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»

Выполнили  
студенты группы 18ВВ1:

Амплеев Д.О.

Колобов К.А.

Приняли:

к.т.н., доцент Дубравин А.В.

к.т.н., доцент Карамышева Н.С.

2020

**Цель работы:** изучить методы генерации случайных чисел, разработать генератор случайных чисел, используя один из методов.

**Задания:** Разработать генератор случайных чисел, используя метод в соответствии с номером варианта. Исследовать качество генератора, путем оценки распределения генерируемых чисел. Для этого необходимо разделить весь диапазон генерируемых чисел на 10 равных интервалов и подсчитать количество чисел, попадающих в каждый интервал.

В качестве начального значения следует выбирать текущее время в формате Unix time (можно получить, используя функцию time\_t time(time\_t\* timer)).

Для линейного конгруэнтного метода значение m всегда должно быть 231 -1.

*Таблица: Источники энтропии*

|  |  |
| --- | --- |
| № Варианта | Метод генерации случайных чисел |
| 1 | Метод серединных квадратов. Разрядность при вычислении 16 бит, разрядность результата 8 бит |

Листинг:

// Метод серединных квадратов. Разрядность при вычислении 32 бита,

// разрядность результата 16 бит.

#include <string>

#include <clocale>

#include <vector>

#include <bitset>

#include <iostream>

#include "windows.h"

#include <stack>

#include <time.h>

using namespace std;

int random(int& startNumber){

if (startNumber != 0) {

bitset<32> randomies = (startNumber << 15);

bitset<16> create = { 0 };

int out;

for (int i = 0; i < 16; i++)

create[i] = randomies[i];

out = create.to\_ullong();

out = out \* out;

//while (out > 10) {

// out = out / 10;

//}

cout << out << ' ';

random(out);

}

else {

cout << endl;

return 0;

}

}

int main() {

//time\_t timec = time(0);

//double startNumber = timec;

while(true) {

time\_t timec = time(0) \* time(0)/21;

int startNumber = timec;

cout << startNumber << ':';

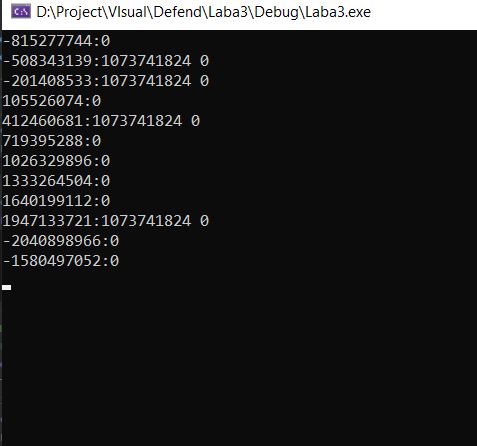
random(startNumber);

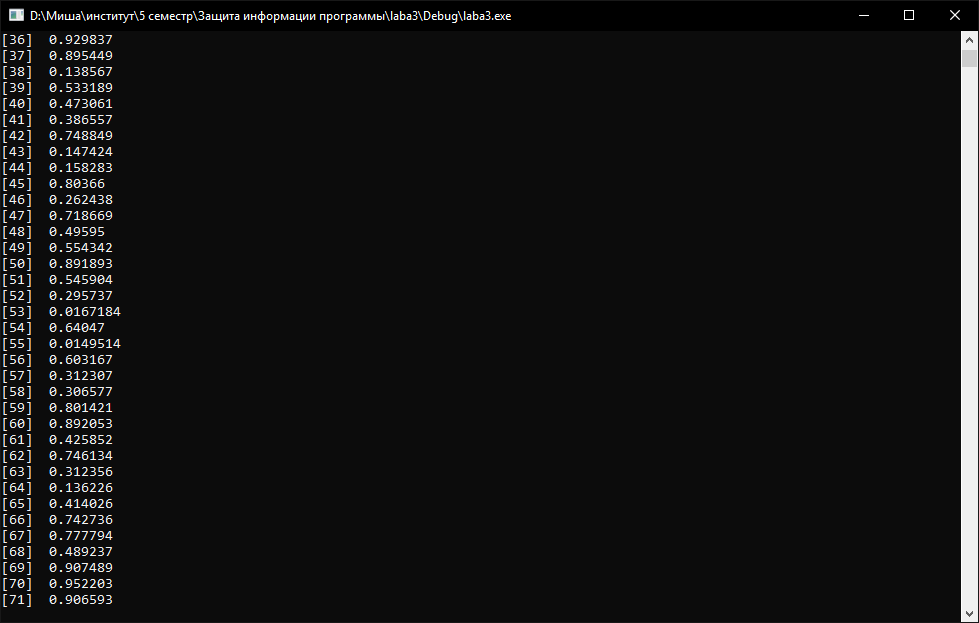
Sleep(2000);

