КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.687
УДК 343.140.01

Онищук Оксана Олександрівна
к.т.н., доцент
Волинський національний університет, Луцьк, Україна
ORCID ID: 0000-0002-8342-3011
oksanaoo2024@gmail.com

КРИМІНАЛІСТИЧНІ ДОСЛІДЖЕННЯ МОБІЛЬНИХ ПРИСТРОЇВ: ПОРІВНЯННЯ АПАРАТНО ПРОГРАМНИХ ЗАСОБІВ ШИФРУВАННЯ МОБІЛЬНОГО ЗВ'ЯЗКУ

Анотація. Сьогодні мобільні пристрої стали незамінними інструментами в особистій та професійній сферах, що вимагає високого рівня безпеки зберігання та передачі даних. Стаття присвячена порівнянню платформ Android та iOS у контексті шифрування мобільного зв'язку, а також їх використанню в цифровій криміналістиці. Розглянуто особливості архітектур цих платформ, механізми безпеки, Trusted Execution Environment у Android і Secure Enclave у iOS, та процеси завантаження, що впливають на захист даних. Проаналізовано ключові методи виявлення цифрових доказів і їхню ефективність при роботі з відкритими джерелами. Зроблено висновки щодо переваг і недоліків кожної платформи в аспекті забезпечення інформаційної безпеки та криміналістичних досліджень. Особливу увагу приділено методикам дослідження зашифрованої інформації, використанню алгоритмів AES-256 у режимі GCM, а також можливостям платформ у збереженні та аналізі цифрових доказів. Дослідження визначає переваги та недоліки механізмів захисту даних обох платформ, акцентуючи на впливі їх архітектури на ефективність криміналістичного аналізу. Окремо розглянуто рішення компанії Secusmart GmbH як приклад інтегрованого підходу до забезпечення безпеки мобільного зв'язку. Дослідження демонструє, що iOS є більш захищеною платформою, проте Android пропонує більшу гнучкість для дослідників і розробників. Шифрувальні рішення, що пропонує Secusmart GmbH, підтверджують важливість безпеки мобільного зв'язку. Подальші дослідження повинні мають перспективу створення інноваційних методів захисту, що враховують як потреби користувачів, так і вимоги правоохоронних органів. Рекомендується для Android стандартизувати безпекові оновлення, а для iOS ключовим розвивати механізми захисту без погіршення користувацького досвіду та використання шифрувальних рішень.

Ключові слова: Android; iOS; захист даних; шифрування; криміналістичний аналіз; Secusmart GmbH.

ВСТУП

У сучасному світі безпека використання мобільних пристроїв має вирішальне значення. Мобільні пристрої виконують широкий спектр функцій, забезпечуючи зв'язок, зберігання даних і підтримку різноманітних операцій у приватному та професійному середовищах. Вони критично важливі для управління ресурсами, планування та реалізації проектів у багатьох галузях.

Ця стаття присвячена порівнянню платформ Android і iOS у контексті шифрування мобільного зв'язку. Особливу увагу приділено ролі платформ у криміналістиці, методикам виявлення доказових даних та використанню сучасних механізмів шифрування, таких як рішення компанії Secusmart GmbH.

Постановка проблеми. Сучасними завданнями цифрової криміналістики слугують пошук і аналіз цифрових слідів, аналіз даних (в т.ч. — метаданих), збирання

доказової інформації у цифровому середовищі. Найбільш складними і масштабними сьогодні є завдання щодо пошуку у відкритому доступі та аналізу потенційних джерел доказів, а саме величезної кількості загальнодоступних відео- та аудіо-записів, фото- та супутникових знімків, текстів, звітів, публікацій в соціальних мережах.

