**Міністерство освіти і науки України**

**Національний технічний університет України «Київський політехнічний**

**інститут імені Ігоря Сікорського"**

**Факультет інформатики та обчислювальної техніки**

**Кафедра інформатики та програмної інженерії**

**Звіт**

З лабораторної роботи № 5 з дисципліни

«Протоколи й алгоритми електронного голосування»

“**Протокол Е-голосування з розділенням комісії на незалежні частини**”

| **Виконав(ла)** | *ІП-13 Бабіч Денис* |  |  |
| --- | --- | --- | --- |
|  | (шифр, прізвище, ім'я, по батькові) |  |  |

| **Перевірив** | *Нестерук А. О.* |  |  |
| --- | --- | --- | --- |
|  | (посада, прізвище, ім'я, по батькові) |  |  |

Київ 2024

**ЛАБОРАТОРНА РОБОТА № 5**

**Тема роботи**: Протокол Е-голосування з розділенням комісії на незалежні частини.

**Мета роботи**: Дослідити протокол Е-голосування з розділенням комісії на незалежні частини.

**Основне завдання:**

Змоделювати протокол Е-голосування з розділенням комісії на незалежні частини будь-якою мовою програмування та провести його дослідження. Для кодування повідомлень використовувати метод RSA, для реалізації ЕЦП використовувати алгоритм DSA.

Умови: В процесі голосування повинні приймати участь не менше 2 кандидатів та не менше 4 виборців. Повинні бути реалізовані сценарії поведінки на випадок порушення протоколу (виборець не проголосував, проголосував неправильно, виборець не має права голосувати, виборець хоче проголосувати повторно, виборець хоче проголосувати замість іншого виборця та інші).

На основі змодельованого протоколу провести його дослідження (Аналіз повинен бути розгорнутим та враховувати всі можливі сценарії подій під час роботи протоколу голосування):

1. Перевірити чи можуть голосувати ті, хто не має на це права.
2. Перевірити чи може виборець голосувати кілька разів.
3. Чи може хтось (інший виборець, ВК, стороння людина) дізнатися за кого проголосували інші виборці?
4. Перевірити чи може інший виборець чи стороння людина проголосувати замість іншого зареєстрованого виборця.
5. Чи може хтось (інший виборець, ВК, стороння людина) таємно змінити голос в бюлетені?
6. Чи може виборець перевірити, що його голос врахований при підведенні кінцевих підсумків?

**Виконання завдання:**

Для реалізації завдання було створено класи виборчих комісій, а саме центральної виборчої комісії, яка відповідає за реєстрацію користувачів, підбиття фінальних підсумків, а також звичайної виборчої комісії, яка займається прийомом голосів. Обидва класи зберігають проміжні та фінальні результати голосування у асоційованому масиві, де з кожним айді виборця асоціюється його голос (ще зашифрований, або вже ні). Також у центрального класу є метод для фінального об’єднання голосів після завершення процедури голосування. Код класу центральної виборчої комісії можна побачити на рисунках 1.1 – 1.4.



