3. Рахматуллин Х.А. Основы газодинамики взаимопроникающих движений сжимаемых сред [Текст] // ПММ. –1956.—Т.20. – В.1.—С.184-195

4. Нигматулин Р.И. Динамика многофазных сред [Текст] // М.: Наука, 1987.–Ч.1.—464с.

5. Русяк И.Г., Ушаков В.М. Внутрикамерные гетерогенные процессы в ствольных системах [Текст] // Екатеринбург: УрО РАН, 2001. 259с.

6. Численное решение многомерных задач газовой динамики [Текст] / С.К. Годунов [и др.] // М.: Наука, 1976.—400с.

М.В. Соловьев

МОБИЛЬНАЯ ГЕНЕРАЦИЯ СЛУЧАЙНЫХ ЧИСЕЛ

(Самарский университет)

Введение. Генераторы случайных чисел широко используются в компьютерной безопасности и криптографии, в научных вычислениях и в различных играх. Их можно разделить на две основные категории [1].

1. Генераторы псевдослучайных чисел – это генераторы основанные на сложной математической функции, которая имитирует случайность.

2. Генераторы истинных случайных чисел – это генераторы, которые порождают случайные числа на основе хаотически изменяющихся параметров физического процесса. Работа таких устройств основана на источниках энтропии. Эти процессы абсолютно непредсказуемы и их случайность проверяется с помощью специальных статистических тестов.

Мобильные устройства уже давно получили широкое распространение и превратились в уменьшенные персональные компьютеры с наборами различных быстродействующих датчиков. Как раз эти датчики и могут стать надежными источниками энтропии для создания генератора случайных чисел.

1. Постановка задачи. Таким образом, ставится задача разработки мобильного генератора случайных чисел.

2. Анализ задачи. Для создания генератора случайных чисел необходимо выбрать источники энтропии [2]. Такие источники могут быть выбраны из набора датчиков мобильного устройства таких, как акселерометр, микрофон, гироскоп, люксметр, магнетометр. Последовательностям чисел на выходе генератора должны быть предъявлены требования: 1) «равномерности», то есть равной вероятности появления различных чисел, битовых фрагментов чисел и групп чисел; 2) «случайности», то есть непредсказуемости появления отдельных чисел или групп чисел.

3. Описание решения. Для разработки генератора необходимо определить алгоритм генерации случайных чисел. Для рассмотрения были выбраны несколько таких алгоритмов.

1. Yarrow - это криптографически стойкий генератор случайных чисел, разработанный Б.Шнайером и Н.Фергюсоном [7]. Он состоит из четырёх основных компонентов:

a) аккумулятора энтропии, который собирает образцы из источников энтропии в два пула (быстрый и медленный);

b) механизма пересева, периодически засеивающего ключ новой энтропией из пулов;

c) механизма генерации, выполняющего генерацию случайной последовательности из ключа.

d) подсистемы управления пересевом, определяющего, когда нужно пересеять ключ.

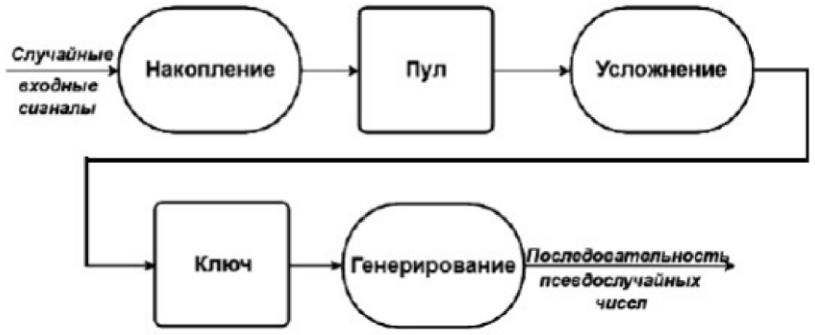

Рис. 1. Общий вид алгоритма

В настоящее время алгоритм Yarrow считается сильно защищенным генератором случайных чисел. Это позволяет использовать его для широкого спектра задач: шифрования, электронной подписи, целостности информации и других задач.

2. Fortuna – алгоритм генерации случайных чисел, который является усовершенствованием алгоритма Yarrow [6].

Основным отличием Fortuna от Yarrow является иной подход к работе аккумулятора энтропии — Yarrow требует наличия механизмов оценки количества энтропии и использует только два пула.

