*УДК 621.391*

*Радзимовский Б. К.*
*Радзімовський Б. К.*
*Radzimovskiy B.K.*

# БИНАРНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ НА ОСНОВЕ СИСТЕМ С ДИНАМИЧЕСКИМ ХАОСОМ

# БІНАРНІ ПОСЛІДОВНОСТІ НА ОСНОВІ СИСТЕМ З ДИНАМІЧНИМ ХАОСОМ

# BINARY SEQUENCES BASED ON THE DYNAMIC CHAOS SYSTEMS

***Аннотация***. Для конфиденциальных систем связи предложены алгоритмы генерирования 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 бінарних послідовностей на основі різних дискретних відображень у генераторах хаосу. Розглянуті статистичні характеристики, що генерують послідовності з оцінкою їх якості.

***Summary.*** Several algorithms for confidential telecommunication systems for generating 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.

Развитие современных высокоскоростных телекоммуникационных систем, обеспечивающих высокую помехоустойчивость и скрытность передаваемой информации, основано на использовании широкополосных сигналов с большой информационной емкостью [1]. Основой для формирования таких сигналов являются псевдослучайные бинарные последовательности (ПСП), которые должны обладать большим размером ансамбля, сбалансированностью структуры, допустимыми автокорреляционными (АКФ) и взаимокорреляционными (ВКФ) функциями последовательностей сигналов в ансамбле. Одновременно бинарные последовательности ансамбля должны удовлетворять критериям случайности и обладать свойством уравновешенности (число 1 отличается от числа −1 в последовательности не более, чем на единицу), свойством серий (в последовательности примерно половина серии 1 и −1 имеет длину 1, четверть − 2, восьмая часть − 3 и т.д.) и свойством корреляции (при поэлементном сравнении последовательности с её циклическим сдвигом число совпадений отличается от числа несовпадений не больше чем на единицу).

Используемые в качестве ПСП линейные М-последовательности, последовательности Голда, Касами и ряд других не обеспечивают требуемой структурной скрытности из-за их предсказуемости, поэтому разработка алгоритмов построения больших ансамблей нелинейных ПСП с хорошими взаимокорреляционными и структурными свойствами и их исследование является актуальной проблемой. Решение проблемы может дать применение сигналов, формируемых нелинейными системами с динамическим хаосом.

Известно [1,2], что системы с использованием хаотических сигналов имеют повышенную информационную ёмкость, высокую помехозащищенность и обеспечивают скрытность передаваемых сообщений. В [3] предложен метод синтеза шумового сигнала гауссова типа на основе нелинейных дискретных систем с динамическим хаосом. Предложенный метод позволяет формировать воспроизводимые реализации хаотического сигнала неограниченной длины с отсутствием периодичности в последовательностях их амплитудных значений. Так как последовательность амплитудных значений синтезированного шумового сигнала является случайным процессом, то появляется возможность, например, путем применения знаковой функции $signx$, определяемой как $signx = 1$ при $x \geq 0$ и $signx = -1$ при $x < 0$, сформировать на его основе нелинейную бинарную последовательность.

Однако в литературе недостаточно исследована такая возможность, поэтому **целью статьи** является разработка метода формирования и исследование больших ансамблей нелинейных бинарных последовательностей на основе различных дискретных отображений в генераторах хаоса.

Свойства дискретных генераторов хаоса определяются значениями управляющих параметров и видом функции отображения

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

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

Для формирования требуемого сигнала используем несколько, например, пять, генераторов хаоса на основе следующих дискретных отображений [4]:

1) логистического

$$x_{n+1} = ax_n(1-x_n), \tag{2}$$

где $x_0 = 0{,}9$, $a = 3{,}9$;

2) степенного

$$x_{n+1} = a(1-|1-2x_n|^l), \tag{3}$$

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

3) логистического с другим начальным значением $x_0$

$$x_{n+1} = ax_n(1-x_n), \tag{4}$$

где $x_0 = 0{,}5$, $a = 3{,}9$;

4) кубического

$$x_{n+1} = (1-4a)x_n + 4ax_n^3, \tag{5}$$

где $x_0 = 0{,}5$, $a = 0{,}92$;

5) сдвига

$$x_{n+1} = ax_n \bmod 1, \tag{6}$$

где $x_0 = 0{,}8$, $a = 3{,}0$.

