МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
им. М.В.ЛОМОНОСОВА
ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи

Чураев Александр Анатольевич

ЗАЩИТА ИНФОРМАЦИИ ПОСРЕДСТВОМ ПРИМЕНЕНИЯ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ

Специальность 01.04.02 — Теоретическая физика

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата физико-математических наук

Москва – 2007

Работа выполнена на физическом факультете Московского государственного университета им. М.В.Ломоносова.

Научный руководитель:

доктор физ.-мат. наук, профессор А.Ю.Лоскутов.

Официальные оппоненты:

доктор физ.-мат. наук, профессор А.С.Дмитриев;

доктор физ.-мат. наук, профессор А.И.Чуличков.

Ведущая организация: Институт общей физики им. А.М.Прохорова РАН.

Защита **состоится** 15 ноября 2007 года в ..... часов на заседании диссертационного совета К.501.001.17 физического факультета МГУ им. М.В.Ломоносова по адресу: 119992, ГСП-2, Москва, Ленинские Горы, МГУ им. М.В. Ломоносова, физический факультет, ауд .....

С диссертацией можно ознакомиться в библиотеке физического факультета МГУ им. М.В.Ломоносова.

Автореферат **разослан** 12 октября 2007 года.

Ученый секретарь

диссертационного совета К.501.001.17

доктор физ.-мат. наук П.А.Поляков

Общая характеристика работы

Актуальность темы

Криптография - наука о шифрах - долгое время была засекречена, так как применялась, в основном, для защиты государственных и военных секретов. В настоящее время методы и средства криптографии используются для обеспечения информационной безопасности не только государства, но и частных лиц, и организаций. Дело здесь совсем не обязательно в секретах. Слишком много различных сведений распространяется по всему свету в цифровом виде. И для этих сведений существуют угрозы недружественного ознакомления, накопления, подмены, фальсификации и т.п. Наиболее надежные методы защиты от таких угроз дает именно криптография.

С каждым днем криптография и криптографические методы все шире входят в нашу жизнь и даже быт. Вот несколько примеров. Отправляя E-mail, мы в некоторых случаях отвечаем на вопрос меню: “Нужен ли режим зашифрования?” Владелец банковской карточки, обращаясь через терминал к банку, вначале выполняет криптографический протокол аутентификации карточки. Пользователи сети Интернет наверняка знакомы с дискуссиями вокруг возможного принятия стандарта цифровой подписи для тех страниц, которые содержат критическую информацию (юридическую, коммерческую и др.). С недавних пор пользователи сетей стали указывать после своих фамилии и инициалов наряду с уже привычным “Email ...” и менее привычное – “Отпечаток открытого ключа ...”.

Появляется множество методов криптографии (защиты информации) и криптоанализа (взлома защиты). Постоянно растут требования к методам, главным образом, касающиеся их криптостойкости и производительности.

В связи с этим вызывают интерес появляющиеся в последние годы приложения нелинейной, и, в частности, хаотической динамики к проблеме защиты информации. В работе предложен, исследован и программно реализован новый метод защиты информации посредством кодирования элементов информации стабилизированными циклами семейств хаотических отображений.

Метод разработан в лаборатории хаоса и нелинейных явлений (Московский государственный университет им. М.В. Ломоносова, физический факультет, кафедра физики полимеров и кристаллов) под руководством профессора доктора физико-математических наук Александра Юрьевича Лоскутова.

Чтобы обоснованно подойти к практической реализации нового криптографического метода, необходимо провести эксперименты и получить ряд характеризующих его оценок. Этим обусловлены последовательность, состав и содержание этапов работы.

Объект исследования

Объектом исследования является приложение метода хаотической динамики, заключающегося в стабилизации циклов отображений нелинейных динамических систем, к шифрованию информации.

Цель диссертационной работы

Основной целью проводимых работ является комплексный анализ предлагаемого нового (что обуславливает большой объем исследовательских работ) криптографического метода на предмет применения для защиты информации от постороннего наблюдателя как при передаче по каналам связи, так и при сохранении на носителях информации, и практическая реализация шифрования этим методом. Практическая реализация целесообразна только при удовлетворительных результатах аналитических и исследовательских работ.

