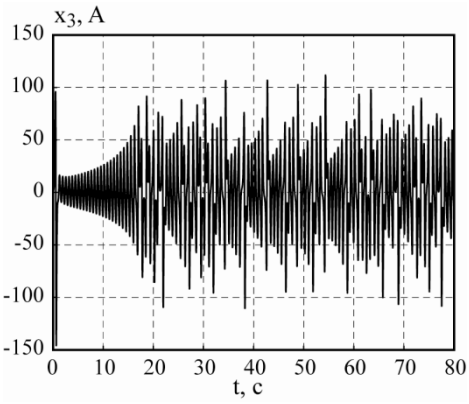


Рис. 7. Ток и напряжение якоря

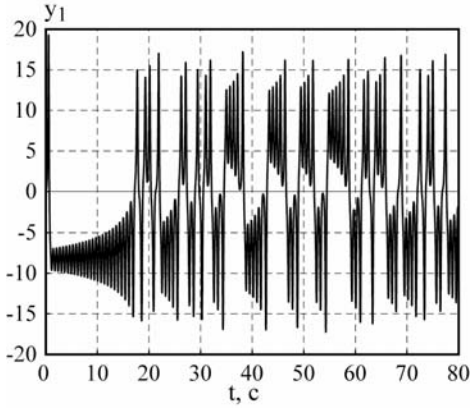


Рис. 8. Эталонная переменная

Заключение. Результаты моделирования подтверждают обоснованность изложенного в статье подхода и справедливость теоретических выкладок. Таким образом, разработанная методика синтеза может получить широкое применение при построении алгоритмов управления различными техническими системами для генерации режимов регулярных и хаотических колебаний управляемых переменных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Колесников А.А.* Синергетические методы управления сложными системами: теория системного синтеза. – М.: КомКнига, 2006. – 240 с.
2. Современная прикладная теория управления: Ч.II. Синергетический подход в теории управления / Под ред. А.А. Колесникова. – М.–Таганрог: Изд-во ТРТУ, 2000.
3. *Попов А.Н., Колесников Ал.А.* Синергетический синтез генераторов нелинейных электромеханических колебаний // Нелинейный мир. – 2004. – Т. 2, № 4. – С. 278-284.

Статью рекомендовал к опубликованию д.т.н., профессор И.М. Першин.

Попов Андрей Николаевич – Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге; e-mail: andypriest@mail.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634360707; кафедра синергетики и процессов управления; к.т.н.; доцент.

Popov Andrey Nickolaevitch – Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: andypriest@mail.ru; 2, Chekhov street, Taganrog, 347928, Russia; phone: +78634360707; the department of synergetics and control; cand. of eng. sc.; associate professor.

УДК 004.056.55

С.И. Колесникова

ПРИМЕНЕНИЕ УПРАВЛЯЕМОЙ МОДЕЛИ ФЕЙГЕНБАУМА В КОДИРОВАНИИ ИНФОРМАЦИИ

Рассматривается проблема нежелательного влияния метода хранения данных на основе математики с плавающей запятой на характер хаотичности нелинейных систем. Представление числа с плавающей запятой для хранения действительных чисел в битовой строке с некоторой конечной точностью приводит к усилению влияния ошибки округления

на каждой итерации в силу нелинейности модели. Предложен подход к поддержанию хаотического поведения нелинейного объекта на примере модели Фейгенбаума, использующий идеологию управления на многообразиях, реализованную в методе АКАР.

Нелинейный объект; синергетическое управление; генератор псевдослучайной последовательности; кодирование информации.

S.I. Kolesnikova

APPLICATION OF CONTROLLABLE OF FEIGENBAUM MODEL IN INFORMATION CODING PROBLEM

It is well known that data storage on base mathematics with floating-point has negative effect on state of chaos of nonlinear object. Representation of real number in bit string with some finite accuracy reduces to increasing of rounding error at every iteration. Approach to maintenance of the existing chaotic behavior of nonlinear object is suggested and by the Feigenbaum model is illustrated. Ideology control on the base ACAR is used.

Nonlinear object; synergetic control; pseudorandom number generator; information coding.