На выходах приведенных генераторов получаем непериодические хаотические последовательности заданной длины, например, $N = 450000$ значений. Так как хаотический сигнал в общем случае имеет ненулевое математическое ожидание $m$, то будем использовать центрированный $\overline{x_n} = x_n - m$ хаотический процесс.

Заметим, что отдельные последовательности каждого из приведенных генераторов характеризуются разными распределениями вероятности амплитудных значений, а небольшие изменения параметров или начальных условий приводят к совершенно другим реализациям. Например, генераторы с разными начальными значениями $x_0$ в логистических отображениях (1) и (3) генерируют последовательности с коэффициентом корреляции $r_{1,3} = -8{,}682 \cdot 10^{-4}$. Как видим, при небольшом изменении начальных условий генератора, он порождает совершенно иной, некоррелированный с первым, процесс.

Рассмотрим алгоритм формирования бинарных последовательностей на основе вышеперечисленных генераторов. Применяя знаковую функцию *signx* сформируем на основе последовательностей $\overline{x_n}$ каждого генератора бинарные последовательности $y_n$, в которых из общего числа не учитываются из-за переходных процессов начальные и последние 25000 бит. Полученные последовательности $y_n$, в нашем случае длиной 400000 бит, являются исходными для генерирования с помощью процедуры прореживания выборок требуемой длины. Например, прореживанием сформируем бинарные последовательности длиной 50001 бит и определим их статистические характеристики. На рис. 1 приведены АКФ бинарных последовательностей длиной 50001 бит, сформированных на основе логистического и сдвига отображений. Из рисунка видно, что АКФ бинарных последовательностей являются непериодическими и стремятся к нулю за достаточно малый промежуток времени. Но тестирование данных последовательностей на уравновешенность и серийность показало, что такими свойствами они не обладают.

Путем суммирования значений одноименных членов последовательностей $\overline{x_n}$ каждого генератора усложним алгоритм и сформируем новую реализацию нормированного хаотического процесса $\overline{y_n}$.

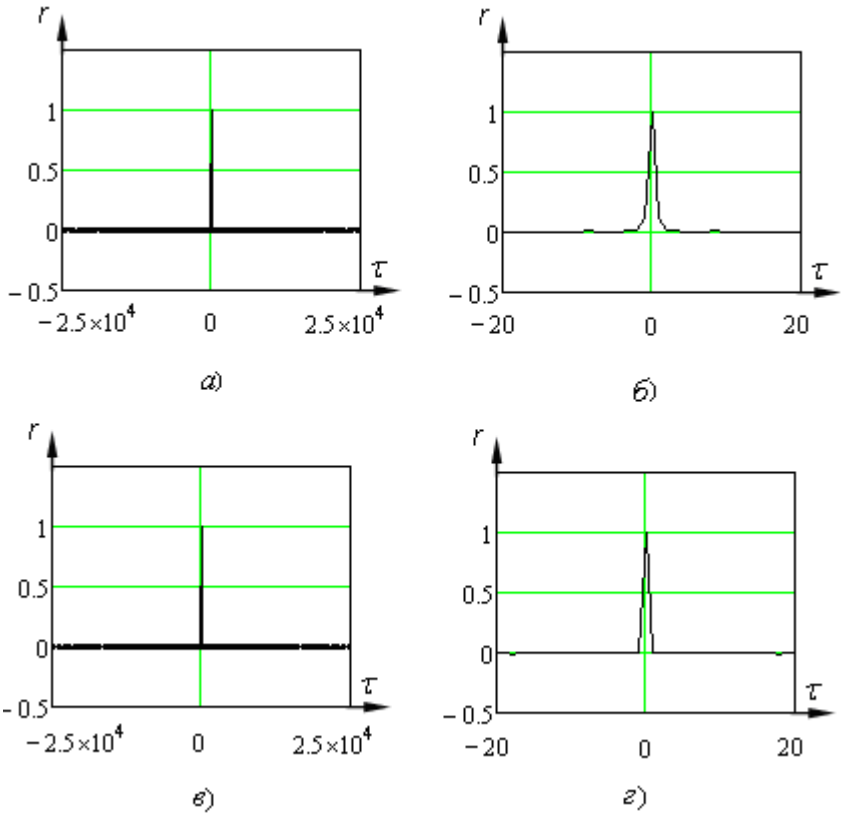


Рисунок 1 – АКФ бинарной последовательности отображения сдвига (*а*), фрагмент её локальной области максимума (*б*), логистического отображения (*в*), фрагмент локальной области её максимума (*г*)

