Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

Исследование алгоритмов генерации и верификации эцп

Выполнил:

студент 3 курса 4 группы

специальности ПОИТ

Матюх А.А.

Минск 2020

1. **Теоретические сведения**

Электронная цифровая подпись (ЭЦП) является важным элементом современных информационных систем, использующих методы и технологии криптографического преобразования информации.

Определение 1. Электронная цифровая подпись – контрольная характеристика сообщения, которая вырабатывается с использованием личного ключа, проверяется с использованием открытого ключа, служит для контроля целостности и подлинности сообщения и обеспечивает невозможность отказа от авторства.

Таким образом, ЭЦП выполняет те же функции, что и собственноручная (поставленная «от руки») подпись:

• аутентифицировать лицо, подписавшее сообщение;

• контролировать целостность подписанного сообщения;

• защищать сообщение от подделок;

• доказать авторство лица, подписавшего сообщение, если это лицо отрицает свое авторство

Определение 2. Электронная цифровая подпись – бинарная (или в ином виде) последовательность символов, являющаяся реквизитом электронного документа, зависящая от содержания этого документа и предназначенная для подтверждения целостности и подлинности электронного документа

Классическая технология использования ЭЦП предусматривает подписание не самого сообщения (обозначим его здесь Мо), а его хеша, H(Mо). Это сокращает время генерации/верификации подписи и снижает вероятность появления случайных ошибок в итоговом документе.

1. **Практическая часть**

В данной лабораторной работе необходимо разработать приложение для генерации и верификации ЭЦП на основе алгоритмов RSA, ЭльГамаля и Шнорра.

В связи с поставленными требованиями было разработано приложение на основе встроенного пакета crypto в Node.js.

Пример ЭЦП RSA:



Рисунок 2.1 – ЭЦП RSA

Пример ЭЦП ЭльГамаля:



Рисунок 2.1 – ЭЦП ЭльГамаля

Пример ЭЦП Шнорра:



Рисунок 2.1 – ЭЦП Шнорра

**Вывод**

В данной лабораторной работе я закрепил теоретические знания по ЭЦП. А также, разработал приложение для генерации и верификации по 3 алгоритмам.