Аналіз останніх досліджень і публікацій. Важливість і актуальність розвитку цифрової криміналістики в усьому світі підтверджується тим, що у 2012 р. був прийнятий спеціальний міжнародний стандарт ISO/IEC 27037:2012 [1], який містить настанови щодо роботи із цифровими доказами. Дотримуючись цього стандарту, журналісти-розслідувачі інтернет-видання Bellingcat на основі аналізу цифрової інформації (телефонних розмов, відеозаписів, супутникових знімків та ін.) встановили, що до авіакатастрофи с пасажирським Boeing-777 MH17 причетні військові РФ. Для допомоги у вирішенні таких складних завдань Центром прав людини Університету Берклі в Каліфорнії та Офісом Верховного комісара ООН з прав людини у 2020 р. представлений Протокол Берклі (практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права), який містить стандарти і методологічні підходи до «збору, зберігання та аналізу інформації у відкритому доступі, яка може бути представлена як доказ у кримінальних процесах». [2, с. 6, 3]. Розробники Протоколу наголошують на важливості встановлення достовірності доказової інформації та забезпеченні її збереження. У Протоколі Берклі викладені алгоритми пошуку, накопичення, аналізу та збереження цифрової інформації з відкритих джерел із дотриманням принципів об’єктивності, компетентності, підзвітності, відповідності законодавству, безпеки, точності, незалежності, прозорості, дотримання прав людини. Автори Протоколу надають рекомендації щодо визначення меж вирішуваного завдання з метою економії часу та забезпечення особистої безпеки свідків і потерпілих, а також — для безпеки апаратного і програмного забезпечення [3],[4].

Серед інструментів цифрової криміналістики акцентується увага на таких: пошук за ключовими словами та хештегами, списки яких попередньо підготовлені, моніторинг радарів та системи офіційного моніторингу суден Marine Traffic, аналіз супутникових знімків, використання технології аналізу «великих даних» (Big Data); аналіз геолокаційних міток, дослідження фото- та відеоматеріалів у відкритому доступі та наданих слідству, використання програм для аналізу та обробки цифрових зображень, дослідження телефонних розмов, аналіз електронних пристроїв, аналіз ігрових систем, система розпізнавання облич і пошуку їх у відповідних базах даних (в Україні використовують додаток з розпізнавання облич Clearview Af для ідентифікації потенційних злочинців і загиблих) [5, с. 32]. В інших джерелах виокремлюються такі сучасні напрями цифрово криміналістики: 1) дослідження хмарних сховищ; 2) дослідження мобільних пристроїв (телефонів); 3) дослідження програм (месенджерів та інших застосунків для смартфонів, що використовуються для обміну інформацією); 4) дослідження інтернет-речей (IoT); 5) мережеві дослідження; 6) дослідження новітніх приладів і додатків (Alexa від Amazon, Google Assistant, Siri від Apple та ін.); 7) дослідження додатків не для телефону (дослідження баз даних, Spotlight, America online instant messaging, дронів, волатильно пам’яті, Даркнету, засобів анти криміналістики, видалених і фрагментованих файлів, зображень, флеш-пам’яті, криптовалют); 8) цифрови аналіз поведінки окремих осіб, груп людей та їх взаємозв’язків і відносин; 9) цифрова криміналістична розвідка та розвідка на основі відкритих джерел тощо [6] – [8].

Метою роботи є аналіз і порівняння платформ Android та iOS у питаннях: методик виявлення доказових даних, механізмів шифрування мобільного зв'язку та визначення найефективніших підходів до захисту інформації.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

У криміналістичному дослідженні мобільних пристроїв важливе значення має інфраструктура апаратних і програмних платформ. Сучасні процесори, наприклад, інтегрують модулі безпеки, такі як Trusted Execution Environment (TEE) для Android та Secure Enclave для iOS. Ці механізми можуть бути як перешкодою, так і ключем до доступу до даних у криміналістиці.

Android має модульну архітектуру, яка забезпечує гнучкість і масштабованість. Стек архітектури Android включає декілька шарів, кожен із яких виконує свою функцію. Завантаження Android включає кілька етапів, кожен із яких виконує важливу функцію. Він включає такі рівні як Linux kernel — базовий рівень, що забезпечує роботу драйверів, Hardware Abstraction Layer (HAL) — прошарок, який дозволяє додаткам взаємодіяти з апаратними компонентами. та Android Runtime (ART) — забезпечує виконання додатків. Завантаження Android починається з виконання Bootloader, який перевіряє криптографічні підписи системи, що важливо для криміналістичного аналізу з метою перевірки автентичності даних.

Завантаження iOS є складним і багаторівневим процесом, який гарантує безпеку та стабільність системи. Архітектура iOS включає наступні рівні: Core OS — ядро системи, що відповідає за базову функціональність, Security Frameworks — включає шифрування файлів, автентифікацію та інші механізми. Процес завантаження iOS побудований на Chain of Trust, де кожен етап перевіряє наступний. Це робить неможливим модифікацію системи без доступу до приватних ключів Apple. iOS відома своєю закритою архітектурою, високим рівнем безпеки та оптимізованою продуктивністю. Архітектура iOS включає декілька шарів, кожен із яких виконує специфічні функції, пов'язані з роботою апаратного забезпечення та програмного забезпечення.

