

Для створення додатка було використано мову програмування С# і середовище розробки Visual Studio.

Застосування сучасних засобів розробки для створення моделей фізичних явищ сприятиме подальшому удосконаленню і модернізації цих моделей.

Список використаних джерел

1. Базурін В.М. Структура та інтерфейс програмних засобів для дослідження фізичних процесів на комп'ютерних моделях. *Інформаційні технології та засоби навчання*. 2014. № 6. URL: <http://journal.iitta.gov.ua/index.php/itlt/article/view/1137#.VOOfzui9p5I>

2. Bazurin V.M. Computer Models as a Means of Teaching Physics in Higher Educational Institutions. *ICT in Education, Research and Industrial Application: Integration, Harmonization and Knowledge Transfer* (Proceedings of the 14th International Conference, ICTERI 2018 (14–17 May 2018, Kyiv). Kyiv, 2018. P.469-472. URL: <http://ceur-ws.org/Vol-2105/10000469.pdf>

3. Пасько О. О., Однодворець Л. В. Фундаментальний фізичний експеримент у навчанні фізики : навчальний посібник. – Суми : Сумський державний університет, 2021. – 121 с.

КРИПТОГРАФІЧНИЙ ЗАХИСТ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

КАТЕРИНА ЗБИЦЬКА,

студентка І курсу 9 м групи,

Державний торговельно-економічний університет,

м. Київ, Україна

ТЕТЯНА САВЧЕНКО,

доцент кафедри інженерії програмного забезпечення

та кібербезпеки,

Державний торговельно-економічний університет,

м. Київ, Україна

(orcid.org/0000-0002-8884-5360)

Голосування є важливим етапом у прийнятті ключових моментів для народу в демократичній державі. У зв'язку зі стрімким розвитком технологій, а також змінами у політичному стані країни високої

популярності набуває можливість електронного голосування й інтерпретувати таке поняття можна у двох аспектах [1]:

- змістовному (процес прийняття значущих рішень у політичних та юридичних моментах населення);
- формальному (процес фіксування волевиявлення виборців, при використанні електронних технологій).

Можливість приймати важливі для держави та народу рішення вимагає надійного захисту зі сторони кібербезпеки. В цьому випадку можуть бути застосовані наступні методи захисту.

Шифрування даних

Для віддаленого електронного голосування у виборців існують сучасні технологічні засоби – комп'ютер чи телефон. Підключення відбувається за допомогою Інтернет-провайдерів і до провайдерів серверної сторони за допомогою Інтернет. Серверна частина складається із двох підсистем: Підсистеми А, яка відповідає за збір зашифрованих бюлетенів, та Підсистеми Б, яка дешифрує бюлетені, підраховує та архівує голоси, генерує результати. TLS, так само як і попередник що був до нього SSL – це криптографічні протоколи, завдяки яким забезпечується захист даних при передачі між вузлами в мережі Інтернет [2]. Вони обидва використовують декілька видів шифрування для різних цілей. Так, асиметричне шифрування використовується для автентифікації, симетричне – для конфіденційності.

Сліпий цифровий підпис

Протокол сліпого підпису дозволяє забезпечити дотримання принципу таємного голосування. Громадянин отримує можливість верифікувати свою особу за допомогою електронного підпису, залишаючись анонімним для виборчих комісій і всіх третіх осіб [3].

Роботу алгоритму сліпого підпису можна представити у вигляді наступної послідовності дій:

- Виборча громада отримує документ для голосування в зашифрованому вигляді і передає його виборцям.
- Виборець ставить свій голос і відправляє документ, що надходить назад до виборчої громади.
- В свою чергу громада отримує підписаний документ і розшифровує його.

Описаний метод буде достатньо безпечним, оскільки на розшифрованому документі залишається підпис користувача без його особистих даних.

Аутентифікація користувача

Аутентифікація може відбуватися двома методами: за допомогою пароля та сертифіката\ключа. В першому випадку виборці

авторизуються за допомогою паролю. Перевагами такого методу є те, що він знайомий кожному і є нескладним в своєму використанні. З іншого боку, такий метод має і суттєві недоліки – слабкий рівень безпеки, оскільки пароль можна підглядіти, вгадати, передати сторонній особі, застосувати технічні засоби для злому.