Модель М. Фейгенбаума (МФ) [1] с описанием:

$$x_{n+1}=\lambda x_n(1-x_n),\ n\geq 0 \qquad (1)$$

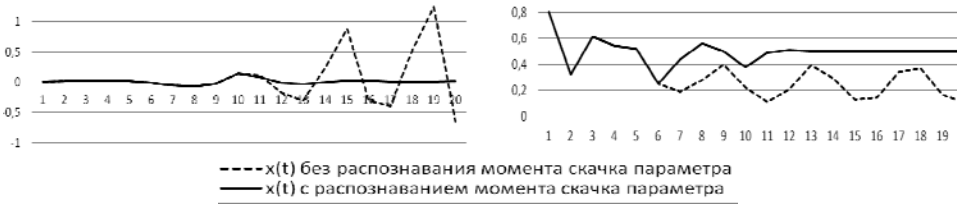
с хаотическим поведением при определенных значениях параметра λ является основой объяснения многих процессов: превращение ламинарного потока жидкости в турбулентный; изменение в популяции от поколения к поколению; поведение шумовой составляющей сигнала в механических, электрических и химических осцилляторах; поведение гамильтоновых систем; переход нормального ритма сердца в угрожающий жизни режим фибрилляции, изменение экономических и экологических показателей во времени и многие другие.

Общей чертой в поведении вышеперечисленных явлений (сложных нелинейных объектов) является изменение поведения от «обычного» и «ожидаемого» к хаотическому при изменении какого-либо фактора извне – параметра модели, начальный момент и характер флуктуации которого зачастую точно неизвестен, поскольку фактически наблюдаются величины $y_n=x_n+\xi_n$, где величина x_n подчиняется (1), а последовательность $\{\xi_n\}$ характеризует шумовые помехи измерительного характера. В связи с этим управление режимами сложного объекта (для описания поведения которого выбрана данная модель), возникающих при изменении параметра λ, способствовало бы выполнению целевых установок, например стабилизации объекта на заданном уровне.

Целью данной работы является изложение подхода к поддержанию хаотического поведения объекта (1) с целью применения в криптографии. Подход использует идеологию управления на многообразиях, а именно, классический метод АКАР [2].

Задача стабилизации поведения объекта на основе управления с распознаванием режимов его функционирования. Экспериментально несложно убедиться, что управление для МФ, сконструированное согласно АКАР, устойчиво устремляет процесс x_n к желаемому аттрактору даже в случае отсутствия неподвижных точек ($3<\lambda\leq 4$) для объекта (1), по крайней мере, для определенных сочетаний (x_0, λ). Для случаев наблюдения с шумом ($y_n=x_n+\xi_n$) ранее был предложен алгоритм оценивания состояния объекта на основе разметки ряда символами по определенному правилу [3] и переключение на соответствующий вид управления (рис. 1), использующий полученную информацию [4].

На рис. 1 рассмотрен случай скачкообразного изменения параметра λ, интерпретируемого как изменение режима функционирования объекта (1), приводящего к нежелательным последствиям в условиях отсутствия перестройки в управлении.



а) x_0=0,008; ψ=x–0,01=0 *б*) x_0=0,8; ψ=x–0,5=0

Рис. 1. Отсутствие перестройки управления при скачках параметра λ не выводит объект на заданный аттрактор: а) один скачок: $\lambda_1(t)$=2, t<9; $\lambda_2(t)$=0,5, $t\geq$9; б) два скачка: $\lambda_1(t)$=2, t<9; $\lambda_2(t)$=1, 9≤t<12; $\lambda_3(t)$=0,5, $t\geq$12; γ=0,009

Отметим, что алгоритм из работы [3] может быть преобразован в схему принятия решения о наличии/отсутствия скачка по значению функции энтропии значений разметки ряда (рост энтропии – признак скачка).

Задача поддержания хаотического поведения объекта для применения в криптографии. Известны работы (например, [5–7]), где обсуждаются возможности применения хаотических систем (в том числе и МФ) в криптографических целях для кодирования информации, а именно, систем, играющих роль генератора псевдослучайной последовательности (гамма-последовательности) в поточном шифровании/дешифрировании данных.

