

# МОДЕЛЬ СОЦІАЛЬНОЇ КРИПТО-МЕРЕЖІ

М. М. Орел<sup>1, а</sup>, О. М. Барановський<sup>1</sup>

<sup>1</sup>Національний технічний університет України «Київський політехнічний інститут»

## Анотація

В роботі розглянута теоретична модель соціальної мережі з посиленням механізмом захисту конфіденційності. Розглянуті проблеми, які виникають при побудові такої мережі. Наведені методи вирішення поставлених задач.

**Ключові слова:** соціальна мережа, криптографія, конфіденційність інформації.

## Вступ

Соціальні мережі на сьогодні є одним з основних методів комунікацій, пошуку зв'язків та обміну як загальнодоступною так і конфіденційною інформацією. Проте зі зростанням об'ємів інформації, зростає й загроза порушення найважливішої властивості – конфіденційності. Метою роботи було забезпечення цілісності та конфіденційності при обміні та зберіганні інформації у соціальній мережі.

## 1. Основні інформаційно-комунікаційні блоки соціальних мереж

Соціальна мережа - інтерактивний багатокористувачський веб-сайт, контент якого наповнюється самими учасниками мережі. Такий ресурс являє собою автоматизоване соціальне середовище, що дозволяє спілкуватися групі користувачів, об'єднаних спільними інтересами, слідкувати за життям користувачів.

Саме тому, проаналізувавши основні ресурси, було виділено основні інформаційні блоки що зустрічаються у кожній соціальній мережі. Такі блоки можна назвати базовими і вони є найбільш важливими в процесі моделювання мережі з посиленими механізмами захисту.

Далі приведений перелік інформаційно-комунікаційних блоків:

- Профіль – сторінка, яка містить інформацію про користувача та зазвичай містить мікроблог. Профіль може переглядатись усіма користувачами мережі, яким надав права на це власник профілю.
- Особиста переписка – зазвичай даний блок реалізований як засіб для комунікації між двома користувачами.
- Публічні сторінки – це сторінка, в якій усі бажаючі можуть залишати свою думку під певними записами.

Згідно з даними блоками було розроблено моделі функціонування захищеної соціальної мережі.

## 2. Принципи функціонування системи

Основна ідея соціальної мережі з посиленням механізмом захисту конфіденційності полягають у наступному:

- Сервер зберігає лише зашифровану інформацію. Доступ до відкритих даних має лише власник цих даних та довірені особи.
- Все шифрування відбувається на стороні клієнта.
- Для шифрування використовуються алгоритми симетричного шифрування (AES), для обміну ключами – алгоритми асиметричного шифрування (RSA).
- Публічні сторінки мають свої ключі (відкриті, закриті), які зберігаються у власника.
- Сервер повинен надавати відкриті ключі і гарантувати їх ідентичність.

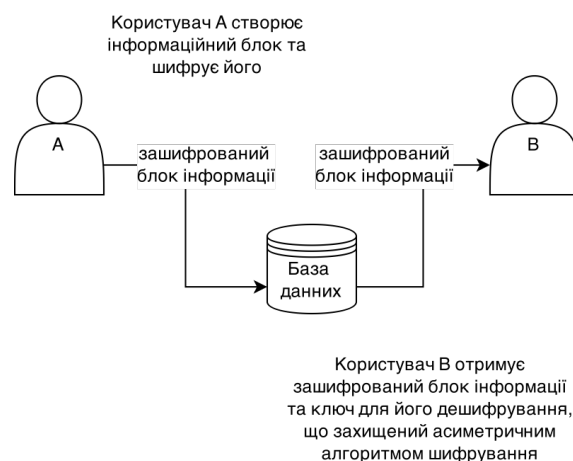


Рис. 1. Загальна схема соціальної мережі з посиленням механізмом захисту конфіденційності.

Таким чином скомпроментований сервер не буде нести загрози так як дані, що він зберігає, знаходяться в зашифрованому вигляді. Саме це і реалізовує принцип захищеності.

Розробка моделей відбувалась з урахуванням тих факторів, що у будь який час  $t$ , доступ до даних має

<sup>а</sup>mail.ormark@gmail.com

$n$  користувачів, а у будь який інший момент  $t + 1$  кількість цих користувачів може зрости чи зменшитись. Якщо новий користувач отримує доступ до даних у момент  $t$ , він повинен мати також можливість переглянути дані у моменти  $t - 1, t - 2 \dots t_0$ .

