УДК 517.929, 51-74

ИСПОЛЬЗОВАНИЕ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

А. Ю. Лоскутов, А. А. Чураев

(*кафедра физики полимеров и кристаллов*)

E-mail: loskutov@chaos.phys.msu.ru

Описаны свойства предложенного ранее [1] нового метода защиты информации посредством хаотических отображений. Представлены анализ криптостойкости посредством тотального опробования и корреляционный анализ шифров. Произведена оценка предсказуемости значений шифра. Описано разработанное сетевое приложение, позволяющее пользователям обмениваться текстовыми сообщениями, защищенными представленным методом.

Введение

Процесс, обладающий свойствами динамического хаоса, может использоваться как носитель информации, как средство ее преобразования к новому виду и, наконец, как комбинация того и другого. В случае использования хаоса для преобразования сигнала можно говорить о хаотическом шифровании–дешифровании. Хаотическое шифрование может непосредственно выполнять задачу обеспечения определенного уровня конфиденциальности передаваемой информации, т. е. задачу традиционной криптографии. К настоящему моменту предложен и апробирован ряд конкретных алгоритмов и схем хаотического шифрования (см., напр., [1–12] и приведенные там ссылки), обеспечивающих различную степень конфиденциальности. Часть из них базируется на использовании неустойчивых циклов хаотических систем, другие основаны на явлении синхронизации. С их помощью достигаются высокая защита информации, высокая производительность шифрования, а также устойчивость к шуму.

Работа является продолжением исследований криптографического метода, кратко описанного в статье [1]. Результаты, описанные в указанной работе, отражают возможность эффективного применения хаотических отображений для шифрования и скрытой передачи полезной информации. Представленный метод дает возможность при относительно малых затратах создавать шифровальные устройства принципиально нового типа. Этот метод базируется на одном известном факте [12–14]: для достаточно общих семейств одномерных и n–мерных отображений существуют периодические возмущения, приводящие к *стабилизации* циклов определенного периода и таким образом к выводу системы на регулярный режим. Информация может быть зашифрована с помощью взаимно однозначного соответствия символов периодам устойчивых циклов возмущенного отображения. В качестве передаваемого сигнала используются возмущения, а ключом для расшифровки полученного сообщения служит вид отображения (т. е. функция, задающая отображение).

1. Алгоритм шифрования

В операционных системах персональных компьютеров информация о печатных символах содержится в виде так называемых кодов ASCII, которые представляют собой трехзначные целые числа, принадлежащие отрезку $[0;255]$. На первом этапе шифрования необходимо получить ASCII-коды всех символов, входящих в шифруемый текст, т. е. некоторую последовательность ASCII-кодов. Представим эту последовательность в виде числового массива, каждый элемент которого есть одна из трех составляющих кода ASCII некоторого шифруемого символа. Например, символу «a» с ASCII-кодом 97 соответствует тройка чисел $n_1 = 0$, $n_2 = 9$, $n_3 = 7$. Значит, в созданный массив мы вносим значения n_i, равные 0, 9 и 7. Теперь каждый член последовательности n_i необходимо интерпретировать (в терминах нелинейной динамики) как период цикла, который совершает некоторая динамическая система (количественная характеристика поведения динамической системы — динамическая переменная). Поэтому, чтобы избежать присутствия вырожденных циклов (периода 0) и устойчивых точек (циклов периода 1), к каждому n_i следует прибавить двойку. Избавляться от циклов периода 1 следует потому, что эти циклы не изменяют значения динамической переменной $x = \{x_1, \ldots, x_m\}$. При этом значения управляющего параметра $\hat{a} = \{a_1, \ldots, a_n\}$, стабилизирующего такие циклы, повторяются, что отрицательно сказывается на криптостойкости метода (устойчивости к взлому). Кроме того, единицы в совокупности составляющих ASCII-кодов встречаются чаще других цифр.

Далее необходимо получить последовательность чисел, имеющую длину, равную сумме всех n_i (уве-

личенных на два). При этом желательно наличие у этой последовательности свойств, характеризующих ее как случайную. Эту последовательность случайных чисел интерпретируем как последовательность значений динамической переменной x. Для образования такой последовательности не используются сторонние генераторы случайных чисел. Последовательности формируются на основе применения некоторых известных фактов хаотической динамики.

