Министерство науки и высшего образования Российской Федерации

Пензенский государственный университет

Кафедра «Вычислительная техника»

**ОТЧЕТ**

по лабораторной работе №3

по курсу «Защита информации в сети Internet»

на тему «Генераторы псевдослучайных последовательностей»

Вариант 2

Выполнили  
студенты группы 18ВВ1:

Коротов В.О.

Максимова Д.Р.

Приняли:

к.т.н., доцент Дубравин А.В.

к.т.н., доцент Карамышева Н.С.

**2020**

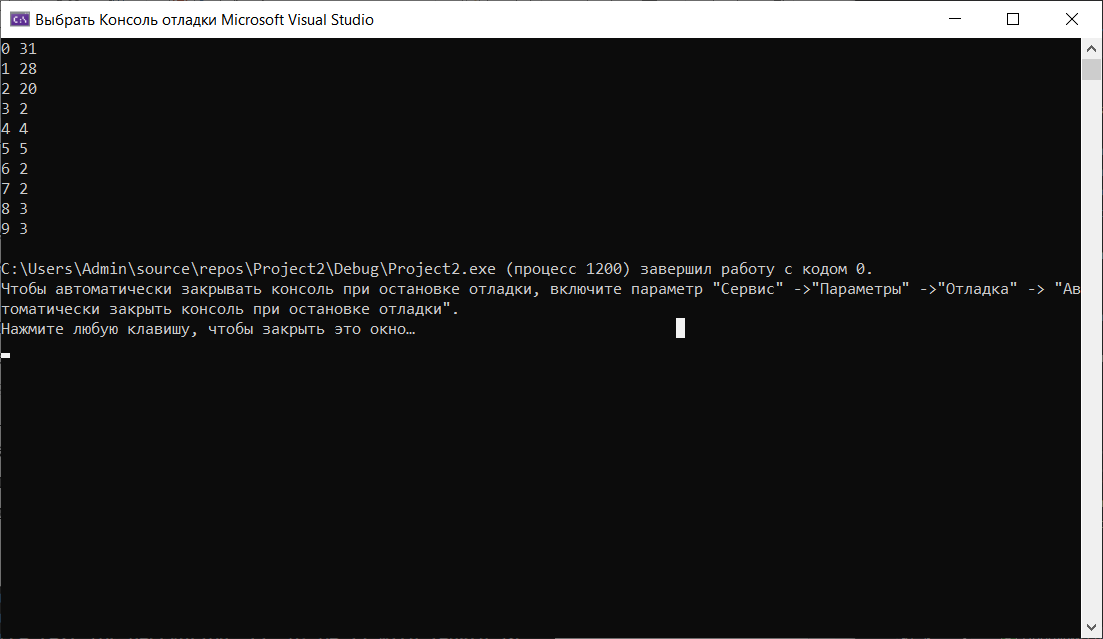
**Цель работы:** разработать генератор случайных чисел, используя метод серединных произведений. Исследовать качество генератора, путем оценки распределения генерируемых чисел.

**Задание:**

|  |  |
| --- | --- |
| Номер варианта | Метод генерации случайных чисел |
| 2 | Метод серединных произведений. Разрядность при вычислении 16 бит, разрядность результата 8 бит. |

**Описание работы программы:** в функции get\_random() был разработан генератор случайных чисел с помощью метода серединных произведений. Для генерации были сгенерированы множители R0 и R1. В функции timer() был взят остаток от деления на 100 от текущего времени в секундах. Эти значения были присвоены множителям R0 и R1. Алгоритм генерации чисел: R0 и R1 мы перемножаем и записываем в R2. Далее мы вырезаем из R2 середину и дописываем к строке ”0.”. Таким образом мы получаем случайное число. В конце функции переприсваиваем значения R0 и R1, значениям R1 и вырезанной строки соответственно. Статистику мы собираем с помощью функции statistic(). В этой функции мы считаем сколько чисел попало в каждый диапазон (10 диапазонов от 0 до 1)

Результат работы программы:



Листинг:

#include <bitset>

#include <iostream>

#include <string>

#include <time.h>

#include <map>

using namespace std;

unsigned char R0, R1;

const size\_t TRIM\_SIZE = 8;

const size\_t BITSET\_SIZE = 16;

void timer()

{

time\_t timer;

struct tm y2k = { 0 };

double seconds;

y2k.tm\_min = 0; y2k.tm\_sec = 0;

time(&timer);

R0 = timer % 100;

R1 = timer % 100;

}

float get\_random()

{

short R2;

R2 = R1 \* R0;

float random;

string R2str, trimed;

bitset <BITSET\_SIZE> bs(R2);

R2str = bs.to\_string();

trimed = R2str.substr(4, 8);

bitset <TRIM\_SIZE> bs2(trimed);

random = stof("0." + to\_string(bs2.to\_ulong()));

R0 = R1;

R1 = stoi(trimed);

return random;

}

void statistic()

{

map <int, int> rang;

for (int i = 0; i < 200; i++) {

float rand = get\_random();

int r\_rand = rand \* 10;

rang[r\_rand]++;

}

for (int i = 0; i < 10; i++) {

cout << i << " " << rang[i] << endl;

}

}

int main()

{

timer();

get\_random();

statistic();

}

**Вывод:** в ходе работы был разработан генератор случайных чисел, с использованием метода серединных произведений. Было исследовано качество генератора, путем оценки распределения генерируемых чисел.