АНАЛІЗ АТАК ЧЕРЕЗ ЗАГРОЗУ ШИФРУВАННЯ ДАНИХ ЗА ДОПОМОГОЮ СХЕМИ ЕЛЬ-ГАМАЛЯ

Яхно С.С., В'юхін Д.О., Шулік П.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Атаки на шифрування за схемою Ель-Гамаля можуть становити серйозну загрозу для конфіденційності інформації, якщо не дотримано належного рівня криптографічної обережності.

В доповіді розглянуто докладний аналіз потенційних атак, що можуть бути застосовані проти схеми шифрування Ель-Гамаля, а також шляхи їх запобігання.

Метою доповіді є аналіз загроз, пов'язаних з використанням схеми Ель-Гамаля, зокрема, у контексті фішингових атак. Дослідження фокусується на фішингових атаках, які здійснюються через електронну пошту, оскільки цей вектор атаки є одним з найчастіше використовуваних [1].

Незважаючи на складну математичну основу, сучасні криптографічні бібліотеки роблять реалізацію схеми Ель-Гамаля відносно простою, що відкриває доступ до неї зловмисникам з різними технічними навичками. У долповіді зроблений порівняльний аналіз обраної схеми з іншими найбільш популярними алгоритмами.

Виходячи з проведеного аналізу схема Ель-Гамаля стає потенційним вибором зловмисника для атаки на електронну пошту з кількох причин. Її відносна простота реалізації, поєднана з високим рівнем безпеки при належному використанні, робить її привабливою для тих, хто прагне забезпечити конфіденційність своїх дій.

Шифрування за схемою Ель-Гамаля може бути надійним за умови правильного використання. Основні вразливості пов'язані з реалізацією, особливо з генерацією випадкових чисел, повторним використанням параметрів, та відсутністю CCA-захисту.

Для підвищення безпеки рекомендується:

- використовувати гібридні криптосистеми;
- захищати канали обміну ключами;
- застосовувати сучасні модифікації на основі еліптичних кривих.

Список літератури

1. Методики розслідування фішингових атак: [Електронний ресурс]. URL: https://openarchive.nure.ua/server/api/core/bitstreams/63036cab-5814-4191-ab31-5cf94f4da284/content».

2. Сєвєрінов О.В., Шевцов В.О., Сокол-Кутиловська А.С.. Аналіз сучасних методів атак на електронні ресурси органів управління. *Системи озброєння і військова техніка* 1 (2017): 65-68.

3. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. // IEEE Transactions on Information Theory. [1] — 1985. — Т. 31, № 4. — С. 469—472. [Електронний ресурс]. URL: https://bibliotekanauki.pl/articles/305780.