УДК 004.05+004.77:007

О. В. Клювак, канд. економ. наук,
О. В. Грендус, здобувач вищої освіти
Львівський національний університет імені Івана Франка, Україна

АНАЛІЗ РІВНЯ ЗАХИЩЕНОСТІ СУЧАСНИХ СИСТЕМ ОБМІНУ МИТТЄВИМИ ПОВІДОМЛЕННЯМИ

O. Kliuvak, PhD in Economics
O. Grendus, higher education applicant
Ivan Franko National University of Lviv, Ukraine

ANALYSIS OF THE SECURITY LEVEL OF MODERN INSTANT MESSAGING SYSTEMS

Безсумнівним є те, що на сьогоднішній час складно знайти людей, які б не використовували у своєму житті, професійній діяльності та підприємницькій діяльності сучасні системи миттєвого обміну повідомленнями. Це обумовлюється значними перевагами таких систем у порівнянні із іншими каналами комунікацій, таких як: висока швидкість передачі повідомлень, наявність Push-повідомлень, персоналізація, різноманітний контент, низька ціна (безкоштовне використання, менший трафік), можливість створення бесід і груп тощо [1].

Проте така поширеність використання та популярність цих систем породжує і негативні явища, пов’язані із загрозами інформаційній безпеці під час передачі персональних даних та іншої інформації. Особливої актуальності питання інформаційної безпеки під час обімну миттєвими повідомлення набуває в умовах російської-української війни.

Серед основних критеріїв захищеності інформації у системах обміну миттєвими повідомленнями можна виокремити такі: знаходження під юрисдикцією розвідувального альянсу “Five Eyes”, моніторинг (стеження) зі сторони уряду, надання звіту про прозорість, джерело фінансування, збір даних про користувачів, шифрування за замовчуванням, криптографічні примітиви, наявність відкритого коду додатку чи сервера, можливість анонімної реєстрації у програмі, можливість вручну добавляти контакти без використання сервера каталогів, можливість перевірки відбитків пальців користувачів, можливість модифікації служби каталогів під час атаки «Людина посередині» (MitM), хешування персональної інформації, шифрування метаданих, використання протоколу Transport Layer Security (TLS) та сертифікату для нього, локальна автентифікація, шифрування повідомлення під час їх резервного копіювання у хмару. Умовно індикатори загроз відповідно до цих критеріїв захищеності сучасних систем обміну миттєвими повідомленнями можна назвати “червоний” (високий рівень загрози), “жовтий” (середній рівень загрози), “зелений” (низький рівень загрози). У табл.1 представлений порівняльний аналіз рівня захищеності сучасних систем миттєвих повідомлень “Threema”, “Signal”, “Telegram” [1-4].

Таблиця 1

Порівняння рівня захищеності сучасних систем миттєвих повідомлень

Назва критеріїв захищеності сучасних систем обміну миттєвими повідомленнями	**Характеристика критеріїв рівня захищеності та індикатори загроз безпеці (“червоний-жовтий-зелений”) системи миттєвих повідомлень**		
	Threema	**Signal**	**Telegram**
Юрисдикція підприємства-розробника (знаходження під юрисдикцією Five Eyes)*	Швейцарія / “жовтий”	США/ “червоний”	США, Великобританія, ОАЕ/ “червоний”