При построении алгоритма используются дискретные динамические системы, задающиеся отображениями. Особенностью таких систем является то, что система изменяет свое состояние только через определенные интервалы времени. Поэтому поведение дискретной динамической системы можно задать набором значений динамической переменной, каждое из которых описывает состояние системы на некотором шаге отсчета времени. При этом хорошо известно, как связаны системы с непрерывным временем с отображениями [15–17].

Теперь задача состоит в том, чтобы «заставить» x изменяться циклически. Циклов должно быть столько, сколько членов содержится в последовательности n_i (число символов шифруемого текста, умноженное на три), а периоды этих циклов должны равняться значениям n_i. Это нетрудно реализовать, используя описанную в [1] теорию.

Поставим в соответствие периоду каждого стабилизированного цикла определенный символ алфавита. Найдем возмущение, стабилизирующее данный цикл. При передаче такого возмущения на приемник реализуется трансляция зашифрованного символа. Расшифровка состоит в том, что полученное периодическое возмущение применяется к отображению, которое зашито в приемнике. В результате динамическая переменная этого отображения совершает некоторое количество циклов. По периодам стабилизированных циклов определяют, какой символ был получен по каналу связи. Таким образом исходный текст расшифровывается. Очевидно, ключом шифрования является вид семейства отображения.

2. Корреляционный анализ

Корреляционный анализ получаемых шифров позволит ответить на вопрос о степени предсказуемости значений кодовой последовательности (что самым непосредственным образом влияет на надежность криптографического метода — степени трудоемкости взлома шифра).

Надежность данного метода шифрования в большой степени зависит от характеристик применяемого метода генерации псевдослучайных чисел, так как на одном из начальных этапов шифрования мы вносим изменения в псевдослучайную числовую последовательность. Представляет интерес анализ последовательности значений динамической переменной с внесенной в нее информацией о необходимом количестве и параметрах совершаемых циклов. Эта последовательность заведомо не обладает равномерным распределением. Мы оценили ее корреляцию с последовательностью, подчиняющейся равномерному закону распределения, и автокорреляцию [15]. Затем был исследован и сам шифр, т. е. выполнен его автокорреляционный анализ.

Таким образом, задачи корреляционного анализа сводились к следующему: 1) найти соотношение между законом распределения получаемой последовательности значений динамической переменной и равномерным законом распределения; 2) выполнить автокорреляционный анализ последовательности значений динамической переменной; 3) выполнить автокорреляционный анализ последовательности значений управляющего параметра (шифра).

При анализе использовалась последовательность динамических переменных длиной 9000 значений, полученная для шифрования сообщения, содержащего 1000 символов «о». Передача символа «о» представляет собой наиболее опасный случай работы описываемого метода защиты, так как код ASCII этого символа равен 111. Это означает, что при шифровании того или иного сообщения информация об «о» будет содержаться в трех следующих друг за другом циклах периода $n_i(=1)+2=3$ и повторение этих циклов особенно нежелательно. Соответствующие случайные числа представляют собой целые из интервала $(0;10)$. Удовлетворительные результаты решения поставленной задачи в этом случае позволят говорить о еще большей надежности метода при шифровании других групп символов.

В результате решения первой задачи получен коэффициент корреляции $r=0.0077$ и уравнение регрессии $y=4.9322905+0.00499911509x$. При этом среднее значение в выборке составляет 4.96478169. Таким образом, здесь можно говорить об отсутствии корреляции.

В ходе решения второй задачи получена функция автокорреляции, близкая к дельта-функции: уже при $\tau=2$ функция попадает в коридор $(-0.02;0.02)$ и больше его не покидает. Это говорит о том, что автокорреляционная связь в исследуемой последовательности практически отсутствует.

Нужно сказать, что при шифровании символа «о» вероятность полного повторения цикла при выбранных параметрах генерации псевдослучайных чисел равна 1/64. Однако предсказать точки следующего цикла по предыдущим весьма затруднительно, о чем свидетельствуют результаты расчетов.

