УДК 621.391.1

А. Е. Новиков – магистрант кафедры микро- и нанотехнологий аэрокосмического приборостроения
Д. К. Шелест (д-р техн. наук, проф.) – научный руководитель

ОЦЕНКА СООТВЕТСТВИЯ ПОЛУЧЕННОГО ПСЕВДОСЛУЧАЙНОГО БИНАРНОГО СИГНАЛА ИМИТАТОРА ЗАДАННОМУ ЗАКОНУ РАСПРЕДЕЛЕНИЯ

Проблема создания имитаторов псевдослучайных сигналов для оперативного тестирования и контроля радиосредств сталкивается с необходимостью решения ряда актуальных задач. Среди которых можно выделить:

- производительность формирования псевдослучайных сигналов;
- соответствие полученных законов распределения псевдослучайных последовательностей заданному теоретическому распределению;
- выбор меры близости соответствия полученных законов распределения к заданному теоретическому распределению;
- возможность оперативного изменения параметров сигнала, изменяя форму и параметры реализуемого закона распределения;
- оперативный выбор заданной длины псевдослучайной последовательности имитатора;
- оперативный выбор закона распределения формируемой последовательности.

Наиболее распространенными законами распределения псевдослучайных сигналов является, равномерный закон (белый шум) и нормальный закон распределения [1].

Следовательно, задача достоверной оценки соответствия и выбора меры близости закона распределения полученного псевдослучайного сигнала имитатора заданному закону распределения является актуальной.

Для реализации этой задачи используются два основных подхода [1]:

- программная реализация генерирования псевдослучайных последовательностей;
- аппаратная реализация формирования псевдослучайных последовательностей.

Для построения имитаторов может быть использованы и тот и другой подходы. Однако программная реализация позволяет получить более гибкие алгоритмы формирования последовательностей псевдослучайных сигналов с большей длиной цикла. Преимущества аппаратной реализации определяется оперативностью и мобильностью формирования псевдослучайных сигналов непосредственно на объекте тестирования и контроля. Указанные особенности определяют области использования того или иного подхода.

Наибольшее распространение в настоящее время получили сигналы с бинарной фазовой манипуляцией. Случайным параметром, которым является положение (время возникновения) фронта последующего импульса [1].

Рассмотрим алгоритмы формирования псевдослучайных последовательностей, получившие наибольшее распространение.

Регистр сдвига с линейной обратной связью – аппаратный метод, получивший наибольшее распространение. На рис. 1, представлена схема регистра сдвига с линейной обратной связью.

Регистр сдвига с обратной связью состоит из двух частей: регистр сдвига и функции обратной связи. Длина регистра сдвига выражается числом битов. При каждом извлечении бита все биты регистра сдвига сдвигаются на право, на одну позицию.

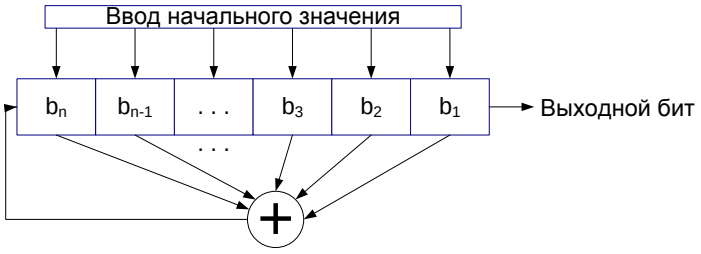

Рис. 1. Регистр сдвига с линейной обратной связью [1]

Обратная связь представляет собой операцию сумма по модулю два над некоторыми битами регистра [1].

Алгоритм *SHA* – программный метод реализации псевдослучайных последовательностей. На рис. 2 представлена схема работы основного этапа алгоритма *SHA*. Алгоритм *SHA* реализует хеш-функцию, построенную на идее функции сжатия [3].