Напомним, что в поточном шифре каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости от используемого ключа и от его расположения в потоке открытого текста.

Среди отмеченных недостатков применения хаотических систем в криптографии наиболее существенной нерешенной проблемой является нежелательный эффект, связанный с влиянием математики с плавающей запятой на характер хаотичности, приводящий к возможному его исчезновению (покидание аттрактора исходной системы и вхождение в стационарный режим фактически уже в системе с другим, неизвестным, вообще говоря, функциональным описанием).

Нетрудно убедиться, что представление числа с плавающей запятой для хранения действительных чисел в битовой строке с некоторой конечной точностью, приводит к усилению влияния ошибки округления на каждой итерации в силу нелинейности модели. На рис. 2 (см. также результаты моделирования в [6]) представлены траектории, полученные по аналитической формуле (с точечным начертанием) и по итерационной формуле (со сплошным начертанием), при этом, при точности представления числа с 15-ю знаками после запятой заметное отличие начинается после 45-го отсчета; с тремя знаками после запятой - после 10-го отсчета.

Возникает задача поддержания хаотического режима, необходимого для надежного кодирования/декодирования. Задача является в определенном смысле «обратной» по отношению к задаче стабилизации.

Для решения этой проблемы, весьма ограничивающей применение хаотических систем в криптографии, предлагается использовать в качестве гаммирующей последовательности (с ключом в виде пары значений (x_0, λ)) не модель типа (1), а синергетически управляемую модель вида

$$\begin{aligned} \tilde{x}_n^{it} &= \lambda \tilde{x}_{n-1}^{it}(1-\tilde{x}_{n-1}^{it}), \\ u_n &= -\lambda \tilde{x}_{n-1}^{it}(1-\tilde{x}_{n-1}^{it}) + c_{0,n} + \gamma(\tilde{x}_{n-1}^{it} - c_{0,n-1}),\ n>0. \end{aligned} \qquad (2)$$

Для вывода управления, удовлетворяющего условию $\psi_n = x_n - c_{0,n} = 0$, использовалась классическая техника метода АКАР [2].

Задача в постановке (2) сводится к нахождению такой целевой последовательности $c_{0,n}$, $n > 0$, которая «сохранит и приумножит» степень хаотичности поведения системы. При этом, согласно смыслу задачи шифрования/дешифрования, желательно не выходить за рамки генерируемой итерационной последовательности $\tilde{x}_n^{it}$ (и/или x_n^{it}), где $\tilde{x}_n^{it}$ – координата системы (2), x_n^{it} – координата объекта (1), согласно итерационной формуле (iterative model) $x_n^{it} = \lambda x_{n-1}^{it}(1 - x_{n-1}^{it})$, $n > 0$.

В силу специфики данной задачи – использования МФ в качестве хаотического генератора – интересен случай отсутствия неподвижных точек ($3<\lambda\leq 4$) для объекта (1).

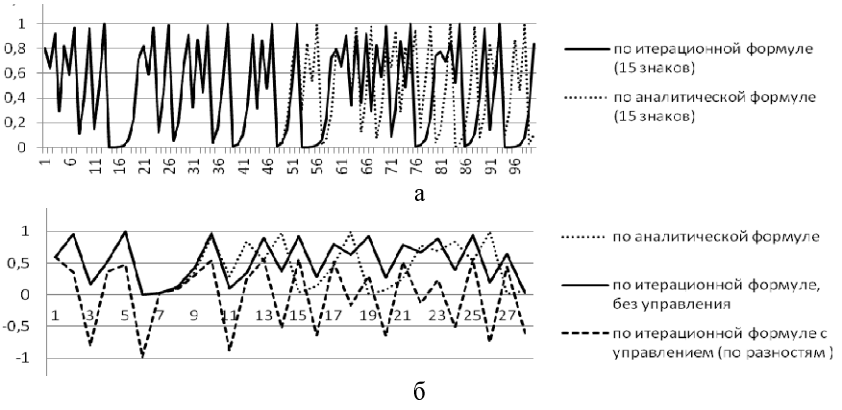


Рис. 2. Графики рядов x(t), полученные по формулам: точной (x_n^{am}), итерационной (x_n^{it}), итерационной формуле (2) с управлением ($\tilde{x}_n^{it}$) с разным числом знаков в дробной части: а – 15 знаков, x_0=0,8: б – 3 знака, x_0=0,6

