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

Шаклеин В. В. \_\_\_\_\_\_  
 «\_\_» \_\_\_\_\_2021г

Проверил преподаватель:

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. 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*. 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**

Задача решена с помощью языка программирования Python, используются следующие дополнительные модули: numpy, matplotlib, seaborn, они необходимы для упрощения использования математических операций над массивами чисел и построения гистограмм.

**Описание интерфейса**

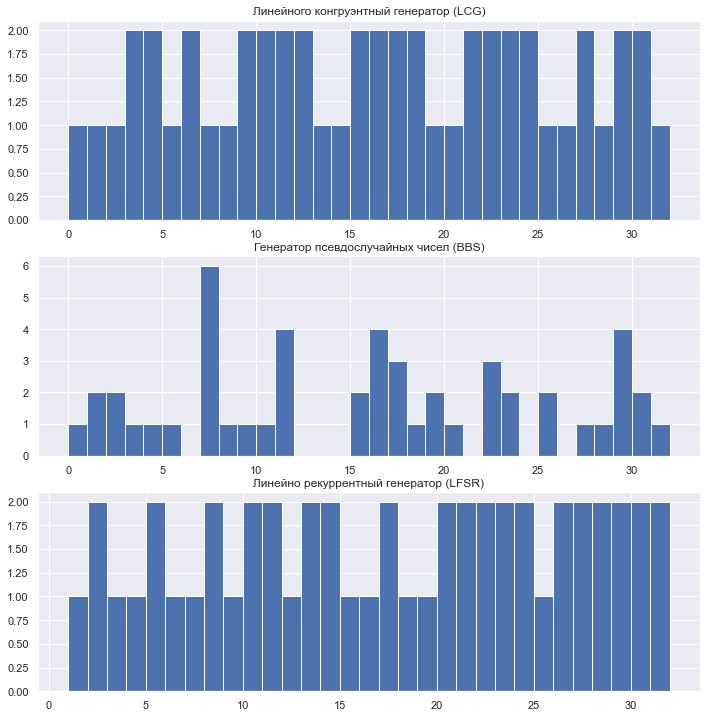
Все входные значения жёстко задаются в коде, так что программа не имеет пользовательского интерфейса в привычном понимании.

**Код программы**

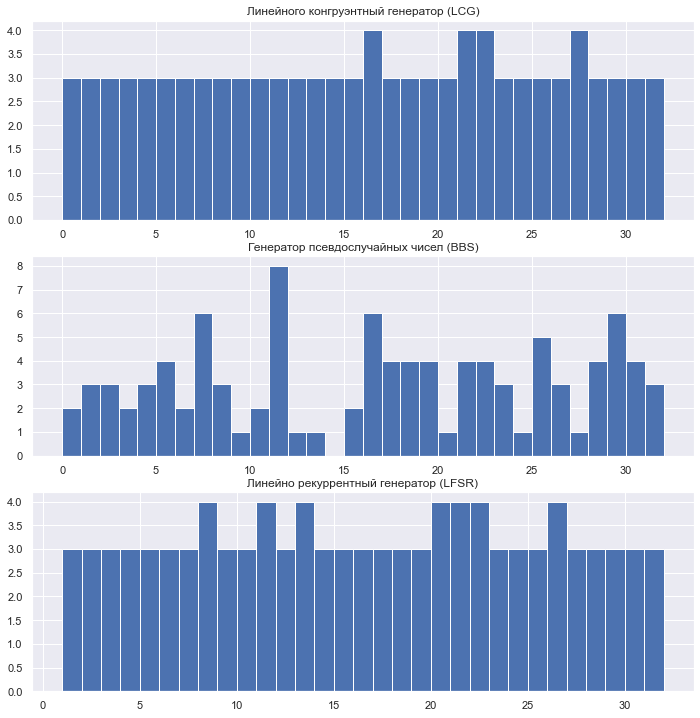
Код программы находится в папке с отчетом в файле *generators.ipynb* (так же код с возможностью запуска онлайн доступен по адресу <https://mybinder.org/v2/gh/sevskii111/infosec_reports/HEAD?filepath=lab01%2Fgenerators.ipynb>).

**Результат работы программы**

*Длина символов 50:*

****

Длина символов 100:



Длина символов 1000:

****

**Вывод**Для решения поставленных задач был выбран ЯП Python, также были построены гистограммы, из которых видно что генераторы LCG и LFSR дают равномерные распределения, а BBS относительно близкое к равномерному распределению.