Таблиця 1

Порівняння стеків архітектур та процесів завантаження Android та iOS

	Android	iOS
Стек архітектури та процес завантаження	• Linux Kernel (ядро): забезпечує доступ до апаратного забезпечення та захист через SELinux. • Hardware Abstraction Layer (HAL): абстрагує взаємодію між апаратним забезпеченням та API. • Android Runtime (ART): відповідає за виконання Java-додатків із використанням Ahead-of-Time (AOT) та Just-in-Time (JIT) компіляції. • Native Libraries: забезпечують функціонал графіки, мультимедіа та шифрування. • Application Framework: надає API для розробки додатків.	• Core OS (ядро): базовий шар, який забезпечує взаємодію апаратного та програмного забезпечення. • Core Services: включає сервіси для роботи з базами даних, iCloud та Bluetooth. • Media: обробляє графіку, звук і відео. • Cocoa Touch: відповідає за інтерфейс користувача та сенсори.

Процес завантаження	1. Boot ROM: завантажує Bootloader. 2. Bootloader: перевіряє цифрові підписи системи, завантажує ядро Linux. 3. Kernel (ядро): запускає драйвери апаратного забезпечення. 4. Init: конфігурує систему. 5. Zygote: створює процеси додатків. 6. System Server: запускає системні сервіси. 7. Home Screen: забезпечує взаємодію користувача з інтерфейсом.	1. Boot ROM: виконує перевірку цифрового підпису Bootloader. 2. Low-Level Bootloader (LLB): ініціалізує базові компоненти. 3. iBoot: завантажує ядро iOS. 4. Kernel (ядро): запускає драйвери та служби. 5. Launchd: основний процес, який активує системні сервіси. 6. SpringBoard: забезпечує домашній екран і запуск додатків.

Обидві операційні системи мають потужну підтримку для додатків, але Android використовує більше відкритих технологій, а iOS є більш закритою та інтегрованою системою, що дає більший контроль Apple над екосистемою. iOS забезпечує високий рівень безпеки і контроль за тим, що саме може бути запущено на пристрої. Починаючи з Boot ROM, система перевіряє цифрові підписи для запобігання запуску неавторизованого коду, потім ініціалізує базові компоненти та переходить до запуску користувацького інтерфейсу. Процес завантаження Android строго розділений на кілька етапів, що забезпечує модульність та безпеку системи.

МЕТОДИКА ДОСЛІДЖЕННЯ

Проаналізовано теоретичним методом безпекові аспекти двох провідних мобільних платформ — Android та iOS — у контексті шифрування мобільного зв’язку. Особливу увагу приділено архітектурним відмінностям, методам завантаження системи, а також механізму захисту даних. Розглянуто сучасні технології шифрування та методом через CommonCrypto та стандартні API для AES-256 в режимі GCM для IOS та API Cipher для шифрування за допомогою AES в режимі GCM для Android. Аналітично визначено ключові переваги та недоліки кожної платформи з точки зору захисту інформації та можливостей виявлення доказових даних.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для криміналістичного дослідження мобільних пристроїв критичне значення мають засоби шифрування мобільного зв’язку і застосовуються за допомогою фізичного аналізу(вилучення даних з пам’яті пристрою), логічного аналізу (доступ до інформації через офіційні API та додатки) та аналізу шифрованих даних — декодування з використанням спеціалізованих інструментів або злам криптографічних ключів [9], [10]. Аналіз шифрованих даних — це складний процес, який включає методи дослідження захищеної інформації без порушення конфіденційності або з метою відновлення доступу у випадках кримінальних розслідувань [11] – [16]. Цей процес базується на криптоаналізі, інженерії зворотного проектування, а також дослідженні залишкових даних [17], [18].

Розглянемо етап аналізу шифрованих даних, які включає збір даних, аналіз мережевого трафіку (перехоплення зашифрованих пакетів). Для початку важливо ідентифікувати тип шифрування через визначення використаного алгоритму (AES, RSA, ECC) та вивчити метадані (заголовків, сертифікатів). Потім можемо проаналізувати

криптографічні протоколи, зокрема перевірка наявності слабких місць у реалізації (наприклад, у TLS) та використати вектори атаки. Методи аналізу шифрованих даних здійснюються криптоаналізом (дослідження математичних властивостей алгоритмів шифрування), атака на обраний текст (chosen plaintext attack), атака по часу (timing attack), аналізом залишкових даних (витяг незашифрованих фрагментів даних із залишків на диску або в пам'яті), застосування апаратних вразливостей (використання недоліків апаратного забезпечення (наприклад, вразливість TEE)).