В итоге для реализации мобильного генератора случайных чисел был выбран алгоритм Yarrow.

Для тестирования полученной энтропии из источников был выбран программный комплекс NIST SP 800-22, разработанный Национальным Агентством по Стандартизации США. Он содержит сравнительно небольшой, тщательно отобранный комплект статистических тестов, предназначенных для исследования «случайности» и «равномерности» битовых последовательностей, производимых «криптографически стойкими» ГПСЧ [3]. В ходе исследований двоичные данные, полученные с датчиков были проверены двумя тестами [5,8].

1. Частотный побитовый тест. Цель теста - выяснить, действительно ли число нулей и единиц в последовательности приблизительно одинаковы, как это можно было бы предположить в случае истинно случайной бинарной последовательности.

2. Частотный блочный тест. Цель теста - выяснить действительно ли частота повторения единиц в блоке длиной m бит приблизительно равна m/2, как можно было бы предположить в случае абсолютно случайной последовательности.

После проведенных исследований некоторые датчики, такие как магнетометр, люксметр, гироскоп были исключены из-за плохих результатов. Тем не менее, микрофон и акселерометр показали хорошие результаты. С каждого датчика были получены 32-битные числа, которые были протестированы отдельно по битам и блоками. Результаты тестирования отображены на тепловой карте (рис. 1). Черным цветом обозначены «хорошие» биты, которые будут использоваться в качестве энтропии [9].

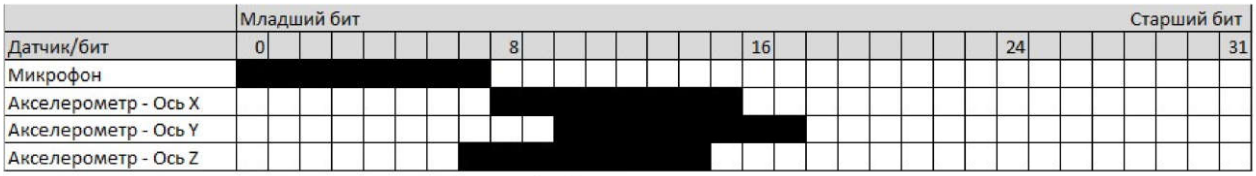

Рис. 1. Тепловая карта

Статистические тесты продемонстрировали какие датчики подходят в качестве источников энтропии для разработки генератора случайных чисел – это микрофон и акселерометр. Из рассмотренных алгоритмов генерации был выбран Yarrow. Таким образом, мобильное устройство подходит для разработки на его основе быстродействующего и качественного генератора случайных чисел.

Был составлен алгоритм работы генератора, использующего эти датчики.

1. Накопитель энтропии конкатенирует значения, полученные с микрофона и акселерометра в файл в памяти мобильного устройства, но только те биты, которые были выбраны выше, как «хорошие».

2. Запуск алгоритма Yarrow [4], в котором для шифрования используется алгоритм *DES* (функция $E_k()$), а в качестве хэш-функции $h()$ – *SHA-1*.

3. Задание начальных значений:

1) Задать размер шифруемого сообщения n = 64, т.к. для шифрования используется алгоритм DES;

2) Задать $k = 64$ – размер ключа K, используемого при шифровании;

3) Задать значение P_g ($0 < P_g < 2^{n/3}$, обычно $P_g = 10$), определяющее количество бит, после генерации которых нужно обновить значение ключа K;

4) Задать значение P_t ($P_t > P_g > 0$), определяющее количество бит, после генерации которых нужно запустить механизм обновления ключа K и счётчика C_i, используя накопитель энтропии, и сформировать v – следующее значение из файла накопленной энтропии;

5) Задать $t = 0$, где t – количество запусков механизма обновления ключа и счётчика;

6) Задать некоторое начальное значение n–битного счётчика C_0;

7) Присвоить $curP_g = P_g$, $curP_t = P_t$.

4. Для $i = 1,m$ выполнить:

1) Если $curP_g = 0$, то:

a) с помощью функции $G(i)$ сгенерировать k бит, которые будут использоваться в качестве нового ключа K;

b) присвоить $curP_g = P_g$.