Научная новизна

Научная новизна работы состоит в том, что в ней впервые представлен, теоретически обоснован, и практически реализован новый метод защиты информации, базирующийя на некоторых результатах теории нелинейных динамических систем. Приведены результаты корреляционного анализа метода, анализа криптостойкости, основные технические характеристики метода. Применение отображений с хаотическими свойствами для шифрования информации описанным образом представляется новым и достаточно интересным результатом.

Научная и практическая ценность

Научная ценность определяется новизной разрабатываемого в диссертации метода шифрования и и его комплексным анализом.

Практическая ценность работы состоит в возможности использования нового криптографического алгоритма для передачи информации по каналам связи в компьютерных сетях. Показано, что метод способен достаточно надежно и с большой производительностью защ-

ищать передаваемую информацию.

Защищаемые положения

1. Построено теоретическое обоснование нового криптографического метода, основанного на стабилизации циклов нелинейных динамических систем.
2. Сформирован алгоритм шифрования-дешифрования текста;
3. Экспериментально получены кодовые последовательности (шифры);
4. Проведен корреляционный анализ метода;
5. Проведен анализ криптостойкости (методом тотального опробования);
6. Разработан программный продукт, реализующий обмен текстовыми сообщениями, зашифрованными представленным методом;
7. Получены основные технические характеристики метода;
8. Проведен сравнительный анализ метода с наиболее распространенными на сегодняшний день криптографическими методами.

Публикации

Основные результаты диссертационной работы изложены в 3 публикациях, перечень которых приведен в конце автореферата, и апробированы на 9 международных конференциях (всего 15 апробаций).

Содержание работы

Диссертация состоит из введения, 7-и глав и заключения.

Во введении кратко рассмотрена история вопроса, обоснована актуальность темы и приведено краткое содержание диссертации.

Первая глава посвящена обзору литературы по теме диссертации. Описана типовая задача криптографии, введены основные понятия: законные пользователи, незаконные пользователи, ключ и др. Ситуация, в которой возникает задача криптографии, описывается следующей схемой (см. рис. 1).

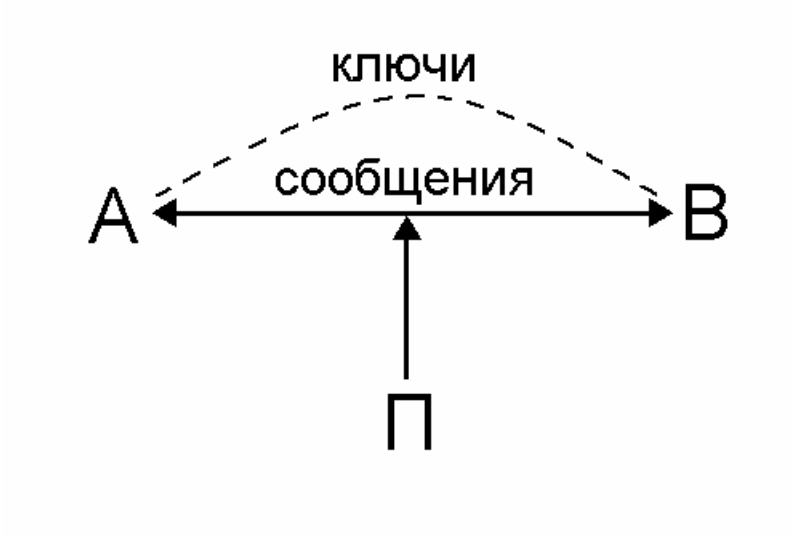

Рис. 1: Схема типовой задачи криптографии

Здесь А и Б — удаленные законные пользователи защищаемой информации, желающие обмениваться информацией по общедоступному каналу связи. П — незаконный пользователь (*противник*), который может перехватывать передаваемые по каналу связи сообщения и пытаться извлечь из них интересующую его информацию. Эту

формальную схему можно считать моделью типичной ситуации, в которой применяются криптографические методы защиты информации. Важнейшим элементом при использовани и криптографических методов является, так называемый, ключ метода. Под в криптографии понимают сменный элемент шифра. При анализе угрозы взлома шифра считается, что принцип шифрования известен противнику и доступен для предварительного изучения, и для злоумышленника задача взлома сводится к подбору ключа. Концепция использования ключей приводит к тому, что законные польщователи А и Б до начала обмена зашифрованными сообщениями должны обменяться ключами. Для этого должен использоваться альтернаивный канал связи (показан на рис.1 пунктиром).

