Лілія ШЕВЧЕНКО
к.е.н., доцент,
доцент кафедри державного управління
і місцевого самоврядування,
НТУ «Дніпровська політехніка»

Олексій КАРАМБОВИЧ
здобувач вищої освіти за освітньою програмою «Інформатика»,
ДНУ імені Олеся Гончара

Костянтин ЗОЛОТЬКО
к.т.н., доцент,
доцент кафедри комп'ютерних технологій,
ДНУ імені Олеся Гончара

АКТУАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ ПРИВАТНИХ МЕСЕНДЖЕРІВ У ГРОМАДАХ

Останнім часом цифрові технології змінюють повсякденне життя, створюючи засади для сталого соціально-економічного розвитку громад і територій; неможливо уявити інфраструктурний та інвестиційний розвиток без комплексного застосування сучасних інформаційних технологій.

З метою досягнення Цілі сталого розвитку № 11, що полягає у забезпеченні відкритості, безпеки, життєстійкості та екологічної стійкості міст і громад, де мешканці мають гідний рівень життя, формуються засади економічного процвітання та соціальної стабільності без завдання шкоди довкіллю, орієнтовані на впровадження цифрових технологій.

Протягом останніх двох років без перебільшення усі сфери життєдіяльності громад змінилися під впливом абсолютно нових викликів. Пандемія COVID-19 порушила екосистему та інфраструктуру територій, у той же час вона значно прискорила процеси цифровізації, породивши не лише нові потреби та можливості, але й нові залежності і проблеми. Попри очевидні позитиви, притаманні інформаційним технологіям (підвищення рівня інноваційності, покращення системи освіти та охорони здоров'я, підвищення рівня енергоефективності тощо), вони можуть збільшувати територіальні цифрові «розриви», формувати ризики дезінтеграції громад окремих віддалених територій, а також поглиблювати вразливість економіки та населення до кібератак. Саме проблема кібербезпеки на тлі збільшення цифрових технологій визначена однією з ключових під час Всесвітнього економічного форуму (січень 2021 р.), де було висунуто припущення про поширення так званої «кіберпандемії» [1].

24 лютого 2022 року у зв'язку з військовою агресією Російської Федерації проти України Президент України підписав Указ № 64/2022 «Про введення воєнного стану в Україні». Правовий режим воєнного стану в Україні висунув на порядок денний низку питань, пов'язаних як загалом з проблемою кібербезпеки, так і, зокрема, з проблемою забезпечення приватності засобів комунікації у межах окремих громад. Мова йде про необхідність протидії витоку інформації

військового характеру за межі обмеженого кола людей (членів громади). Це інформація, яка стосується, наприклад, розміщення об’єктів інфраструктури, волонтерських штабів, бомбосховищ, блок-постів, місць ракетних ударів, відповідних фото- та відеоматеріалів тощо. Також особливої приватності потребує комунікація працівників військових адміністрацій, органів місцевого самоврядування.

Передача інформації через месенджери давно стала невід’ємною частиною повсякденності. Месенджери дозволяють швидко і легко налагодити комунікацію між членами громади щодо різних питань: робота, навчання, розваги, особисті контакти. Функції сучасних месенджерів давно вийшли за межі звичаного обміну повідомленнями, фото, відео. За допомогою цього засобу комунікації можна здійснювати аудіо- та відеодзвінки, робити покупки, сплачувати рахунки за комунальні послуги, отримувати довідкову інформацію, замовляти продукти харчування, таксі, квитки та багато іншого [2].

Розвиток хмарних технологій також посилив вплив месенджерів на розвиток громад, тому що їх використання не обмежується побутовим спілкуванням, вони є зручним засобом комунікації у системі управління (надзвичайно спрощується процес передачі важливих файлів, листування, контактів тощо).

Враховуючи нові виклики на шляху розвитку громад і територій, про які йшлося вище, постає питання вибору месенджера, який би найкраще відповідав обраним критеріям і, у першу чергу, забезпечував приватність обміну інформацією.

Signal – це багатоплатформова служба зашифрованих миттєвих повідомлень, розроблена Signal Foundation та Signal Messenger LLC. Вона використовує Інтернет для надсилання індивідуальних та групових повідомлень, які можуть містити файли, голосові нотатки, зображення та відео. Також сервіс може бути використаний для здійснення голосових та відеодзвінків, а версія для Android може додатково функціонувати як програма для надсилання і отримання SMS [3].

Signal використовує стандартні номери стільникових телефонів як ідентифікатори та забезпечує повний зв'язок з іншими користувачами Signal за допомогою наскрізного шифрування. Додатки сервісу мають механізми, за допомогою яких користувачі можуть самостійно перевіряти особистість своїх контактів та цілісність каналу даних.

Все програмне забезпечення Signal є безкоштовним та відкритим. Його клієнти публікуються під ліцензією GPLv3, тоді як код сервера публікується під ліцензією AGPLv3. Некомерційний фонд Signal був заснований у лютому 2018 р. з початковим фінансуванням 50 млн. дол [3].

Протокол Signal спрямований на передачу зашифрованих повідомлень від однієї сторони до іншої. На високому рівні Signal – це асинхронний протокол безпечного каналу, ключі якого обчислюються за допомогою багатоетапного протоколу AKE, за допомогою сервера розподілу ключів, який лише зберігає та передає інформацію між сторонами, але не виконує жодних обчислень.

Signal передбачає, що кожна сторона має довгострокову пару відкритих і приватних ключів, які називають ключами ідентифікації.

