**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 № 3 з дисципліни

«Протоколи й алгоритми електронного голосування»

“**Протокол Е-голосування з двома виборчими комісіями**”

| **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 № 3**

**Тема роботи**: Протокол Е-голосування з двома виборчими комісіями.

**Мета роботи**: Дослідити протокол Е-голосування з двома виборчими комісіями.

**Основне завдання:**

Змоделювати протокол Е-голосування з двома виборчими комісіями будь-якою мовою програмування та провести його дослідження. Для кодування повідомлень використовувати метод Ель-Гамаля, 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:**

Реєстраційне бюро представлено відповідним класом (рис. 1.1) та має метод для реєстрації виборця у випадку наявності прав для голосування.

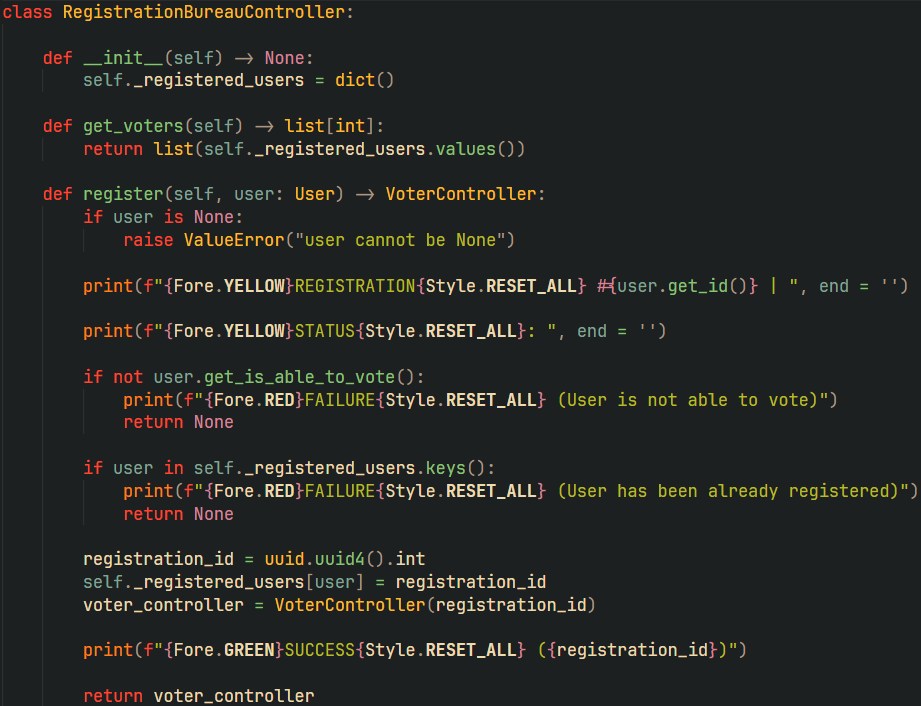


Рисунок 1.1 – Клас реєстраційного бюро

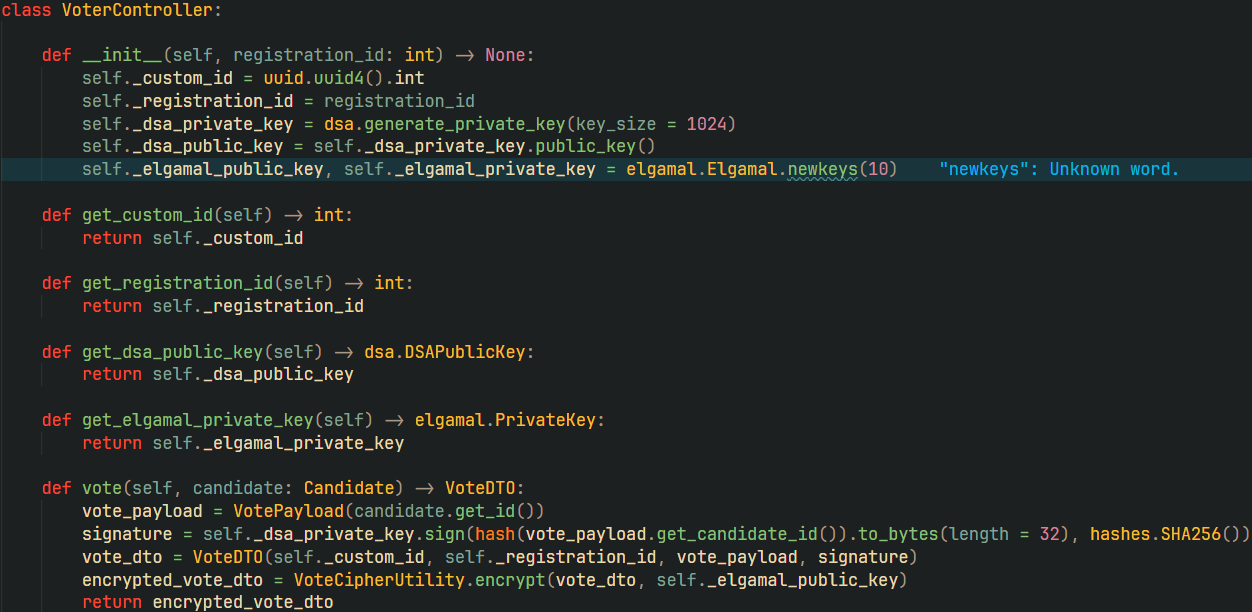


Рисунок 1.2 – Клас виборця

Виборець представленик класом VoterController, у якому є поля dsa-ключів, ключів Ель-Гамаля.

Клас ВК представлений завдяки ElectionCommission, у якому метод register\_vote перевіряє розшифровує повідомлення, валідує сам голос і зараховує його у кінцевому результаті.