Также в этой главе приведены и описаны основые угрозы при обмене сообщениями высокой важности. Кроме того, описаны необходимые условия, позволяющие применять те или ины средства защиты.

Во **второй главе** изложен теоретический аппарат, лежащий в основе предлагаемого метода шифрования информации, который подробно описан в главе 3.

Метод базируется на одном известном факте из теории динамических систем: для достаточно общих семейств одномерных и n–мерных отображений существуют периодические возмущения, приводящие к *стабилизации* циклов определенного периода и, таким образом, выводу системы из хаотического на регулярный режим. Информация может быть зашифрована с помощью взаимно однозначного соответствия символов устойчивым циклам возмущенного отображения. В

качестве передаваемого сигнала используются возмущения, а ключом для расшифровки полученного сообщения служит вид отображения (т.е. функция, задающая отображение).

Рассмотрим отображение некоторой области M из $\mathbf{R}^j$ в себя,

$$T_a : \mathbf{x} \longmapsto \mathbf{f}(\mathbf{x}, a) \ , \tag{1}$$

где a — параметр из множества допустимых значений $A \subset \mathbf{R}$, $\mathbf{x} = \{x_1, \ldots, x_j\}$ и $\mathbf{f} = \{f_1, \ldots, f_j\}$. Введем понятие параметрического возмущения. Самым естественным способом является задание отображения по параметру, которое определяло бы его значение в каждый момент времени: $G : A \to A$. Тогда возмущенное отображение будет выглядеть следующим образом:

$$\mathbf{T}_a : \begin{cases} \mathbf{x} \longmapsto \mathbf{f}(\mathbf{x}, a) \ , \\ \\ a \longmapsto g(a) \ . \end{cases} \tag{2}$$

Возмущение назовем *периодическим* с периодом τ, если функция $g(a)$ определена только в τ точках $a_1, \ldots, a_\tau$ следующим образом: $a_{i+1} = g(a_i), i = 1, \ldots, \tau - 1$ и $a_1 = g(a_\tau)$. Другими словами, возмущение задается посредством τ параметров, которые последовательно подставляются в отображение (1). В этом случае *совокупность* возмущений периода τ может быть поставлена в соответствие множеству $\mathbf{A} = \{\hat{a} \in \underbrace{A \otimes A \otimes \cdots \otimes A}_{\tau} : \ \hat{a} = (a_1, \ldots, a_\tau), \ a_i \neq a_j, \ 1 \leq i, j \leq \tau, \ i \neq j, \ a_1, \ldots, a_\tau \in A\}$, $\mathbf{A} \subset \mathbf{R}^\tau$.

Введем подмножество $A_c \subset A$ множества параметрических значений такое, что если $a \in A_c$, то отображение (1) будет обладать хаотическим

поведением. В ряде работ было аналитически обосновано, что при $j = 1$ и $j = 2$ посредством периодических возмущений можно подавить хаос и стабилизировать определенные циклы отображений. Иными словами, было показано, что для некоторых одномерных и двумерных хаотических отображений существуют такие возмущения $\hat{a} = (a_1, a_2, \ldots, a_\tau)$, что при $\hat{a} \in \mathbf{A}_c$, $\mathbf{A}_c = \underbrace{A_c \otimes A_c \otimes \cdots \otimes A_c}_{\tau}$, (или $g(a) \in A_c$, см. (2)) возмущенное отображение (2) будет регулярным и обладающим устойчивым циклом периода $t = \tau n$. Данный результат был доказан для широкого класса отображений. По-видимому, при достаточно общих условиях на вид семейства отображений, свойство проявлять периодическую динамику вследствие внешних воздействий является типичным.

Для практического воплощения метода шифрования информации посредством возмущенных отображений необходимо уметь находить такие τ–периодические преобразования $G : a \mapsto g(a)$ для отображения (2), при которых оно будет обладать *устойчивым* циклом. В работе рассматриваются только одномерные ($j = 1$) отображения. Для таких отображений удается обобщить развитую ранее теорию и эффективно использовать метод поиска возмущений, приводящих к стабилизации *заранее заданных* циклов в практических целях.

Также в данной главе приведены выкладки для расчета допустимого уровня искажений шифра при передаче и условия устойчивости используемых циклов.

В **третьей главе** описан способ применения метода стабилизации циклов для шифрования текстовой информации, вводимой с клавиат-

уры персонального компьютера. Кратко он может быть представлен следующим образом.