Інфраструктурна юрисдикція (знаходження під юрисдикцією Five Eyes)*	Швейцарія / “жовтий”	США/ “червоний”	Великобританія, Сінгапур, США, Фінляндія/ “червоний”
Моніторинг (стеження) зі сторони уряду	Немає/ “зелений”	Немає “зелений”	Немає “зелений”
Звіт про прозорість	Так/ “зелений”	Так/ “зелений”	Ні “червоний”
Фінансування	Користувачі, Afinum Management AG “зелений”	Фонд свободи преси, Фонд Найта, Фонд Шаттлворта, Фонд відкритих технологій, Signal Фонд (Браян Ектон) / “зелений”	Павло Дуров “зелений”
Збір даних про користувачів	Номер телефону / “жовтий”	Мінімальні метадані, номер телефону/ “жовтий”	Номер телефону,IP-адреса, дата і час надсилання повідомлень/ “червоний”
Шифрування за замовчуванням	Так / “зелений”	Так / “зелений”	Тільки секретні чати / “червоний”
Криптографічні примітиви	Curse 25519 256/XSalsa20 256/Poly1305-AES128 “жовтий”	Curve25519&Kyber-1024/AES-256/HMAC-SHA256/512 “зелений”	RSA 2048/AES256/SHA-256 “жовтий”
Наявність відкритого коду додатку чи сервера	Ні, лише додатку/ “жовтий”	Так/ “зелений”	Ні, лише API “жовтий”
Можливість анонімної реєстрації у програмі	Так/ “зелений”	Ні / “червоний”	Ні / “червоний”
Можливість вручну добавляти контакти без використання сервера каталогів	Так (за допомогою Threema ID) / “зелений”	Ні / “червоний”	Ні / “червоний”
Можливість перевірки відбитків пальців користувачів	Так / “зелений”	Так / “зелений”	Ні / “червоний”
Можливість модифікації служби каталогів, щоб її не використати з метою MitM**	Ні / “червоний”	Ні / “червоний”	Ні / “червоний”
Хешування персональної інформації	Так/ “зелений”	Переважно так ,частково/ “жовтий”	Ні / “червоний”
Шифрування метаданих	Так / “зелений”	Так / “зелений”	Ні / “червоний”
Використання протоколу Transport Layer Security (TLS) та сертифікату для нього	Так / “зелений”	Так / “зелений”	Ні / “червоний”
Локальна автентифікація	Так / “зелений”	Так / “зелений”	Так / “зелений”
Шифрування повідомлення під час їх резервного копіювання у хмару	Так / “зелений”	Ні, виключено з резервних копій (iCloud/iTunes і Android) / “червоний”	Ні, виключено з резервних копій (iCloud/iTunes і Android) / “червоний”

Примітки. * **Five Eyes** — розвідувальний альянс, до якого входять такі країни: Австралія, Канада, Нова Зеландія, США та Велика Британія. Ці країни, з подібною системою загального права, є учасниками багатосторонньої угоди UKUSA, договору про спільну радіотехнічну розвідувальну діяльність. ****«Людина посередині» (Man-in-the-Middle, MitM)** — вид атаки, коли зловмисник здійснює атаку, щоб витягти інформацію з вашого з'єднання з інтернетом.

Розроблено авторами на основі: [1-4].

Отже, система "Threema" забезпечує найвищий рівень конфіденційності та безпеки завдяки шифруванню всіх даних, мінімальному збиранню інформації про користувача, можливості анонімної реєстрації та здійснення взаємної ідентифікації без сервера каталогів. Системи "Telegram" та "Signal" значно поступаються за рівнем безпеки у порівнянні із системою "Threema". Проте, найбільш слабкою ланкою з точки зору безпеки у всіх програмах обміну повідомленнями є сервер каталогів, який може додавати неавторизований пристрій, надавати іншому користувачеві доступ до облікового запису користувача або тимчасово зіставляти одного користувача з іншим. Вирішенням цієї проблеми є можливість вручну добавляти контакти та відповідно здійснювати взаємну ідентифікацію без використання сервера каталогів, сповіщення про зміну відбитка пальця користувача, а також наявність серверної частини системи з відкритим кодом.

Література

1. Проскурніна Н. В. Аналіз інтерактивних комунікаційних каналів зв'язку операторів роздрібної торгівлі зі споживачами. Інноваційно-інвестиційні процеси у маркетингу: монографія. Дніпро: Національна металургійна академія України. 2019. С. 255-269

2. Атака «Людина посередині» (MitM). URL: https://it-osvita.diia.gov.ua/task/item/21cadbcd-2818-4752-acd2-324d3af66ece;

3. Secure messaging APP. URL: https://www.securemessagingapps.com/

4. *What Is The Five Eyes Alliance?.* URL: https://www.forbes.com/advisor/business/what-is-five-eyes/

5. Білокуров О. О., Майба М. А., Шлома О. К., Дробяз М. О. Аналіз методів захисту інформації, що знаходять використання у сучасних месенджерах. Матеріали Восьмої Міжнародної науково-технічна конференція «Проблеми електромагнітної сумісності перспективних безпроводових мереж зв'язку (ЕМС-2022)» (м. Харків, Харківський національний університет радіоелектроніки, 24-25 листопада 2022). С. 71-73.