Рассмотрим вариант λ=4 и обозначим за x_n^{am} - значение координаты x_n, вычисляемое по аналитической (точной) формуле (accurate model):

$$x_n^{am} = \sin^2\left(2^n \arcsin\sqrt{x_0}\right). \qquad (3)$$

Положим $c_{0,n} = x_n^{it} - x_{n-1}^{it}$, $n > 0$ и исследуем свойства рядов данных $\left\{x_n^{it}\right\}$ и $\left\{\tilde{x}_n^{it}\right\}$, приняв за меру их хаотичности функцию энтропии (неопределенности выбора состояния в конкретный момент времени при фиксированной совокупности состояний). Энтропия обладает «удобными» свойствами для статистического описания исследуемого процесса, позволяющими использовать данный показатель в качестве критерия относительной степени упорядоченности состояний двух систем.

Исследования проведем, во-первых, с целью показать, что энтропия управляемого ряда данных $\left\{\tilde{x}_n^{it}\right\}$ не меньше энтропии ряда данных $\left\{x_n^{it}\right\}$, полученного итеративно с накоплением ошибки; во-вторых, обосновать выбор целевой последовательности $c_{0,n} = x_n^{it} - x_{n-1}^{it}$, $n > 0$.

При расчетах диапазон [-1, 1] возможных значений элементов рядов разбивался на «карманы» $[z_i, z_i + h)$, $i = \overline{1,11}$ длиной h. Значения энтропий $H(X^{it})$, $H(\tilde{X}^{it})$ систем $X^{it} = \{x_n^{it}\}$ и $\tilde{X}^{it} = \{\tilde{x}_n^{it}\}$ для скользящего окна, глубиной L, вычислялись по формуле

$$H(X) = -\sum_{i=1}^{L} p_i \log_2(p_i),\ p_i = P\left(X \in [z_i, z_i + h)\right).$$

В табл. 1 приведен фрагмент вычислений: значения энтропий для скользящего окна $L = 27$ с величиной сдвига в 5 отсчетов, подтверждающие правомерность и целесообразность предложенного подхода для кодирования/декодирования информации.

Таблица 1

Номер окна (i)	$H^{(i)}(X^{it})$	$H^{(i)}(\tilde{X}^{it})$
1	2,40884	2,74930
2	2,44879	2,62955
3	2,45714	2,65596
4	2,43374	2,62060

Заметим теперь, что энтропии двух систем: Δ_n^{it}, Δ_n^{am}, $n > 0$, где $\Delta_n^{it} = x_n^{it} - x_{n-1}^{it}$, $\Delta_n^{am} = x_n^{am} - x_{n-1}^{am}$ по первому окну L равны $H(\Delta^{it}) = 3{,}123$, $H(\Delta^{am}) = 3{,}169$, а сами выборки (рис. 3) обладают «похожими» статистическими свойствами (рис. 3). Напомним, что величина Δ_n^{am} – приращение «идеальной» хаотической несущей, найденной по аналитической формуле (с меньшей погрешностью округления).

Таким образом, поскольку разность $x_n^{it} - x_{n-1}^{it}$ содержит потерянную за счет округления нелинейно преобразованную информацию, то ее косвенное использование в конструкции (2) позволяет получить последовательность $\{\tilde{x}_n^{it}\}$ с лучшими хаотическими свойствами, чем последовательность $\{x_n^{it}\}$ с итеративным накоплением ошибки.

