УДК 621.391.7

Мойсейкин И. А., Шишкин А. В.

МЕТОДИКА ВЫБОРА ОПТИМАЛЬНЫХ ПАРАМЕТРОВ ДИНАМИЧЕСКОЙ СИСТЕМЫ ХАОТИЧЕСКОГО КОДЕРА

На сегодняшний день рост производительности процессоров сводит на нет многие традиционные алгоритмы шифрования данных, стимулирует разработку новых альтернативных принципов кодирования информации. В связи с этим интерес представляет шифрование данных, основанное на явлениях хаотической динамики. В основе системы кодирования методом детерминированного хаоса лежит генератор псевдослучайных последовательностей чисел. Он представляет собой динамическую систему, которая описывается системой нелинейных дифференциальных уравнений. Решением этой системы будет последовательность псевдослучайных чисел, формирующих хаотический сигнал. Суть шифрования заключается в сложении полезного и хаотического сигнала, полученного генератором псевдослучайных чисел.

На практике многие системы шифрования, основанные на явлениях хаотической динамики, оказываются криптографически более слабым по сравнению с их традиционными аналогами. Это происходит из-за неверного выбора параметров динамической системы, формирующей хаотический сигнал. Однако в работах, посвященных разработке хаотических кодеров [1–3], эта проблема не рассматривается. В связи с этим возникает проблема выбора оптимальных параметров, при которых формируемый сигнал будет обеспечивать максимальную криптостойкость зашифрованных данных.

Целью данной работы является разработка методики выбора оптимальных параметров динамической системы хаотического кодера для обеспечения максимальной защищенности зашифрованных данных. Разработанная методика может использоваться при проектировании криптосистем, основанных на явлениях хаотической динамики.

Криптостойкость системы шифрования с помощью хаотических сигналов во многом зависит от качества псевдослучайной последовательности чисел, то есть от того, насколько они предсказуемы. В теории детерминированного хаоса предсказуемость поведения временных рядов характеризует показатель Ляпунова [4, 5]. С этой точки зрения можно сделать вывод, что чем выше значение показателя Ляпунова динамической системы, тем надежнее хаотический кодер будет шифровать информацию и тем сложнее ее будет раскрыть.

Предложенная методика заключается в определении таких управляющих параметров динамической системы, при которых показатель Ляпунова будет максимальным. На первом этапе необходимо задать диапазон параметров: их минимальное и максимальное значения, а также количество точек этого диапазона. Чем больше количество точек, тем точнее будет расчет.

Перебирая все возможные комбинации параметров из заданного диапазона, и подставляя их в исходную динамическую систему, можно найти координаты особых точек. Зная их, можно определить собственные значение якобиана в этой точке [6]. Действительные части собственных значений якобиана будут являться показателями Ляпунова при текущих параметрах системы.

Полученные значения выводятся в виде графика зависимости показателей Ляпунова от управляющих параметров динамической системы. По этому графику определяются значения параметров, при которых показатели Ляпунова достигают своего максимального значения.

С помощью данной методики можно также определить положение особых точек системы в фазовом пространстве.

В качестве примера рассмотрим динамическую систему, состоящую из дифференциальных уравнений:

$$\begin{cases} \dot{X}_1 = A \cdot (X_2 - X_1); \\ \dot{X}_2 = X_1 \cdot (X_3 - B); \\ \dot{X}_3 = C - X_1 \cdot X_2 , \end{cases} \qquad (1)$$

где A, B, C – безразмерные коэффициенты.

Перебирая точки плоскости параметров A и B, и, находя каждый раз координаты особых точек, можно определить собственные значения якобиана в этой точке, а по ним можно определить значение показатели Ляпунова.

Для выявления хаотического поведения системы сначала необходимо определить знак показателя Ляпунова. Выполненные с помощью предложенной методики расчеты показывают, что максимальный показатель Ляпунова положительный, следовательно, система обладает хаотической динамикой и ее можно рассматривать в качестве генератора псевдослучайных последовательностей для систем шифрования информации.

Численное решение системы (1) методом Рунге-Кутта четвертого порядка с постоянным шагом интегрирования позволяет наглядно убедиться в хаотичности поведения системы. График зависимости координаты $X_1(t)$, построенный с использованием пакета MathCad, показан на рис. 1.