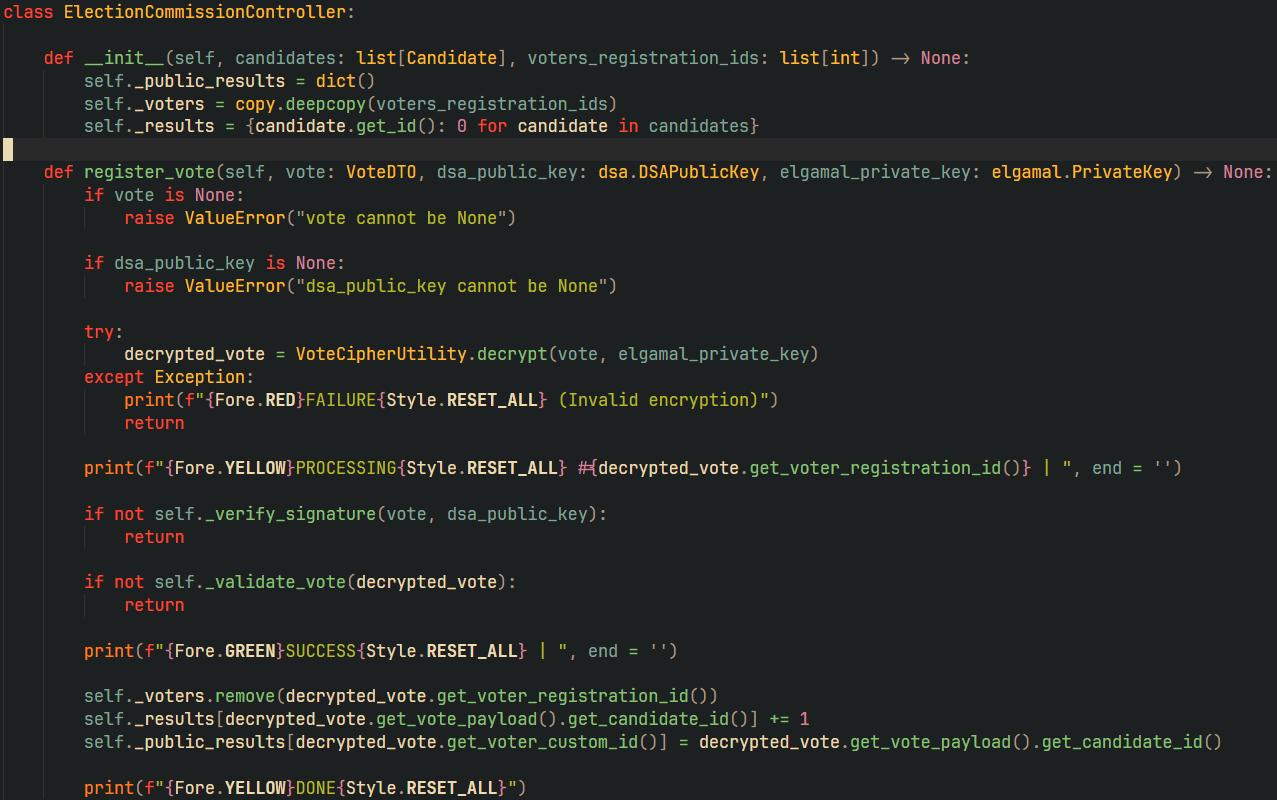


Рисунок 1.3 – Метод register\_vote класу ElectionCommission

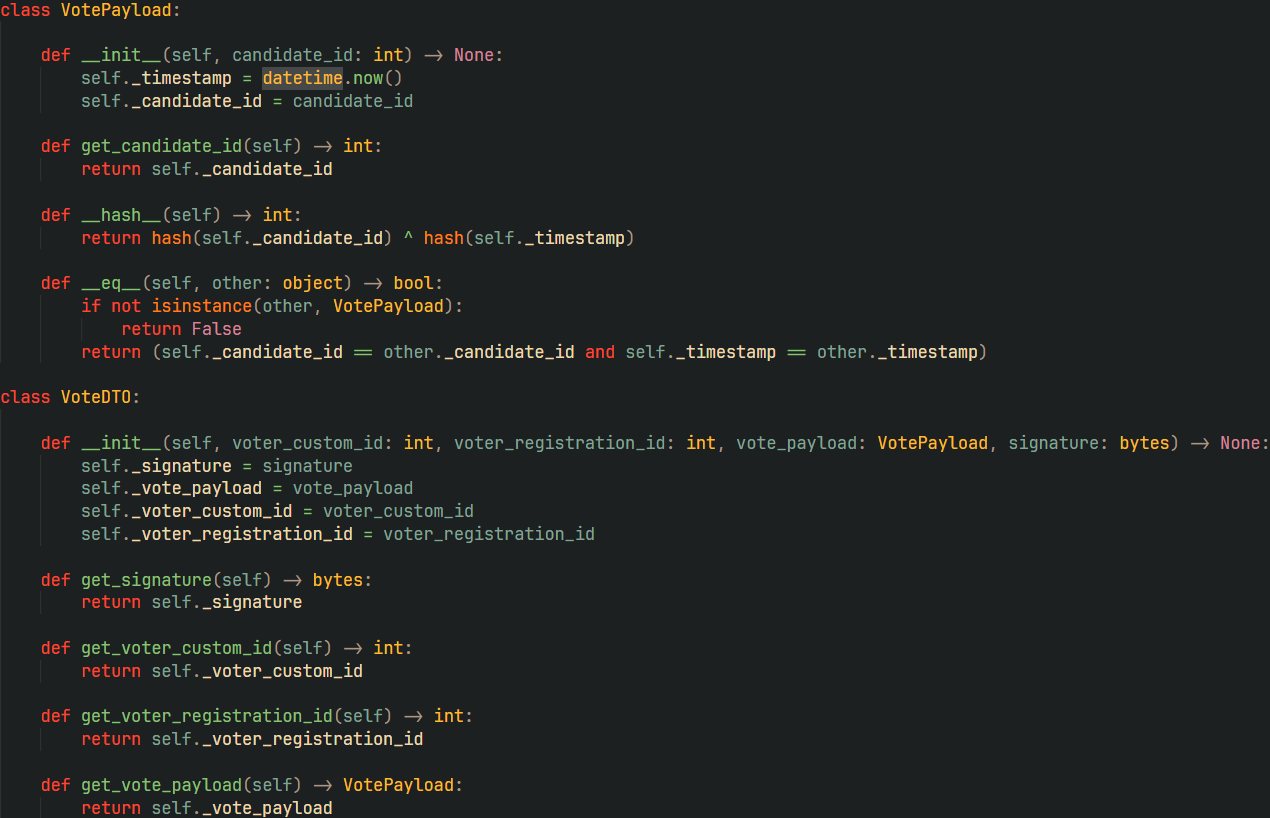


Рисунок 1.4 – Класи-моделі представлення голосів

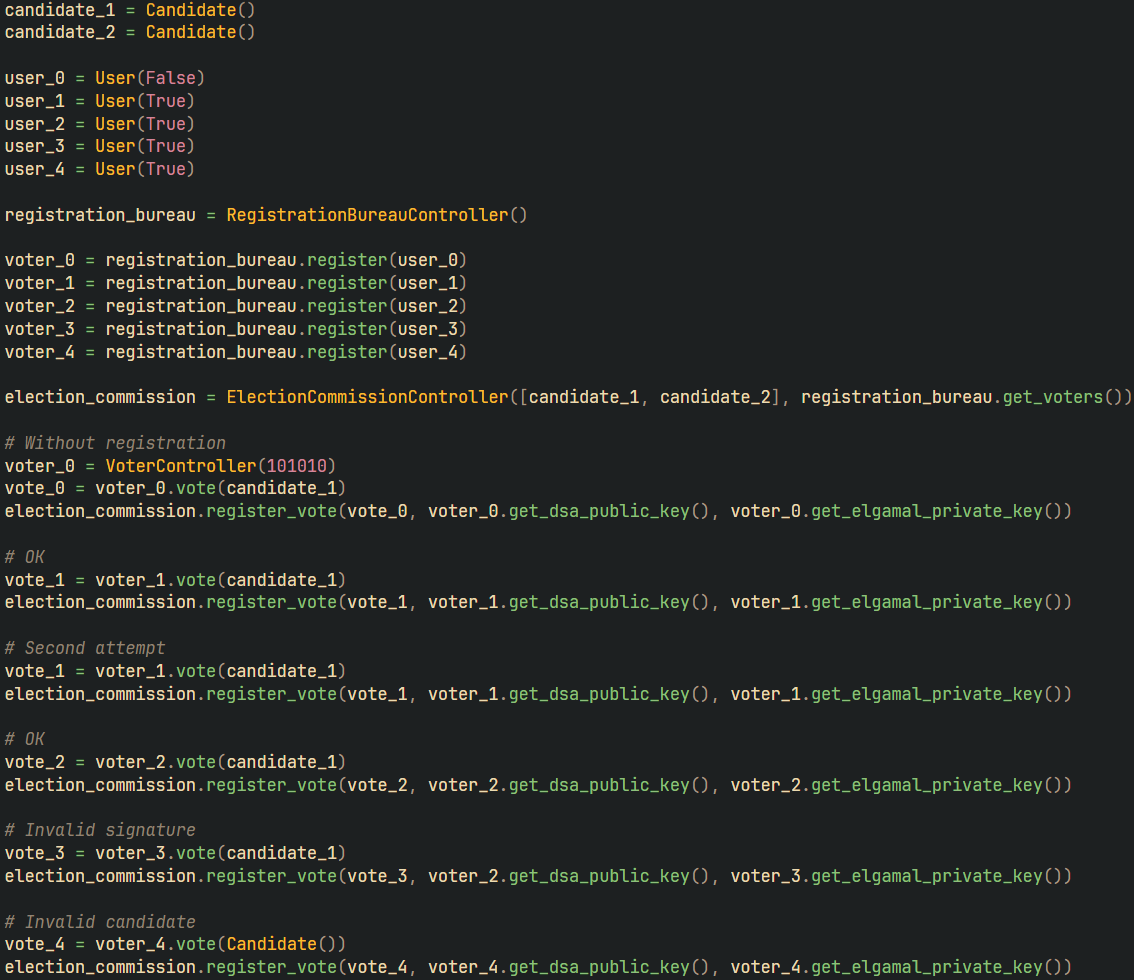


Рисунок 1.5 – Сценарії виконання

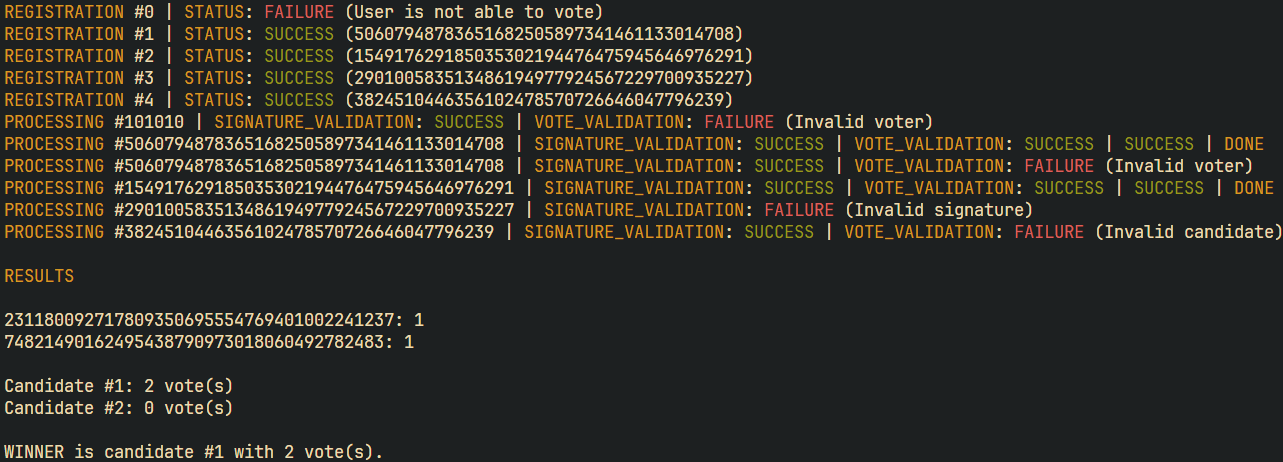


Рисунок 1.6 – Результати виконання

**Дослідження протоколу:**

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

Ні, не можуть, оскільки відбувається попередня валідація виборця за допомогою реєстраційного бюро. Навіть якщо такий виборець спробує надіслати свій бюлетень, то його голос не буде зараховано, оскільки його немає у списку від бюро. Звісно, що не можна відкидати варіант з шахраюванням з боку реєстраційного бюро, або виборчої комісії.

1. Перевірити чи може виборець голосувати кілька разів.