Рисунок 1.1 – Код класу центральної виборчої комісії



Рисунок 1.2 – Продовження коду класу центральної виборчої комісії

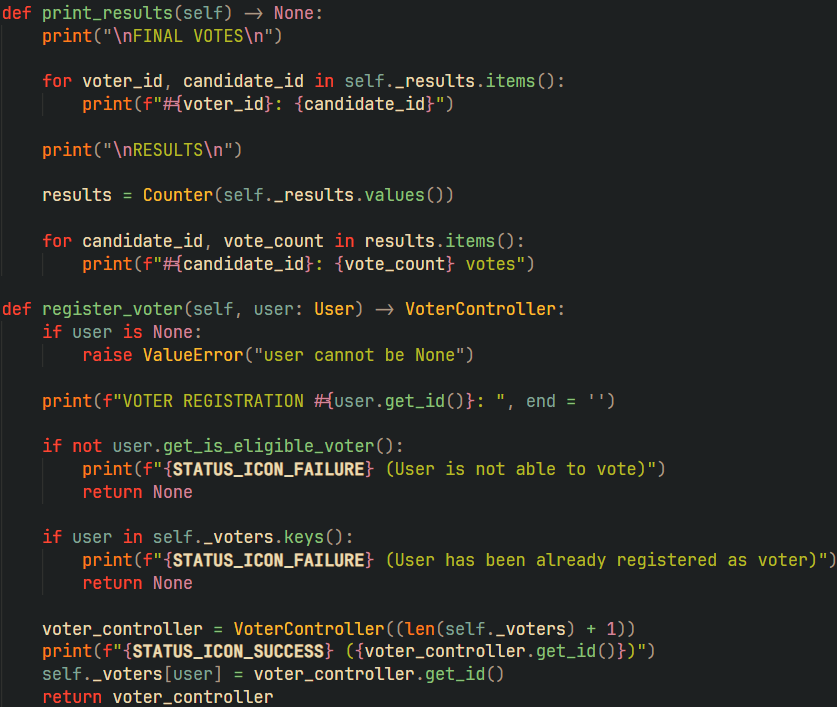


Рисунок 1.3 – Продовження коду класу центральної виборчої комісії



Рисунок 1.4 – Код генерації випадкового айді кандидата таким чином, щоб він завжди мав бодай 1 пару дільників

Код логіки розділення числа на пари множників наведено на рисунку 1.5.

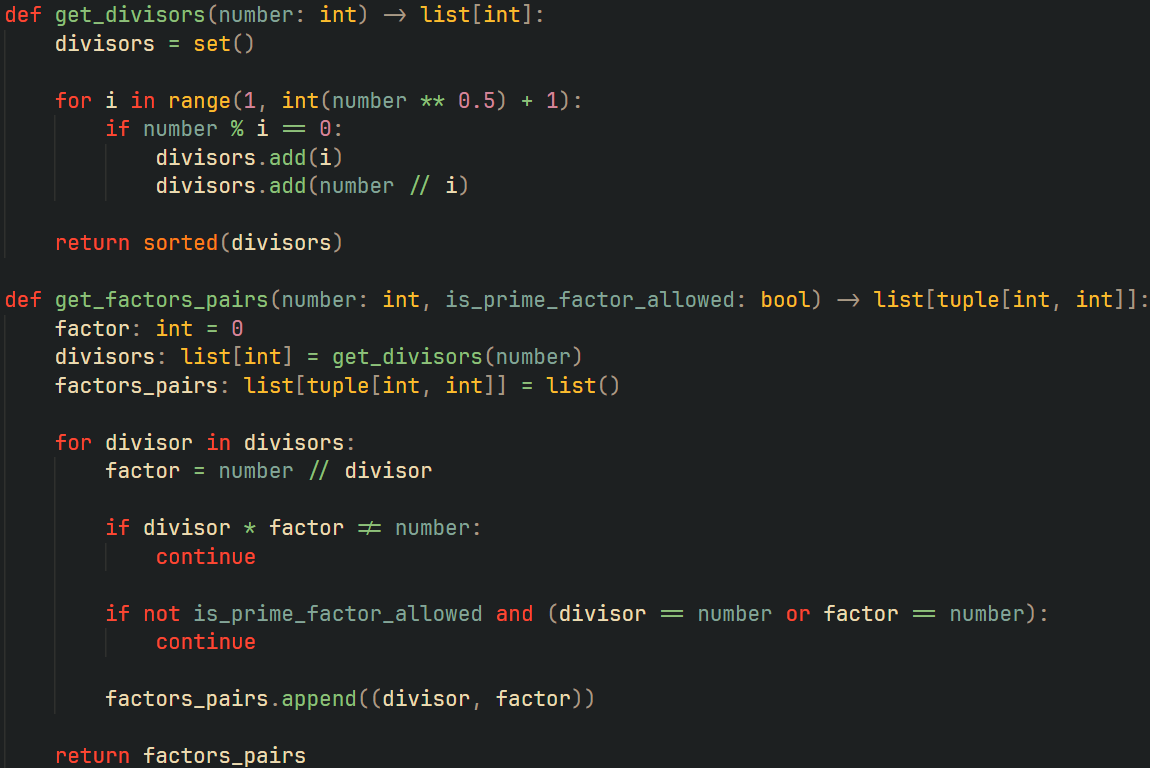


Рисунок 1.5 – Код знаходження дільників числа

Код класу локальної виборчої комісії наведено на рисунках 1.6 – 1.8.