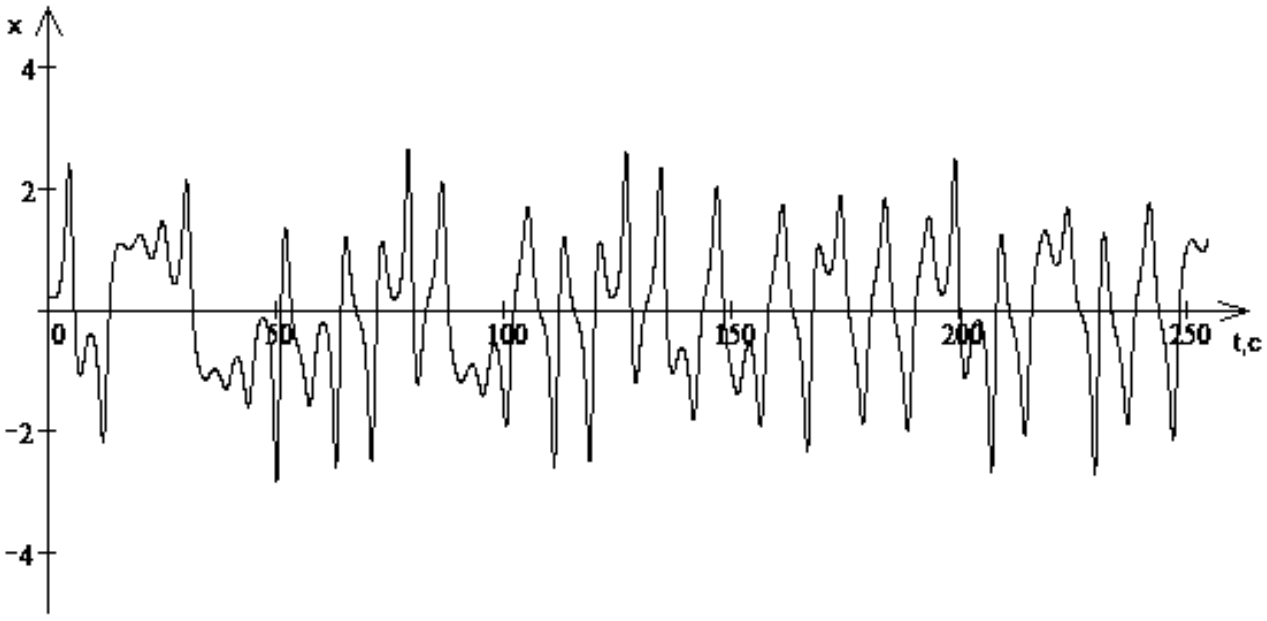

Рис. 1. График изменения координаты X_1 во времени

Проведенный с помощью предложенной методики анализ системы дифференциальных уравнений (1) позволил определить зависимость координат особых точек (рис. 2, а) и показателей Ляпунова (рис. 2, б) от управляющих параметров A и B.

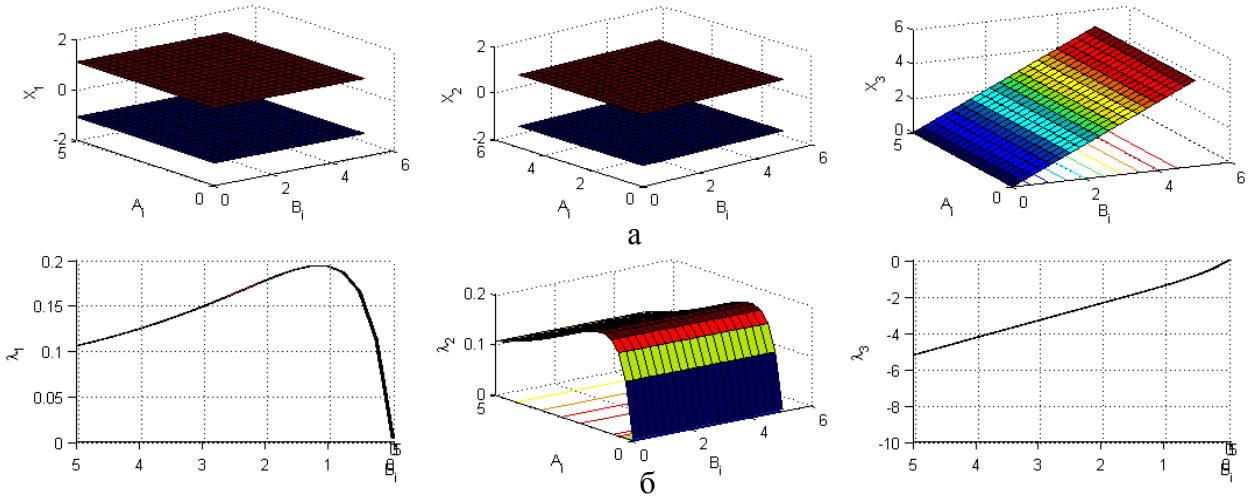

Рис. 2. Графики зависимости координат особых точек (а) и показателей Ляпунова (б) от управляющих параметров *A* и *B*