Однак, оскільки сторони можуть бути в автономному режимі в будь-який момент часу, стандартний аутентифікований обмін ключами (AKE) рішення не можна застосовувати безпосередньо. Наприклад, використання обміну ключами DH для досягнення ідеальної конфіденційності вимагає від обох сторін надати нові ефемерні ключі DH, але одержувач може бути офлайн на момент відправлення.

Замість цього Signal реалізує асинхронний протокол передачі, вимагаючи від потенційних одержувачів попередньо надсилати пакети ефемерних відкритих ключів під час реєстрації або пізніше. Коли відправник бажає надіслати повідомлення, він отримує ключі для одержувача від проміжного сервера (який діє лише як буфер), і виконує протокол, подібний до AKE, використовуючи довгострокові та ефемерні ключі для обчислення ключа шифрування повідомлення [4].

Це базове налаштування потім розширюється, роблячи ключі повідомлення залежними від усіх виконаних раніше обмінів між сторонами, використовуючи комбінацію «храпових» механізмів для формування «ланцюгів». Новий випадковий та секретні значення також вводяться в обчислення у різні моменти, впливаючи на майбутні ключі повідомлень, розраховані співрозмовниками (рис.).

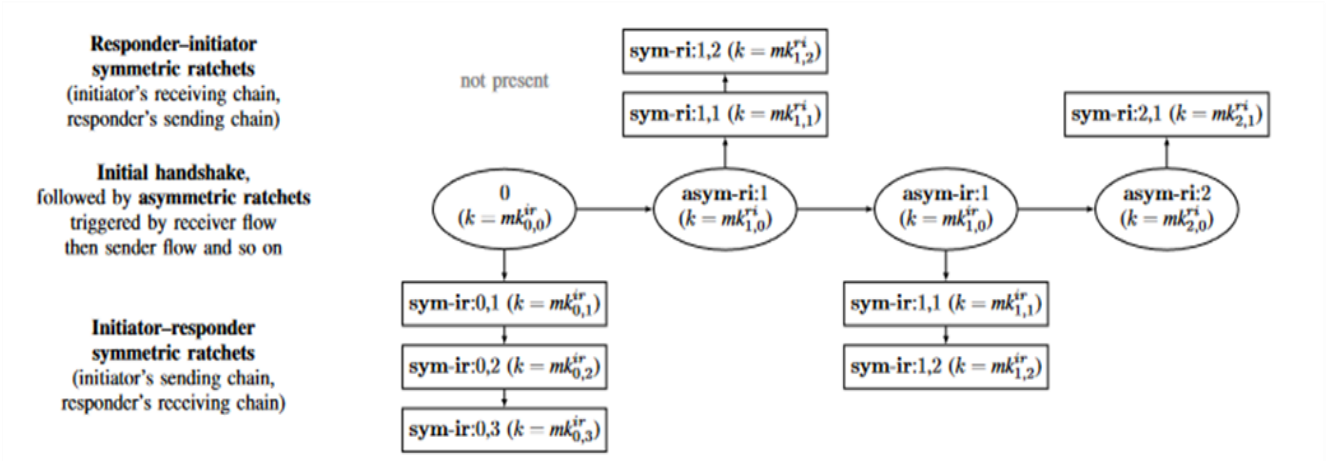

Рис. Дерево стадій тестового запуску Signal

У результаті порівняння характеристик найбільш популярних месенджерів (табл.) [2], було зроблено висновок, що Signal найбільше відповідає основним критеріям безпеки та має переваги серед інших месенджерів. Використання месенджеру Signal може бути рекомендованим для використання в громадах у сучасних умовах, зокрема під час воєнного стану в Україні.

Список використаних джерел

1. Smart-інфраструктура у сталому розвитку міст: світовий досвід та перспективи України. URL: https://razumkov.org.ua/uploads/other/2021-SMART-%D0%A1YTI-SITE.pdf.

2. Сравнительный анализ безопасности и приватности мессенджеров. URL: https://www.anti-malware.ru/compare/Messengers-security-and-privacy.

Таблиця

Порівняльні характеристики месенджерів за основними критеріями безпеки

Функція (критерій безпеки)	Signal	Wickr Me	Telegram	Viber
Підтримка наскрізного шифрування за замовчуванням	Так	Так	Ні (потрібно самостійно розпочати захищений чат)	Так
Підтримка наскрізного шифрування для дзвінків / відеодзвінків	Так	Так	Так	Так
Відсутність збору особистих даних користувача з боку адміністрації месенджера	Так	Так	Ні (контактна інформація, контакти, ідентифікатори)	Ні (контент користувача, розташування, ідентифікатори, покупки, контактна інформація, контакти)
Повністю відкритий вихідний код (як серверної, і клієнтської частин)	Так	Ні	Ні	Ні
Додаток генерує та зберігає ключ безпосередньо на пристрої	Так	Так	Так	Так
Застосовуються надійні криптографічні алгоритми	Так (Curve25519 / AES-256 / HMAC-SHA256)	Так (ECDH512/AES-256/HMAC-SHA256)	Так (RSA 2048 / AES-256 / SHA-256)	Так (Curve25519 256 / Salsa20 128 / HMAC-SHA256)
Шифрування метаданих	Так	Так	Ні	Ні
Підтримка двофакторної аутентифікації	Так	Так	Так	Ні
Відсутність зберігання листування на сервері	Так	Ні	Ні	Ні
Відсутність передачі особистих даних користувача державним органам безпеки	Так	Так	Ні	Так

3. Signal. URL: https://uk.wikipedia.org/wiki/Signal.

4. A Formal Security Analysis of the Signal Messaging Protocol. URL: https://eprint.iacr.org/2016/1013.pdf.

Отримано редакційною колегією: 28.03.2022.