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. Таким образом, мы получаем некоторую последовательность целых чисел. 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 как период цикла, который имеет некоторая динамическая система.

Чтобы избежать присутствия вырожденных циклов (периода 0) и устойчивых точек (циклов периода 1) к каждому n следует прибавить двойку. Избавляться от циклов периода 1 следует потому, что эти циклы не изменяют значения динамической переменной $x = \{x_1, ..., x_m\}$. При этом значения управляющего параметра $\hat{a} = \{a_1, ..., a_n\}$, стабилизирующего такие циклы, повторяются, что отрицательно скажется на криптостойкости метода. Это вызвано, в частности, тем, что единицы в совокупности составляющих ASCII-кодов встречаются чаще других цифр.

Далее, необходимо получить последовательность чисел, имеющую

длину, равную сумме всех n_i (увеличенных на два) плюс 1 (смысл этого прибавления единицы раскрыт в диссертационной работе). При этом желательно наличие у этой последовательности свойств, характеризующих ее как случайную. Теперь последовательность чисел необходимо интерпретировать как последовательность значений динамической переменной x.

Необходимо сказать несколько слов о генерации числовой последовательности со случайными свойствами. Для образования такой последовательности в работе не используются сторонние генераторы случайных чисел. Последовательности формируются на основе результатов, известных из теории динамических систем. Например, известно, что определенные растягивающие отображения могут порождать последовательности, обладающие заданной степенью случайности. Также семейство квадратичных отображений при определенных значениях параметров может обладать свойствами случайного процесса.

Допустим, что мы сформировали последовательность значений динамической переменной x. 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 посредством замен нужных значений в последовательности x на близкие к x_c (определенное значение, характеризующее используемое отображение) с учетом теории, описанной во второй главе диссертационной работы.

Поставим в соответствие периоду каждого стабилизированного цикла определенную компоненту символов алфавита (n_i). Найдем теперь возмущение, стабилизирующее данный цикл. Такие возмущения всегда существуют. При передаче такого возмущения на приемник реализуется трансляция зашифрованного символа. Расшифровка состоит в том, что полученное периодическое возмущение, использованное при шифровании, 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.

Принцип шифрования может быть представлен в следующем виде:

Таблица 1. Принципиальная схема шифрования символа

$$\left\{\begin{array}{c}\mathbf{Y}\\ \text{символ}\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\mathbf{n_1},\ \mathbf{n_2},\ \mathbf{n_3}\\ ASCII-\text{код}\end{array}\right\} \longrightarrow$$

$$\longrightarrow \left\{\begin{array}{c}\{\mathbf{a_1},\ldots,\mathbf{a_{n_1+2}}\},\{\mathbf{b_1},\ldots,\mathbf{b_{n_2+2}}\},\{\mathbf{c_1},\ldots,\mathbf{c_{n_3+2}}\}\\ \text{наборы параметров (периодическое возмущение)}\end{array}\right\} \longrightarrow$$

$$\longrightarrow \left\{\begin{array}{c}\mathbf{a_1},\ldots,\mathbf{c_{n_3+2}}\\ \text{посл-ть}\quad\text{чисел}\end{array}\right\}$$

В **четвертой главе** описаны задачи и результаты корреляционного анализа представляемого метода.

Для того чтобы ответить на вопрос о надежности метода, необходимо провести корреляционный анализ получаемых шифров. Под надежностью в данной главе диссертационной работы понимается степень непредсказуемости значений кодовой последовательности (что самым непосредственным образом влияет и на надежность криптографического метода в ее традиционном понимании – степени трудоемкости взлома шифра).

Представляет интерес анализ последовательности значений динамической переменной со 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. Затем был проведен автокорреляционный анализ и самого шифра.

Таким образом, задачи корреляционного анализа сводились к следующему.

- Найти соотношение между законом распределения получаемой последовательности значений динамической переменной и равномерным законом распределения;
- Выполнить автокорреляционный анализ последовательности значений динамической переменной;
- Выполнить автокорреляционный анализ последовательности значений управляющего параметра (шифра).