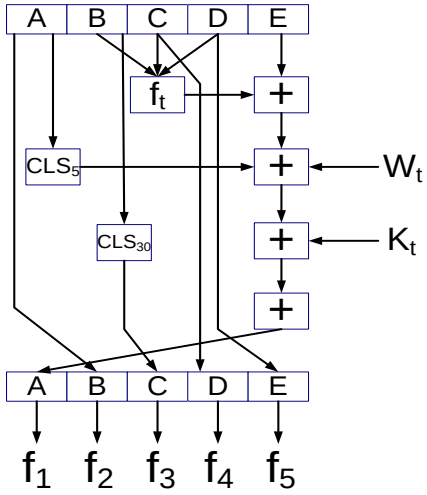

Рис. 2. Схема работы основного этапа алгоритма *SHA*
A, B, C, D, E – пять слов из буфера, f_t – элементарная логическая функция,
CLS_s – циклический левый сдвиг 32-битного аргумента на *s* битов,
W_t – 32-битное слово, полученное из текущего входного 512-битного блока, K_t – дополнительная константа,
+ – сложение по модулю 2, f_1-f_5 – набор выходных функций [3].

Алгоритм *SEAL* – программный метод реализации псевдослучайных последовательностей. На рис. 3 представлена схема работы алгоритма *SEAL* [3]. Особенность алгоритма *SEAL* заключается в том, что в действительности это не традиционный потоковый шифр, а семейство псевдослучайных функций [3].

Основной характеристикой псевдослучайной последовательности является закон распределения. В настоящие время при контроле и тестирования радиосредств используются нормальный и равномерный законы распределения (белый шум).

В теории математической статистики известны критерии согласия законов распределения: Пирсона, Колмогорова и др. При использовании критерия Пирсона сравнивают относительные частоты попадания случайной величины в интервалы гистограмм сравниваемых распределений [5].

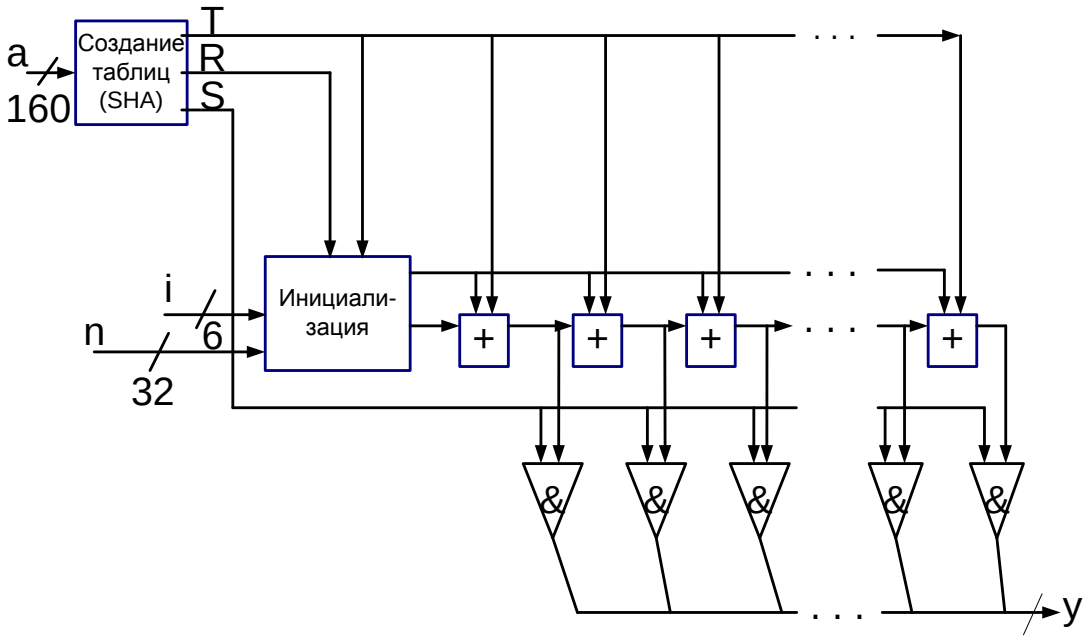

Рис. 3. Схема работы алгоритма *SEAL:*
a – входная последовательность, *T,R,S* – таблицы, полученные по алгоритму *SHA*, *n* – индекс, *l* – номер позиции, + – сложение по модулю 2, *&* – операция логического *И*, *y* – выходная последовательность [3].

$$\chi^2 = \sum_{\tau^2}^{k} \frac{(n_i + np_i)}{np_i},$$

где n – общее число наблюдаемых изделий, $p_i = n_i / n$ – частотность i-го интервала статистического ряда, k – число интервалов статистического ряда.

