# Теория псевдослучайных генераторов. Лабораторная работа

## Постановка задачи

***Цель***

1. Сгенерировать псевдослучайную последовательность заданным методом.
2. Исследовать полученную псевдослучайную последовательность на случайность.

***Исходные данные***

Исходными данными для лабораторных занятий являются метод генерации псевдослучайных чисел, диапазон генерации случайных чисел, функция распределения, которой должны подчиняться случайные числа, количество генерируемых чисел.

## Задачи

1) Сгенерировать последовательность из 10000 случайных чисел из диапазона [0,1]. Исходной программой для генерации ПСЧ может быть программа, созданная в рамках практической работы по данному курсу.
2) Протестировать статистические свойства последовательности псевдослучайных чисел:
   a) Вычислить математическое ожидание последовательности;
   b) Вычислить среднеквадратичное отклонение последовательности;
   c) Сравните полученные оценки с заданными в пп. 1 параметрами. Постройте графики зависимостей оценок от объема выборки. Оцените относительные погрешности для какой-либо одной выборки.
   d) Вычислить значение и дать ответ на вопрос удовлетворяет ли ППСЧ
      i) Критерию хи-квадрат;
      ii) Критерию серий;
      iii) Критерию интервалов;
      iv) Критерию разбиений;
      v) Критерию перестановок;
      vi) Критерию монотонности;
      vii) Критерию конфликтов.

**На входе:** текстовый файл с ПСЧ, обозначения критерия.
**На выходе**: точечные оценки параметров ППСЧ, ответ о соответствии ППСЧ указанному критерию.
Итогом лабораторной работы будет отчет, составленный по результатам проделанных вычислений. Титульный лист отчета представлен в приложении 1. Форма содержания отчета представлена в приложении 2. 2

Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

# ТЕОРИЯ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ

## ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ

студента X курса XXX группы

факультета компьютерных наук и информационных технологий

*Иванова Ивана Ивановича*

фамилия, имя, отчество

Научный руководитель

Ст. преподаватель _____ И.И. Слеповичев

подпись, дата

Саратов 2016

# Приложение 2. Описание отчета.

В отчете должны содержаться данные:

1) Функция распределения и параметры генерации ППСЧ;
2) Точечные оценки параметров ППСЧ;
3) Результаты проверки точечных оценок и критериев ППСЧ.

Таблица 1. Результаты проверки ПСП различными критериями

| | **lc** | **add** | **5p** | **lfsr** | **nfsr** | **mt** | **rc4** | **rsa** | **bbs** |
|---|---|---|---|---|---|---|---|---|---|
| **Хи-квадрат** | | | | | | | | | |
| **серий** | | | | | | | | | |
| **интервалов** | | | | | | | | | |
| **разбиений** | | | | | | | | | |
| **перестановок** | | | | | | | | | |
| **монотонности** | | | | | | | | | |
| **конфликтов** | | | | | | | | | |