Ні, не може, оскільки відбувається попередня перевірка на те, чи присутній реєстраційний номер кандидата у відповідному списку від бюро. Звісно, що не можна відкидати варіант з шахраюванням з боку виборчої комісії.

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

Так, оскільки після виборів виводиться список власних айді виборців та вміст їх бюлетенів, але для цього потрібно знати якому виборцю належить який айді. Стосовно самої виборчої комісії, то особистість виборця прихована за спеціальним айді виборця, оскільки остаточний бюлетень присилається без прив’язки до особи, але реєстраційне бюро зберігає повноту інформація про голосувальники та його особистість.

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

Це можливо зробити, якщо вгадати айді реєстрації іншого виборця й проголосувати до нього раніше. Звісно, що не можна відкидати варіант з шахраюванням з боку виборчої комісії.

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

Таємно цього зробити не вдасться, оскільки публікується остаточний список бюлетенів та їх вміст після завершення процесу голосування. Звісно, що не можна відкидати варіант з шахраюванням з боку виборчої комісії.

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

Так, оскільки виводиться список бюлетенів та їх вміст після голосування. Звісно, що не можна відкидати варіант з шахраюванням з боку виборчої комісії.

**Висновок:**

У ході виконання лабораторної роботи було змодельовано та досліджено протокол електронного голосування з двома виборчими комісіями, де для кодування повідомлень використовувався метод Ель-Гамаля, а для реалізації електронного цифрового підпису – алгоритм DSA.

Під час дослідження було встановлено, що протокол ефективно запобігає голосуванню неавторизованих осіб завдяки попередній верифікації виборців реєстраційним бюро. Також виборці не можуть проголосувати кілька разів через перевірку статусу кожного виборця перед голосуванням. Протокол забезпечує певний рівень анонімності, оскільки бюлетені шифруються без прив’язки до особистості виборця. Однак можливе ідентифікування виборців через реєстраційні ID. Можливість проголосувати замість іншого виборця існує за умов доступу до ID реєстрації, але це малоймовірно без шахрайства з боку реєстраційного бюро або виборчої комісії. Зміна голосу після його відправки також малоймовірна, оскільки після завершення голосування публікуються бюлетені з їхнім вмістом, що забезпечує контроль за підсумками.

Таким чином, протокол забезпечує базові функції безпеки, верифікації виборців і шифрування голосів, однак не може повністю гарантувати абсолютну анонімність та захист від маніпуляцій.