УДК 004.49
Нікітченко С.О.[1] , Скрупський С.Ю.[2]
[1] студ. гр. КНТ-514м НУ «Запорізька Політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

КІБЕРЗАГРОЗИ В МЕСЕНДЖЕРАХ: АНАЛІЗ ВРАЗЛИВОСТЕЙ ТА МЕТОДИ ЇХ ЕКСПЛУАТАЦІЇ

Сучасні месенджери є ключовими засобами комунікації, що робить їх привабливими цілями для кіберзлочинців. Основні типи атак включають фішинг, перехоплення повідомлень, соціальну інженерію, шкідливі програми та атаки на конфіденційність, що становлять серйозну загрозу для безпеки користувачів. Тому метою даної роботи стало розглянути механізми цих атак, їхні наслідки та ефективні методи захисту, зокрема end-to-end шифрування, багатофакторну автентифікацію, аналіз поведінкових аномалій та підвищення обізнаності користувачів у сфері кібербезпеки.

У даній науковій роботі було проаналізовано питання безпеки у месенджерах та виділено основні загрози, які можуть становити ризик для користувачів:

– фішингові атаки – спроби виманювання конфіденційних даних через підроблені повідомлення та сайти;

– перехоплення даних (Man-in-the-Middle, MITM) – це тип атак, що дозволяє зловмисникам не лише прослуховувати комунікацію між двома сторонами, а й потенційно змінювати або підмінювати передану інформацію без відома учасників зв’язку.

– використання вразливостей у протоколах шифрування – недоліки у реалізації криптографічних алгоритмів, які можуть дозволити зловмисникам розшифрувати передані дані;

– соціальна інженерія – це сукупність психологічних методів маніпуляції, спрямованих на введення жертви в оману з метою отримання доступу до облікових записів, конфіденційної інформації або примушення до виконання певних дій, вигідних зловмиснику [1].

Атаки у месенджерах можуть загрожувати безпеці користувачів та їхній особистій інформації, включають фішинг, перехоплення повідомлень (MITM), соціальну інженерію, шкідливі програми та атаки на конфіденційність. У таблиці 1 наведеніо приклади основних атак та їх опис, що дозволяє краще зрозуміти механізми загроз та їх вплив на користувачів [2].

Серед найбільш поширених методів атак можна виділити створення фішингових сайтів, що імітують справжні месенджери. Окрім цього, існує ризик атак через заражені файли, а також експлуатацію слабких паролів

користувачів, що може призвести до несанкціонованого доступу до їхніх облікових записів.

На рисунку 1 представлена схема проведення фішингової атаки, а у таблиці 1 – приклади основних атак та їх опис.

Таблиця 1 – Приклади основних атак та їх опис

Вид атаки	Опис
Фішинг	Шахрайство, спрямоване на викрадення даних користувачів
MITM	Перехоплення комунікації між двома сторонами
Злом шифрування	Використання вразливостей для розшифрування повідомлень

Щоб ефективно захистити себе від можливих кіберзагроз під час використання месенджерів і зберегти конфіденційність своїх даних, доцільно використовувати такі ключові заходи безпеки, які допоможуть мінімізувати ризики несанкціонованого доступу, втрати інформації та інших небажаних наслідків:

– використовувати багатофакторну автентифікацію (2FA);

– застосовувати сучасні алгоритми шифрування (наприклад, Signal Protocol);

– перевіряти автентичність повідомлень та посилань перед відкриттям;

– шифрування повідомлень;

– використання унікальних паролів;

– регулярне оновлення програмного забезпечення допомагає усувати виявлені вразливості та покращувати рівень безпеки;

– застосовувати заходи для захисту від соціальної інженерії [3].

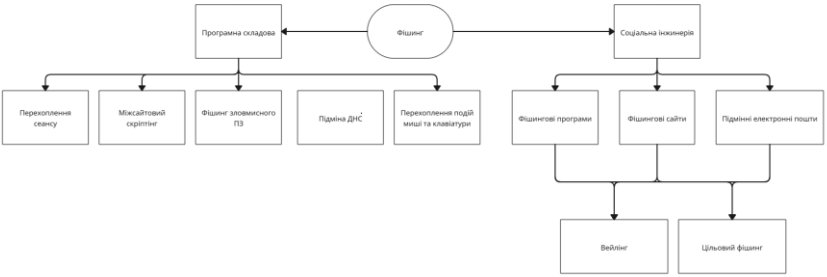

Рисунок 1 – Схема проведення фішингової атаки

Таким чином, кіберзагрози у месенджерах становлять значну небезпеку, яка потребує уваги як з боку користувачів, так і з боку розробників. Для зменшення ризиків необхідно використовувати сучасні методи захисту, такі як багатофакторна автентифікація, покращене шифрування даних та підвищення обізнаності користувачів щодо можливих атак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Smith, A. Messenger security: How encrypted chats can be compromised. / Smith, A. // Cyber Defense Review. - 2018. – Випуск 12 (4), P. 89-102. DOI: 10.1234/cdr.2018.004.

2. Zhang, Z., The Dark Forest: Understanding Security Risks of Cross-Party Delegated Resources in Mobile App-in-App Ecosystems. / Zhang, Z., Zhang, L., Yang, G., Chen, Y., Xu, J., & Yang, M. // IEEE Transactions on Information Forensics and Security. – 2024.

3. Національний координаційний центр кібербезпеки. Кіберзагрози у месенджерах та методи їх нейтралізації. Київ: НКЦК при РНБО України. 2021.