УДК 691.321.25

Захарченко Н. В., Радзимовский Б. К., Корчинский В. В.
Захарченко М. В., Радзімовський Б. К., Корчинський В. В.
Zaharchenko M.V., Radzimovsky B.K., Korchinsky V.V.

СЛУЧАЙНЫЕ ЧИСЛА И ПОСЛЕДОВАТЕЛЬНОСТИ НА ОСНОВЕ СИСТЕМ С ДИНАМИЧЕСКИМ ХАОСОМ

ВИПАДКОВІ ЧИСЛА ТА ПОСЛІДОВНОСТІ НА ОСНОВІ СИСТЕМ З ДИНАМІЧНИМ ХАОСОМ

RANDOM NUMBERS AND SEQUENCES BASED ON THE DYNAMIC CHAOS SYSTEMS

Аннотация. Для конфиденциальных систем связи предложены алгоритмы генерирования ряда случайных чисел и бинарных последовательностей на основе различных дискретных отображений в генераторах хаоса. Рассмотрены статистические характеристики генерируемых последовательностей с оценкой их качества.

Анотація. Для конфіденційних систем зв'язку запропоновані алгоритми генерування ряду випадкових чисел і бінарних послідовностей на основі різних дискретних відображень у генераторах хаосу. Розглянуті статистичні характеристики генерованих послідовностей з оцінкою їх якості.

Summary. Several algorithms for confidential telecommunication systems for generating random numbers and binary sequences based on different digital mapping in the chaos generators were proposed. The statistical characteristics of the generated sequences with their quality assessment were discussed.

Случайные числа и их генераторы находят самое широкое применение в криптографических алгоритмах защищенных систем связи, вычислительных методах при статистическом и имитационном моделировании, а также в различных приложениях [1]. Генерируемые последовательности чисел должны быть статистически неотличимы от истинно случайных, поэтому поиск и исследование таких генераторов является актуальной проблемой.

В [2] предложен метод синтеза шумового сигнала на основе дискретных систем с динамическим хаосом и показана перспективность его использования в современных системах передачи информации. Системы с использованием шумовых сигналов имеют повышенную информационную емкость, высокую помехозащищенность и обеспечивают конфиденциальность передаваемых сообщений. Предложенный метод позволил сформировать шумовой сигнал гауссова типа с помощью простых по структуре генераторов, в которых управление хаотическими режимами осуществляется путем малых изменений их параметров. Такие генераторы могут формировать реализации хаотического сигнала неограниченной длины с отсутствием периодичности в последовательностях их амплитудных значений. Если рассматривать последовательность амплитудных значений как ряд чисел случайного процесса, свойствами которого обладает хаотический сигнал, то появляется возможность генерирования такими генераторами неограниченного ряда возможно случайных чисел.

Однако в литературе недостаточно исследована такая возможность, поэтому целью статьи является разработка методов генерирования ряда случайных чисел и бинарных последовательностей с оценкой их качества на основе различных дискретных отображений в генераторах хаоса.

Свойства дискретных генераторов хаоса определяются видом функции отображения и значениями управляющих параметров [3]. Генерировать хаотическое колебание x_n можно в соответствии с разностным уравнением вида:

$$x_{n+1} = f(x_0; x_n; a), \quad (1)$$

где $f(\cdot)$ – нелинейная функция отображения; a – управляющий параметр, x_0, x_n, x_{n+1} – начальное, текущее и последующее значения соответственно.

Рассмотрим несколько дискретных отображений в генераторах хаоса [3]:

1) степенное

$$x_{n+1} = a(1 - |1 - 2x_n|^l), \quad (2)$$

где $x_0 = 0{,}8$, $a = 0{,}9$, $l = 0{,}8$;

2) логистическое

$$x_{n+1} = ax_n(1 - x_n), \quad (3)$$

где $x_0 = 0{,}9$, $a = 3{,}9$;

3) кубическое

$$x_{n+1} = (1 - 4a)x_n + 4ax_n^3, \quad (4)$$

где $x_0 = 0{,}5$, $a = 0{,}92$;

4) сдвига

$$x_{n+1} = ax_n \bmod 1, \quad (5)$$

где $x_0 = 0{,}8$, $a = 3{,}0$;

5) логистическое

$$x_{n+1} = ax_n(1 - x_n), \quad (6)$$

где $x_0 = 0{,}5$, $a = 3{,}9$.