### 3. Моделі функціонування інформаційно-комунікаційних блоків

Кожен користувач системи має свій відкритий та закритий ключ  $\{e, n\}, \{d, n\}$  відповідно до алгоритму RSA, та ключ  $k$  для AES. Кожен користувач має список друзів, що являє собою список відкритих ключів тих користувачів, яким він довіряє –  $\{e_1, n_1\}, \{e_2, n_2\} \dots \{e_N, n_N\}$ .

Розглянемо моделі наступних інформаційних блоків детальніше.

**Профіль.** Користувач  $A(k, \{e, n\}, \{d, n\})$  створює профіль –  $P$ . Шифрує профіль за допомогою ключа  $k$  та алгоритму AES, в результаті чого отримує зашифрований профіль  $F$ . Наступним кроком для кожного користувача зі списку друзів за допомогою відкритого ключа шифрує ключ  $k$  та зберігає його та повідомлення у базу у наступному вигляді  $[F, \{RSA_{e_1}(k), e_1\}, RSA_{e_2}(k), e_2, \dots, \{RSA_{e_N}(k), e_N\}]$  (рис. 2). При додаванні нового користувача до списку друзів він дописує до запису профілю новий масив  $\{RSA_{e_L}(k), e_L\}$ . У випадку видалення користувача зі списку друзів, власник профілю повинен перешифрувати профіль новим секретним ключем  $k_1$  та створити для кожного користувача зі списку друзів нові ключі  $\{RSA_{e_i}(k_1), e_i\}$ .

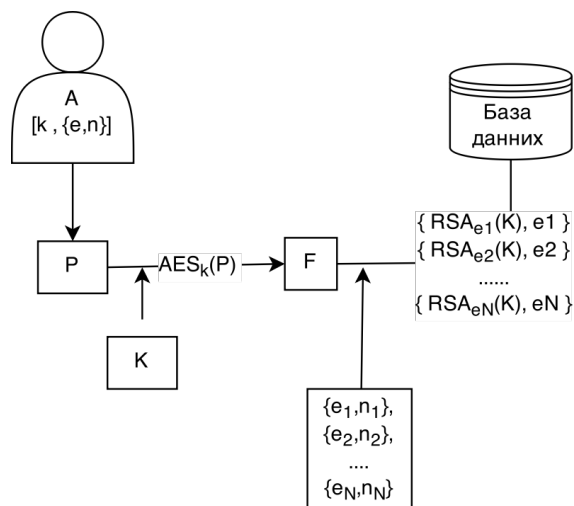


Рис. 2. Модель створення та шифрування профілю.

**Особиста переписка.** Користувач  $A(k, \{e, n\}, \{d, n\})$  хоче написати повідомлення користувачу  $B(k_1, \{e_1, n_1\}, \{d_1, n_1\})$ . Для цього користувач  $A$  генерує випадковий ключ  $m$  для конкретного повідомлення  $M$ . Шифрує повідомлення  $M$  за допомогою ключа  $m$  та алгоритму AES. Далі, за допомогою свого відкритого ключа шифрує ключ  $m - RSA_e(m)$ . Аналогічну операцію він проводить

і за допомогою ключа  $e_1$ , в результаті чого отримує  $RSA_{e_1}(m)$ . Далі зберігає данні у базу (рис. 3) у вигляді  $[AES_m(M), \{RSA_{e_1}(m), e_1\}, \{RSA_e(m), e\}]$ . Таким чином навіть якщо один ключ буде скомпроментовано, інша частина інформації буде захищена. Завдяки двом прикріпленим зашифрованим ключам  $m$ , дешифрування повідомлення може відбуватись як відправником, так і отримувачем.

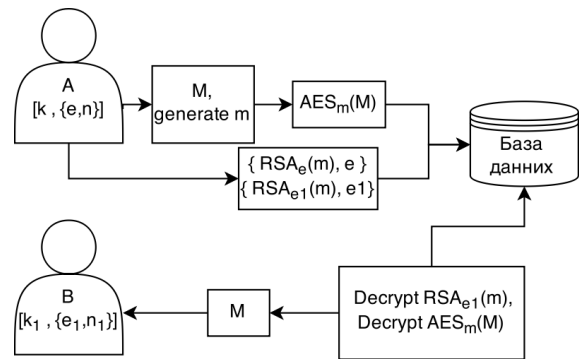


Рис. 3. Модель шифрування особистої переписки.