В свою чергу, використання сертифікату\ключа для аутентифікації користувача є більш надійним та безпечним способом входу, оскільки інформація зберігається на цифровому носії, а не в пам'яті користувача. Серед недоліків може бути складність у використанні такого методу або втрата самого носія з ключем.

Proof-of-Work

Використання блокчейн технологій в електронному голосуванні, ще не набуло активного використання, але сприяє надійному захисту цілісності даних. Одним із алгоритмів запобігання підробки блоків є Proof-of-Work (PoW).

Proof-of-Work (в перекладі з англ. «Доказ роботи») – це алгоритм, за допомогою якого до блокчейну додається новий блок, що верифікує єдину версію реєстру в кожній з його копій, що зберігають окремі коди [4]. Головна мета цього методу полягає в тому, щоб швидко перевірити великий обсяг даних в короткий термін, виконуючі доволі складне та тривале завдання. Такий метод доцільно використовувати для проведення електронного голосування та обробки його результатів.

Mixnets

MixNet – це технологія, яка допомагає зберігати конфіденційність і безпеку інформації, що надсилається через Інтернет. Це робиться шляхом змішування даних з різних джерел перед тим, як відправити їх до місця призначення, що ускладнює пошук джерела та призначення даних стороннім особам. На рисунку 1 наведено приклад застосування даного методу [5, 6].

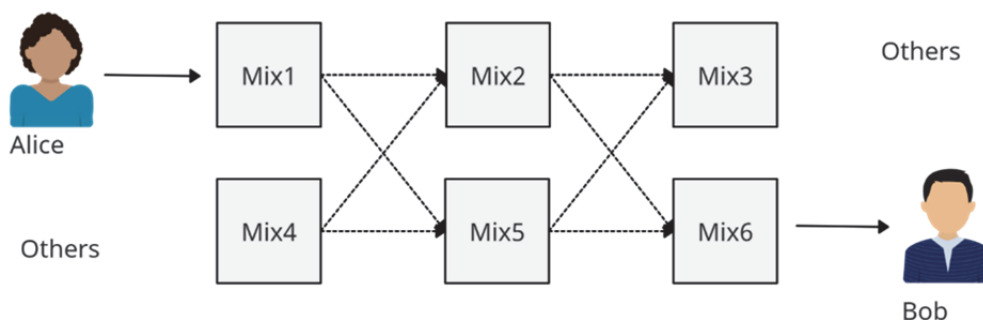


Рис. 1. Застосування методу mixnets

Застосування методів криптографічного захисту для електронного голосування є важливим етапом під час проведення виборів. Забезпечення конфіденційності та цілісності голосів є найважливішою складовою проведення електронного голосування. Саме тому застосування декількох методів криптографічного захисту є більш надійним способом, ніж використання лише одного конкретного метода. Так, виходячи з раніше описаних методів, поєднання таких криптографічних заходів як Proof-of-Work та MixNet, може не тільки забезпечити додаткову анонімність голосів виборців, а ще й відслідковувати несанкціоновані зміни неавторизованих користувачів. Отже, розглянуті методи можуть бути використані окремо або в поєднанні для створення комплексної системи захисту електронного голосування. Проте, важливо також враховувати не лише технічні аспекти, а й соціальні та правові, щоб забезпечити повну довіру до електронного голосування.

Список використаних джерел

1. Гусаревич Н. Електронне голосування: концептуальні підходи. – Аспекти публічного управління. – Том 9, № 4, 2021. – С. 104–110. – DOI: <https://doi.org/10.15421/152142>
2. Що робить TLS? – URL: <https://vtrata.zapisi.cx.ua/ukraincyam/shho-robit-tls.html>
3. Culnane C., Ryan P.Y., Schneider S., Teague V. vVote: a Verifiable Voting System. – DOI: <https://doi.org/10.48550/arXiv.1404.6822>
4. Що таке алгоритм Proof-of-Work (PoW)? – URL: <https://forklog.com/cryptorium/chto-takoe-proof-of-work-i-proof-of-stake>
5. What Is a MixNet and How Does It Work? – <https://www.makeuseof.com/what-is-a-mixnet/>
6. A simple introduction to mixnets. – <https://www.constructiveproof.com/posts/2020-02-17-a-simple-introduction-to-mixnets/>