На выходах приведенных генераторов получаем непериодические хаотические последовательности заданной длины, например, $N = 500000$ значений. Математическое ожидание последовательности $m = \frac{1}{N}\sum_{n=0}^{N-1} x_n$, дисперсия $D = \frac{1}{N}\sum_{n=0}^{N-1}(x_n - m)^2$. Так как хаотический сигнал в общем случае имеет ненулевое математическое ожидание, то будем использовать центрированный $\overline{x_n} = x_n - m$ и нормированный процесс на интервале (0,1).

Заметим, что каждое из приведенных отображений характеризуется разными распределениями вероятности амплитудных значений, а небольшие изменения параметров или начальных условий приводят к совершенно другим реализациям. Например, генераторы с разными начальными значениями в логистических отображениях (2) и (5) генерируют реализации, с коэффициентом корреляции $r_{2,5} = -8{,}682 \cdot 10^{-4}$.

Для проверки генераторов случайных и псевдослучайных чисел известны многие статистические критерии: критерий χ^2 Пирсона, критерий Колмогорова-Смирнова, критерий Стьюдента и др. Наиболее удобным и универсальным считается критерий χ^2, достоинством которого является независимость от распределения случайной величины.

Как отмечено в [4], с помощью статистического критерия χ^2 Пирсона можно реализовать такие проверочные тесты, как проверка распределения (тест частот), проверка серий (тест пар), проверка интервалов (тест интервалов), проверка комбинаций (покер-тест).

Первый тест в работе является основным. Он предназначен для проверки критерия согласия между эмпирическим и теоретическим распределениями. С помощью второго и третьего тестов проверяется критерий статистической независимости следующих друг за другом вырабатываемых чисел. Четвертый тест используется для проверки критерия случайности. Таким образом, данные тесты охватывают проверку тех свойств, которыми должны обладать случайные числа. Порядок применения критерия χ^2 и выбор необходимого критерия значимости рассмотрены в [1, 4].

Для проверки согласия между эмпирическим и теоретическим распределениями в [1] предлагается выбирать двусторонний критерий значимости с 5 и 95 %-ми уровнями, при которых вероятности соответственно равны $P_H(\chi^2) = 0{,}05$ и $P_B(\chi^2) = 0{,}95$. Вероятности $P_H(\chi^2)$ и $P_B(\chi^2)$ образуют доверительный интервал для вычисляемых значений χ_i^2. Результаты испытаний считаются удовлетворительными, если x_i^2 не выходит за пределы этого доверительного интервала, т. е. $P_{\text{Н}}(\chi^2) < P(\chi_i^2) < P_{\text{В}}(\chi^2)$. При этом, чем меньше значение $P(\chi^2)$ в доверительном интервале, тем большее отклонение эмпирического распределения от теоретического и, наоборот, в противном случае. Близкие к единице значения $P(\chi^2)$ свидетельствуют о достаточно хорошем согласовании. При этом в [1] отмечается, что такое эмпирическое распределение настолько хорошо согласуется с теоретическим распределением, что считать эксперимент случайным нельзя.

Для первоначального выбора базового датчика по критерию согласия между эмпирическим и теоретическим распределением в нашем случае используем следующее условие: $P(\chi_i^2) > P_{\text{Н}}(\chi^2)$.

Очевидно, что чем ближе $P(\chi_i^2)$ к значению 0,5, тем лучше. Вероятность $P(\chi_i^2)$ события $x^2 \geq x_i^2$ находим из [4] (табл. 2, Приложение 2).

Для перечисленных выше генераторов дискретных отображений на рис. 1 приведены графики зависимости $P(x^2)$ от значений *n*, которые вычисляются в процессе генерирования чисел через интервал $\Delta n = 2 \cdot 10^3$ для длин реализаций 450000 значений.

