



Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Московский государственный технический университет  
имени Н.Э. Баумана  
(национальный исследовательский университет)»  
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления»

КАФЕДРА «Программное обеспечение ЭВМ и информационные технологии»

### Лабораторная работа № 1

Дисциплина: **Моделирование**

Тема: **«Исследование псевдослучайных последовательностей»**

Студент: **Барсуков Н.М.**

Группа **ИУ7-76Б**

Оценка (баллы) \_\_\_\_\_

Преподаватель : **Рудаков И.В.**

Москва.

Рис. 1.

# Содержание

1	Аналитический раздел	3
1.1	Цель работы . . . . .	3
1.2	Псевдослучайные числа . . . . .	3
1.3	Способы получения . . . . .	3
1.4	BlumBlumShub . . . . .	5
1.5	Критерий сериальной корреляции . . . . .	5
2	Экспериментальная часть	6
3	Заключение	9
	Список использованных источников	10

# 1 Аналитический раздел

В данном разделе поставлена цель работы и указаны задачи необходимые для выполнения данной. Описаны способы получения псевдослучайных чисел. Разобран метод VBS. Выбран критерий случайности

## 1.1 Цель работы

Реализовать критерий оценки случайности последовательности. Сравнить результаты работы данного критерия на одноразрядных, двухразрядных и трехразрядных последовательностях псевдослучайных целых чисел. Последовательности получать алгоритмическим способом, табличным способом и путём ручного ввода.

Для выполнения выше поставленной цели необходимо выполнить следующие:

- 1) Ответить на вопросы:
  - а) Что такое псевдослучайные числа
  - б) Способы получения
- 2) Выбрать и реализовать алгоритмический метод получения псевдослучайных целых чисел.
- 3) Выбрать и реализовать критерий для оценки случайности

## 1.2 Псевдослучайные числа

Данные числа называют псевдослучайными поскольку даже пройдя все статистические испытания на случайность и равномерность распределения остаются полностью детерминированными. То есть, если каждый цикл работы генератора начинается с теми же условиями, то на выходе мы получим одни и те же последовательности.

## 1.3 Способы получения

На практике используются 3 основных способа:

- 1) Аппартный
- 2) Табличная схема
- 3) Алгоритмический способ

Каждый из данных способов обладает своими достоинствами и недостатками:

#### 1) Аппаратный

##### а) Достоинства:

- Запас чисел неограничен;
- Расходуется мало операций;
- Не занимает место в ОП.

##### б) Недостатки:

- Требуется периодическая проверка на случайность;
- Нельзя воспроизводить последовательность;
- Используются спец устройства. Надо стабилизировать;

#### 2) Табличный

##### а) Достоинства:

- Требуется однократная проверка;
- Можно воспроизводить последовательность;

##### б) Недостатки:

- Запас чисел ограничен;
- Занимает место в оперативной памяти и требует время на обращение;

#### 3) Алгоритмический

##### а) Достоинства:

- Одна проверка;
- Многократное воспроизведение;
- Относительно малое место в ОП;

- Не использует внешнее устройство;
- б) Недостатки:
  - Запас чисел ограничен ее периодом;
  - Требуются затраты машинного времени;

## 1.4 BlumBlumShub

Широкое распространение получил алгоритм генерации псевдослучайных чисел, называемый алгоритмом BBS (от фамилий авторов — L. Blum, M. Blum, M. Shub) или генератором с квадратичным остатком. Для целей криптографии этот метод предложен в 1986 году. Он заключается в следующем. Вначале выбираются два больших простых<sup>1</sup> числа  $p$  и  $q$ . Числа  $p$  и  $q$  должны быть оба сравнимы с 3 по модулю 4, то есть при делении  $p$  и  $q$  на 4 должен получаться одинаковый остаток 3. Далее вычисляется число  $M = p \cdot q$ , называемое целым числом Блюма. Затем выбирается другое случайное целое число  $x$ , взаимно простое (то есть не имеющее общих делителей, кроме единицы) с  $M$ . Вычисляем  $x_0 = x^2 \bmod M$ .  $x_0$  называют стартовым числом генератора.

На каждом  $n$ -м шаге работы генератора вычисляется  $x_{n+1} = x_n^2 \bmod M$ . Результатом  $n$ -го шага является один (обычно младший) бит числа  $x_{n+1}$ . Иногда в качестве результата принимают бит чётности, то есть количество единиц в двоичном представлении элемента.

## 1.5 Критерий сериальной корреляции

Можно подсчитать следующую статистику:

