

УДК 004.5

Казекин Р.С.¹, Киричек Г.Г.²

¹ студ. гр. КНТ- 510сп, НУ «Запорізька політехніка»

Передача інформації за допомогою месенджерів є невід'ємною частиною повсякденності. Сучасна людина щодня використовує декілька месенджерів для обміну повідомленнями, файлами, контактами, розташуванням та отримує послуги, новини і вирішує важливі робочі завдання [1]. Величезна кількість різних конфіденційних даних проходить через ці системи. Збереження та безпека таких даних є актуальним напрямом досліджень. Метою цього дослідження є аналіз безпеки при використанні розповсюджених месенджерів.

Вибір додатку для обміну повідомленнями, частіше за все, залежить від критеріїв, які мають вплив на рівень безпеки та по-різному важливі для груп користувачів. До таких критеріїв відносяться: відсутність доступу до даних для постачальника мобільного інтернету; забезпечення безпечного сеансу обміну повідомленнями та шифрування повідомлень для підтримки конфіденційності. Важним аспектом захисту даних, що передаються з використанням месенджерів, є спосіб шифрування та аутентифікації цих даних [2]. Найкращим сьогодні вважається наскрізне захищене з'єднання, коли вихідне повідомлення обробляється на мобільному пристрої відправника, а обробка вхідного повідомлення також повністю відбувається на мобільному пристрої одержувача. Воно використовується у таких популярних месенджерах як WhatsApp та Telegram (рис.1).

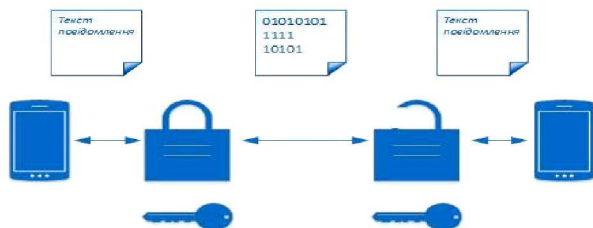


Рисунок 1 - Наскрізне шифрування E2EE (End-to-end encryption)

На початку 2022 року в мережі зафіксовано десятки програм для обміну повідомленнями, які позиціонують себе захищеними. До основних характеристик безпечного месенджера віднесемо: незалежність від великих технологічних компаній; наскрізне шифрування; підтримку різних платформ та декілька типів обміну інформацією.

В Україні найбільш популярними є Viber, Telegram та Facebook Messenger [4]. Телеграм не використовує режим наскрізного шифрування за замовчуванням і секретні чати призначені лише для спілкування двох

клієнтів. Для надсилання повідомлень він використовує власний протокол MTProto [5]. Facebook Messenger використовує наскрізне шифрування між користувачами для всіх чатів за замовчуванням [6]. А у Viber обмін повідомленнями, дзвінки, надсилання фото і відео за замовчуванням захищено наскрізним шифруванням [7]. Сервер програми постійно генерує та оновлює криптографічні ключі. Розглянемо критерії безпечного використання наскрізного шифрування для месенджерів (табл.1).

Таблиця 1 – Порівняльний аналіз наскрізного шифрування месенджерів

Критерії E2EE	Telegram	Facebook Messenger	Viber
E2EE	+	+	+
Режим роботи	потрібно самостійно розпочати захищений чат	за замовчуванням	за замовчуванням
Протокол	MTProto	Signal	Proteus (модифікація Signal)
Розмір ключа	256-бітний ключ	256-бітний ключ	256-бітний ключ
Метод обміну ключами	класичний протокол Діффі - Хеллмана	потрійного перетворення Діффі - Хеллмана	потрійного перетворення Діффі - Хеллмана

Використання наскрізного шифрування не дозволяє отримати доступ до криптографічних ключів з боку третіх осіб. Це означає, що призначена для користувача інформація стає недоступною навіть для серверів, які передають дані. Абсолютний захист від витоку інформації не надає жодна програма миттєвого обміну повідомленнями.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Global No.1 Business Data Platform [Electronic resource]. Access mode: <https://www.statista.com/>
2. Соловійов Е. Г. Аналіз способів захисту обміну повідомленнями в мобільних додатках. 2020. Одеса : ОНАХТ, 2020. Ч. I. С. 186–188
3. Дудикевич В. Б., Томашевський Б. П., Сергієнко Р. В. Протоколи і механізми безпеки інформації в комп'ютерних системах і мережах. Захист інформації. Т. 11. №. 2 (43). С. 39-54.
4. Ісайкіна О., Зленко А. Інформаційна безпека як інструмент захисту національного медіапростору. Соціум. Документ. Комунікація. 2019. №8. С. 134-155.