По критерию Колмогорова соответствие теоретического и экспериментального распределений проверяется по выполнению условия[5].

$$D\sqrt{k} < 1,$$

где D – наибольшее отклонение теоретической кривой распределения от экспериментальной, k – общее количество экспериментальных точек.

Метод сопоставления полученного закона распределения с заданным (теоретическим) позволяет давать ориентировочную оценку расхождения или совпадений законов распределений. При большом числе наблюдений (n > 100) неплохие результаты дает вычисление выборочных параметров формы распределения: эксцесса и асимметрии. Принято говорить, что предположение о нормальности распределения не противоречит имеющимся данным, если асимметрия близка к нулю, то есть лежит в диапазоне от -0,2 до 0,2, а эксцесс – от 2 до 4 [4].

Области использования критериев согласия заключаются в том, что для проведения максимально быстрой оценки согласия можно использовать критерий Колмогорова, который требует меньшей статистической информации о формируемой псевдослучайной последовательности. При подробном анализе псевдослучайной последовательности следует использовать критерий Пирсона.

Для оперативного получения закона распределения созданной псевдослучайной последовательности необходимо решить задачу измерения случайных параметров и построения гистограммы псевдослучайной последовательности, которая является самостоятельной задачей.

Одним из способов её реализации является запоминание полученной псевдослучайной последовательности или её достоверной выборки с последующим анализом случайных параметров и построение гистограммы. Реализация такого способа наиболее подходящая при программной реализации алгоритма формирования псевдослучайной последовательности.

Программная реализация алгоритма позволяет отследить все параметры получаемой псевдослучайной последовательности, измерить выходные значения и на их основе построить гистограмму.

Так же при исследовании можно выявить ряд факторов, которые влияют на основные параметры получаемой псевдослучайной последовательности и как результат варьирования этими факторами возможность получить наиболее близкую псевдослучайную последовательность к заданной.

При аппаратной реализации алгоритма формирования псевдослучайной последовательности строят первоначальную модель. Как правило, модель создают в программном виде и проводят все возможные исследования программной реализации алгоритма, после чего создают аппаратную модель. Однако, полноценное исследование полученной псевдослучайную последовательности при аппаратной реализации является довольно сложной задачей.

Основное исследование полученной псевдослучайной последовательности можно провести при помощи анализатора спектра, например «белого шума», т.е. убедиться в равномерном распределении частот по спектру. Исследование значений полученной псевдослучайной последовательности возможно только при построении специальной аппаратуры имеющей туже частоту дискретизации, что и сам имитатор и позволяющей сохранять полученные значения псевдослучайной последовательности.

Обобщая приведенные результаты создания имитаторов, можно сделать следующие выводы.

1. В качестве меры близости соответствия закона распределения формируемой псевдослучайной последовательности и заданного закона следует выбирать критерии согласия Пирсона и Колмогорова.

2. В зависимости от условий применений для реализации выбирается программный или аппаратный метод реализации псевдослучайных последовательностей.

3. Задача измерения случайных параметров псевдослучайной последовательности является самостоятельной задачей для получения экспериментальных данных.

4. Среди известных методов формирования псевдослучайных последовательностей наиболее перспективным является программная реализация, так как программный способ формирования псевдослучайных последовательностей позволяет более точно исследовать полученную псевдослучайную последовательность и выявить факторы, влияющие на её параметры.

Библиографический список

1. Шумоподобные сигналы в системах передачи информации / Под ред. В.Б. Пестрякова. М.: Сов. радио, 1973. – 424с.
2. Поляк М.Д. Моделирование случайных процессов с заданными закона распределения / Сборник докладов. 63 – я СНТК ГУАП. Технические науки. СПб.: ГУАП, 2010. Часть 1. – с. 263 – 266.
3. Иванов М.А. Криптографические методы защиты информации в компьютерных система и сетях. М.: КУДРИЦ-ОБРАЗ, 2001.-368с.
4. Кобзарь А. И. Прикладная математическая статистика. Справочник для инженеров и научных работников. — М.: Физматлит, 2006. — 816 с.
5. Р 50.1.037-2002 Прикладная статистика. Правила проверки согласия опытного распределения с теоретическим. Часть II. Непараметрические критерии.