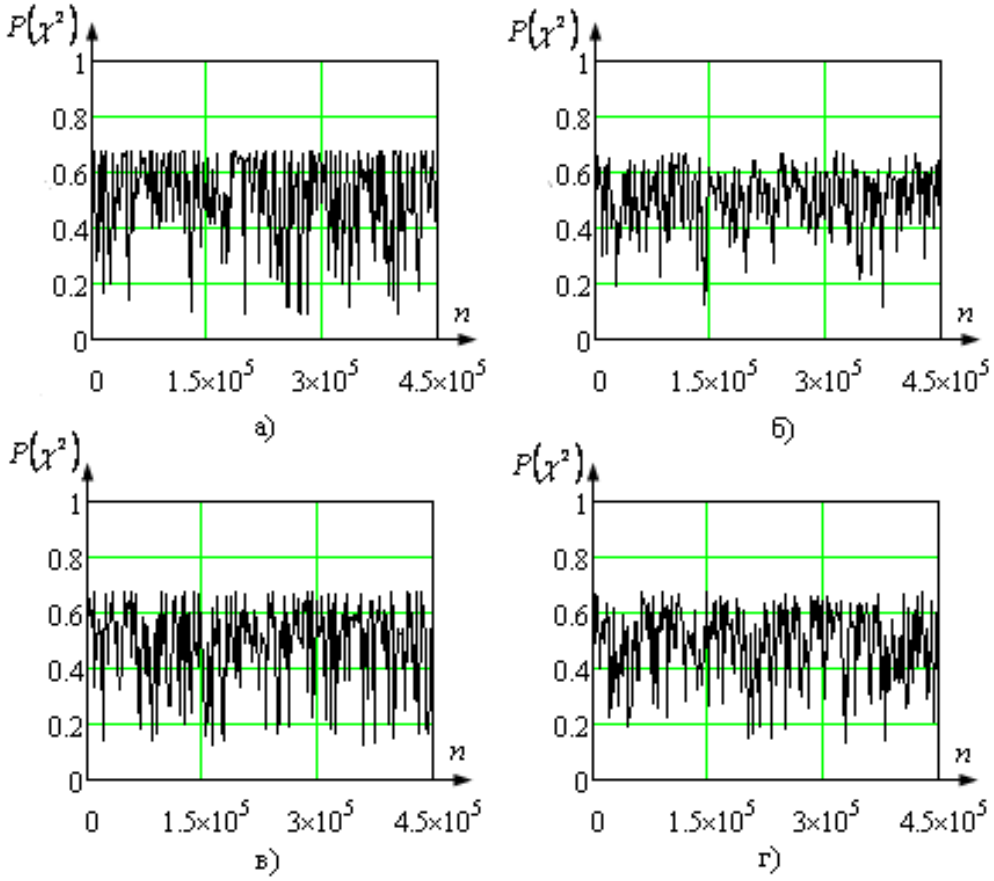

Рисунок 1 – Графики зависимости $P(\chi^2)$ от значений *n*, чисел, генерируемых генераторами дискретных отображений: степенного (а), логистического (б), кубического (в) и сдвига (г)

Рассмотрим алгоритм формирования случайных последовательностей на основе вышеперечисленных генераторов. Путем суммирования значений одноименных членов рассмотренных последовательностей $\overline{x_n}$ каждого генератора сформируем новую реализацию хаотического процесса $\overline{y_n}$. Осуществим нормировку процесса $\overline{y_n}$ на интервале (0,1) и применим критерий χ^2. График зависимости $P(\chi^2)$ от значений *n* последовательности $\overline{y_n}$ для длины реализации 450000 значений показан на рис. 2,а.

Далее последовательность $\overline{y_n}$ перемешаем путем ее циклического сдвига и последующего суммирования значений, например, пятикратного, при этом получаем после нормировки новую последовательность $\overline{z_n}$ на интервале (0,1). На рис. 2,б приведен график зависимости $P(\chi^2)$ от значений *n* последовательности $\overline{z_n}$.

