Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное учреждение высшего образования

«Новгородский государственный университет имени Ярослава Мудрого»

Кафедра «Информационных технологий и систем»

**Лабораторная работа №1**  
по дисциплине:

«Защита информации»

Разработал:

Студент группы 8091

Васильев И.В.  
 «\_\_» \_\_\_\_\_2021г

Проверил:

Жгун Т. В. \_\_\_\_\_\_

«\_\_» \_\_\_\_\_2021г

**Великий Новгород**

**2021**

**Задача:**

Реализовать работу генераторов псевдослучайных величин.

1. Линейно конгруэнтный генератор (*LCG*)
2. Генератор псевдослучайных чисел *BBS*
3. Линейный рекуррентный генератор (*LFSR*) при *n*=5.

**Описание алгоритмов:**

1. Линейного конгруэнтный генератор (*LCG*)

Генератор определяется рекуррентным соотношением :

*X n + 1 = (a X n + c) mod m*

У последовательности, созданной с помощью *LCG* и определённой целыми параметрами *m, a, c* и *X0,* период максимален и равен числу *m,* когда выполняются следующие условия:

* *c* и *m* – взаимно просты  (наибольший общий делитель *c* и *m* равен 1).
* *b = а-1* - кратно любому простому числу, являющемуся делителем *m*.
* 3.Если *m* кратно 4, тогда *b* также кратно 4.

Популярным выбором *m* является степень двойки *2n .* Очень часто в качестве *m* выбирают одно из простых чисел Мерсенна , где *p –*простое число (*р* = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257).

1. Генератора псевдослучайных чисел *BBS* (L. Blum, M. Blum, M. Shub) (генератор с квадратичным остатком).
2. Вначале выбираются два больших простых числа *p* и *q:*



1. Вычисляем число M = p q, называемое целым числом Блюма.
2. 3.Выбирается случайное целое число *х*, взаимно простое с М.



1. Вычисляем стартовое число генератора *х*0 : 

Последовательность вырабатывается по правилу:



Результатом *n*-го шага является один (обычно младший) бит числа *хn+1*. (Иногда в качестве результата принимают бит чётности). Для целей криптографии этот метод предложен в 1986 году.

1. Линейным рекуррентным генератором (*LFSR*) при *n*=5.

Работа генератора в поле  моделируется уравнением

.

Генератор вырабатывает последовательность максимальной длины, если матрица А имеет вид: , – коэффициенты неприводимого в поле  многочлена.

**Реализация**

Поставленная задача решена с помощью языка программирования С++ на фреймворке QT.

**Описание интерфейса**

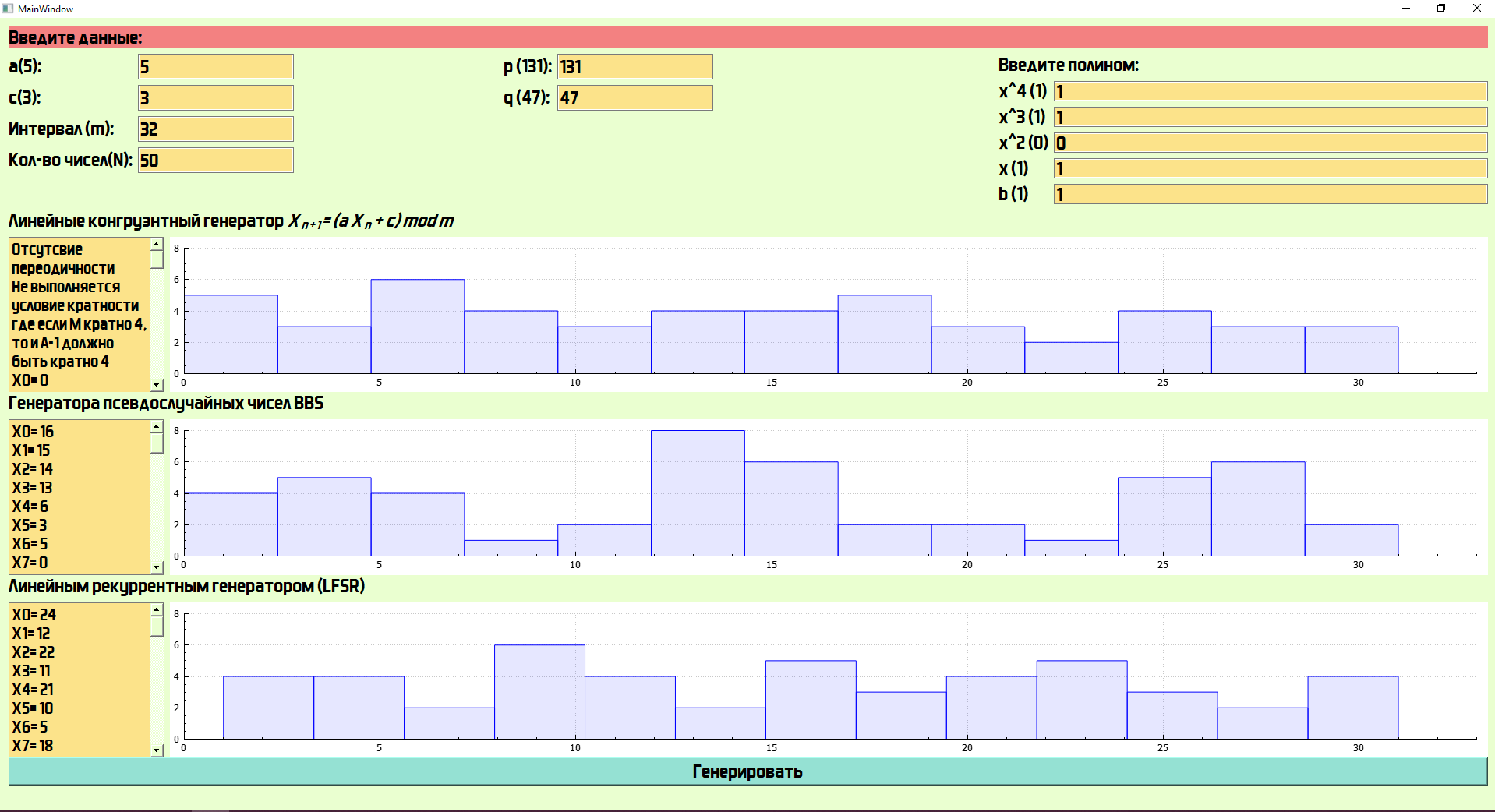
Программа предоставляет пользовательское окно с полями для ввода входных значений для генераторов.

Пользователю доступны следующие поля для ввода информации:

1. а (для формулы )
2. с (для формулы )
3. m (для формулы )
4. N – кол-во чисел для генерации
5. p (для формулы M = p q)
6. q (для формулы M = p q)
7. Коэффициенты x^4, x^3, x^2, x, b для полинома генератора *LFSR*

В главном окне, пользователь может видеть результат выполнения работы генераторов в графическом представлении в виде гистограмм. Программа предоставляет 3 гистограммы для всех предложенных генераторов.  
  
Для запуска программы, необходимо нажать на кнопку “Генерировать”

**Результат работы программы**



**Вывод**Для выполнения поставленной задачи, была разработана программа, осуществляющая генерацию чисел заданными генераторами.