УДК 004.056.5
Дьячук Т.С.[1], Дружко Р.В.[2]
[1] старш. викл. НУ «Запорізька політехніка»
[2] студ. гр. КНТ-512 НУ «Запорізька політехніка»

АТАКИ НА МЕСЕНДЖЕРИ ТА МЕТОДИ ЗАХИСТУ: END-TO-END ШИФРУВАННЯ ТА SIGNAL PROTOCOL

В умовах масової цифровізації комунікацій питання безпеки обміну повідомленнями набуває критичного значення. Месенджери – WhatsApp, Signal, Telegram, Viber – стали основним каналом передачі конфіденційної інформації як для приватних осіб, так і для організацій. Водночас зростає кількість і складність атак, спрямованих саме на ці платформи. Метою даної роботи є аналіз основних векторів атак на сучасні месенджери та дослідження механізмів захисту на основі наскрізного (end-to-end) шифрування і, зокрема, протоколу Signal.

Серед основних категорій атак на месенджери виділяють: атаки типу «людина посередині» (Man-in-the-Middle, MitM), перехоплення трафіку на транспортному рівні, компрометацію серверів, атаки на резервні копії повідомлень, соціальну інженерію та фішинг, а також атаки через вразливості клієнтських застосунків. Особливу загрозу становлять атаки на метадані: навіть якщо вміст повідомлень захищено шифруванням, аналіз метаданих (хто, коли, з ким і як довго спілкувався) може розкрити критичну інформацію [1]. Модель безпеки месенджера можна подати як сукупність взаємодії користувачів через захищений канал передачі даних, що знижує ризик перехоплення повідомлень.

End-to-end шифрування (E2EE) є фундаментальним механізмом захисту, що гарантує: повідомлення шифруються безпосередньо на пристрої відправника і можуть бути розшифровані виключно на пристрої отримувача. Жодна третя сторона – включно з провайдером сервісу – не має доступу до відкритого тексту повідомлень. Концептуально E2EE базується на асиметричній криптографії: кожен учасник генерує пару ключів (публічний і приватний), де публічний ключ вільно поширюється, а приватний зберігається виключно на пристрої користувача.

Signal Protocol – відкритий криптографічний протокол, розроблений Open Whisper Systems, є де-факто стандартом E2EE у сучасних месенджерах. Він лежить в основі Signal, WhatsApp, а також використовується у Facebook Messenger (у секретних чатах) та Google Messages. Протокол поєднує кілька криптографічних примітивів: алгоритм Extended Triple Diffie-Hellman (X3DH) для початкового встановлення сеансового ключа та механізм Double Ratchet для генерації унікального ключа шифрування для кожного окремого

повідомлення [2]. Signal Protocol критично мінімізує збір метаданих, унеможливлюючи аналіз соціальних зв'язків користувачів навіть при доступі до серверів.

Механізм Double Ratchet забезпечує дві ключові властивості безпеки: пряму секретність (Forward Secrecy) – компрометація поточного ключа не дозволяє розшифрувати попередні повідомлення, та властивість Break-in Recovery (Post-Compromise Security) – після компрометації ключа система автоматично відновлює безпеку каналу за рахунок безперервного оновлення ключового матеріалу. Це принципово відрізняє Signal Protocol від статичних схем шифрування, де одна компрометована пара ключів ставить під загрозу весь обсяг переписки.

Порівняльний аналіз популярних месенджерів демонструє суттєві відмінності у рівні захисту. Signal застосовує E2EE для всіх видів комунікацій (текст, голос, відео, групові чати) і мінімізує збір метаданих. WhatsApp також реалізує E2EE на основі Signal Protocol, проте зберігає суттєвий обсяг метаданих, а резервні копії у хмарі (iCloud/Google Drive) можуть зберігатися без наскрізного шифрування. Telegram за замовчуванням використовує шифрування лише між клієнтом і сервером (не E2EE); E2EE доступне лише у режимі «Секретних чатів» і не підтримується у групових розмовах [3]. Що створює ризик доступу третіх сторін до листування у разі компрометації серверної інфраструктури.

Таким чином, Signal Protocol забезпечує найвищий на сьогодні рівень криптографічного захисту для месенджерів. Однак технологічні засоби захисту не є достатніми самі по собі: значна частина успішних атак реалізується через компрометацію пристрою користувача (зловмисне ПЗ, незахищені резервні копії), людський фактор (соціальна інженерія) або вразливості у реалізаціях клієнтських застосунків. Комплексний підхід до захисту інформації в месенджерах вимагає поєднання надійних криптографічних протоколів, своєчасного оновлення прогамного забезпечення та підвищення цифрової грамотності користувачів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Unger N., Dechand S., Bonneau J., Fahl S., Perl H., Goldberg I., Smith M. SoK: Secure Messaging. 2015 IEEE Symposium on Security and Privacy (SP). San Jose, CA, USA, 2015. P. 232–249. DOI: 10.1109/SP.2015.22.

2. Marlinspike M., Perrin T. The Double Ratchet Algorithm. Signal Foundation, 2016. . URL: https://signal.org/docs/specifications/doubleratchet/ (дата звернення: 03.04.2026).

3. Ermoshina K., Musiani F., Halpin H. End-to-End Encrypted Messaging Protocols: An Overview. Internet Science (INSCI 2016). Cham: Springer, 2016. P. 244–254.