Далее последовательность $\overline{y_n}$ перемешаем путем её циклического сдвига и последующего суммирования значений, например, семикратного, при этом получаем после нормировки новую последовательность $\overline{z_n}$, в которой из общего числа также не учитываются из-за переходных процессов начальные и последние 25000 значений последовательности. Применяя знаковую функцию $signx$ сформируем на основе последовательности $\overline{z_n}$ бинарную последовательность $\ddot{z}_n$. Полученная последовательность $\ddot{z}_n$, в нашем случае длиной 400000 бит, является исходной для генерирования с помощью процедуры прореживания выборки требуемой длины. Например, двойным прореживанием с разным шагом сформируем бинарную последовательность диной 50001 бит и проверим её на уравновешенность. Если $X$ обозначить сумму 1 и −1 в бинарной последовательности, то в нашем случае

$$X = \sum_n \ddot{z}_n = 1 \qquad (7)$$

свидетельствует о том, что число 1 отличается от числа −1 в последовательности на единицу. Приведенное равенство сохраняется и при поэлементном сравнении последовательности с её циклическим сдвигом на любое число позиций, т.е. последовательность обладает и свойством корреляции. Сформированная предложенным алгоритмом бинарная последовательность и последовательности ее циклического сдвига образуют ансамбль нелинейных бинарных последовательностей.

Рассмотрим корреляционные свойства ансамбля бинарных последовательностей. На рис. 2 приведены графики АКФ бинарной последовательности длиной 50001 бит и её копии, циклически сдвинутой на 45000 позиций.

На рис. 3 приведены графики ВКФ бинарной последовательности и некоторых её копий, циклически сдвинутых на разное число позиций. Из графиков на рис. 2 и 3 видно, что сформированный ансамбль нелинейных бинарных последовательностей обладает хорошими авто - и взаимокорреляционными функциями.

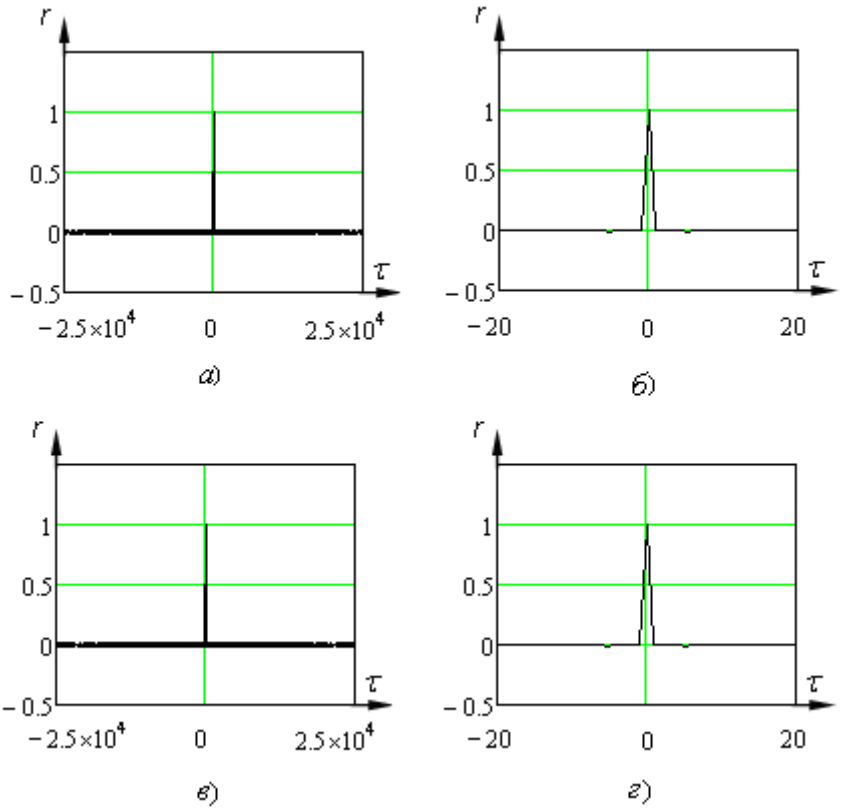


Рисунок 2 – АКФ бинарной последовательности ансамбля (*а*), её локальная область максимума (*б*) и копии, циклически сдвинутой на 45000 позиций (*в*), её локальная область максимума (*г*)