При проведении численных экспериментов в ходе решения третьей задачи для шифрования информации использовались отображения с квадратичными и экспоненциальными функциями. Функция автокорреляции как для первых, так и для вторых практически сразу спадает до нуля (рис. 1), однако при использовании квадратичных отображений она сильно осциллирует в окрестности нуля. Наличие

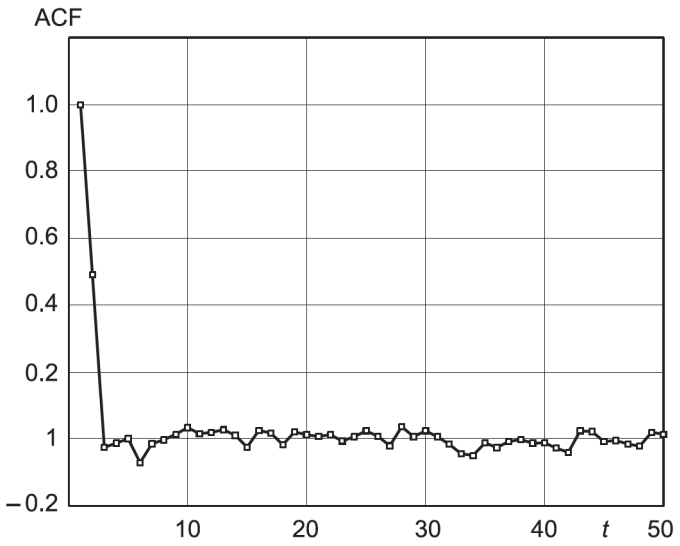

Рис. 1. Функция автокорреляции. Зашифровано 9000 символов «о» (лат.)

таких колебаний влияет на предсказуемость числовых значений, составляющих шифр. Поэтому более предпочтительными для шифрования оказываются отображения экспоненциального вида.

3. Анализ криптостойкости

Основными количественными мерами криптографической стойкости шифра служат так называемые трудоемкость метода криптографического анализа и его надежность. Трудоемкость дешифрования обычно измеряется усредненным по ключам шифра и открытым текстам количеством времени или условных вычислительных операций, необходимых для реализации алгоритма. Надежность метода — это вероятность дешифрования, характеристика метода взлома шифра (криптоанализа). Раз метод криптоанализа несет в себе определенную случайность, например неполное опробование ключей, то и положительный результат его применения возможен с некоторой вероятностью. Наша задача состоит в том, чтобы оценить трудоемкость дешифрования и надежность выбранного метода криптоанализа применительно к исследуемому методу.

Опишем проведение анализа криптостойкости одним из наиболее распространенных методов криптоанализа — методом тотального опробования, который заключается в последовательном случайном и равновероятном опробовании без повторений r ключей из множества ключей K. Процесс опробования заканчивается при опробовании k ключей. При этом $k = j$, где $1 \leqslant j < N$, — номер первого ключа, при котором соответствующий расшифрованный текст будет признан критерием за содержательный текст, или $k = N$, если такое событие не произойдет при любом $j \leqslant N$.

Для оценки содержательности расшифровываемого текста вводятся следующие гипотезы: 1) H_0 — текст открытый (исходный, расшифрованный); 2) H_1 — текст случайный (несодержательный). При составлении вероятностной модели задачи эту оценку определяют следующие ошибки:

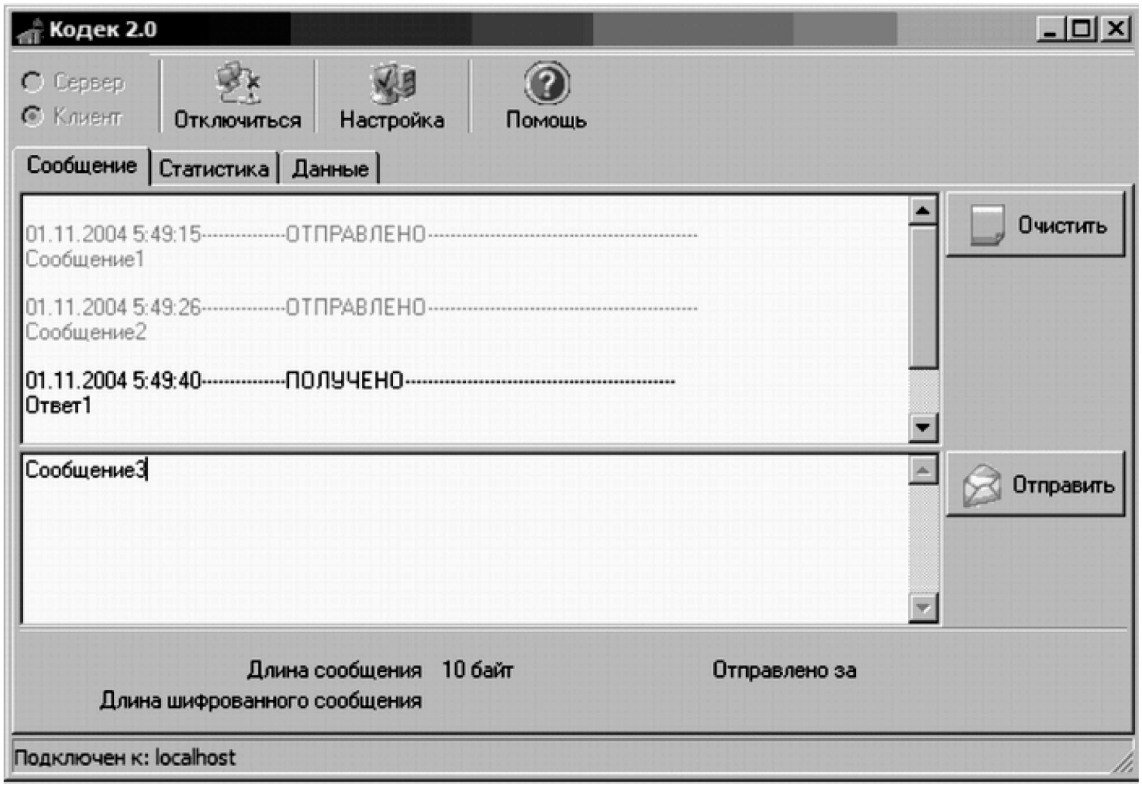

Рис. 2. Диалоговое окно обмена сообщениями программы

1) $\alpha = P(H_1/H_0)$ — вероятность отбраковки содержательного текста; 2) $\beta = P(H_0/H_1)$ — вероятность принятия несодержательного текста за содержательный.

Формализация процесса вычисления трудоемкости криптографического анализа метода выглядит следующим образом [18, 19]:

$$E^{\alpha,\beta}(|K|) = \frac{1}{|K|}\sum_{k=1}^{r} k(1-\beta)^{k-1} \times$$
$$\times \left[\beta(r-k)+\frac{\alpha\beta}{1-\beta}(k-1)+(1-\alpha)\right]+\frac{r}{|K|}r\alpha(1-\beta)^{r-1}+$$
$$+\frac{|K|-r}{|K|}\left(\sum_{k=1}^{r} k(1-\beta)^{k-1}\beta + r(1-\beta)^{r}\right),$$