Из зависимости (рис. 2, а) можно судить о наличии в системе двух особых точек, расположенных симметрично. При этом координаты X_1 и X_2 особых точек не зависят от параметров *A* и *B*, а на X_3 влияет только параметр B.

График на рис. 2, б показывает влияние параметров *A* и *B* системы на значение показателей Ляпунова. Можно судить о том, что параметр *B* не оказывает на них никакого влияния, в то время как при увеличении параметра *A* показатели Ляпунова сначала резко возрастают, а затем постепенно уменьшаются.

Проведенные исследования показали, что максимальное значение показателя Ляпунова наблюдается при значении параметра *A*, близкому к 1,2, при этом параметр *B* не оказывает влияния на величину показателя Ляпунова, что нетрудно заметить по совмещенным графикам (рис. 3).

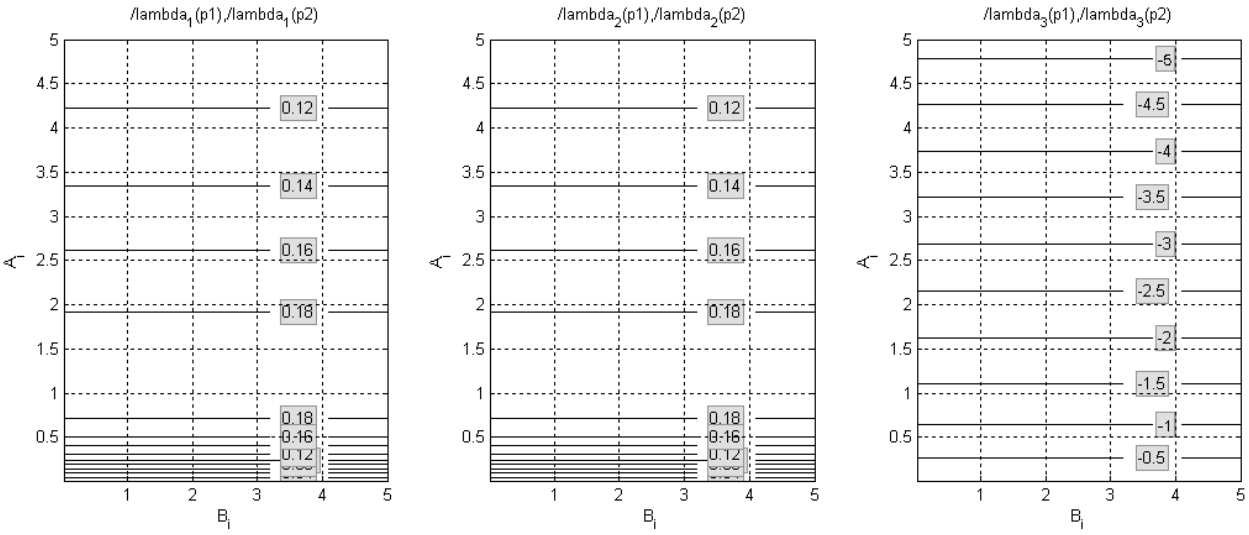

Рис. 3. Совмещенные графики зависимости показателей Ляпунова от управляющих параметров *A* и *B*

Численное решение системы (1) методом Рунге-Кутта четвертого порядка с постоянным шагом, выполненное в среде Mathcad, позволяет наглядно увидеть изменение типа аттрактора в зависимости от различных комбинаций управляющих параметров *A* и *B*. На рис. 4 показаны проекции аттрактора на оси X_3, X_1.

