

Забезпечення свободи волевиявлення в системі Інтернет-голосування (ІГ)

Володимир Вишняков¹, Михайло Пригара²

1. Кафедра інформаційних технологій, Київський національний університет будівництва та архітектури, УКРАЇНА, м. Київ, просп.. Повітрофлотський, 31,
E-mail: volodymyr.vyshniakov@gmail.com

2. Кафедра інформаційних технологій, Київський національний університет будівництва та архітектури, УКРАЇНА, м. Київ, просп.. Повітрофлотський, 31,
E-mail: misha_prigara@ukr.net

Анотація The experience of elections in Ukraine identified a number of opportunities for abuse that are able to distort the results.

In this paper we consider the question of how, based on the achievements of modern science and technology to build a voting system so as to fully overcome the challenges to free and fair elections

Ключові слова – голосування, дільниця, захист, шифрування, JavaScript, алгоритм Диффі-Хелмана, шифр Вернама.

Вступ

Досвід проведення виборів в Україні виявив ряд можливостей для зловживань, які здатні спотворювати результати виборів.

Проблема забезпечення дійсності волевиявлення виборців полягає в тому, що як на членів комісій, так і на самих виборців можна впливати погрозами, залякуванням або підкупом.

У роботі розглядаються питання про те як, спираючись на досягнення сучасної науки і техніки, побудувати систему голосування так, щоб у повній мірі подолати труднощі на шляху до вільних і чесних виборів.

Виклад основного матеріалу

Судячи з матеріалів останньої міжнародної конференції з питань електронного голосування EVOTE2014 <http://e-lected.blogspot.com>, яка відбулася в Австрії 28-31 жовтня 2014 року, бачимо, що в жодній країні ще не було створено цілком відкритої систему для дистанційного голосування.

Наша система побудована за принципом цілковитої відкритості [1], бо надається доступ для перегляду усіх без винятку файлів на сервері усім зацікавленим особам.

Таємниця голосів виборців забезпечується алгоритмами шифрування та новою технологією ІГ. У цій технології передбачено три етапи.

Протягом першого етапу (періоду) виборці повинні зареєструватись. Цей період охоплює майже весь час між виборами.

Протягом другого етапу, який настає за 1-2 тижні до виборів, виборець має прийти у відділ реєстрації і самостійно ввести пароль для ІГ. Цей період починається з запуску на серверах виборчих дільниць програми, яка буде діяти весь час до завершення ІГ. Програма одноразово завантажує з бази даних ІГ інформацію про виборців і продовжує роботу оперуючи тільки внутрішніми даними, а обмін даними відбувається через надійно захищений шифруванням інтерфейс.

З метою подолання впливу (підкупом або залякуванням) виборець може ввести два паролі, один – для справжнього голосування, а другий – для імітації голосування.

Завершується другий період за 1-2 доби до початку голосування формуванням списку учасників ІГ. Цей список надається виборчим дільницям для заборони учасникам ІГ голосувати традиційним методом. Пауза між другим і третім періодами потрібна для обробки списків виборців з врахуванням учасників ІГ, а також для завантаження на сервер електронних бюлетенів.

Третій період (саме ІГ) співпадає в часі зі звичайним голосуванням.

Виборцям для ІГ достатньо мати браузер та доступ до електронної пошти на довільному пристрої.

Програмне забезпечення створено на мовах HTML та JavaScript. На серверах встановлено операційну систему *OpenBSD* зі пакетом *NodeJS*.

Для захисту даних під час обміну між сервером та клієнтами використано криптографічні алгоритми Диффі-Хелмана та шифр Вернама. Стійкість захисту при цьому забезпечується надзвичайною складністю задачі дискретного логарифмування над елементами полів Галуа $GF(2^{503})$ та $GF(2^{743})$.

Під час випробувань нашої системи ІГ, яке проводилось у НТТУ «КПІ», НАУ та КНУБА, встановлено, що сервер здатен обслуговувати до 1800 виборців за годину. Відомо, що кількість виборців на дільницях в Україні (по законодавству) не може перевищувати 2500.

Висновок

Впровадження Інтернет технологій не тільки спрощує процедуру голосування для виборців, але за умов надання всім зацікавленим особам можливості повного контролю за роботою системи голосування в реальному часі, гарантує неможливість зловживань, які можуть стати перешкодою чесному волевиявленню громадян

Література

1. Вишняков В.М., Пригара М.П., Воронін О.В. Відкрита система таємного голосування// Управління розвитком складних систем. – 2014. – Вип. 20. – С. 110 – 115