ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І.І.МЕЧНИКОВА
(повне найменування вищого навчального закладу)

Факультет математики, фізики та інформаційних технологій
(повне найменування інституту, назва факультету (відділення))

Кафедра математичного забезпечення комп'ютерних систем
(повна назва кафедри (предметної, циклової комісії))

Дипломна робота

на здобуття ступеня вищої освіти «магістр»
(освітньо-кваліфікаційний рівень)

на тему: Система таємного електронного голосування

The system of secret electronic voting

Виконав: студент денної форми навчання
спеціальності 123 – Комп'ютерна інженерія
(шифр і назва напряму підготовки, спеціальності)
Тарасов Артур Ігорович
(прізвище, ім'я, по-батькові)
Керівник к.ф.-м.н, доцент Шпінарева І.М.
(науковий ступінь, вчене звання, прізвище та ініціали, підпис)

Рецензент к.техн.н., доцент Левченко А.О.
(науковий ступінь, вчене звання, прізвище та ініціали)
Рецензент к.техн.н., доцент Гришин С.І.
(науковий ступінь, вчене звання, прізвище та ініціали)

Рекомендовано до захисту:
Протокол засідання кафедри
№_____ від «___»_____ 2019 р.

Завідувач кафедри
_____ Є.В. Малахов
(підпис) (прізвище, ініціали)

Захищено на засіданні ЕК № ___
протокол № __ від «___» ____ 2019 р.
Оцінка _____/_____/_____
(за національною шкалою, шкалою ECTS, бали)
Голова ЕК
_____ О.О. Арсірій
(підпис) (прізвище, ініціали)

Одеса - 2019

АНОТАЦІЯ

Мета дипломної роботи – підвищення безпеки криптографічного захисту системи електронного голосування шляхом модифікації протоколу голосування з використанням технології блокчейн.

Під час дослідження здобуто знання та навички технології блокчейн. Виявлено переваги реалізації системи електронного голосування з застосуванням технології блокчейн. У дипломній роботі розроблені вимоги до системи електронного голосування та запропонована модифікація протоколу електронного голосування на основі блокчейн.

Використано найсучасніші методи та алгоритми криптографічного захисту, що забезпечують високий рівень стійкості та головні принципи протоколу електронного голосування. Алгоритм створення хеш-образу bcrypt забезпечує надійний захист пароля користувача у системі з додаванням «солі», що ускладнює обчислення хеш-образу. Алгоритм хешування SHA256, призначений для знаходження хеш-образу під час майнинга блока. Створення ЕЦП виконується криптографічним алгоритмом ECDSA на основі еліптичної кривої.

Запропонована модифікація забезпечує більш швидкий процес голосування та відповідає усім вимогам протоколу електронного голосування. Забезпечується анонімність та таємність голосування.

Спроектована система з використанням протоколу електронного голосування з застосуванням технології блокчейн. Голосуванням запропонованої системі є створення транзакції на адресу кандидата та майнинга блока, що забезпечує цілісність даних та можливість перевірити свій голос. Також кожен виборець може споглядати за виборами в режимі онлайн.

АННОТАЦИЯ

Цель дипломной работы – повышение безопасности криптографической защиты системы электронного голосования путем модификации протокола голосования с использованием технологии блокчейн.

Во время исследования приобретены знания и навыки технологии блокчейн. Выявлены преимущества реализации системы электронного голосования с применением технологии блокчейн.

В дипломной работе разработаны требования к системе электронного голосования и предложена модификация протокола электронного голосования на основе блокчейн.

Использованы современные методы и алгоритмы криптографической защиты, обеспечивающие высокий уровень устойчивости и основные принципы протокола электронного голосования. Алгоритм создания хеш-образа bcrypt обеспечивает надежную защиту пароля пользователя в системе с добавлением «соли», что затрудняет вычисления хэш-образа. Алгоритм хеширования SHA256, используется для нахождения хэш-образа во время майнинга блока. Создание ЭЦП выполняется криптографическим алгоритмом ECDSA на основе эллиптической кривой.

Предложенная модификация обеспечивает более быстрый процесс голосования и отвечает всем требованиям протокола электронного голосования. Обеспечивается анонимность и секретность голосования.

Спроектирована система с использованием протокола электронного голосования на основе технологии блокчейн. Голосованием предложенной системе является создание транзакции в адрес кандидата и майнинг блока, что обеспечивает целостность данных и возможность избирателю проверить свой голос. Каждый избиратель может наблюдать за выборами в режиме онлайн.