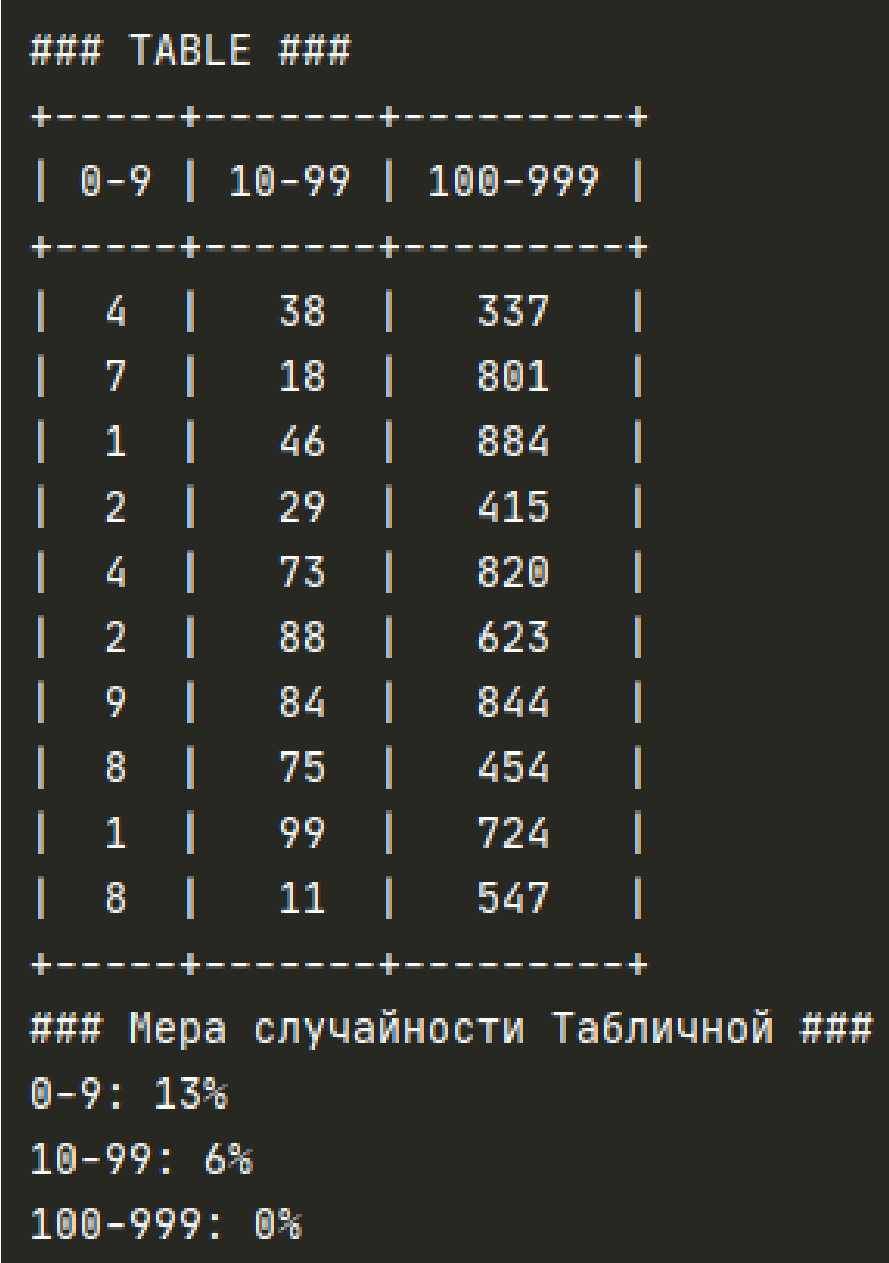
$$C = \frac{n \cdot (U_0 \cdot U_1 + U_1 \cdot U_2 + \dots + U_{n-2} \cdot U_{n-1} + U_{n-1} \cdot U_0) - (U_0 + U_1 + \dots + U_{n-1})^2}{n \cdot (U_0^2 + U_1^2 + \dots + U_{n-1}^2) - (U_0 + U_1 + \dots + U_{n-1})^2}$$

Это коэффициенты сериальной корреляции, мера зависимости  $U_{j+1}$  от  $U_j$ . Коэффициент корреляции всегда лежит между -1 и 1. Когда он равен 0 или очень мал, значит величины  $U_{j+1}$  и  $U_j$  независимы одна от другой (между ними нет линейной зависимости); если же значение коэффициента корреляции равно +1 или -1, это означает полную линейную зависимость.

## 2 Экспериментальная часть

В данном разделе рассмотрен вывод программы

На изображении 2 отображены результаты работы алгоритма BBS и мера случайности.



```
### TABLE ###
+-----+-----+-----+
| 0-9 | 10-99 | 100-999 |
+-----+-----+-----+
| 4 | 38 | 337 |
| 7 | 18 | 801 |
| 1 | 46 | 884 |
| 2 | 29 | 415 |
| 4 | 73 | 820 |
| 2 | 88 | 623 |
| 9 | 84 | 844 |
| 8 | 75 | 454 |
| 1 | 99 | 724 |
| 8 | 11 | 547 |
+-----+-----+-----+
### Мера случайности Табличной ###
0-9: 13%
10-99: 6%
100-999: 0%
```

Рис. 2. Результаты BBS

На изображении 3 отображены табличные значения и мера случайности

На изображениях 4 и 5 отображена мера случайности ручного ввода.

```

+-----+-----+-----+
| 0-9 | 10-99 | 100-999 |
+-----+-----+-----+
| 5 | 90 | 720 |
| 5 | 12 | 827 |
| 0 | 53 | 215 |
| 3 | 44 | 875 |
| 1 | 30 | 387 |
| 6 | 88 | 665 |
| 6 | 31 | 859 |
| 3 | 10 | 578 |
| 2 | 51 | 311 |
| 7 | 86 | 394 |
+-----+-----+-----+
### Мера случайности BSS ###
0-9: 33% #
10-99: 11%
100-999: 11%

```

Рис. 3.

```

### Проверка критерия ###
Введите количество символов: 6

Enter the numbers : 23 75 123 5 32 0
Мера случайности: 20%

```

Рис. 4.

```
### Проверка критерия ###  
Введите количество символов: 10  
  
Enter the numbers : 1 2 3 4 5 6 7 8 9 10  
Мера случайности: 100%
```

Рис. 5.



### 3 Заключение

В ходе реализации лабораторной работы, были получены навыки в написания генератора псевдослучайных чисел, а также в оценки критерий случайности последовательности алгоритмическим путём.

## Список использованных источников

1. Лекции "Моделирование"
2. Основы криптографии // URL: *https* :  
*//intuit.ru/studies/courses/691/547/lecture/12383?page = 3* (Дата  
обращения : 04.12.20)