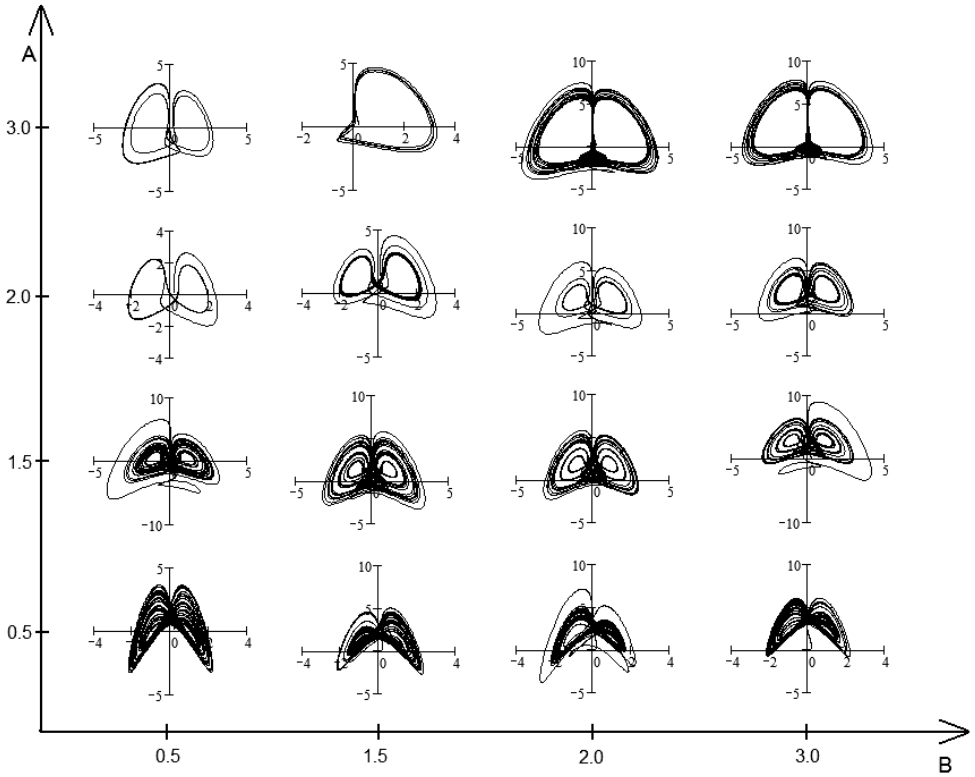

Рис. 4. Изменение вида аттрактора динамической системы при вариации управляющих параметров *A* и *B*

Полученная диаграмма позволяет определить значения параметров *A* и *B*, при которых можно получить странный аттрактор. В исследуемой системе в зависимости от комбинаций управляющих параметров можно получить два типа аттракторов: предельный цикл (например, при $A = 3$, $B = 1{,}5$) и странный аттрактор ($A = 1{,}5$, $B = 1{,}5$). Именно странный аттрактор, а не предельный цикл, необходим для работы хаотического кодера.

Приведенные выше расчеты показывают, что оптимальное значение параметра *A* составило 1,2. Диаграмма на рис. 4 подтверждает правильность выбора – из диаграммы видно, что при $A = 1{,}5$ получаем именно странный аттрактор, что и требуется для функционирования хаотического кодера.

ВЫВОДЫ

Была предложена методика выбора оптимальных параметров динамической системы хаотического кодера с целью обеспечения максимальной защищенности зашифрованных данных. Суть предложенной методики заключается в получении зависимости показателей Ляпунова от управляющих параметров динамической системы и определения таких параметров, при которых показатели Ляпунова будут максимальными.

ЛИТЕРАТУРА

1. *Кальянов Г. Н. Шифрование информации при использовании хаотических решений детерминированных уравнений / Г. Н. Кальянов, Э. В. Кальянов // Письма в ЖТФ. – 2005. – Т. 31. – Вып. 24.*

2. *Garcia P. Communication through chaotic map systems / P. Garcia, J. Jimenez // Phys. Lett. – 2002. – A 298. – P. 35–40.*

3. *Baptista M. S. Cryptography with chaos / M. S. Baptista // Phys. Lett. – 1998. – A 240. – P. 50–54.*

4. *Шустер Г. Детерминированный хаос. Введение / Г. Шустер. – М. : Мир, 1988. – 253 с.*

5. *Чуличков А. И. Математические модели нелинейной динамики / А. И. Чуличков. – М. : ФИЗМАТЛИТ, 2000. – 296 с.*

6. *Мун Ф. Хаотические колебания : вводный курс для научных работников и инженеров / Ф. Мун ; [пер. с англ. Ю. А. Данилова, А. М. Шукурова]. – М. : Мир, 1990. – С. 207–209.*