ABSTRACTION

The aim of the master theses work increasing the security of cryptographic protection of the electronic voting system by modifying the voting protocol using blockchain technology.

During the research, knowledge and skills of blockchain technology were acquired. The advantages of implementing an electronic voting system using blockchain technology have been identified. In the thesis, the requirements for the electronic voting system are developed and a modification of the electronic voting protocol based on the blockchain is proposed.

Modern methods and algorithms of cryptographic protection, which provide a high level of stability and the basic principles of the electronic voting protocol, are used. The bcrypt hash algorithm provides reliable protection of the user's password in the system with the addition of “salt”, which makes it difficult to calculate the hash image. SHA256 hash algorithm is designed to find a hash image during block mining. ECDSA algorithm based on cryptography using an elliptic curve.

The proposed modification provides a faster voting process and meets all the requirements of the electronic voting protocol. Anonymity and secrecy of the vote is ensured.

The system was developed using the electronic voting protocol based on blockchain technology. Voting process of the proposed system is the creation of a transaction in the address of the candidate and mining block, provides data integrity and the ability to check your vote. Also, each voter can observe the elections online.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ І ТЕРМІНІВ

ЕЦП – електронно-цифровий підпис.

СЕГ – система електронного голосування.

ЦВК – центральна виборча комісія.

Peer-to-peer (P2P) – це однорангова, децентралізована комп'ютерна мережа, заснована на рівних правах усіх учасників.

Хешування – це перетворення вхідного масиву даних довільної довжини у вихідний рядок фіксованої довжини. Такі перетворення також називаються хеш-функціями або функціями згортки, вхідний масив – прообразом, а результати перетворення – хешем.

Хеш-функція – легко обчислювана функція, яка перетворює вхідне повідомлення довільній довжини (прообраз) в повідомлення фіксоване довжини (хеш-образ), для якої не існує ефективного алгоритму пошуку колізій.

ВСТУП

Всеохоплюючий розвиток інформаційних систем створює умови для розробки і впровадження сучасних інформаційних засобів, що дозволяють автоматизувати, і, тим самим, більш ефективно реалізовувати процеси управління. У той же час, у зв'язку зі зростаючою складністю інформаційних систем і використовуваних в них інформаційних технологій, зростає обсяг вимог, що до них висовуються.

Одним з таких процесів, які необхідно автоматизувати, є проведення таємного голосування, наприклад, на раді акціонерів будь-якої великої компанії, при голосуванні в великих компаніях, що мають розподілену структуру, в будь-якій організації, де періодично проводяться голосування, в тому числі в навчальних закладах при проведенні поточних виборів професорсько-викладацького складу. Крім того, великий інтерес являє собою можливість автоматизувати державні вибори різних рівнів. Саме тому більшість розробок на даний момент здійснюється в цьому напрямку.

Розвиток системи інтернет-голосування тільки починає набирати обертів. Переваги проведення виборів через мережу загального користування є очевидними. Серед них можна виділити:

– можливість дистанційної участі у виборах;
– конфіденційність волевиявлення виборця;
– можливість перегляду підрахунку голосів;
– економія часу виборця;
– відповідність до рекомендацій кодексу корпоративного управління;
– здійснення підрахунку голосів в більш короткі час;
– простота використання сервісу;

Метою дипломної роботи є підвищення безпеки криптографічного захисту системи електронного голосування шляхом модифікації протоколу голосування з використанням технології блокчейн.

Основну роль в забезпеченні безпеки у проектованій системі повинні грати напрацьовані і перевірені методи сучасної криптографії. Використання того чи іншого криптографічного протоколу або алгоритму має бути продиктовано необхідністю і обґрунтовано.

Об'єктом дослідження є процес захисту інформації в системі електронного голосування з використанням технології блокчейн.

Предметом дослідження є методи і способи підвищення безпеки криптографічного захисту систем електронного голосування з використанням технології блокчейн.

Для досягнення поставленої мети необхідно вирішити такі основні задачі:

1) дослідження протоколів електронного голосування;
2) огляд систем електронного голосування і області застосування;
3) дослідження криптографічних методів, використовуваних в системах електронного голосування;
4) модифікація протоколу електронного голосування з використанням технології блокчейн.

ВИСНОВКИ

У дипломній роботі було проведено дослідження протоколів електронного голосування та розроблено модифікацію протоколу електронного голосування з застосуванням технології блокчейн, що надає підвищений рівень безпеки криптографічного захисту системи електронного голосування, а також відповідає усім вимогам, що були поставлені у роботі.

