Секція 1

## МЕСЕНДЖЕРИ: ЗАГРОЗА КОНФІДЕНЦІЙНОСТІ ДЛЯ ДЕРЖАВНИХ СТРУКТУР

Подгорний Р. С.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Харченко В. С.

**Актуальність.** Сьогодні месенджери стали невід'ємною частиною повсякденного життя людей та використовуються у різних сферах, включаючи великий бізнес, банківський сектор та медицину. Також їх використання поширилося і на державні структури. Месенджери забезпечують швидке та зручне спілкування, але також можуть бути джерелом витоків конфіденційної та критичної інформації, що є значною загрозою безпеці країни.

**Метою** роботи є аналіз загроз, пов'язаних з використанням месенджерів у державних структурах, та запропонування рішення щодо використання месенджерів та серверів, які контролюються державою.

**Основні положення.** Месенджери, були створені з метою передачі інформації, і важливо враховувати, що державні службовці особисто можуть обмінюватися конфіденційною інформацією один з одним або залишати її в «нотатках» месенджерів. Необхідно враховувати, що в сучасних додатках часто присутні можливості використання різних датчиків смартфона.

Месенджери зазвичай збирають і зберігають такі дані: профіль користувача, список контактів користувача, історія листування, геолокацію користувача, дані пристроїв, дані активності.

Потенційні можливості негласного збору інформації. Сучасні месенджери часто отримують привілеї доступу до камери, мікрофона та різних датчиків пристроїв. Це означає, що потенційно вони мають можливість негласно збирати різні типи інформації [1], збереження фото та відео з галереї, фіксація місцеперебування, месенджер, потенційно, може збирати дані від датчиків телефону, інформацію про використання пристрою. У разі використання месенджерів в державних структурах, практично будь-які дані, які так чи інакше потрапляють до месенджера, можуть бути використані для компрометації безпеки держави.

У доповіді розглядаються додаткові ризики використання месенджерів держслужбовцями. До таких ризиків відносяться сервери, які розташовані в різних країнах світу, і відповідно підпорядковані законодавству цих країн, можливість зміни власників компаній, яким належать месенджери, достовірно не відомо, які дані збираються і як обробляються. У кого та який є фактичний доступ до зібраних даних, найбільш популярні месенджери мають повністю, або частково закритий код додатків та/або серверів.

Враховуючи обсяг інформації, яка збирається, або може збиратися месенджерами, зловмисники, або спецслужби іноземних держав, які отримають доступ до всієї цієї інформації, зможуть заволодіти таємною інформацією, скласти повні портрети держслужбовців та їх взаємозв'язки, з'ясувати маршрути пересування, графіки активності та підібрати експлойти для їх пристроїв. Що, своєю чергою, дасть можливість пошуку слабких місць для планування подальших атак.

У доповіді пропонується варіант розробки національного підконтрольного месенджера для використання держслужбовцями, та зберігання інформації на підконтрольних захищених серверах.. Одним із відповідних проєктів є «Matrix» - відкритий та вільний протокол для спілкування в реальному часі. Він може бути використаний для надсилання миттєвих повідомлень та файлів, аудіо- та відеозв'язку [2]. Сьогодні спілкування на базі протоколу «Matrix» вже випробувано у низці країн: у Франції для спілкування державних службовців [3], у збройних силах Німеччини [4].

**Висновки.** Найбільш безпечним та швидким варіантом розв'язання проблеми було б використання власних контрольованих месенджерів та серверів для зберігання даних, створених на базі чинних рішень з відкритим вихідним кодом. Одним із таких рішень, вже випробуваним у низці європейських країн, є «Matrix».

**Список літератури**

1. Твіт Фоад Дабірі. *Twitter.* URL – https://twitter.com/foaddabiri/status/1654856617723301888 (дата звернення: 7.10.23);
2. What is Matrix? *Matrix.* URL – https://matrix.org/ (дата звернення: 10.10.23);
3. «La messagerie instantanée des agents de l'État». *Modernisation.* URL – https://references.modernisation.gouv.fr/uploads/CP_TCHAP-699761.pdf (дата звернення: 10.10.23);
4. «Matrix» ist einheitlicher Messenger-Standard für die Bundeswehr. *Bwi.* https://www.bwi.de/magazin/artikel/open-source-matrix-ist-einheitlicher-messenger-standard-fuer-die-bundeswehr (дата звернення: 15.10.23).

**Відомості про автора**

Подгорний Руслан Сергійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», ruslanroool@gmail.com
Харченко Вячеслав Сергійович, завідуючий кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, v.kharchenko@csn.khai.edu