Ключевые слова: Защита, информационная безопасность, организация, безопасность организации.
Keywords: Protection, information security, organization, security of the organization.
***Науковий керівник**: д. фіз. - мат. н., професор Василенко М. Д.*

Пальчук Андрій Вікторович
Національний університет «Одеська юридична академія»,
студент 4-го курсу факультету кібербезпеки
та інформаційних технологій

Саніцька Інна Валеріївна
Національний університет «Одеська юридична академія»,
студент 4-го курсу факультету кібербезпеки
та інформаційних технологій

ОБРОБКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ СИСТЕМИ IOS: ПРОБЛЕМИ РЕАЛІЗАЦІЇ

Безпека системи є головною складовою зменшення кількості злочинів, здійснюваних у кіберпросторі. Поява сучасних технологій та стрімкий розвиток IT-сфери створює сприятливе середовище для вибору користувачами новітніх засобів для реалізації найрізноманітніших задач, включаючи соціальні мережі та спілкування.

Однією з найбезпечніших мобільних операційних систем вважається iOS. iOS – це мобільна операційна система для смартфонів, електронних планшетів, а також програвачів і деяких інших пристроїв, що розробляється і випускається американською компанією Apple [1].

Оскільки смартфони стають все більш поширеними по всьому світу, компаніям неминуче доводиться боротися з проблемами, пов'язаними з безпекою та конфіденційністю цих пристроїв. технологія збереження конфіденційності вдосконалюється, проблеми з конфіденційністю користувачів не були повністю розглянуті самою технологією. Відповідні регуля-

тивні засоби захисту також відіграють певну роль у захисті конфіденційності користувачів смартфонів. В даний час існує багато прогалин між регулюванням та технологіями: вони не є належним чином поєднані для забезпечення бажаного захисту. Існує перелік поширених проблем захисту персональних даних, обумовлених організаційними і технічними аспектами.

Обробкою персональних даних є будь-яка дія, так звана операція, або сукупність дій, що здійснюються з використанням засобів автоматизації з персональними даними. До обробки входить збір та запис даних, їх систематизація, зберігання, накопичення та оновлення, використання та передача [2].

При зберіганні персональних даних можливі такі помилки як: небезпечне зберігання, витік даних, деякі компоненти операційної системи можуть зберігати чутливі дані, неправильна криптографія, слабка або повністю відсутня захист виконуваних файлів. Щоб зберегти конфіденційні дані програм, користувачі даної операційної системи повинні використовувати служби безпеки, надані компанією самою компанією Apple.

В iOS вбудований механізм шифрування файлів на диску самого пристрою. Таких механізм дозволяє користувачеві віддалено і швидко очистити файлову систему, захищаючи при цьому дані при установці флеш-пам'яті в інший телефон. Якщо встановлений пасскод, прочитати вміст цих файлів без нього неможливо.

Захист файлів реалізована через ієрархію криптографічних ключів. iOS присвоює кожному файлу 256 бітний AES ключ. Дані записуються на накопичувач тільки в зашифрованому вигляді.

AES – симетричний алгоритм шифрування. Уряд США використовує AES з ключем 256 біт для зберігання секретних документів. Симетричність означає, що для шифрування і розшифровки даних використовується один і той же ключ.

В iOS існує кілька класів захисту файлів. Кожен клас захисту має свій крипто-ключ [3].

Ключ файлової системи створюється випадковим способом при першій установці iOS або очищення пристрою. Ключ зберігається в стирається сховище. Коли користувач очищає пристрій опцією Erase all content and settings або віддалено через iCloud, ключ файлової системи видаляється. Тепер всі файли недоступні, система не може розшифрувати метадані, в яких зберігається ключ файлу. Безпечне видалення ключів настільки ж важливо, як і їх створення. Це особливо складно на флеш-накопичувачах, де через зношування дані можуть дублюватися в декількох місцях. Тому в iOS пристрої містять Ефективне сховище (Effaceable Storage). Ця функція дозволяє стирати невеликі блоки даних з пристрою зберігання на найнижчому рівні.

Існує ряд проблем захисту персональних даних в операційній системі iOS. Як правило, персональні дані користувачів при виконанні мережевих запитів зберігаються в кеші HTTP або в Cookies. Крім того, вони розміщуються в додатках, що є небезпечно. Іноді користувачі не встановлюють Passcode або просто проявляють недбалість по відношенню до захисту персональних даних. Саме тому компанія рекомендує звертати увагу на екран авторизації з пінкодом або Touch ID, що служить розблокуванням і захистом персональних даних користувача шляхом зчитування його рис обличчя. Йдеться про додатковий захист даних на рівні користувача інтерфейсу.

З іншого боку, будь-яке шифрування може бути зламано і захист користувачів повністю покладається на компанії, що виробляють продукт техніки, і вони будуть забезпечувати його безпеку лише тому, що це відповідає їх бізнес-інтересам і іміджу.

Натомість сама компанія Apple визнає, що шифрування, яке захищає персональні дані користувачів пристроїв, може бути зламано за допомогою шкідливого програмного забезпечення.

Так, в 2018 році турецький дослідник інформаційної безпеки Мелих Севім знайшов вразливість захисту персональних даних користувачів. В ході його експерименту в iCloud,

система дозволила йому переглядати деякі дані чужих акаунтів в сервісі – наприклад, замітки в облікових записах. Дослідник зміг отримати доступ як до даних випадкових акаунтів, так і цілеспрямовано розкривати інформацію конкретних користувачів – для цього йому потрібно було знати пов'язаний з сервісом номер телефону. Після цієї історії Мелих офіційно звернувся до компанії Apple з проханням переглянути політику конфіденційності та усунути всі можливі проблеми системи, які створили кібернебезпечне та вразливе середовище для користувачів і клієнтів даної компанії. [4]

Список використаних джерел:

1. Офіційний сайт компанії Apple. Електронний ресурс. URL: https://www.apple.com/ru/ios/

2. Яремчук Ю. Є. Комплексні системи захисту інформації: навчальний посібник / Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. – Вінниця: ВНТУ, 2017. – 120 с.

3. Офіційний сайт компанії Apple. Електронний ресурс. URL: https://www.apple.com/business/resources/docs/iOS_Security_Overview.pdf

4. Офіційний сайт BBC News. URL: https://www.bbc.com/russian/science/2010/12/101229_apple_class_action

Ключові слова: iOS, Apple, персональні дані, операційна система, шкідливе програмне забезпечення, користувачі, криптографія, шифрування файлів.

Ключевые слова: iOS, Apple, персональные данные, операционная система, вредоносное программное обеспечение, пользователи, криптография, шифрование файлов.

Keywords: iOS, Apple, personal data, operating system, malicious software, users, cryptography, encryption of files.

***Науковий керівник**: д. фіз. - мат. н., професор Василенко М. Д.*