Схема аналізу шифрованих даних:

1. Витяг даних:
   – Чип-level extraction
   – Аналіз мережевого трафіку
   ↓
2. Ідентифікація алгоритму:
   – AES, RSA, ECC
   – Метадані
   ↓
3. Аналіз протоколів:
   – TLS, SSL
   – Уразливості
   ↓
4. Відновлення ключів:
   – Атака грубої сили
   – RAM, кеш
   ↓
5. Розшифрування даних:
   – Реконструкція
   – Аналіз змісту

Схеми захисту та атаки:

- **Схема шифрування:** 1. Вхідні дані → 2. Генерація ключа → → 3. Шифрування (AES-256) → 4. Зашифрований текст.
- **Атака:** 1. Перехоплення даних → 2. Аналіз ключів у пам'яті → 3. Атака на алгоритм → 4. Розшифрування.

Результати досліджень вказують, що складність шифрування і безпекових механізмів стримує доступ до даних, але професійні криміналістичні інструменти здатні подолати ці обмеження. Зокрема, застосування технологій компаній типу Secusmart GmbH ускладнює витік інформації, але створює виклики для криміналістики.

На iOS шифрування зазвичай здійснюється через CommonCrypto та стандартні API для AES-256 в режимі GCM. На Android для шифрування використаємо API Cipher для шифрування за допомогою AES в режимі GCM. Для обох платформ необхідно дбати про безпечне зберігання ключів і IV (ініціалізаційний вектор), щоб уникнути витоків даних. Аналіз шифрованих даних зводиться до пошуку вразливостей в алгоритмах і недостатнього управління ключами або даними. Проаналізована надійність TEE (Android) пов'язана з архітектурними особливостями TEE і працює паралельно з основною операційною системою, але ізольовано від неї. Використання ARM TrustZone забезпечує розподіл між «звичайним» і «захищеним» світами. Перевагами тут є захист конфіденційних даних (наприклад, ключів шифрування, біометричних даних), унеможливлення доступу до захищених даних навіть у разі компрометації основної ОС

та гарантія інтеграції з апаратним забезпеченням. Варто відмітити, можливості атак через вразливості у мікропрограмі та атаки сторонніх каналів (наприклад, через споживання енергії чи електромагнітні випромінювання). Нами проведено для платформ iOS та Android шифрування та аналіз шифрованих даних з використанням стандартного підходу. Реалізація схеми шифрування та аналізу здійснювалася для обох платформ.

Використовуємо AES-256 в GCM режимі (Galois/Counter Mode), який забезпечує конфіденційність і цілісність даних. Додатково додамо IV (ініціалізаційний вектор) для кожного блоку даних та ключ для шифрування. Вхідні дані: Plain text (вхідний текст): «Sensitive Information». Ключ шифрування: випадковий 256-бітний ключ (наприклад, за допомогою алгоритму генерації ключа на платформі).

```
import CommonCrypto

func encryptData(data: Data, key: Data) -> Data? {
    var cryptor: CCCryptorRef? = nil
    var result = Data(count: data.count + kCCBlockSizeAES128)

    let iv = Data(count: kCCBlockSizeAES128)  // Ініціалізаційний вектор (IV)
    let status = CCCryptorCreateWithMode(
        CCOperation(kCCEncrypt), // Шифрування
        CCMode(kCCModeGCM),       // Режим GCM
        CCAlgorithm(kCCAlgorithmAES), // Алгоритм AES
        CCPadding(kCCPaddingNone),    // Без паддінгу
        iv.bytes, iv.count,
        key.bytes, key.count,
        nil, 0, 0, 0, &cryptor
    )

    // Шифрування
    var dataOutMoved: size_t = 0
    CCCryptorUpdate(cryptor,  data.bytes,  data.count,  &result,  result.count,
&dataOutMoved)
    return result
}
```