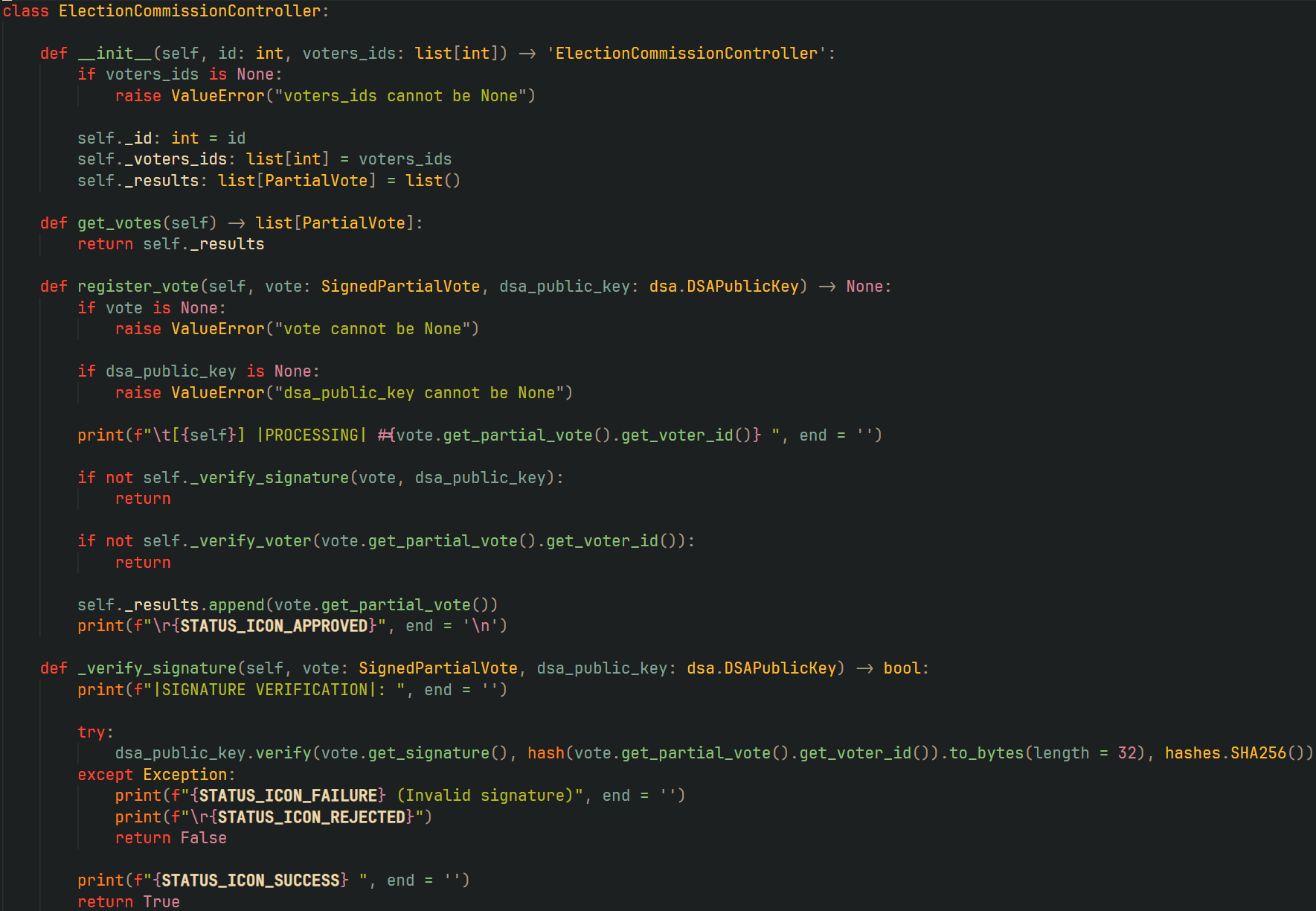


Рисунок 1.6 – Код класу виборчої комісії

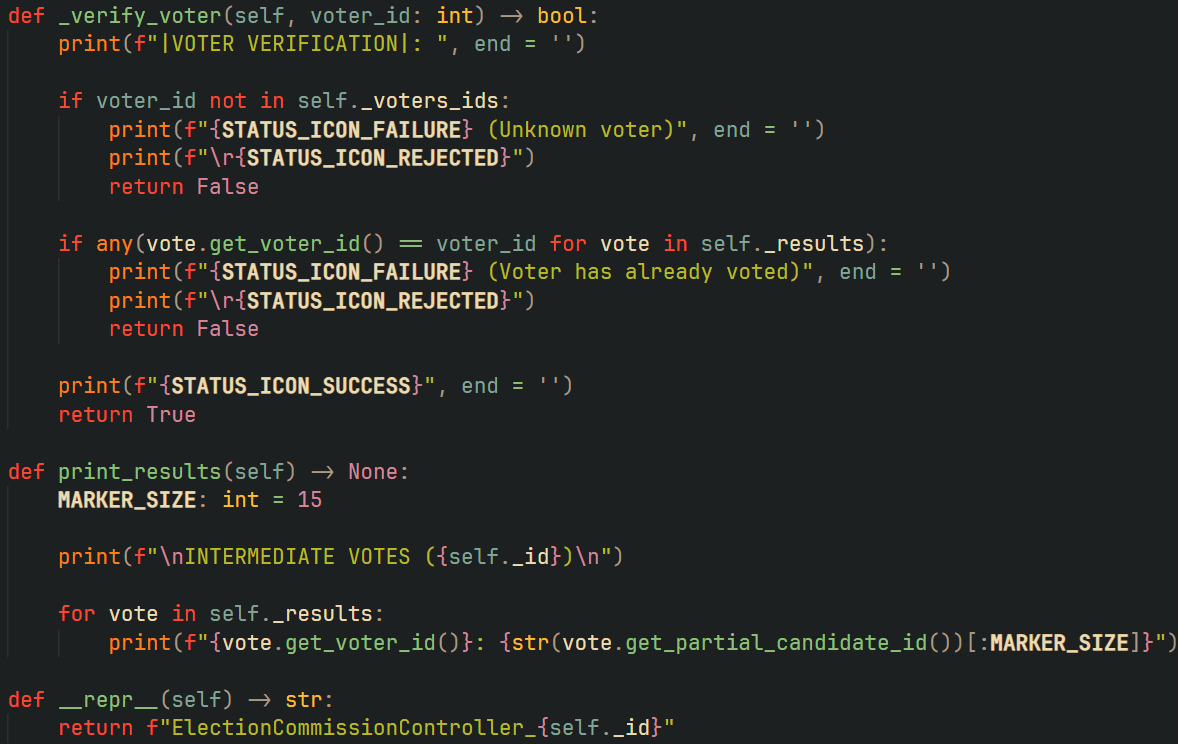


Рисунок 1.7 – Продовження коду класу локальної виборчої комісії

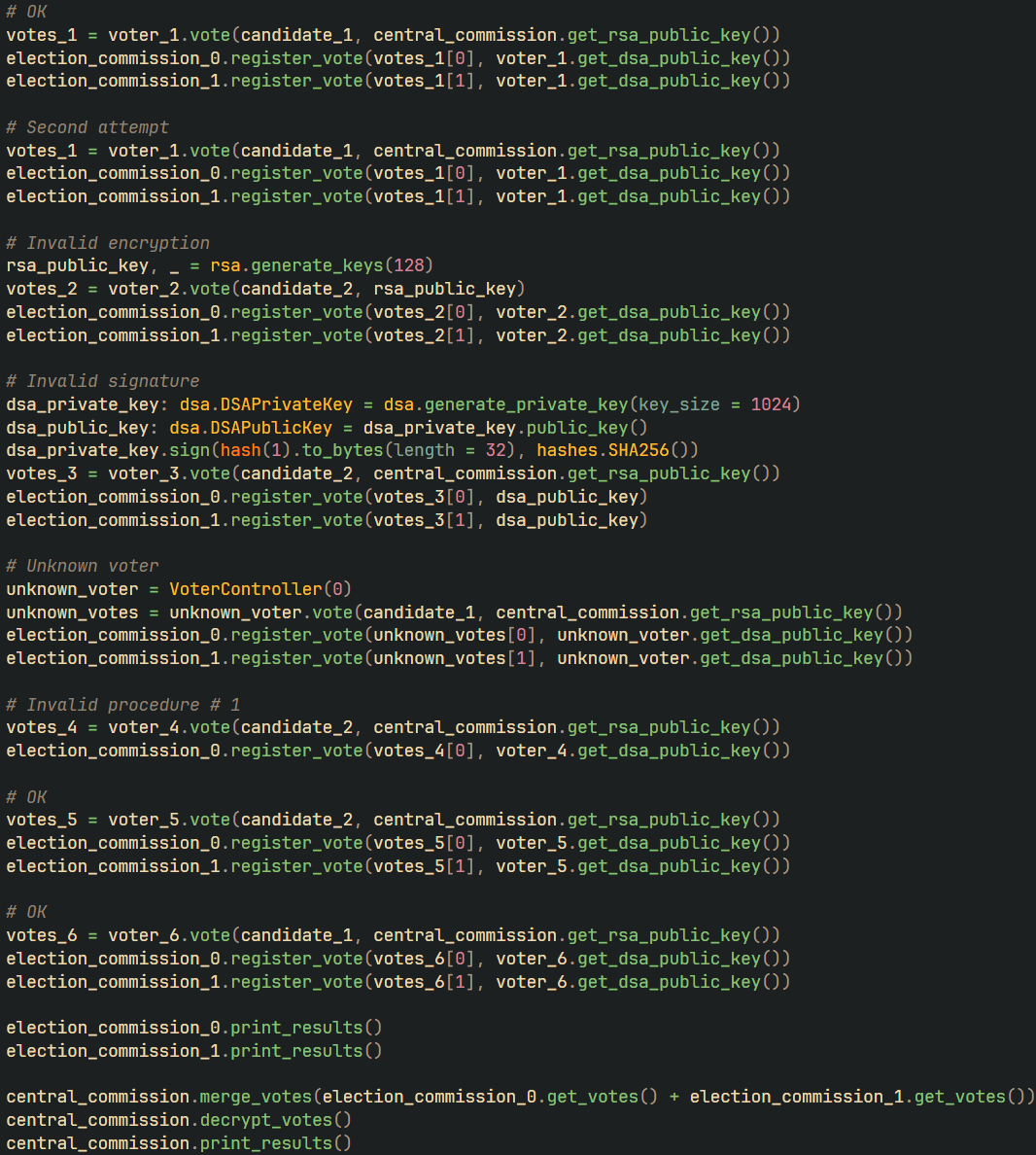


Рисунок 1.8 – Код верифікації процедури голосування



Рисунок 1.9 – Верифікація процедури голосування

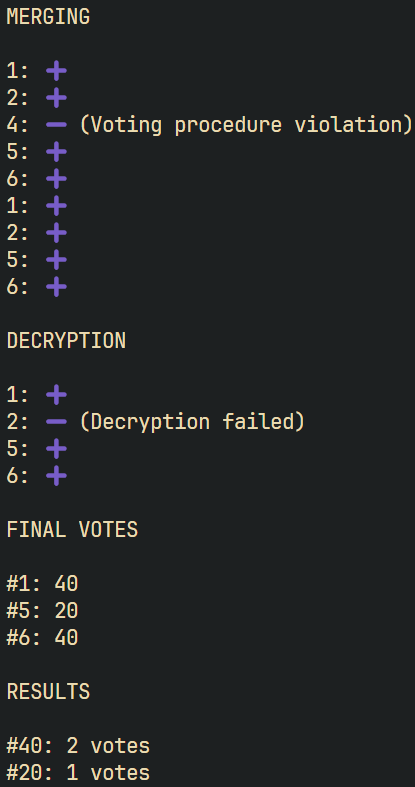


Рисунок 1.10 – Продовження верифікації процедури голосування

**Дослідження протоколу:**

1. Перевірити чи можуть голосувати ті, хто не має на це права.

Ні, не можуть, оскільки центральна виборча комісія на етапі реєстрації перевіряє чи має користувач право голосу. Звісно, що не можна відкидати варіанти шахраювання, бо центральна виборча комісія може дати право голосу тому, кому не потрібно, або інші виборчі комісії можуть прийняти голос від не валідного виборця (але центральна комісія додатково перевіряє цей момент на етапі злиття голосів).

1. Перевірити чи може виборець голосувати кілька разів.

