розблокування пристрою

користувачем після завантаження системи. Ключі шифрування для більшої кількості інформації застосовуються (розшифровуються) та зберігаються в оперативній пам’яті (Secure Enclave iOS, TrustZone Android).

Розуміння механізмів захисту та шифрування може суттєво допомогти під час дослідження пристроїв і розроблення власних інструментів для вилучення та подолання захисту та шифрування.

Перелік джерел посилання

1. Full-disk encryption. URL: https://source.android.com/docs/security/features/encryption/full-disk (дата звернення: 16.09.2025).
2. File-based encryption. URL: https://source.android.com/docs/security/features/encryption/file-based (дата звернення: 16.09.2025).
3. Apple Platform Security. URL: https://support.apple.com/uk-ua/guide/security/ (дата звернення: 17.09.2025).
4. Seeing is believing. URL: https://www.msab.com/blog/bfu-seeing-is-believing/ (дата звернення: 17.09.2025).