На Android аналогічно використаємо AES-256 для шифрування. Використовується API Cipher для шифрування даних, режим GCM для забезпечення автентичності та конфіденційності, додамо IV (ініціалізаційний вектор) і використаємо SecretKeySpec для ключа.

```
import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
import javax.crypto.spec.GCMParameterSpec;
import java.util.Base64;

public String encryptData(String plainText, String secretKey) throws Exception {
    Cipher cipher = Cipher.getInstance("AES/GCM/NoPadding");
    SecretKey key = new SecretKeySpec(secretKey.getBytes(), "AES");

    byte[] iv = new byte[12]; // Ініціалізаційний вектор (IV)
    SecureRandom secureRandom = new SecureRandom();
    secureRandom.nextBytes(iv);
    GCMParameterSpec spec = new GCMParameterSpec(128, iv); // 128 біт автентичності
    cipher.init(Cipher.ENCRYPT_MODE, key, spec);

    byte[] encryptedData = cipher.doFinal(plainText.getBytes());
    return Base64.getEncoder().encodeToString(encryptedData);
}
```

На цьому етапі зловмисник може перехопити зашифровані дані (шифротекст). Оскільки ми використали AES-256 в режимі GCM, дані передаються з IV, а також, можливо, із додатковими метаданими (зокрема, тег автентичності, що дозволяє перевірити цілісність). Після того, як зловмисник можливо перехопив зашифровані дані, може спробувати отримати доступ до ключа шифрування, що зберігається в пам'яті. На iOS перехоплення значно складніше завдяки функціям, таким як Secure Enclave, які використовуються для захисту ключів. Однак на Android (для нашого підходу), якщо ключ зберігається в пам'яті без додаткового захисту, зловмисник може спробувати витягнути його через side-channel атаки або за допомогою спеціальних інструментів для доступу до пам'яті (наприклад, за допомогою root-доступу або через інші уразливості). Зловмисник може спробувати атакувати сам алгоритм або його реалізацію. Якщо зловмисник отримав ключ шифрування (наприклад, через вразливості в пам'яті) або здобув інформацію про IV і алгоритм, він може спробувати розшифрувати дані.Якщо використовується режим GCM, навіть якщо зашифрований текст буде отриманий, він не буде розшифрований без правильного IV та ключа, оскільки GCM перевіряє автентичність даних. Якщо зловмисник намагається змінити шифротекст або IV, то під час перевірки автентичності буде виявлено несумісність, і дані не будуть розшифровані.

Для того, уникнути атаки варто провести статистичний аналіз шифрованих даних, при якому будемо аналізувати повторювані блоки в шифрованих даних (в разі використання режиму GSM, де один і той самий вхід дає однаковий шифр) та вивчити в зашифрованих даних уразливості. Тому варто досить ретельно підходити до вибору шифрованих текстів. Якщо зловмисник має доступ до зашифрованих даних, то варто через brute-force методи перевірити різні ключі шифрування. На Android та iOS для дешифрування можемо застосувати ті ж самі алгоритми, що і для шифрування, з використанням Cipher.DECRYPT_MODE на Android або еквівалентного методу на iOS.

Надійність iOS аналогічно відзначається архітектурними особливостями співпроцесора, який ізольований від основного чипа A-серії. Він використовує власну пам'ять і операційну систему та має захист чутливих даних, таких як Touch ID, Face ID, ключі шифрування. При цьому існує неможливість доступу навіть для iOS та інших компонентів, оскільки використовується апаратний генератор випадкових чисел. Недоліком являється надзвичайно складний доступ до даних, але можливі атаки через фізичне втручання у мікросхеми.

Обидві технології є ключовими для забезпечення безпеки даних і стійкими до більшості атак. Однак вони створюють значні труднощі, оскільки доступ до даних у таких ізольованих середовищах обмежений і потребує спеціалізованих інструментів або вразливостей.

Оскільки апаратна та програмна інфраструктура мобільних пристроїв визначає способи збереження, захисту та обробки інформації, то найбільш ефективним підходом до захисту даних є визначення місць збереження доказових даних.

Основні місця, де зберігаються доказові дані: локальна пам'ять (файлова система, бази даних), хмарні сервіси (Google Drive, iCloud), кеш додатки та лог-файли. Визначення цих місць є критичним для збору доказів під час криміналістичного аналізу. Найкращі місця збереження доказових даних на мобільних пристроях — це локальна пам'ять пристрою. Сюди належать файли додатків, кеші, бази даних SQLite, журнали викликів, SMS, MMS, електронна пошта, хмарні сервіси: iCloud, Google Drive, OneDrive зберігають синхронізовані дані. Крім того, доступ можливий через облікові записи та ключі авторизації або залишкові дані в оперативній пам'яті, які часто містять ключі шифрування або сесійні токени. Через аналіз мережевого трафіку може виявити

скомпрометовані дані, тому варто використовувати спеціалізовані інструменти для витягу даних, наприклад, Cellebrite, Oxygen Forensic та аналізувати метадані для встановлення джерела і часу створення файлів, вивчати залишкові сліди навіть після видалення інформації (наприклад, через відновлення даних з NAND-флеш-пам'яті).