Ні, не може, оскільки виборча комісія перевіряє чи не надсилав цей виборець голос до цього, а центральна з’єднує голоси на фінальному етапі й також переконується у коректній кількості бюлетенів від кожного виборця. Також можливо шахраювання, якщо буде змова комісій.

1. Чи може хтось (інший виборець, ВК, стороння людина) дізнатися за кого проголосували інші виборці?

Так, бо публікуються результати у кінці проведення голосування й для цього потрібно знати айді іншого виборця.

1. Перевірити чи може інший виборець чи стороння людина проголосувати замість іншого зареєстрованого виборця.

Це можливо лише у випадку, коли відомий реєстраційний айді іншого виборця, його dsa-ключі і якщо надіслати голос раніше за нього. Також можливо шахраювання, оскільки виборчі комісії можуть вписати голос замість когось, але такі дії будуть помічені ще на етапі голосування самим виборцем (не зможе надіслати голос) та після підбиття підсумків, оскільки виводиться список бюлетенів.

1. Чи може хтось (інший виборець, ВК, стороння людина) таємно змінити голос в бюлетені?

Ні, бо айді кандидата за якого відданий голос розділяється на множники та шифрується приватним rsa-ключем, тому виборчі комісії не можуть змінити голос (хоча й можуть помітити однакові патерни). Центральна комісія може змінити голос на етапі злиття бюлетенів, але оскільки результати публікуються, то змінити його таємно не вдасться.

1. Чи може виборець перевірити, що його голос врахований при підведенні кінцевих підсумків?

Так, бо значення бюлетенів публікуються зашифрованими на проміжному етапі (коли виборчі комісії публікують свої результати) та у кінці процедури голосування публікуються повноцінні розшифровані бюлетені.

**Висновок:**

У даній лабораторній роботі було реалізовано та досліджено протокол електронного голосування з розділенням комісії на незалежні частини. Для забезпечення захищеності повідомлень використовувався метод шифрування RSA, а цифровий підпис за алгоритмом DSA. Було створено симуляції, що включає центральну виборчу комісію, яка відповідає за реєстрацію виборців і підбиття підсумків, та локальні комісії, що приймають голоси. Така структура забезпечує поділ обов'язків і дозволяє підвищити надійність та захист процесу.

Аналіз моделі підтвердив відповідність протоколу основним вимогам безпеки. Голосувати можуть лише зареєстровані виборці, можливість багаторазового голосування виключена завдяки перевіркам на рівні комісій. Також забезпечується анонімність голосування, оскільки результати публікуються зашифрованими, що унеможливлює ідентифікацію виборця без знання його ID. Кожен голос шифрується, що захищає його від несанкціонованих змін, а виборці можуть перевірити врахування свого голосу за підсумками голосування.

Отже, змодельований протокол е-голосування демонструє високий рівень захищеності та стійкість до різних видів атак і маніпуляцій.