

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИ ЛАБОРАТОРНОЙ РАБОТЫ №7**

**В РАМКАХ ДИСЦИПЛИНЫ «МЕТОДЫ И СРЕДСТВА КРИПТОРГАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»**

Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

Отчет по заданиям

1. Линейный конгруэнтный генератор (ЛКГ)

Формула ЛКГ:

Начальное значение: .

* 1. Параметры: a=5, b=7, c=17

Вычисляем последовательность:

Последовательность:

0 7 8 13 4 10 6 3 5 15 14 9 1 12 16 2

Период:  
т.к K12=K0, то период – 16

* 1. Параметры: a=6, b=3, c=23

Вычисляем последовательность:

Последовательность:

0 3 21 14 18 19 2 15 1 9 11

Период:

т.к K11=K0 период повторения 12. Полный период 23

1. Метод Фибоначчи

где ki — вещественные числа из диапазона [0,1], 3, 1 — целые положительные числа, параметры генератора. Для работы фибоначчиеву датчику требуется знать max {3,1} предыдущих сгенерированных случайных чисел.

Вычислите последовательность из десяти чисел, генерируемую методом Фибоначчи с запаздыванием начиная с ka при следующих исходных данных:

* 1. a= 3, b = 1, k0=0.6; k1=0.3; k2=0.5;
  2. a = 4, b = 2, k0=0.9; k1=0.3; k2=0.5; k3=0.9

1. Значения k0, k1, k2, k3, полученные с помощью линейного конгруэнтного генератора, равны: k0 = 1, k1 = 12, k2 = 3, k3 = 6. Найдите параметры а, b и c генератора ПСЧ.

Для нахождения параметров составим систему уравнений

НОД (11a+9, 2a+6) = НОД (a – 21, 48). Тогда минимальный модуль с должен быть больше, чем максимальный k (12). Тогда = НОД (a – 21, 48) = 16.

Тогда с = 16, (a+b) mod 16 = 12 и (2a+6) mod 16 = 0

Из второго уравнения (2a+6) mod 16 = 0 получим (2a) mod 16 = -6, однако остаток должен лежать в ограничении , тогда -6 + 16 = 10, следовательно (2a) mod 16 = 10,поле деления на 2 получим (a)mod8 = 5 тогда a = 5+8t, где

Тогда a = [5,13]

При а = 5, b = (12 -5) mod 16 = 7

При a = 13 b= (12-13) mod 16 = -1 = 15

Проверка вариантов для (a, b, c) = (13,15,16)

Получено не соответствие.

Проверка вариантов для (a, b, c) = (5,7,16)

Проверка удалась (a, b, c) = (5,7,16).

1. Вычислить х11 по методу генерации псевдослучайных чисел BBS, если p = 11, q = 19, х = 3.

Для вычисления используется формула

Тогда