Серед надійних технологій типу Secusmart GmbH можемо шифрувати голосові дзвінки, SMS, електронну пошту, що забезпечує можливість перехоплення даних у реальному часі. Така платформа сумісні із різними платформами, які підтримують Android, iOS та навіть стаціонарні телефони, має високий рівень криптографії, оскільки використовує алгоритми AES-256 і апаратні ключів, що гарантує захист навіть від потужних атак.

Оскільки засоби шифрування мобільного зв'язку мають важливе значення, то технології Secusmart GmbH забезпечують захист голосових дзвінків і повідомлень через апаратне та програмне шифрування (SecuVOICE, SecuTABLET). Сучасні українські оператори мобільного зв'язку є вкрай незахищеними. Як варіант, технології компанії Secusmart GmbH є прикладом високо захищеного мобільного зв'язку. Їх рішення базуються на апаратах шифрування, тобто інтегровані чипи для захисту голосового зв'язку (SecuVOICE), програмних засобах — мобільні додатки, що використовують криптографію для захисту SMS і електронної пошти. Інтеграція з існуючими мережами та адаптація під корпоративні та державні системи. Технології Secusmart GmbH є прикладами інноваційного підходу до забезпечення безпеки, які довели свою ефективність у різних галузях: урядові організації: захист конфіденційних розмов і документів; запобігання промисловому шпигунству; військові структури; безпечне управління операціями та комунікація між підрозділами. Ці рішення дозволяють гарантувати високий рівень безпеки, залишаючи при цьому комунікацію зручною для користувачів.

Таблиця 2

Технології	Криптографічні особливості	Функціональність
SecuSUITE for Government Ця технологія призначена для захисту голосових дзвінків і текстових повідомлень.	Використання алгоритму AES-256 для шифрування. Генерація ключів за допомогою захищених апаратних модулів.	Шифрування голосових викликів у реальному часі. Захист повідомлень SMS та MMS. Підтримка різних пристроїв, включаючи смартфони та стаціонарні телефони.
SecuVOICE Технологія для захисту голосового зв'язку.	Захист від прослуховування під час телефонних дзвінків навіть у публічних мережах. Зручний інтерфейс для урядових і бізнес-користувачів.	Інтеграція в SIM-карту спеціального криптографічного чипа. Використання кінцевого шифрування (end-to-end encryption).
SecuTABLET Захищений планшет для роботи з конфіденційними даними.	Шифрування даних у пам'яті планшета. Захист VPN для безпечного з'єднання з корпоративними мережами.	Побудований на основі апаратного забезпечення Samsung Galaxy Tab S. Інтеграція рішень BlackBerry для управління мобільними пристроями (MDM).
SecuSMART Card Спеціальна SD-карта з інтегрованим криптографічним модулем.	Інтегрований криптографічний модуль	Захист голосових дзвінків і текстових повідомлень. Сумісність із смартфонами, які підтримують використання SD-карт.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі було виявлено, що криміналістичний аналіз мобільних пристроїв потребує глибокого розуміння архітектури операційних систем, шифрування та збереження даних. Поєднання інноваційних технологій та сучасних методів дозволяє успішно виявляти й використовувати докази, незважаючи на захисні механізми пристроїв. **iOS** забезпечує високий рівень безпеки завдяки закритій архітектурі, централізованому контролю над оновленнями та строгій політиці допуску додатків до App Store. Secure Enclave є вагомим аргументом для захисту криптографічних операцій. Хоча платформа **Android** є більш відкритою, це створює ризики для кінцевих користувачів, проте використання технологій на зразок SELinux та TEE дозволяє захищати критичні дані. На Android завдяки відкритості екосистеми доступ до файлової системи та інструментів аналізу є більш гнучким.