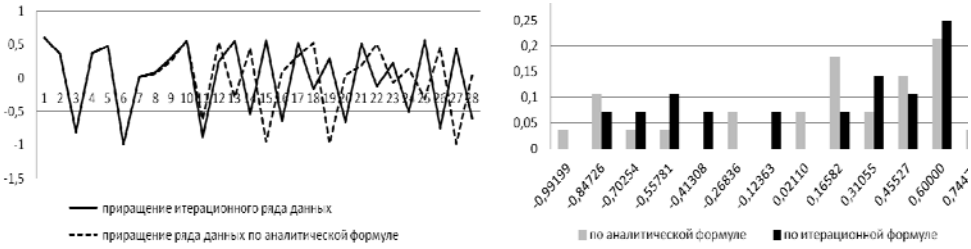


Рис. 3. Гистограмма относительных частот выборок $\tilde{x}_n^{it}$, x_n^{am}, $n = \overline{1,27}$ с числовыми характеристиками: средними значениями 0,001; 0,002 и дисперсиями 0,293, 0,285 соответственно

Замечание 1. Понятно, что в качестве гаммы-последовательности может быть использована собственно сама последовательность $\Delta_n^{it} = x_n^{it} - x_{n-1}^{it}$, $n > 0$, однако конструкция (2) дает определенную степень свободы в способе выбора последовательности $c_{0,n}$, влияющей на «характер хаотичности».

Замечание 2. По-видимому, применение других критериев меры хаотичности не добавит информации, так как в силу конечного числа разрядов, используемых для машинного представления анализируемых величин, степень расхождения траекторий будет ограничена (см., например, поведение показателя Ляпунова для псевдослучайных последовательностей в [6. С. 47).

Замечание 3. В силу детерминированности рядов (1), (2) выводы по результатам численного исследования энтропийных свойств указанных рядов достаточны для вынесения решений в практических задачах.

В заключение отметим целесообразность проведения исследований относительно оценивания криптостойкости предложенного подхода, связанного с оценкой числа необходимых операций для вскрытия ключа.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Фейгенбаум М.* Универсальность в поведении нелинейных систем // Успехи физических наук. – 1983. – Т. 141. – Вып. 2. – С. 343-374.
2. *Колесников А.А.* Синергетические методы управления сложными системами: теория системного синтеза. – М.: Едиториал УРСС, 2005. – 230 с.
3. *Колесникова С.И.* Метод распознавания и оценивания состояний слабоформализованного динамического объекта на основе разметки временного ряда // Известия РАН. Теория и системы управления. – 2011. – № 5. – С. 41-52.
4. *Колесникова С.И.* Использование апостериорной информации для управления плохо формализуемым динамическим объектом // Автометрия. – 2010. – Т. 46, № 6. – С. 78-89.
5. *Kosarev L.* Chaos-based cryptography: a brief overview // Circuits and systems. – 2001. – Vol. 3. – С. 6-21.
6. *Птицын Н.* Приложение теории детерминированного хаоса в криптографии. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2002. – 81 с.
7. *Болтенков В.А., Никольский Е.С.* Анализ алгоритмов хаотического шифрования изображений // Цифровые технологии. – 2010. – № 7. – С. 61-66.

Статью рекомендовал к опубликованию д.т.н. Г.Е. Веселов.

Колесникова Светлана Ивановна – Томский государственный университет систем управления и радиоэлектроники; e-mail: skolesnikova@yandex.ru; 634050, г. Томск, пр. Ленина, 40; тел.: 83822510530; к.ф.-м.н.; доцент.

Kolesnikova Svetlana Ivanovna – Tomsk State University of Control Systems and Radioelectronics; e-mail: skolesnikova@yandex.ru; 40, Lenin aven., Tomsk, 634050, Russia; phone: +73822510530; cand. of eng. sc.; associate professor.

УДК 681.51

Ал.А. Колесников

МЕТОД НЕЛИНЕЙНОГО АДАПТИВНОГО УПРАВЛЕНИЯ СИСТЕМАМИ АКТИВНОЙ ВИБРОЗАЩИТЫ

Предложен новый нелинейный закон адаптивного управления электромагнитной системой активной виброзащиты (САВ), позволяющий компенсировать внешние гармонические возмущения на разные классы технологических и подвижных объектов, что непосредственно связано с их технологической безопасностью. Синтезированный закон управления САВ обладает значительными преимуществами перед известными, например линейными законами управления САВ разных объектов. Предложенный метод может найти применение при создании САВ разного применения. Существенной новизной метода является, во-первых, процедура каскадного синтеза законов управления, во-вторых, создание единства процессов технологической самоорганизации и управления.

Виброзащита; электромагнитная система; закон адаптивного управления; внешние гармонические возмущения.