В. В. Пантелеев, А. В. Никитенко

ИССЛЕДОВАНИЕ ФУНКЦИИ ГЕНЕРАЦИИ СЛУЧАЙНЫХ ЧИСЕЛ НА ФИЗИЧЕСКИХ И СИНТЕТИЧЕСКИХ ПЛАТФОРМАХ

Исследуется процесс генерации случайных чисел на различных компиляторах и платформах, а так же физические источники случайностей. Нахождение более оптимального способа получения случайных чисел.

Введение

Современная информатика широко использует псевдослучайные числа в самых разных приложениях — от метода Монте-Карло и имитационного моделирования до криптографии. При этом от качества используемых источников случайных чисел напрямую зависит качество получаемых результатов.

I. Синтетические источники случайностей

Энтропия – мера беспорядка системы. В большинстве компиляторов используются математические методы, завязанные на времени. Из этого можно сделать вывод, что генерируемые числа являются псевдослучайными, так как их можно предсказать, зная алгоритм и исходные данные. Так как математические модели генерации псевдослучайных чисел различны, следовательно, у каждого способа есть свои преимущества и недостатки. Основные характеристики генераторов это их скорость и уровень энтропии. Чтобы оценить уровень энтропии, мы будем сравнивать полученные результаты с контрольным образцом, который представляет собой самый доступный генератор случайных чисел – монетка. Так как мы не располагаем необходимым оборудованием, мы не сможем объективно оценить уровень энтропии из экспериментальных данных. Но, полагаясь на документацию, мы сделаем выводы об уровне энропии.

Таблица 1 – Результаты эксперимента

Компилятор	Время генерации
C	≈ 0
C++	≈ 0
Java	≈ 0
Bash	≈ 0
PHP	0,008
/dev/random	35

Время работы PHP обусловлено тем, что это интерпретируемый язык. Время работы псевдоустройства /dev/random объясняется тем, что оно использует шумы из драйверов устройств и других источников для генерации чисел.

II. Физические источники случайности

Но кроме синтетических генераторов существуют физические (природные) источники случайностей. Их энтропия не вызывает сомнения. Но многократно возрастает время получения чисел из данных источников. Рассмотрим самые доступные из них:

- Подбрасывали монетку, орёл – 1, решка – 0.
- Просили человека назвать любое число. Чётное – 1, нечётное – 0.
- Смотрели номера проезжающих мимо машин, получая 4 цифры. Чётная – 1, нечётная – 0.

Таблица 2 – Результаты эксперимента

Способ	Время генерации
Монетка	6 мин
Номера машин	20 мин
Опрос людей	3 ч 12 мин

Выводы

Проведённые нами опыты наглядно демонстрируют преимещуства и недостатки всех типов генераторов псевдослучайных чисел. Синтетические генераторы многократно ускоряют процесс получения случайных чисел. Но, ставится под сомнение уровень энтропии полученных результатов, кроме псевдоустройства в ОС Linux/Unix /dev/random, у которого в основе лежат физические процессы, происходящие в устройствах компьютера. Физические же генераторы обладают высоким уровнем энтропии, но требуют намного больше времени. Выбор генератора зависит от конкретной задачи.

Пантелеев Владимир Валерьевич, Никитенко Артур Владимирович, студенты группы 240301 БГУИР.

Научный руководитель: Кривоносова Татьяна Михайловна, доцент кафедры вычислительных методов и программирования БГУИР, krivonosova@bsuir.by