При анализе использовалась последовательность динамических

переменных длиной 9000 значений, полученная для шифрования сообщения, содержащего 1000 символов единственного символа «o». Передача символа «o» представляет собой наиболее опасный случай работы описываемого метода защиты, т.к. код ASCII этого символа равен 111. Это означает, что при шифровании того или иного сообщения информация об «o» 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 корреляционного анализа коэффициент корреляции составил $c = 0,0077$, а уравнение регрессии имеет вид: $y = 4,9322905 + 0,00499911509x$. При этом среднее значение в выборке $4,96478169$. Таким образом, здесь можно говорить об отсутствии корреляции.

Опишем результаты автокорреляционного анализа последовательности значений динамической переменной. Вид функции автокорреляции близок к дельта-функции, так что 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 «o» вероятность полного повторения цикла при выбранных параметрах генерации псевдослучайных чисел равна $1/64$. Однако предсказать точки след-

ующего цикла по предыдущим весьма затруднительно, о чем свидетельствуют результаты расчетов.

Для оценки предсказуемости значений в последовательности шифра необходимо построить его функцию автокорреляции. При проведении численных экспериментов для шифрования информации использовались отображения с квадратичными $f = ax^2 + bx + c$ и экспоненциальными $f = ae^{(b-x)}$ функциями. Функция автокорреляции, как для первых, так и для вторых, практически сразу спадает до нуля (рис.2), однако при использовании квадратичных отображений она сильно осциллирует в окрестности нуля. Наличие таких колебаний влияет на предсказуемость числовых значений, составляющих шифр. Поэтому более предпочтительными для шифрования оказываются отображения экспоненциального вида.

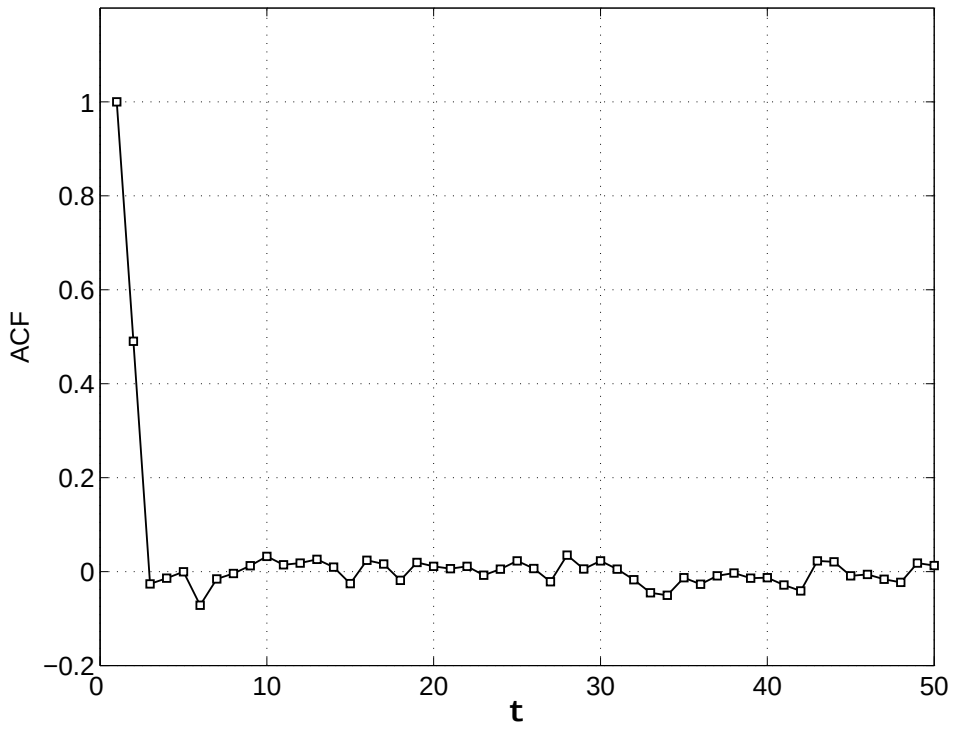

Рис. 2: Функция автокорреляции. Зашифровано 9000 символов "о"(лат.))

Таким образом, выполненный корреляционный анализ показал, что метод защиты информации, основанный на стабилизации циклов отображений, обладает высокой надежностью в части предсказуемости значений последовательностей шифров и способен защищать текстовые сообщения значительных размеров.

В **пятой главе** приведено описание и результаты анализа криптостойкости исследуемого метода.

Основными количественными мерами криптографической стойкости шифра служат так называемые трудоемкость метода криптографического анализа и его надежность. Трудоемкость дешифрования 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.