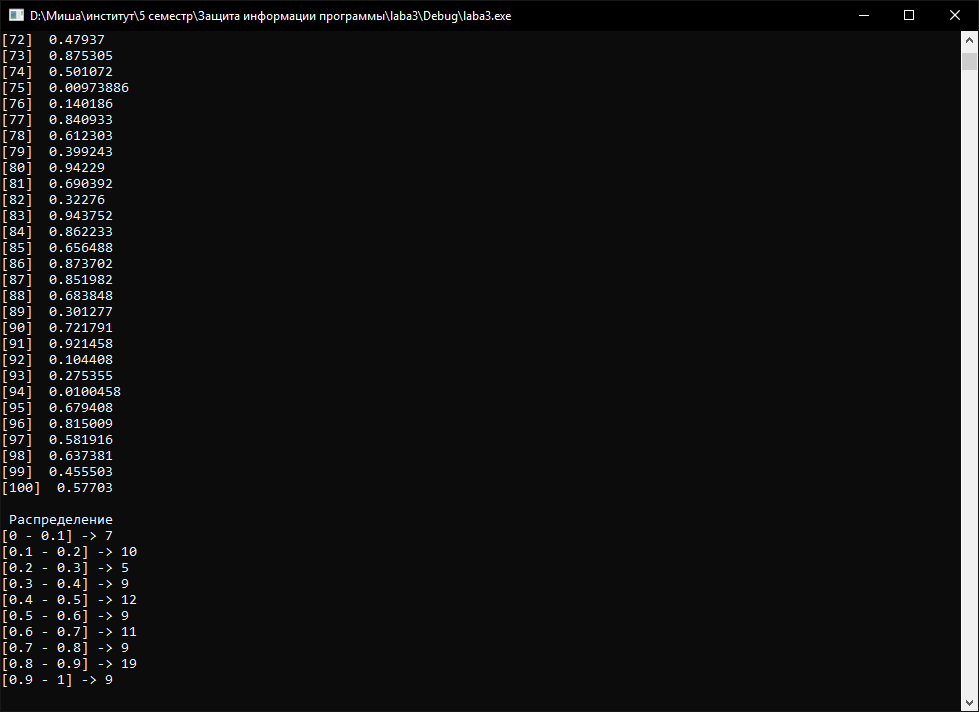
//startNumber = startNumber + 2832;

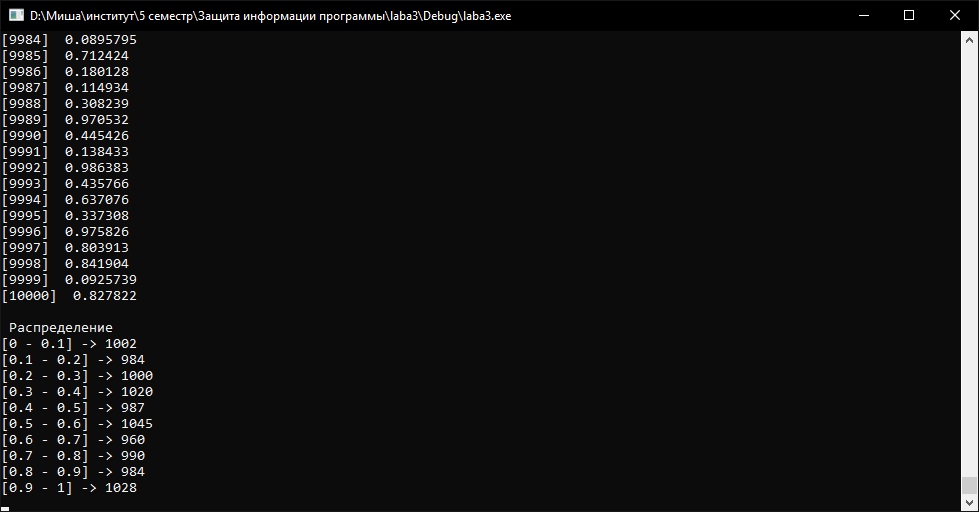
}

}Вывод программы:









Вывод: в ходе лабораторной работы разработали генератор случайных чисел, используя линейный конгруэнтный метод.