АНАЛІЗ ЗАХИЩЕНОСТІ END-TO-END ШИФРУВАННЯ АУДІО ТА ВІДЕО-ВИКЛИКІВ У СУЧАСНИХ МЕСЕНДЖЕРАХ

Мельникова О.А., Гузенко Н.В.
Харківський національний університет радіоелектроніки, Харків, Україна

У наш час існує багато месенджерів, які надають користувачам можливість спілкуватися у текстовому, відео або аудіо-форматі. Вони стали невід'ємною частиною нашого життя, адже забезпечують легкий обмін інформацією. З розвитком цифрових технологій все більшу актуальність набирають питання безпеки персональних даних та захищеності переданих повідомлень.

Метою доповіді є аналіз сучасних месенджерів щодо забезпечення безпеки під час аудіо та відео-викликів. У доповіді розглянуто реалізації end-to-end шифрування в різних месенджерах, що дає змогу проаналізувати їх захищеність. Були проаналізовані такі месенджери: Telegram, Signal, WhatsApp, Facebook Messenger та Viber.

В одному з найпопулярніших месенджерів, Telegram, end-to-end шифрування реалізовано лише для секретних чатів. Звичайні чати, групи та канали використовують шифрування типу "клієнт–сервер", тобто Telegram має доступ до всієї інформації з цих чатів. Секретні чати Telegram створюються лише між двома пристроями й доступні лише у мобільній версії застосунку. Дані для таких чатів, зокрема всі повідомлення, зберігаються локально та забезпечують справжнє E2EE (end-to-end encryption) на основі протоколу MTProto 2.0 [1].

Для всіх дзвінків, навіть у звичайних чатах, Telegram використовує E2EE шифрування [2]. Протокол MTProto 2.0, на якому базується Telegram, застосовує алгоритм Діффі-Геллмана для розподілу ключів, AES-256 для симетричного шифрування, RSA-2048 для ініціалізації обміну ключами та SHA-256 для ґешування.

Signal не є одним із найпопулярніших месенджерів, проте у всіх його чатах, дзвінках і викликах використовується end-to-end шифрування. Реалізацію його протоколу опубліковано на GitHub, тобто будь-який користувач може отримати доступ до повного вихідного коду, наприклад, для аудиту. Signal використовує дволанцюговий алгоритм шифрування, у якому кожне повідомлення має власний ключ. Це означає, що при розкритті одного ключа інші залишаються повністю захищеними. Для додаткового захисту та анонімності Signal приховує частину метаданих, зокрема інформацію про відправника, щоб навіть сервер не міг визначити, хто є ініціатором повідомлення або виклику. Для обміну ключами Signal застосовує алгоритм Extended Triple Diffie-Hellman [3], який дозволяє створювати сеанси навіть тоді, коли отримувач перебуває офлайн. Для шифрування повідомлень використовується AES-256-CBC, для ґешування – SHA-256, а для підпису – EdDSA. WhatsApp використовує Signal Protocol [4] для забезпечення end-to-end шифрування у всіх чатах, а також аудіо та відео-викликах. За заявою

компанії, всі ключі шифрування зберігаються лише на пристроях користувачів. Водночас WhatsApp збирає метадані та передає їх компанії Meta. Під час ініціалізації чату, якщо отримувач перебуває офлайн, WhatsApp використовує prekeys — одноразові ключі, що зберігаються на сервері та призначені для встановлення сесії, коли інша сторона знову з'явиться онлайн. Для шифрування повідомлень використовується AES-256, для ґешування — SHA-256.

Наступний популярний месенджер — Facebook Messenger, який також належить компанії Meta, використовує за основу Signal Protocol (протокол, розроблений Signal). Однак end-to-end шифрування, на відміну від Signal та WhatsApp, за замовчуванням вимкнене, хоча доступне у секретних чатах — подібно до Telegram. Для шифрування повідомлень застосовується [5] AES-256 у режимі CTR, SHA-256 для ґешування та EdDSA для підпису. Додатково він використовує Labyrinth Protocol для синхронізації E2EE між пристроями та вдосконалює механізм перевірки пристроїв.

Viber з 2016 року підтримує end-to-end шифрування у приватних і групових чатах, а також у дзвінках. Але застосовує власний протокол, принципи якого були оприлюднені. Viber збирає метадані про користувача та його пристрій, однак усі ключі шифрування зберігаються на пристроях користувачів. Сервіс використовує [6] алгоритм Діффі-Геллмана для розподілу ключів, AES-256-CFB для шифрування, SHA-256 для ґешування та EdDSA для підпису.

На основі проведеного аналізу сформовано критерії для порівняння з метою підвищення рівня безпеки. Отримані результати показують, що більшість сучасних месенджерів впроваджують достатньо надійні механізми захисту, але деякі месенджери обмежують E2EE шифрування, наприклад, для використання лише у захищених чатах. Загалом можна стверджувати, що EE2E шифрування поступово стає стандартом у сфері цифрових комунікацій та забезпечує захист приватного спілкування від несанкціонованого доступу.

Список літератури

1. MTProto. URL: https://core.telegram.org/mtproto (дата звернення 15.10.2025).
2. Security Analysis of End-to-End Encryption in Telegram. URL: https://caislab.kaist.ac.kr/publication/paper_files/2017/SCIS17_JU.pdf (дата звернення 15.10.2025).
3. The Double Ratchet Algorithm. URL: https://signal.org/docs/specifications/doubleratchet/ (дата звернення: 15.10.2025).
4. Prekey Pogo: Investigating Security and Privacy Issues in WhatsApp's Handshake Mechanismю URL: https://arxiv.org/pdf/2504.07323 (дата звернення 15.10.2025).
5. Messenger End-to-End Encryption Overview. URL: https://engineering.fb.com/wp-content/uploads/2023/12/MessengerEnd-to-EndEncryptionOverview_12-6-2023.pdf (дата звернення: 15.10.2025).
6. Viber Encryption Overview. URL: https://www.viber.com/app/uploads/viber-encryption-overview.pdf (дата звернення 15.10.2025).