МЕТОДИ ЗАХИСТУ СУЧАСНИХ МЕСЕНДЖЕРІВ

Єгорова Н.В., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні месенджери стали повноцінними комунікаційними центрами, які крім обміну повідомленнями реалізують голосовий та відеозв'язок, обмін файлами чи веб-конференції. Тому безпека та надійність месенджерів є надзвичайно важливими аспектами їх використання. **Метою доповіді** є дослідження та обгрунтування методів захисту сучасних месенджерів. **В доповіді** надані результати аналізу вразливостей сучасних месенджерів, дослідження та порівняльного аналізу існуючих методів та засобів захисту [1]. Найактуальнішими вразливостями месенджерів є такі [2]:

1. Витік даних. Зловмисник отримує максимальний доступ до конфіденційної інформації месенджера шляхом перехоплення відправлених повідомлень, вилучення даних з хмари чи успішної автентифікації.

2. Розкриття місцезнаходження.

3. Вразливість коду або компрометуюче програмне забезпечення. Зловмисник може отримати повний контроль над вашим пристроєм, залишаючись непоміченим.

Безпека месенджерів забезпечується використанням спеціальних методів захисту [2]:

1. Наскрізне шифрування. Забезпечує конфіденційність при передачі повідомлень у месенджері.

2. Відкритий вихідний код. З його допомогою можна проводити комплексний аудит безпеки для виявлення та усунення слабких місць.

3. Шифрування резервних копій у хмарі. Не дозволяє зловмиснику успішно атакувати хмарну інфраструктуру та виток конфіденційної інформації.

4. Підтримка однорангового з'єднання. Ця функція виключає участь третьої сторони, оскільки надіслані повідомлення надходять безпосередньо на пристрій адресата.

5. Використання двофакторної автентифікації.

Для забезпечення високого рівня протидії атакам необхідно використовувати комплексний підхід до забезпечення безпеки, що дозволить корпоративним і приватним користувачам мінімізувати ризики.

Список літератури

1. Арчакова А.І., Сєвєрінов О.В. (2019). Аналіз забезпечення конфіденційності інформації в сучасних мессенджерах. *Комп'ютерні та інформаційні системи і технології.*

2. Jain V., Sahu D.R., Singh Tomar D. An Approach to Identify Vulnerable Features of Instant Messenger. 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP). 2020. P. 71-80. DOI: https://doi.org/10.1109/ISEA-ISAP49340.2020.235003.

3. Найбезпечніші месенджери 2022 року [Електронний ресурс] – URL: https://gloss.ua/ua/lifestyle/139268-najbezpechnishi-mesendzheri-2022-roku.