МИНИСТЕРСТВО ОРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНСТВО ПО ОБРАЗОВАНИЮ

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОВЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ МЕХАНИКИ И ОПТИКИ

Безопасные информационные технологии

Лабораторная работа №1

«Разработка и исследование программных генераторов псевдослучайных последовательностей»

Выполнил:

Патрикеев Р.О. Р3253

Проверил:

Комаров И.И.

Санкт-Петербург

2016

1. Роль и место ГСЧ (ГПСЧ) в задачах обеспечения безопасности информационных технологий.

   ГСЧ – Генератор Случайных Чисел - алгоритм, порождающий последовательность чисел, элементы которой почти независимы друг от друга и подчиняются заданному распределению (обычно равномерному).
   Современная информатика широко использует псевдослучайные числа в самых разных приложениях — от метода Монте-Карло и имитационного моделирования до криптографии. При этом от качества используемых ГПСЧ напрямую зависит качество получаемых результатов.

2. Варианты программной реализации ГСЧ. Их достоинства и недостатки, области применения.

   1) Линейный конгруэнтный метод
      $x_{n+1} = (Ax_n + C) mod\ M.$
      Где M – модуль, A – множитель и C – приращение. Причем 0 ≤ A<M, 0 ≤C<M. Так же задается начальное значение x_0. Так же заданные переменные должны обладать следующими свойствами:
      - Числа C и M взаимно простые.
      - B = A – 1 кратно P для каждого простого P, являющегося делителем M.
      - B кратно 4, если M кратно 4.

      Так же существует набор рекомендация для выбора параметра M:
      - Число M должно быть довольно большим, так как период не может иметь больше M элементов.
      - Значение числа M должно быть таким, чтобы $(Ax_n + C) mod\ M$ вычислялось быстро.

      Стандарт ISO/IEC 9899 (на языке Си)

      ```
      #define RAND_MAX 32767
      static unsigned long int next = 1;
      int rand(void)
      {
          next = next * 1103515245 + 12345;
          return (unsigned int)(next/65536) % RAND_MAX;
      }
      void srand(unsigned int seed)
      {
          next = seed;
      }
      ```

   2) Генератор Фибоначчи с запаздыванием.
      $x_n = (x_{n-l} \star x_{n-k}) mod M$
      Где $\star$ - одна из простых бинарных арифметических операций: +, −,*, $\oplus$;
      l>k>0, при этом l и k, называемые задержками (лагами) выбираются не случайные, а строго определенные. Рекомендуются следующие значения лагов (l, k) = (55. 24), (17, 5) или (97, 33). Основной проблемой генератора Фибоначчи с запаздыванием является инициализация. Выходные значения генератора

очень чувствительны к начальному состоянию, и возникающие при инициализации ошибки могут сильно повлиять на получаемые значения.

3. Разработка ГСЧ.

В ходе выполнения лабораторной работы был разработан ГПСЧ на основе линейного конгруэнтного метода со входными значениями A = 45, C = 21, M = 67, X0 = 2.

Использовался следующий программный код (C++):

```
#include <iostream>
#include <cstdio>
#include <cstdlib>
int a = 45;
int c = 21;
int m = 67;
int seed = 2;

int getRand() {
	seed = (a * seed + c) % m;
	return seed;
}

int main()
{
	for(int i=0; i<22; i++)
		printf("%d ", getRand());
}
```

В результате получили повторяющуюся последовательность псевдослучайных чисел:

44 58 18 27 30 31 9 24 29 53 61 19 5 45 36 33 32 54 39 34 10 2

Что в двоичном виде выглядит следующим образом:

101100 111010 10010 11011 11110 11111 1001 11000 11101 110101 111101 10011 101 101101 100100 100001 100000 110110 100111 100010 1010 10

4. Тестирование ГСЧ

Разработанный генератор был протестирован с помощью частотного побитового тесты из пакета статических тестов NIST (определение отношения количества нулей и единиц в двоичной записи последовательности). Тест оценивает, насколько близка доля единиц к половине. Если вычисленное в ходе теста значение вероятности $p < 0,01$, то данная двоичная последовательность не является истинно случайной. В противном случае последовательность носит случайный характер.

Выполнив расчеты, получаем, что:

Количество единиц - 66, что составляет 57,9% от всей длины.

Количество нулей - 48, что составляет 42,1% от всей длины.

Так как вычисленная вероятность больше, чем 0.01, данная двоичная последовательность носит случайный характер.