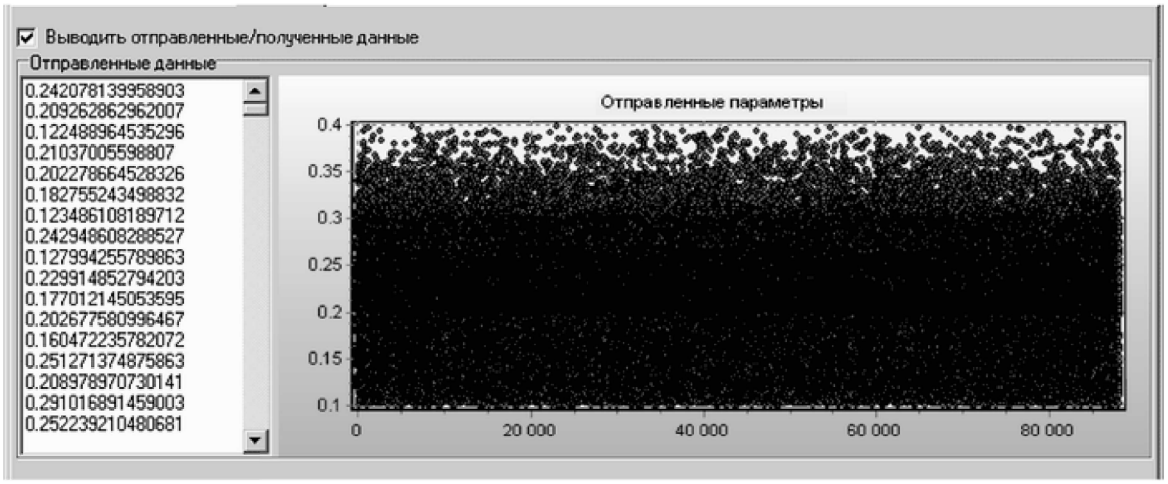

Рис. 3. Диалоговое окно «Данные» программы

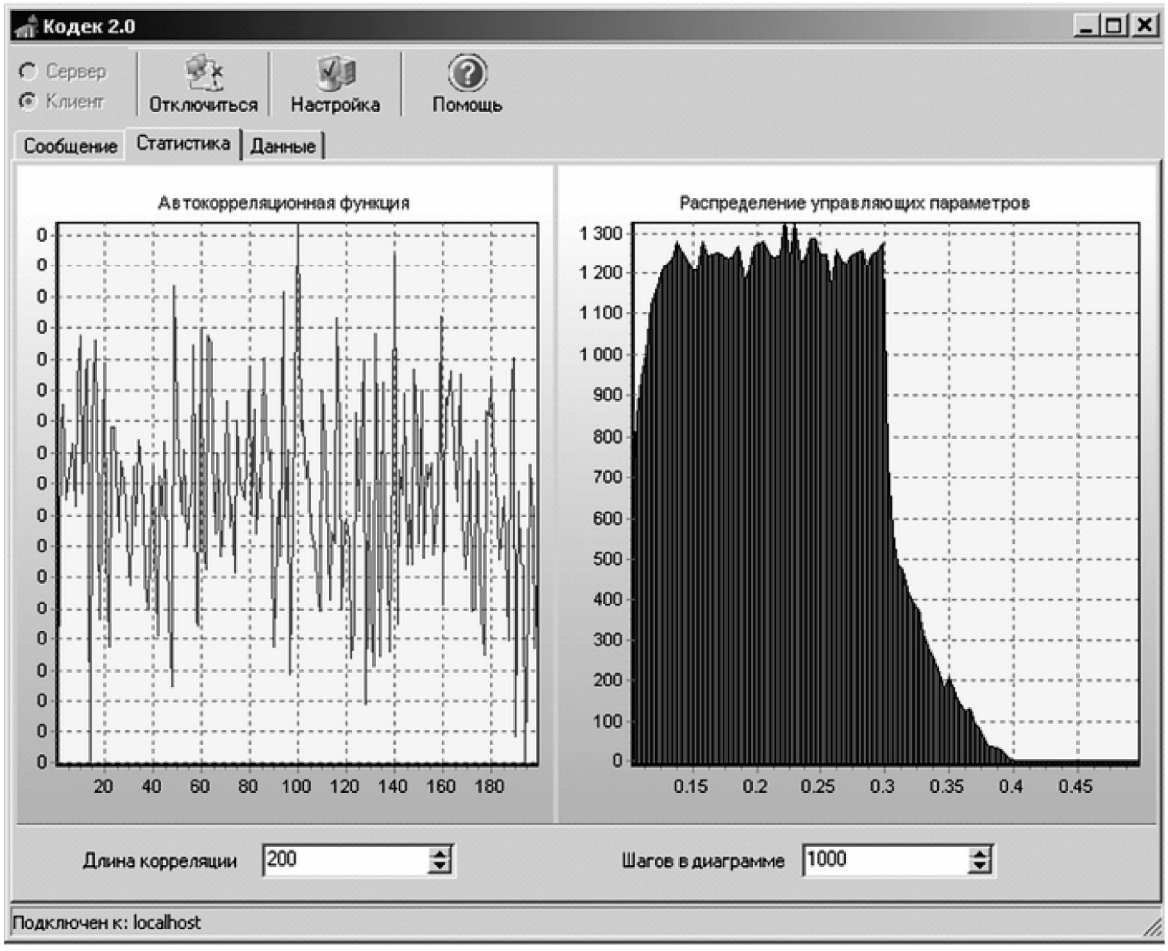

Рис. 4. Диалоговое окно «Статистика» программы

где $E^{\alpha,\beta}$ — трудоемкость криптографического анализа метода, т. е. фактически математическое ожидание случайной величины e, характеризующей окончание процесса опробования, и r — количество опробуемых ключей. Результаты расчета в предположении безошибочной работы механизма принятия решений ($\alpha = 0$, $\beta = 0$) сведены в таблицу. В левой колонке указана одна из настроек метода шифрования — соотношение байт/коэффициент (количество байт, отводимое для хранения каждого значения управляющего параметра). В последней колонке указана трудоемкость, переведенная в единицы времени на основании сведений о производительности современных мейнфреймов (приблизительно 1 инструкция за 1 мкс).