**Публічна сторінка.** Принцип реалізації механізму функціонування блоку «публічна сторінка» є близьким до «особистого профілю». Розглянемо даний механізм детальніше. Користувач  $A$  створює публічну сторінку та додає до неї ті публічні ключі, які належать «читачам» даної сторінки. Таким чином, він отримує список користувачів, які мають доступ до інформації, що буде публікуватись на даній сторінці. При обробці заявки нового користувача публічної сторінки він може відхилити запит та не додавати відкритий ключ нового користувача до системи. При створенні публічної сторінки користувач  $A(k, \{e, n\}, \{d, n\})$ , як власник сторінки, генерує ключі для даної сторінки  $P(k_p, \{e_p, n_p\}, \{d_p, n_p\})$ . Усі повідомлення, які він публікує на дану сторінку, він шифрує за допомогою алгоритму AES та ключа  $k_p$ , та додає до повідомлення зашифрований ключ  $k_p$  за допомогою алгоритму RSA відкритим ключем кожного з користувачів його публічної сторінки, а також його цей ключ шифрований його особистим відкритим ключем. У разі видалення користувача зі списку «читачів» публічної сторінки, власник сторінки повинен згенерувати новий ключ  $k_{p1}$  і надалі виконувати шифрування нових повідомлень за допомогою нового ключа. У разі додавання нового користувача (рис. 4)  $B(k_b, \{e_b, n_b\}, \{d_b, n_b\})$ , власник сторінки, після підтвердження заявки повинен до усіх старих повідомлень додати наступну криптограму  $RSA_{e_b}(k_p)$ . Це надасть змогу новому користувачу читати повідомлення, що були створені у даній публічній сторінці до його участі в цій сторінці.

### Висновки

Модель отримана у роботі є новим підходом для керування потоками інформації у соціальних мережах. Данна система може бути імплементована як у існуючих системах, так і може слугувати фундаментом для нових соціальних мереж. Дана модель

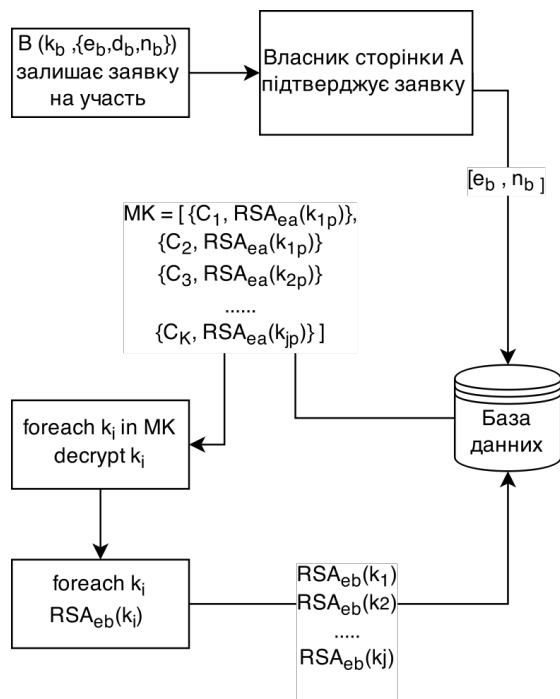


Рис. 4. Схема додавання нового користувача.

має широке застосування у різних сферах де існують інформаційні потоки, що базуються на соціальних мережах. Результатом роботи є три моделі функціонування соціальної мережі, відповідно до виділених інформаційно-комунікаційних блоків.

### Перелік використаних джерел

1. Hill, R. and Dunbar, R. Social Network Size in Humans. // Human Nature — 2002. — 53-72 с.
2. Scott, J Social Network Analysis: A Handbook 2nd Ed. // Newberry Park — 2000.
3. Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. // Communications of the ACM. — 1978. — 2-3 с.
4. Баричев С.Г., Гончаров В.В., Серов Р.Е. Стандарт AES. Алгоритм Rijdael //Основы современной криптографии. — 2002. — 30-35 с.