**Додаток 1**

Форма відомостей про авторів матеріалу та описова інформація для видань ТНТУ

**Авторська довідка**

*(кваліфікаційної роботи бакалавра)*

**Назва кваліфікаційної роботи бакалавра** *Програмна реалізація криптографічного протоколу*

    *підкидання «чесної» монети*

 *назви записувати нижнім регістром (як у реченні)*

**Назва (англ.):** *Software Implementation of a Cryptographic Protocol of “Fair”* *Coin Flipping*

  *переклад англійською*

**Освітній ступінь :**  бакалавр

**Шифр та назва спеціальності:** 125 «Кібербезпека» напр.:151 Автоматизація та комп’ютерно-інтегровані технології

**Екзаменаційна комісія**: Екзаменаційна комісія № 46

 *напр.: Екзаменаційна комісія №1*

**Установа захисту:** Тернопільський національний технічний університет імені Івана Пулюя *напр.: Тернопільський національний технічний університет імені Івана Пулюя*

**Дата захисту:** 24 червня 2022 року  **Місто:** Тернопіль

**Сторінки:**

Кількість сторінок роботи: 50

**УДК:**  004.056

**Автор роботи**

 Прізвище, ім’я, по батькові (укр.): Тернавчук Ігор Васильович

 розкривати ініціали

 Прізвище, ім’я (англ.): Ternavchuk Ihor

 *використовувати паспортну транслітерацію (КМУ 2010)*

Місце навчання (установа, факультет, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп’ютерно- інформаційних систем і програмної інженерії, Кафедра кібербезпеки, м.Тернопіль, Україна

**Керівник**

 Прізвище, ім’я, по батькові (укр.): Загородна Наталія Володимирівна

 повністю

 Прізвище, ім’я (англ.): Zahorodna Nataliia

 *використовувати паспортну транслітерацію (КМУ 2010)*

 Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Україна

 Вчене звання, науковий ступінь, посада: кандидат технічних наук, доцент кафедри КБ

**Рецензент**

 Прізвище, ім’я, по батькові (укр.): Нікітюк В’ячеслав В’ячеславович

 повністю

 Прізвище, ім’я (англ.): Nikitiuk V’iacheslav

 *використовувати паспортну транслітерацію (КМУ 2010)*

 Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп’ютерно- інформаційних систем і програмної інженерії, Кафедра комп’ютерних наук, м.Тернопіль, Україна

 Вчене звання, науковий ступінь, посада: к.т.н., доцент кафедри КН

**Ключові слова**

українською : криптографічний протокол, чесна монета, функція діффі-хелмана, китайська теорема про остачі, квадратний корінь, схема блюма

 *до 10 слів*

англійською cryptographic protocol, fair coin, diffie-hellman function, chinese remaining theorem, square root, bloom s scheme

 *до 10 слів*

**Анотація**

 українською:

Кваліфікаційна робота присвячена розробці програмного забезпечення для криптографічного протоколу підкидання чесної монети по телефону. В роботі обґрунтовано вибір програмного середовища розробки та вибір схеми з допомогою квадратних коренів. Розроблене програмне забезпечення (ПЗ) дозволяє відслідкувати логіку протоколу і може бути використано для навчальних потреб. Продемонстровано роботу програмного забезпечення при коректному використанні параметрів схеми та показано, що коли перша сторона намагається займатись шахрайством, то автоматично виграє друга сторона.

Дану розробку можна використовувати, коли сторони не довіряють одна одній і мають потребу в створенні спільної послідовності випадкових біт.

В першому розділі описано різновиди специфічних криптографічних протоколів та схеми підкидання монети по телефону. В другому розділі проведено вибір програмного середовища та наведено окремі важливі функції ПЗ. В третьому розділі наведено результати тестування розробки та верифікацію результатів роботи програми.

англійською:

Qualification thesis is devoted to the development of software for cryptographic protocol of protocol of flipping a fair coin by the telephone. The paper substantiates the choice of software development environment and the choice of the scheme of flipping a fair coin using square roots method. Developed software allows to track the logic of the protocol and can be used for educational purposes. The operation of the software with the correct use of the parameters of the scheme is demonstrated. It is shown that when the first party tries to commit fraud, the second party automatically wins.

This development can be used when the parties do not trust each other and need to create a common sequence of random bits.

The first section describes the types of specific cryptographic protocols and schemes for tossing a coin over the phone. The second section selects the software environment and lists some important software features. The third section presents the results of development testing and verification of the results of the program.

Бібліографічний опис:

Тернавчук І. В. Програмна реалізація криптографічного протоколу підкидання «чесної» монети: кваліфікаційна робота бакалавра за спеціальністю 125 — Кібербезпека / І. В. Тернавчук. – Тернопіль : ТНТУ, 2022. – 50 c.