Герус В. А., магістрант,
Державний університект «Житомирська політехніка»

НЕОБХІДНІСТЬ ЗАСТОСУВАННЯ ШИФРУВАННЯ В ПРОГРАМАХ ОБМІНУ ПОВІДОМЛЕННЯМИ

В сучасному цифровому світі, де комунікація через Online Social Networks (OSNs) стала не лише зручною, але й невід'ємною частиною нашого щоденного життя, безпека особистих даних і конфіденційності стала найважливішою проблемою. З кожним днем зростає кількість онлайн-злочинів, пов'язаних з несанкціонованим доступом до особистої інформації, що відправляється через месенджери. У зв'язку з цим виникає необхідність у впровадженні надійних методів захисту, а шифрування в програмах обміну повідомленнями стає ключовим інструментом у забезпеченні безпеки та конфіденційності даних користувачів. В даній роботі буде розглянуто значення шифрування у програмах обміну повідомленнями та важливість його застосування в сучасному цифровому середовищі.

Сформулюємо основні проблеми під час передачі даних в месенджерах:

1. Загроза приватності.
2. Ризик перехоплення.
3. Недостатня безпека передачі.
4. Загроза кібератак .
5. Потенційні правові наслідки.

Помічено, що більшість користувачів соціальних мереж не мають достатньої обізнаності про ризики безпеки і конфіденційності, що необхідно враховувати при розробці рішень для протидії загрозам.

Загрози в соціальних мережах виникають, коли хакери та шахраї отримують доступ до особистої інформації та деталей користувача в Інтернеті. Шахраї, як правило, атакують облікові записи з низьким рівнем безпеки та користувачів, які не знають про небезпеку кібератак.

Найкращий спосіб запобігти ризикам соціальних медіа, які потрапляють у ваші цифрові двері, це знати, як їх помітити, і бути проактивним щодо своєї безпеки в Інтернеті. Наведемо кілька способів захисту від загроз у соціальних мережах, а саме, створення складного пароля, регулярне оновлення паролів, багатофакторна аутентифікація, регулярне оновлення програмного забезпечення, фільтрувати запити в друзів, блокувати рекламу, навчитися розпізнавати шахраївські схеми, фішингові атаки та інші види шахрайства, які можуть з'явитися у вас у повідомленнях або коментарях.

Що ви можете зробити, щоб краще захистити свої миттєві повідомлення від крадіжки чи витоку?

1. Увімкніть наскрізне шифрування (Наскрізне шифрування доступне в таких популярних програмах обміну повідомленнями, як WhatsApp, iMessage, Signal, Facebook Messenger і Telegram.)

2. Налаштуйте повідомлення на самознищення (Facebook і WhatsApp, дозволяють автоматично видаляти повідомлення після їх прочитання, а iMessage від Apple, дозволяють автоматично видаляти старі розмови, визначаючи часовий ліміт).

3. Двічі заблокуйте програми для чату (WhatsApp, Signal, Telegram і Facebook Messenger дозволяють встановити додатковий пароль для доступу до програми).

4. Захистіть свої профілі (Перевірте налаштування свого профілю, щоб дізнатися, хто може надсилати вам повідомлення та скільки інформації ви ділитеся публічно).

5. Перевірте резервні копії (ви повинні знати, де зберігаються ваші резервні копії та чи вони зашифровані).

Оскільки ми використовуємо програми обміну миттєвими повідомленнями для всього, вони є золотою жилою цінної інформації для кіберзлочинців. Дотримуючись п’яти описаних тут кроків, ви можете захистити свою конфіденційність і захистити свої повідомлення від крадіжки.

Список використаних джерел

1. Ebinezer M and Suresh B. 2015 Security Strategies for Online Social Networks International Journal of Computer Trends and Technology (IJCTT) 5(5).

2. Abdullah S M 2017 A Multi Secret Sharing Approach for Vulnerability Identificationin Social Media The 1st International Conference on Information Technology (ICoIT'17) p.45.

3. "Cryptography and Network Security: Principles and Practice" by William Stallings.