Сучасні механізми шифрування, особливо на пристроях з останніми версіями операційної системи, ускладнюють отримання доступу до зашифрованих даних. iOS ускладнює проведення криміналістичних досліджень через строгі механізми захисту, включаючи Secure Boot і шифрування на рівні файлової системи. Відновлення даних можливе лише за наявності ключів розблокування або обхідних шляхів. Використання AES-256 із GCM (на iOS) та шифрування через Cipher API (на Android) демонструє високий рівень захисту. Водночас апаратно-програмні рішення, такі як Secusmart, дають змогу забезпечити додатковий рівень безпеки, особливо для урядових і корпоративних користувачів. Проте ці технології ускладнюють процес доступу до даних, створюючи бар’єри для правоохоронних органів.

Технології Secusmart GmbH є прикладом найкращих практик захисту інформації, що робить їх незамінними в умовах постійних загроз кібербезпеки. Такі технології — це оптимальні місця збереження доказів та інноваційні рішення, що забезпечують надійний захист даних. У той же час, вони ускладнюють роботу криміналістів, які потребують спеціалізованих інструментів і високої кваліфікації для аналізу зашифрованої інформації. Технології шифрування голосових дзвінків і повідомлень від Secusmart значно підвищують рівень захисту мобільного зв’язку. Водночас їх інтеграція в систему вимагає значних ресурсів, а також викликає питання щодо адаптивності до різних платформ.

Дослідження демонструє, що **iOS** є більш захищеною платформою, проте **Android** пропонує більшу гнучкість для дослідників і розробників. Шифрувальні рішення, такі як ті, що пропонує Secusmart GmbH, підтверджують важливість інтегрованого підходу до забезпечення безпеки мобільного зв’язку. Подальші дослідження повинні бути спрямовані на створення інноваційних методів захисту, що враховують як потреби користувачів, так і вимоги правоохоронних органів. Рекомендується для **Android** зосередитися на стандартизації безпекових оновлень серед усіх виробників пристроїв. Для **iOS** ключовим завданням є подальший розвиток механізмів захисту без погіршення користувацького досвіду та використання шифрувальних рішень, що сертифіковані міжнародними стандартами, дозволить значно знизити ризики витоку даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence* (ISO/IEC 27037:2012). (2012). https://www.iso.org/standard/44381.html
2. *Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних.* Переклад. (2020). Організація Об’єднаних Націй.

3. *The European Convention on Human Rights. Council of Europe.* (б. д.). https://www.coe.int/en/web/human-rights-convention
4. Думчиков, М. О. (2020). Процеси діджиталізації і криміналістика: ретроспективний аналіз. *Криміналістика і судова експертиза, 65,* 100–108.
5. Колодіна, А. С., & Федорова, Т. С. (2022). Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права, (1),* 176–180.
6. Наджафлі, Е. (2022). Цифрова держава в контексті правової реформи в Україні: теоретико-правовий аспект. *Право і безпека, 2(85),* 202–217.
7. Latysh, K. (2021). Criminalistics analysis of cyber tools for committing crimes. *Problems of Legality, (153),* 165–172. https://doi.org/10.21564/2414-990X.153.230429
8. Laptiev, O., Savchenko, V., Shuklin, G., & Stefurak, O. (2020). *Detection and blocking of means of illegal obtaining of information at objects of information activity.* Kyiv: SUT.
9. Yevseiev, S., et al. (2021). *Synergy of building cybersecurity systems: monograph*. Kharkiv: PC TECHNOLOGY CENTER. https://doi.org/10.15587/978-617-7319-31-2
10. Юрченко, О. М. (2001). *Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник.* К.: Видавництво Європейського університету.
11. *Методи захисту. Системи управління інформаційною безпекою. Вимоги* (ДСТУ ISO/IEC 27001:2015). (2015).
12. *Інформаційні технології. Методи захисту. Звіт практик щодо заходів інформаційної безпеки* (ДСТУ ISO/IEC 27002:2015). (2015).
13. *Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки* (ДСТУ ISO/IEC 27005:2019). (2019).
14. Про захист інформації в інформаційно-телекомунікаційних системах, Закон України № 80/94-ВР (2024) (Україна). https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
15. Про інформацію, Закон України № 2657-XII (2024) (Україна). https://zakon.rada.gov.ua/laws/show/2657-12#Text
16. Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2024) (Україна). https://zakon.rada.gov.ua/laws/show/2163-19#Text
17. Лаптєв, О. А. (2020). *Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації*. К.: Міленіум.
18. Лєнков, С. В., Перегудов, Д. А., & Хорошко В. А. (2008). *Методи та засоби захисту інформації* (в 2-ох томах). К: Арий.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Oksana Onyshchuk
PhD of Technical Sciences, Associate Professor
Volyn National University, Lutsk, Ukraine
ORCID ID: 0000-0002-8342-3011
oksanaoo2024@gmail.com

