МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №11**

по дисциплине «Криптографические методы защиты информации»

на тему: ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ХЕШ-ФУНКЦИЙ

Выполнил студентка 3 курса 5 группы специальность ПОИТ Буранко В.Д.

(Ф.И.О.)

Преподаватель ассистент Савельева Маргарита Геннадьевна

(Ф.И.О.)

**Содержание**

[Практические задания 4](#_Toc136180293)

[Задание 1 4](#_Toc136180295)

[Задание 2 4](#_Toc136180296)

[Выводы 8](#_Toc136180297)

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

**Задачи:**

* Закрепить теоретические знания по алгебраическому описанию и алгоритмам реализации операций вычисления однонаправленных хеш-функций.
* Освоить методику оценки криптостойкости хеш-преобразований на основе «парадокса дня рождения».
* Разработать приложение для реализации заданного алгоритма хеширования (из семейств MD и SHA).
* Оценить скорость вычисления кодов хеш-функций.
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента

# **Практические задания**

Разработать приложение, демонстрирующее работу алгоритма MD5. Оценить быстродействие данного алгоритма хеширование.

Для данной лабораторной работы был выбран алгоритм MD5, из-за его высокой криптостойкости.

В результате работы данного алгоритма является строка длинной 64 символа. Результат работы продемонстрирован на рисунке 1.



Рисунок 1 — Результаты хэширования сообщений «123» и «Buranko Valeria»



Рисунок 2 — Время выполнения хэширования разного количества символов

На рисунке 3 продемонстрирован график скорости выполнения алгоритма в зависимости от количества символов в исходном сообщении.



Рисунок 3 – График зависимости времени выполнения от количества символов

# **Выводы**

В ходе выполнения данной лабораторной работы мы изучили и приобрели практические навыки разработки и использования приложений для зашифрования сообщения при помощи алгоритма хэширования MD5.