БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №9**

**«Исследование криптографических хеш-функций**»

**Выполнила:**

студентка 3 курса 1 группы

Потапейко Полина Павловна

**Проверил:**

Берников Владислав Олегович

Минск 2022

**Цель:** изучение алгоритмов хеширования и приобретение практических навыков их реализации и использования в криптографии.

**Ход работы**

**Задание.** Разработать приложение, которое реализует алгоритм хеширования MD5. Приложение должно обрабатывать входное сообщение.

Результат хешированя сообщения представлен на рисунке 1.



Рисунок 1 – Результат хеширования сообщения

**Вывод:** в ходе лабораторной работы были закреплены теоретические знания по алгебраическому описанию и алгоритмам реализации операций вычисления однонаправленных хеш-функций, освоена методика оценки криптостойкости хеш-преобразований на основе «парадокса дня рождения», разработано приложение для реализации заданного алгоритма хеширования, оценена скорость вычисления кодов хеш-функций.