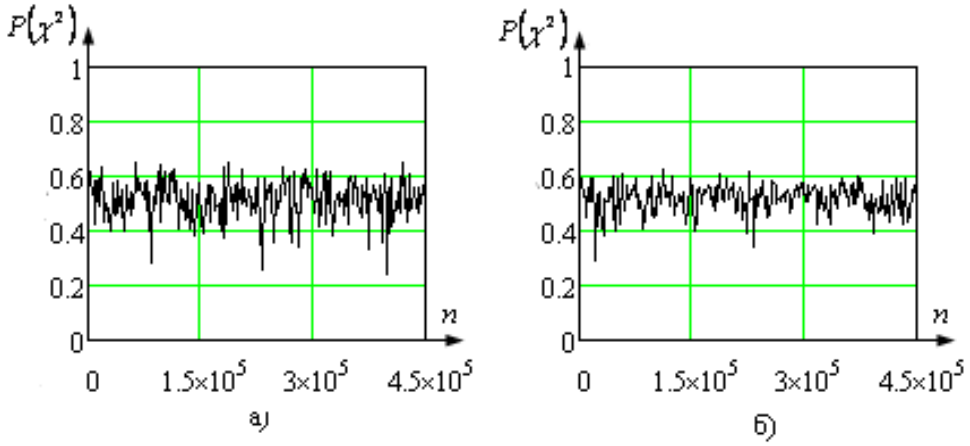

Рисунок 2 – Графики зависимости $P(\chi^2)$ от значений *n*, чисел, генерируемых генераторами до (а) и после (б) перемешивания

Из анализа графиков зависимостей $P(\chi^2)$ видно, что согласно принятому нами критерию, в качестве базового датчика случайных чисел следует принять генератор последовательности $\overline{z_n}$. Можно считать, что значения случайных чисел, порождаемых таким генератором, вполне являются случайными.

В то же время, как показано в работе [2], последовательность $\overline{z_n}$ представляет собой шумовой сигнал. Шумовой сигнал можно считать истинно случайным процессом, пригодным для генерации истинно случайных чисел. Путем применения знаковой функции $signx$, определяемой как $signx = 1$ при $x \geq 0$ и $signx = -1$ при $x < 0$, сформируем на основе шумового сигнала $\overline{z_n}$ бинарную последовательность. Полученная последовательность $\ddot{\overline{z}}_n$ длиной 450000 бит является исходной для генерирования с помощью процедуры прореживания выборки требуемой длины. Например, двойным прореживанием с разным шагом сформируем бинарную последовательность длиной 20000 бит и проверим ее на случайность частотным тестом. Этот тест основан на равенстве частот 1 и −1 в истинно случайной бинарной последовательности. Если X обозначить сумму 1 и −1 в бинарной последовательности, то в нашем случае

$$X = \sum_{i=0}^{20000} \ddot{\overline{z}}_i = -1 \qquad (7)$$

свидетельствует о том, что частотный тест на случайность бинарной последовательности успешно пройден.

В заключение можно сделать следующие выводы.

В работе разработаны методы формирования случайных чисел и бинарных последовательностей на основе систем с динамическим хаосом. Показано, что генератор шумового сигнала $\overline{z_n}$ является идеальной основой для генератора случайной бинарной последовательности, обеспечивающего воспроизводимость и требуемую длину случайной последовательности. Применение таких последовательностей в алгоритмах передачи позволит повысить помехоустойчивость, структурную и информационную скрытность передаваемой информации в системах конфиденциальной связи.

Литература

1. *Кнут Д.* Искусство программирования, том 2. Получисленные алгоритмы; пер. с англ./ *Кнут Д.* – М.: Вильямс, 2000. – 832 с.
2. *Захарченко Н. В.* Метод синтеза шумового сигнала гауссова типа на основе систем с динамическим хаосом / *Н. В. Захарченко, Б. К. Радзимовский, В. В. Корчинский* // Восточно-Европейский журнал передовых технологий. – 2012. – № 2/10 (56). – С. 25–27.
3. Генераторы хаотических колебаний / [*Б.И. Шахтарин, П.И. Кобылкина, Ю.А. Сидоркина* и др.] – М.: Гелиос АРВ, 2007. – 248 с.

4. *Куликов Е. И.* Прикладной статистический анализ / *Куликов Е. И.* – М.: Горячая линия–Телеком, 2008. – 464 с.