Анализ криптостойкости был проведен 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 $1 < j < N$, — номер первого ключа, при котором соответствующий расшифрованный текст будет признан критерием за

содержательный текст, или $k = N$, если такое событие не произойдет при любом $j \leq N$.

Для оценки содержательности расшифровываемого текста были введены следующие гипотезы:

1) H_0 — текст открытый (исходный, расшифрованный);

2) H_1 — текст случаен.

При составлении вероятностной модели задачи эту оценку определяют следующие ошибки: (а) $\alpha = P(H_1/H_0)$ — вероятность отбраковки содержательного текста; (б) $\alpha = P(H_0/H_1)$ — вероятность принять несодержательный текст за содержательный.

Приведем результаты расчета указанных основных характеристик криптостойкости алгоритма шифрования (трудоемкости и надежности). Формализация процесса вычисления трудоемкости криптографического анализа выглядит следующим образом:

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

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

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 таблице 2. В левой колонке указана одна из настроек метода шифрования

— соотношение байт/коэффициент (количество байт, отводимое для хранения значения управляющего параметра). В последней колонке указана трудоемкость, переведенная в единицы времени на основании сведений о производительности современных мейнфреймов (приблизительно одна инструкция за 1 мкс).

Таблица 2. 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}	$6 * 10^8$ лет
4	2^{99}	2^{98}	10^{16} лет
5	2^{123}	2^{122}	$1,5 * 10^{23}$ лет

Для расчета надежности используется следующая формула:

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

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

Показано, что при определенном выборе количества байт, отводимых для хранения значений управляющего параметра, представляемый метод защиты информации обладает достаточно высокой криптоаналитической стойкостью.

Результаты проведенных исследований выявили целесообразность дальнейшей проработки предлагаемого метода защиты информации.

Следующим шагом в этом направлении явилась практическая реализация метода.

В **шестой главе** описывается разработанное сетевое приложение, позволяющее обмениваться текстовыми сообщениями, защищенными представляемым методом, используя каналы связи компьютерных сетей. Приложение реализовано на языке программирования C++ в среде разработки "Microsoft Visual Studio 6.0". В главе приводятся функциональные возможности разработанного программного продукта и рекомендации по его использованию.

В **седьмой главе** представлены основные характеристики метода, определяющие возможность его применения в тех или иных областях, показаны результаты сравнительного анализа с другими широко используемыми сегодня методами криптографической защиты информации, показаны примеры шифрования текста с помощью предлагаемого криптографического метода, освещены его основные достоинства.

В **заключении** суммируются и обобщаются результаты, полученные в диссертации.

Выводы

1. Обоснован и развит метод, позволяющий защищать текстовую информацию, как передаваемую по каналам связи, так и сохраняемую на цифровых носителях информации;

2. Установлена высокая корреляционная стойкость метода;

3. Установлена высокая криптостойкость (исследована с помощью

метода тотального опробования);

4. Программная реализация метода работопособна и обладает высокой производительностью шифрования (600 бит/с);

5. Показаны преимущества и недостатки метода по сравнению с наиболее распространенными на сегодняшний день методами криптографической защиты (RSA и DES);

Публикации

1. Лоскутов А.Ю., Рыбалко С.Д., Чураев А.А. Система кодирования информации посредством стабилизации циклов динамических систем. //*Письма в ЖТФ*.2004, т.30 вып.20, с.1–7.

2. A.Loskutov, S.Rybalko and A.Churaev. Information encoding by stabilized cycles of dynamical systems. //*Technical Phys. Lett.* 2004, v.30, No10, p.843-845.

3. A.Loskutov and A.Churaev. Information safety by suppression of chaos. //*J. Phys.: Conf. Ser.* 23 (2005) 210-214.

4. A.Loskutov and A.Churaev. Information Encoding by Stabilized Cycles of Dynamical Systems. //*SNSA'05, The 2nd Shanghai International Symposium on Nonlinear Science and Applications*. Shanghai, China.

5. A.Loskutov and A.Churaev: "Stabilization of Cycles of Dynamical Systems and Information Security,"//*in Proc. NDES'06*. Dijon, France, 2006, pp. 112-115.

