ВИКОРИСТАННЯ МЕХАНІЗМУ КІЛЬЦЕВОГО ПІДПИСУ ДЛЯ СИСТЕМ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

Курбатов О.С.
Харківський національний університет радіоелектроніки, Харків, Україна
Полуяненко М.О.
Харківський національний університет ім. В.Н. Каразіна, Харків, Україна

Традиційні системи голосування більше не являються ні безпечними ні ефективними (насправді вони ніколи такими не були): паперові бюлетені, псевдо-анонімність виборців, не прозорість у процесах підрахунку голосів, залежність процедури голосування від централізованої організації та ін. Фактично перераховані проблеми є найбільш критичними у існуючих системах голосування. В останні роки все більш активно поширюється процес переносу голосування у цифрову площину. Найбільш визначними прикладами таких систем є система електронного голосування у Естонії з 2005 року [1] та спроба використання подібної системи у Швецарії [2]. Однак існуючі рішення все ще мають велику кількість недоліків, до яких входять вразливості, що пов'язані з централізованою обробкою результатів голосування.

Метою доповіді є представлення системи електронного голосування, що може забезпечити прозорість усіх процесів у системі та цілісність історії голосування. Крім цього, описується концепція, яка здатна забезпечити дійсну анонімність користувачів в процесі голосування [3] і як така система голосування може працювати, забезпечуючи при цьому всі вказані властивості.

Побудована модель такої системи голосування показала, що вона має наступні властивості: є можливість забезпечення перевірки прав користувачів щодо можливості голосування (у випадку якщо ми маємо надійне джерело інформації щодо відкритих ключів та їх власників); досягається анонімність користувачів (третя сторона може тільки з низьким рівнем ймовірності визначити ким був відправлен голос); користувач може перевірити, що його голос був врахований правильно; забезпечується захист від подвійного голосування користувачем (користувач не може проголосувати два рази).

Також ми визначили, що у такій системі можливо забезпечити зміну голосу користувачем, і при цьому тільки останнє значення голосу буде враховуватись при підсумуванні результатів [4]. Однак у цьому випадку потрібно також розробити механізм захисту від спам-атак на мережу.

Список літератури

1. Zissis, D. and Lekkas, D., 2011. Securing e-Government and e-Voting with an open cloud computing architecture. Government Information Quarterly, 28(2), pp.239-251.

2. Maus, S., Peters, H. and Storcken, T., 2007. Anonymous voting and minimal manipulability. Journal of Economic Theory, 135(1), pp.533-544.

3. Maxwell, G. and Poelstra, A., 2015. Borromean ring signatures. https://pdfs.semanticscholar.org/4160/470c7f6cf05ffc81a98e8fd67fb0c84836ea.pdf

4. Van Saberhagen, N., 2013. CryptoNote v 2.0. https://cryptonote.org/whitepaper.pdf