Розроблено систему електронного голосування з використанням технології блокчейн, що надає виборцям можливість проголосувати анонімно з їх особистих пристроїв, зберігаючи таємність голосування та гарантовано лише один раз.

У рамках протоколу електронного голосування технологія блокчейн дозволяє з легкістю перевірити цілісність, верифікованність даних. Найсучасніші методи та алгоритми криптографічного захисту забезпечують високий рівень стійкості та головні принципи протоколу електронного голосування. За допомогою стійкого алгоритму хешування SHA256, що швидко обчислюється, здійснюється майнинг блока. Використано алгоритм електронного підпису на основі еліптичних кривих ECDSA, що надає якісний та перевірений метод захист інформації.

Систему електронного голосування створено з використанням мови програмування JavaScript та її фреймворків Vue, Express, що базується на платформі Node.js. У якості централізованої бази даних, що містить інформацію про голосування, кандидатів, а також користувачів системи, обрано NoSQL документоорієнтовану MongoDB.

Створена система, що складається з веб-додатку, є універсальним з точки зору використовуваного для доступу до нього пристроїв (мобільного телефону, планшета, персонального комп'ютера з виходом в Інтернет), що робить її працездатною на будь-який апаратно-програмній платформі і надає мобільність її користувачам.

ПЕРЕЛІК ПОСИЛАНЬ

1. Тлумачний словник Дмитрієва [Електронний ресурс] – https://dic.academic.ru/dic.nsf/dmitriev/807голосование.
2. Електронне голосування в Естонії. [Електронний ресурс] – https://ega.ee/wp-content/uploads/2016/08/eDem_infomaterjal_i-h22letamine_rus.pdf
3. Яркова, О. Н. Захищена система електронного голосування на основі криптографічних алгоритмів [Електронний ресурс] / О. Н. Яркова, А. А. Осіпова // Вісник УРФО. Безпека в інформаційній сфері,2014. Вип. № 2 (12). – С. 9-15.
4. Peer-to-peer [Електронний ресурс]. – Режим доступу: https://bitcoin.org/bitcoin.pdf.
5. Хеш-функції [Електронний ресурс]. – Режим доступу: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema9
6. Blockchain [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/335994/
7. Пірингові мережі. [Електронний ресурс]. – Режим доступу: http://dwl.kiev.ua /art//p2p/p2p-end.pdf
8. Належне хешування паролів. [Електронний ресурс]. – Режим доступу: https://www.securitylab.ru/analytics/427930.php
9. Алгоритми / Хеш-функція SHA-256. [Електронний ресурс]. – Режим доступу: https://medium.com/dtechlog/алгоритмы-хэш-функция-sha-256-9862302f942f
10. Еліптична криптографія. [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/191240/
11. Bitcoin in a nutshell – Cryptography. [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/319868/
12. Цифровий підпис. Еліптичні криві. [Електронний ресурс]. – Режим доступу: https://www.osp.ru/os/2002/07-08/181696/
13. WebRTC. [Електронний ресурс]. – Режим доступу: https://webrtc.org/

14. Що таке Virtual DOM? [Електронний ресурс] – Режим доступу: https://habr.com/post/256965/ – 15.05.2018
15. Javascript-фреймворки: тенденції 2019 року. [Електронний ресурс]. – Режим доступу: https://habr.com/ru/company/plarium/blog/433926/
16. Введення. Що таке Vue.js? [Електронний ресурс] – Режим доступу: https://ru.vuejs.org/v2/guide/ – 03.01.2018
17. Початок роботи з Node.js. [Електронний ресурс] – Режим доступу: https://medium.com/devschacht/node-hero-chapter-1-239f7afeb1d1
18. Асинхронний http-клієнт, або чому многопоточність – зайве. [Електронний ресурс] – Режим доступу: https://habr.com/ru/post/81716/
19. SQL чи NoSQL. [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/ruvds/blog/324936/
20. Сильні і слабкі сторони NoSQL. [Електронний ресурс] – Режим доступу: https://habr.com/ru/sandbox/113232/
21. Mongoose. [Електронний ресурс] – Режим доступу: https://mongoosejs.com/
22. Тарасов А.И., Шпинарева И.М. Обзор методов электронного голосования.//XVI Всеукр. конференції студентів і молодих науковців «Інформатика, інформаційні системи та технології». Одеса, 2019 р.– С.198-200
23. Тарасов А.І., Шпінарева І.М. Система електронного голосування з застосуванням технології блокчейн// Захист інформації в інформаційно-комунікаційних системах: збірник тез доповідей ІІІ Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів «Захист інформації в інформаційно-комунікаційних системах», Львів, 2019р. – С.121