# Лабораторная работа №1-ИБ. Оценка качества алгоритмов формирования таблиц простых чисел

## Цель работы

Сформировать критерии и выполнить оценку базовых алгоритмов формирования таблиц простых чисел.

## Порядок выполнения

1. Повторить основные термины теории алгоритмов и теории чисел, способы получения таблиц простых чисел (например, методы перебора (простого деления); алгоритмы Эратосфена; Сундарама и Аткина и др.).
2. Провести поиск в литературных источниках и Интернет способов оценки качества алгоритмов. Привести общематематические формулы оценки качества.
3. Для заданных алгоритмов (см.таблицу вариантов) выбрать язык программирования и получить результаты (таблица простых чисел в заданном интервале; данные, подтверждающие вычислительную сложность метода - количество операций сложения/вычитания, умножения/деления либо сдвига, необходимых для получения результата, время выполнения расчета и требуемую для реализации алгоритмов память), программно сформировать таблицу сравнения.
4. Проанализировать результаты, отразить исследование в отчете.

## Требования к отчету:

1. Титульный лист
2. Введение (о применении простых чисел в защите информации);
3. Основной раздел, в котором:

- описать алгоритм и отобразить схемы формирования таблиц простых чисел выбранными методами (см. варианты);

- сформулировать и описать критерий сравнения алгоритмов, указать основные параметры, применимые для получения оценочных характеристик;

- привести программный код разработки с комментариями;

- отобразить полученные результаты (таблицу простых чисел в заданном интервале; таблицу сравнения, привести копии экранов.

1. Сформулировать выводы.

## 

## Таблица 1. Варианты заданий к лабораторной работе №1-ИБ

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п\п** | **m** | **n** | **Исследуемые алгоритмы** |
| 1 | 500 | 894 | Перебора, Эратосфена, Сундарама |
| 2 | 700 | 1063 | Эратосфена, Сундарама, Аткина |
| 3 | 550 | 1241 | Сундарама, Аткина, перебора |
| 4 | 900 | 1387 | Аткина, перебора, Эратосфена |
| 5 | 1000 | 2384 | Эратосфена, перебора, Сундарама |

## Таблица 2. Рекомендуемый вид таблицы сравнения

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| алгоритм | язык прог-раммирования | Кол. слож. | Кол. вычит. | Кол. умнож. | Кол. делен. | общ. кол. арифм. операций | Кол. сдвигов | время вычислений,  формула | время вычислений, мкс | Память, общая оценка, формула | Память,  Кб |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

Примечания:

1. При оценке времени работы алгоритма учитывать «чистое» время работы алгоритма – без процесса формирования таблиц и вывода результатов.
2. При оценке объема требуемой памяти оценивать только память, необходимую непосредственно для получения результата (общий случай, ).