MOBILE DEVICE FORENSICS: COMPARISON OF MOBILE ENCRYPTION HARDWARE AND SOFTWARE

Abstract. Today, mobile devices have become indispensable tools in personal and professional spheres, which requires a high level of security for data storage and transmission. The article is devoted to a comparison of the Android and iOS platforms in the context of mobile communication encryption, as well as their use in digital forensics. The features of the architectures of these platforms, security mechanisms, Trusted Execution Environment in Android and Secure Enclave in iOS, and loading processes that affect data protection are considered. The key methods of detecting digital evidence and their effectiveness when working with open sources are analyzed. Conclusions are drawn on the advantages and disadvantages of each platform in terms of ensuring information security and forensic research. Special attention is paid to the methods of studying encrypted information, the use of AES-256 algorithms in GCM mode, as well as the capabilities of the platforms in storing and analyzing digital evidence. The study identifies the advantages and disadvantages of the data protection mechanisms of both platforms, focusing on the impact of their architecture on the effectiveness of forensic analysis. The solution of Secusmart GmbH is separately considered as an example of an integrated approach to ensuring mobile security. The study demonstrates that iOS is a more secure platform, but Android offers greater flexibility for researchers and developers. The encryption solutions offered by Secusmart GmbH confirm the importance of mobile security. Further research should have the prospect of creating innovative protection methods that take into account both the needs of users and the requirements of law enforcement agencies. It is recommended for Android to standardize security updates, and for iOS, it is key to develop protection mechanisms without degrading the user experience and the use of encryption solutions.

Keywords: Android; iOS; data protection; encryption; forensic analysis; Secusmart GmbH.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence* (ISO/IEC 27037:2012). (2012). https://www.iso.org/standard/44381.html
2. *Berkeley Protocol on Investigations Using Open Digital Data*. Translation. (2020). United Nations.
3. *The European Convention on Human Rights. Council of Europe.* (б. д.). https://www.coe.int/en/web/human-rights-convention
4. Dumchikov, M. O. (2020). Digitalization processes and forensics: a retrospective analysis. *Forensic Science and Forensic Science, 65,* 100–108.
5. Kolodina, A. S., & Fedorova, T. S. (2022). Digital forensics: problems of theory and practice. *Kyiv Law Journal, (1),* 176–180.
6. Najafli, E. (2022). Digital state in the context of legal reform in Ukraine: theoretical and legal aspect. *Law and Security, 2(85),* 202–217.
7. Latysh, K. (2021). Criminalistics analysis of cyber tools for committing crimes. *Problems of Legality, (153),* 165–172. https://doi.org/10.21564/2414-990X.153.230429
8. Laptiev, O., Savchenko, V., Shuklin, G., & Stefurak, O. (2020). *Detection and blocking of means of illegal obtaining of information at objects of information activity.* Kyiv: SUT.
9. Yevseiev, S., et al. (2021). *Synergy of building cybersecurity systems: monograph*. Kharkiv: PC TECHNOLOGY CENTER. https://doi.org/10.15587/978-617-7319-31-2
10. Yurchenko, O.M. (2001). *Information protection in computer systems from unauthorized access: Textbook.* Kyiv: Publishing House of the European University.

11. *Protection methods. Information security management systems. Requirements* (DSTU ISO/IEC 27001:2015). (2015).
12. *Information technology. Protection methods. Report of practices on information security measures* (DSTU ISO/IEC 27002:2015). (2015).
13. *Information technology. Protection methods. Information security risk management* (DSTU ISO/IEC 27005:2019). (2019).
14. On the Protection of Information in Information and Telecommunication Systems, Law of Ukraine No. 80/94-ВР (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.
15. On Information, Law of Ukraine No. 2657-XII (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/2657-12#Text
16. On the Basic Principles of Ensuring Cybersecurity of Ukraine, Law of Ukraine No. 2163-VIII (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/2163-19#Text
17. Laptev, O. A. (2020). *Methodological foundations of automated search for digital means of covert information acquisition.* K. Millennium.
18. Lenkov, S. V., Peregudov, D. A., & Khoroshko, V. A. (2008). *Methods and means of information protection* (in 2 volumes). K: Ary, 2008.