2) Если $curP_t = 0$, то:

a) вычислить $v_0 = h(v \,||\, t)$;

b) вычислить $v_i = h(v_{i-1} \,||\, v_0 \,||\, t)$ для $i = 1, \ldots, t$;

c) вычислить $K = H(h(v_t \,||\, K), k)$;

d) вычислить $C_i = \mathrm{E_K}(0)$;

e) присвоить $curP_g = P_g$, $curP_t = P_t$, $t = t + 1$.

3) Вычислить $x_i = G(i)$, которое является следующим блоком выходной последовательности.

4) Выполнить $curP_g = curP_g - 1$ и $curP_t = curP_t - 1$.

5. В результате предыдущего шага формируется выходная случайная последовательность.

В этом алгоритме использованы функции $G()$ и $H()$, определенные следующим образом.

Функция $G(i)$:

1. Вычислить $C_i = (C_{i-1} + 1) \bmod 2^n$.
2. Вернуть $E_K(C_i)$ как результат вычисления функции.

Функция $H(s,k)$:

1. Вычислить $s_0 = s$.
2. Вычислить $s_i = h(s_0 \,||\, \ldots \,||\, s_{i-1})$ для $i = 1,2\ldots$
3. Вернуть первые k-бит от конкатенации двоичных слов $s_0 \,||\, s_1 \,||\, \ldots$

Выводы. Поставлена задача разработки генератора случайных чисел на основе датчиков мобильного устройства. Выбраны подходящие источники энтропии. Выбран и проанализирован алгоритм генерации чисел на основе энтропии.

Литература

1. Кнут Д. Э. Искусство программирования. Том 2. Получисленные алгоритмы. — М: Вильямс, 2001.— 832 с.

2. Иванов М.А. Теория, применение и оценка генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. - М.: КУДИЦ-ОБРАЗ, 2003. - 240 с.

3. Климентьев К.Е. Выбор и реализация программного генератора псевдослучайных чисел для системы мультиагентного моделирования // Международная научно-техническая конференция "Перспективные информационные технологии (ПИТ 2019)". — 2019. — С. 52-58.

4. Генерация криптографически безопасной псевдослучайной последовательности [Электронный ресурс]. URL: https://ami.nstu.ru/~kurlaev/ib/Materials/lab2.pdf.

5. Статистическая проверка случайности двоичных последовательностей методами NIST [Электронный ресурс]. – URL: https://habr.com/ru/company/ securitycode/ blog/237695/.

6. Алгоритм Fortuna [Электронный ресурс]. – URL: https://ru.wikipedia.org/ wiki/Алгоритм_Fortuna.

7. Криптографическая стойкость генераторов случайных чисел. Алгоритм Ярроу [Электронный ресурс]. – URL: https://cyberleninka.ru/article/ n/kriptograficheskaya-stoykost-generatorov-sluchaynyh-chisel-algoritm-yarrou/ viewer.

8. Статистические тесты NIST [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/Статистические_тесты_NIST.

9. Toward Sensor-Based Random Number Generation for Mobile and IoT Devices [Электронный ресурс]. – URL: http://www.cs.wm.edu/~gzhou/files/ Entropy_IoT16.pdf.

Р.А. Учайкин

МЕТОД АНАЛИЗА ОБЕСПЕЧЕННОСТИ ПОДРАЗДЕЛЕНИЙ ПРЕДПРИЯТИЯ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

(Самарский государственный технический университет)

Введение. Задача оптимального использования средств вычислительной техники (СВТ) на промышленных предприятиях является одной из ключевых в современных информационных технологиях. Современное машиностроительное предприятие имеет в своей структуре комплекс проектных, конструкторских и производственных подразделений. Их задачи обусловлены как созданием новых образцов изделий, так и модернизацией выпускаемой продукции.

В работе [1] разрабатывались методы распределения средств вычислительной техники в информационных системах предприятий. Автором предложен подход к постановке задачи оптимизации распределения компьютерного оборудования на машиностроительном предприятии [2]. Однако решение такой задачи требует предварительной оценки, насколько эффективно используется уже имеющаяся в подразделениях вычислительная техника. Известен метод анализа среды функционирования (Data Envelopment Analysis – DEA), который успешно применялся для сравнения разнородных предприятий [3]. Перспективность метода DEA была подтверждена и в других задачах: использование финансовых ресурсов, анализ водообеспечения регионов, оценка эффективности программных систем и др.

В данной статье рассматривается решение задачи формальной оценки эффективности использования компьютеров в подразделениях предприятия с целью планирования их оптимального распределения и эксплуатации.