Студент 320 группы: Зверев Глеб Петрович

Научный руководитель: Чернов Владимир Александрович

Тема работы: исследование алгоритмов доказательств с нулевым разглашением (Zero-Knowledge Proof) и их применения

План работы:

- 30.09.21 – 06.10.21
  - Криптографическое хеширование: SHA256, SHA512, SHA3 (keccak). Свойства функций хэширования. Библиотеки с реализацией в Python и C/C++?
  - Симметричная и ассиметричная криптография. Принцип работы криптосистемы RSA. Библиотеки в Python и C/C++.
  - Начать изучение эллиптических кривых. Эллиптические кривые и их свойства.
- 07.10.21 – 13.10.21
  - Общие сведения об эллиптических кривых в пространстве R2
  - Эллиптические кривые в дискретных полях. Типовые значения параметров дискретных эллиптических кривых.
  - Схема асимметричной криптографии с эллиптическими кривыми
  - Выбор модуля для языка Python для реализации ECC
- 14.10.21 – 20.10.21
  - Использование ECC для подписи документов
  - Генерация пары публичный/приватный ключ
  - Генерация подписи для хеша документа
  - Проверка подписи хеша документа
- 21.10.21 – 27.10.21
  - Использование ECC для шифрования
  - Шифровка документа
  - Расшифровка документа
- 28.10.21 – 03.11.21
  - С использованием модуля написать утилиту для реализации основных криптографических примитивов. Для хранения приватного и публичного ключей использовать формат утилиты ssh

Москва, 2021

- 04.11.21 – 10.11.21
    - Продолжить реализацию алгоритмов
    - Обзор методов доказательств с нулевым разглашением и методов консенсуса.
    - Подбор соответствующей литературы
- 11.11.21 – 17.11.21
    - Завершить реализацию алгоритмов
    - Начало сравнительного изучения организации блокчейнов с разным уровнем приватности.
- 18.11.21 – 24.11.21
    - Продолжить изучение организации блокчейнов с разным уровнем приватности
    - ZCASH
    - BEAM
- 01.12.21 – 07.12.21
    - Завершить подготовку обзора в тексте семестровой работы
    - Завершить постановку задачи в тексте семестровой работы
    - Приступить к оформлению презентации о проделанной работе
- 24.11.21 – 01.12.21
    - Завершить презентацию с учётом проделанной работы
    - Продолжить написание текста семестровой работы
- 02.12.21 – 08.12.21
    - Оформить семестровую работу согласно требованиям
    - Подготовить отчётные материалы по семестровой работе