6. А.Ю.Лоскутов, Е.О. Петренко, С.Д. Рыбалко, А.А. Чураев. Разработка системы кодирования информации, осуществляемого на основе стабилизации циклов отображений нелинейных динамических систем. //*НАУЧНАЯ СЕССИЯ МИФИ-2004. Сборник научных трудов. В 15 томах. Т.2. Программное обеспечение. Информационные технологии.* М.: МИФИ, 2004.

7. А.Ю.Лоскутов, Е.О. Петренко, С.Д. Рыбалко, А.А. Чураев. Статистический анализ метода кодирования информации, осуществляемого на основе стабилизации циклов отображений нелинейных динамических систем. //*Научная сессия МИФИ-2004. Сборник научных трудов. В 15 томах. Т.2. Программное обеспечение. Информационные технологии.* М.: МИФИ, 2004.

8. А.Ю.Лоскутов, Е.О. Петренко, С.Д. Рыбалко, А.А. Чураев. Анализ криптостойкости метода кодирования информации, осуществляемого на основе стабилизации циклов отображений нелинейных динамических систем. //*Научная сессия МИФИ-2004. Сборник научных трудов. В 15 томах. Т.2. Программное обеспечение. Информационные технологии.* М.: МИФИ, 2004.

9. А.Ю.Лоскутов, Е.О. Петренко, С.Д. Рыбалко, А.А. Чураев. Разработка системы кодирования информации, осуществляемого на основе стабилизации циклов отображений нелинейных динамических систем. //*Научная сессия МИФИ-2004. XI Всероссийская научная конференция "Проблемы информационной безопасности в системе высшей школы". Сборник научных трудов.* М.: МИФИ,

2004.

10. А.Ю.Лоскутов, Е.О. Петренко, С.Д. Рыбалко, А.А. Чураев. Статистический анализ метода кодирования информации, осуществляемого на основе стабилизации циклов отображений нелинейных динамических систем. //*Научная сессия МИФИ-2004. XI Всероссийская научная конференция "Проблемы информационной безопасности в системе высшей школы". Сборник научных трудов.* М.: МИФИ, 2004.

11. А.Ю.Лоскутов, Е.О. Петренко, С.Д. Рыбалко, А.А. Чураев. Анализ криптостойкости метода кодирования информации, осуществляемого на основе стабилизации циклов отображений нелинейных динамических систем. //*Научная сессия МИФИ-2004. XI Всероссийская научная конференция "Проблемы информационной безопасности в системе высшей школы". Сборник научных трудов.* М.: МИФИ, 2004.

12. А.Ю.Лоскутов, Е.О. Петренко, С.Д. Рыбалко, А.А. Чураев. Система кодирования информации, осуществляемого на основе стабилизации циклов отображений хаотических систем. //*Научная сессия МИФИ-2003. Сборник научных трудов. В 14 томах. Т.1. Автоматика. Микроэлектроника. Электроника. Электронные измерительные системы.* М.: МИФИ, 2003.

13. А.Ю.Лоскутов, Е.О. Петренко, С.Д. Рыбалко, А.А. Чураев. Разработка системы кодирорования информации, осуществляемого на основе стабилизации циклов. //*Радиотехника, элек-*

тротехника и энергетика: Тез. Докл. Девятой Междунар. науч.-техн. конф. студентов и аспирантов. В 3-х т. Т.1. М.: Издательство МЭИ, 2003.

14. А.Ю.Лоскутов, А.А.Чураев. Применение хаотических отображений для защиты информации. //*Вестник МГУ*. Принято в печать.

15. А.А.Чураев, А.П.Сычев, П.С.Шильников. Разработка программного инструментального комплекса для работы с данными, соответствующими CALS-стандарту ISO 10303 STEP. //*Доклады 2-ой международной конференции CAD/CAM/PDM-2002*. М.: Институт проблем управления РАН.-2002

16. А.А.Чураев, А.П.Сычев, П.С.Шильников. Разработка программного инструментального комплекса для работы с данными, соответствующими CALS-стандарту ISO 10303 STEP. //*Труды международных конференций "Искусственные интеллектуальные системы"(IEEE AIS'02) и "Интеллектуальные САПР"(CAD-2002)*. М.: Издательство Физико-математической литературы, 2002.

17. Чураев А.А., Сычев А.П., Шильников П.С. Интеллектуализация работы с данными. //*Восьмая национальная конференция по искусственному интеллекту с международным участием (КИИ-2002)*. Коломна, 2002 г.