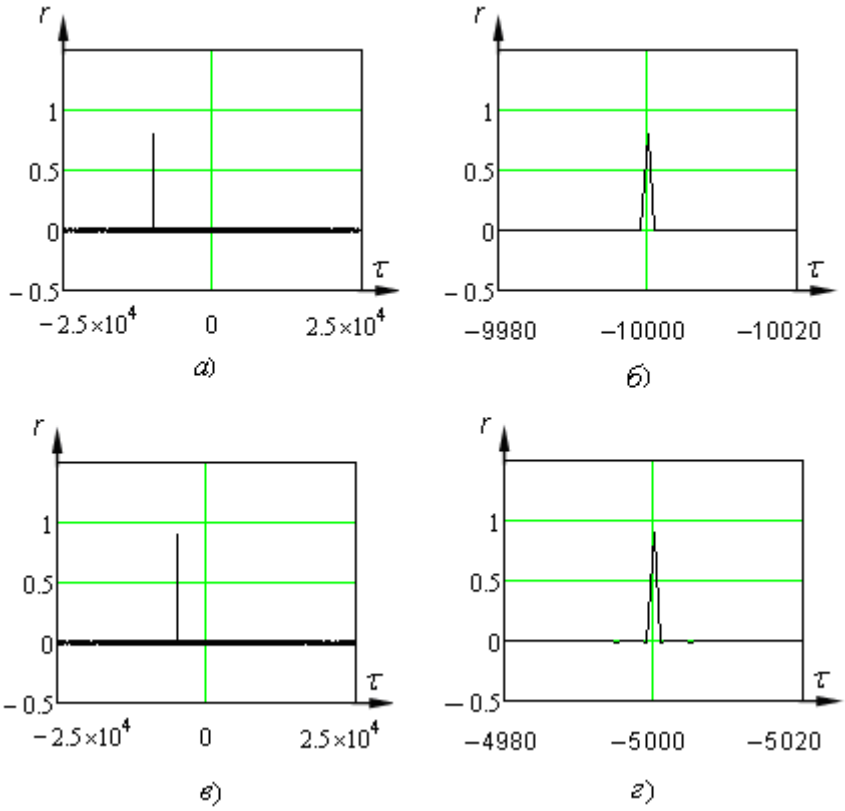


Рисунок 3 – ВКФ бинарной последовательности ансамбля и копии, циклически сдвинутой на 40000 позиций (*а*), её локальная область максимума (*б*), копии, циклически сдвинутой на 45000 позиций (*в*), её локальная область максимума (*г*)

Проверим бинарную последовательность длиной 50001 бит на серийность. Результаты проверки приведены в табл. 1.

Таблица 1 − Количество серий в бинарной последовательности длиной 50001 бит

| $s$ / $k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| −1 | 6338 | 3100 | 1596 | 789 | 392 | 185 | 100 | 45 | 18 | 12 |
| 1 | 6347 | 3172 | 1530 | 761 | 377 | 190 | 106 | 54 | 24 | 10 |

Анализ таблицы показывает, что тестируемая бинарная последовательность обладает свойством серийности ($s$ − длина 1 и −1 в серии; $k$ − количество серий в последовательности).

В заключение можно сделать следующие выводы.

В статье разработан метод формирования ансамбля нелинейных бинарных последовательностей на основе систем с динамическим хаосом. Показано, что такие бинарные последовательности, обладая хорошими корреляционными свойствами, имеют практически неограниченный набор длин, могут образовывать ансамбли сигналов больших объёмов и являются нелинейными, что затрудняет их распознавание. Применение таких бинарных последовательностей в алгоритмах передачи позволит повысить помехоустойчивость, структурную и информационную скрытность передаваемой информации в системах конфиденциальной связи.

***Литература***

1. *Залогин Н.Н.* Широкополосные хаотические сигналы в радиотехнических и информационных системах / Н.Н. Залогин, В.В. Кислов. – М.: Радиотехника, 2006. – 208 с.
2. *Капранов М.В.* Регулярная и хаотическая динамика нелинейных систем с дискретным временем / М.В. Капранов, А.И. Томашевский. – М.: Издательский дом МЭИ, 2010. – 256 с.
3. *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.
4. *Генераторы* хаотических колебаний / [Б.И. Шахтарин, П.И. Кобылкина, Ю.А. Сидоркина и др.]. – М.: Гелиос АРВ, 2007. – 248 с.