Результаты расчета трудоемкости взлома шифра

Байт/коэффициент	$\|K\|$	$E^{\alpha,\beta}$	$t_{(\|E\|)}$
1	2^{27}	2^{26}	67 с
2	2^{51}	2^{50}	30 лет
3	2^{75}	2^{74}	$6 \cdot 10^{8}$ лет
4	2^{99}	2^{98}	10^{16} лет
5	2^{123}	2^{122}	$1.5 \cdot 10^{23}$ лет

Для расчета надежности используется следующая формула:

$$P(r, \alpha, \beta) = \frac{1-\alpha}{|K|} \sum_{t=1}^{r} (1-\beta)^{t-1}.$$

Очевидно, надежность метода тотального опробования в предположении безошибочной работы логики принятия решений ($\alpha = 0$, $\beta = 0$) равна 1.

Заключение

Результаты проведенных исследований выявили целесообразность дальнейшего анализа предлагаемого метода защиты информации. Следующим шагом в этом направлении явилась практическая реализация метода. На сегодняшний день разработано сетевое приложение, позволяющее пользователям обмениваться текстовыми сообщениями, защищенными представленным методом. Работу программы иллюстрируют рис. 2–4.

Проведенные исследования выявили сильные стороны предложенного метода, в частности следующие: 1) каждый символ алфавита может кодироваться подмножеством положительной меры или даже целой областью; 2) не требуется предварительная синхронизация приемника и передатчика; 3) метод обладает высокой криптостойкостью и хорошими корреляционными свойствами; 4) относительная простота данного метода легко позволяет реализовать его на практике.

Литература

1. *Лоскутов А.Ю., Рыбалко С.Д., Чураев А.А.* // Письма в ЖТФ. 2004. **20**, № 30. С. 1.
2. *Дмитриев А.С.* // Радиоэлектроника. 1991. **5**. С. 101.
3. *Dmitriev A., Panas A., Starkov S.* // Proc. of the Int. Conf. on nonlinear dynamics. Nizhnii Novgorod, 1996. P. 36.
4. *Дмитриев А.С., Андреев Ю.В., Булушев А.Г.* // Зарубежн. радиоэлектрон. Усп. совр. радиоэлектрон. 2000. № 11. С. 27.
5. *Дмитриев А.С., Кузьмин Л.В., Панас А.И., Старков С.О.* // Радиотехн. и электрон. 1998. **43**, № 9. С. 1115.
6. *Dmitriev A.S., Kassian G., Khilinsky A.* // Int. J. Bif. and Chaos. 2000. **10**, N 4. P. 749.
7. *Дмитриев А.С., Кяргинский Б.Е., Панас А.И., Старков С.О.* // Радиотехн. и электрон. 2001. **46**, № 2. С. 224.
8. *Dmitriev A., Kyarginsky B., Panas A., Starkov S.* // Proc. of 9th workshop on nonlinear dynamics of electronic systems (NDES'2001). Delft, Netherlands. 21–23 June, 2001. P. 157.
9. *Andreyev Yu.V., Dmitriev A.S., Starkov S.O.* // IEEE transact. on circuits and systems. 1997. **44**, N 1. P. 21.
10. *Андреев Ю.В., Дмитриев А.С., Куминов Д.А.* // Хаотические процессоры. Успехи совр. радиоэлектрон. 1997. № 10. С. 50.
11. *Гуляев Ю.В., Беляев Р.В., Воронцов Г.М.* // Радиотехн. и электрон. 2003. **48**, № 10. С. 1157.
12. *Loskutov A., Shishmarev A.I.* // Chaos. 1994. **4**, № 2. P. 351.
13. *Лоскутов А.Ю., Шишмарев А.И.* // Успехи матем. наук. 1993. **48**, № 1. С. 169.
14. *Loskutov A.* // Comput. Math. and Modeling. 2001. **12**, N 4. P. 314.
15. *Лоскутов А.Ю., Михайлов А.С.* Основы теории сложных систем. М.; Ижевск, 2007.
16. *Loskutov A.* // Nonlinear Dynamics: New Theoretical and Applied Results / Ed. by J. Awrejcewicz. Academie Verlag, 1995. P. 126.
17. *Loskutov A., Tereshko V.M., Vasiliev K.A.* // Int. J. Bif. and Chaos. 1996. **6**, N 4. P. 725.
18. Теория и практика обеспечения информационной безопасности / Под ред. П. Д. Зегжда. М., 1996.
19. Введение в криптографию / Под ред. В. В. Ященко. М., 2000.

Поступила в редакцию
30.05.2007