Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский ядерный университет «МИФИ»
Предуниверситарий НИЯУ МИФИ. Университетский лицей №1523.

Кафедра физики.

ПРОЕКТНАЯ РАБОТА

ТЕМА: Исследование методов генерации случайных и псевдослучайных чисел и их использование

Автор проекта: учащийся 10М класса лицея 1523, Клубничкин И.К.
Руководитель: Мареева Е.С.

Москва, 2022

Введение. Случайные числа играют важную роль в самых разных областях науки. Их активно применяют в задачах моделирования, численного анализа, теории игр. Генераторы случайных чисел (далее - ГСЧ) в качестве механизма получения случайных величин используют разные физические процессы, так как на данный момент не существует математических алгоритмов, которые бы занимались генерацией подлинно случайных чисел. Данная тема крайне обширна и стоит также отметить, что ГСЧ и ГПСЧ (генераторы псевдослучайных чисел) являются ключевым звеном в современной криптографии и информационной безопасности. Таким образом, данная работа посвящена исследованию актуальной области, затрагивающей физику, математику и программирование.

Проблема. Генерация дешевой последовательности истинно случайных чисел.

Гипотеза. Допустим, что можно создать ГСЧ на основе некоторого случайного физического явления.

Актуальность. В наши дни случайные числа широко применяются в криптографии и многих других областях научного знания (случайные числа имеют применение в физике, анализе, программировании, моделировании и т. д.).

Цель. Исследование разных методов генерации случайных и псевдослучайных чисел, воссоздание ГСЧ и его оптимизация.

Задачи:

1. Изучение основных методов генерации случайных и псевдослучайных чисел.
2. Изучение областей применения ГСЧ и ГПСЧ.
3. Создание экспериментальной установки по генерации случайных чисел.
4. Анализ выходных последовательностей, выдаваемых генератором при различных параметрах.

Методы и методики, которые использовались при разработке проекта:

1. Изучение методов генерации случайных и псевдослучайных чисел.
2. Исследование методов определения меры близости заданной последовательности к случайной.
3. Создание экспериментальной установки по генерации случайных чисел и его оптимизация.
4. Проверка случайности последовательности, выдаваемой экспериментальным ГСЧ.

Этапы проектной деятельности:

1. Изучение статей, посвященных исследованию вопроса генерации случайных и псевдослучайных чисел.
2. Создание экспериментальной установки по генерации случайных чисел, ее исследование и оптимизация.
3. Исследование методов определения меры близости заданной псевдослучайной последовательности к случайной.
4. Определение меры близости заданной псевдослучайной последовательности, выдаваемой экспериментальным ГСЧ, к случайной.

Основные выводы по главам:

1. **Исследование проблемы генерации случайных чисел. Введение понятия ГСЧ и ГПСЧ.** Проблема генерации подлинно случайных чисел заключается в том, что если “случайная” последовательность будет создаваться некоторым математическим алгоритмом, то она будет предсказуема, что, к примеру, в задачах информационной безопасности может скомпрометировать безопасность личных данных. Подобные алгоритмы называют генераторами псевдослучайных чисел (сокращенно - ГПСЧ) и их также используют в науке, в задачах, при решении которых не нужна истинная случайность (задачи моделирования, имитация хаотичных действий пользователя ит.д.), а также для повышения производительности ГСЧ. Генераторы случайных чисел (сокращенно ГСЧ) формируют последовательность случайных чисел в зависимости от текущего значения какого-либо атрибута физической среды, который практически невозможно смоделировать при текущем уровне знаний. В рамках данного проекта я изучил эту область, наиболее распространенные методы генерации случайных и псевдослучайных чисел, а также методы проверки случайности некоторой последовательности.
2. **Обзор методов генерации случайных и псевдослучайных чисел.** В рамках данного проекта были изучены методы генерации случайных чисел, основанные на: тепловых колебаниях резистора, квантовых флуктуациях вакуума и атмосферных шумах. Также были изучены некоторые методы генерации псевдослучайных чисел.
3. **Создание экспериментальной установки по генерации случайных чисел.** В процессе реализации проекта был создан генератор случайных чисел, основанный на видеорегистрации движения парафина в лавовой лампе. За движением жидкостей наблюдает камера. Кадры из полученного видео преобразовываются в числа, которые в свою очередь проходят через алгоритм хэширования и превращаются в случайные числа. Используя аналогичный принцип могут быть также созданы ГСЧ, без изменения аппаратного и программного обеспечения, основанные на хаотичных движениях двойного маятника, беспорядочных движениях микроскопических видимых взвешенных частиц твёрдого вещества в жидкости или газе из-за броуновского движения и прочих стохастических макропроцессах.
4. **Методы определения меры случайности числовых последовательностей.** Был изучен пакет статистических тестов NIST для проверки случайности некоторой числовой последовательности. Также была проверена случайность выходных данных, выдаваемых экспериментальным ГСЧ, созданным в рамках проекта, которая подтвердила случайность выходной последовательности ГСЧ.

Выводы. В рамках проекта были изучены основные методы генерации случайных и псевдослучайных чисел, был создан собственный ГСЧ, основанный на случайном физическом процессе, работоспособность которого подтвердили соответствующие тесты. Были также изучены основные методы проверки случайности числовой последовательности.

Практическая значимость. Был создан работающий ГСЧ. Были рассмотрены варианты повышения производительности ГСЧ с помощью ГПСЧ.

Новые знания, полученные при работе над проектом. Для создания проекта был изучен большой пласт информации, посвященный методам генерации случайных и псевдослучайных чисел. Был создан рабочий прототип, генерирующий случайные числа, а также были освоены и изучены статистические тесты NIST.

Список использованных источников:

1. https://ru.wikipedia.org/wiki/%D0%93%D0%B5%D0%BD%D0%B5%D1%80%D0%B0%D1%82%D0%BE%D1%80_%D1%81%D0%BB%D1%83%D1%87%D0%B0%D0%B9%D0%BD%D1%8B%D1%85_%D1%87%D0%B8%D1%81%D0%B5%D0%BB
2. https://en.wikipedia.org/wiki/Lavarand
3. https://ru.wikipedia.org/wiki/%D0%93%D0%B5%D0%BD%D0%B5%D1%80%D0%B0%D1%82%D0%BE%D1%80_%D0%BF%D1%81%D0%B5%D0%B2%D0%B4%D0%BE%D1%81%D0%BB%D1%83%D1%87%D0%B0%D0%B9%D0%BD%D1%8B%D1%85_%D1%87%D0%B8%D1%81%D0%B5%D0%BB#%D0%94%D0%B5%D1%82%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5_%D0%93%D0%9F%D0%A1%D0%A7
4. https://csrc.nist.gov/Projects/Random-Bit-Generation/Documentation-and-Software
5. https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B0%D1%82%D0%B8%D1%81%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D1%82%D0%B5%D1%81%D1%82%D1%8B_NIST