Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. Н. Г. ЧЕРНЫШЕВСКОГО»

*Кафедра компьютерной физики*
*и метаматериалов на базе Саратовского филиала*
*Института радиотехники и электроники*
*им. В.А. Котельникова РАН*

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ ХАОТИЧЕСКОГО КОДИРОВАНИЯ НА БАЗЕ ОТОБРАЖЕНИЙ ГАУССА И ПЕКАРЯ

АВТОРЕФЕРАТ
ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ (МАГИСТЕРСКОЙ) РАБОТЫ
студента 2 курса 256 группы
направления 03.04.02 «Физика» физического факультета
Семёнова Антона Александровича

Заведующий кафедрой
д. ф.-м. н., профессор _____В.М.Аникин

«07» 06.2020

Научный руководитель
д. ф.-м. н., профессор _____В.М.Аникин
«07» 06.2020

Саратов
2020

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

***Актуализация работы.*** Содержание данной работы посвящено выявлению принципиальных возможностей изучению схем конфиденциальной передачи информации *на основе одномерных и двумерных хаотических отображений*.

***Основной целью*** выпускной квалификационной работы является сравнительный анализ криптографических методов 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.

***Условия дистанционного образования актуализировали*** конкретную задачу, связанную с передачей конфиденциальных данных о проводимых видеоконференциях во избежание хакерских атак и несанкционированного входа в системы видеоконференций («зумбомбинга», в частности).

***Объект исследования.*** Для целей кодирования информации рассматривается применение хаотических отображений малой размерности – одномерных и двумерных. Разработка алгоритмов кодирования на основе хаотических отображений вполне естественно и уместно, поскольку они представляют собой генераторы псевдослучайных последовательностей, а использование датчиков псевдослучайных чисел, в том числе получаемых на основе модулярной арифметики, – краеугольный камень схем шифрования. Главным стимулом использования хаотических отображений в схемах кодирования информации прежде всего является, на наш взгляд, стремление получить высокоэффективные и криптоустойчивые схемы кодирования, удобные для различных применений, в том числе для реализации во внутрикорпоративных компьютерных сетях с целью решения вполне определенного класса задач, в том числе собственно задачи конфиденциальной передачи данных, задач идентификации отправителя и получателя информации, установления подлинности передаваемой информации и т.п.

Возникает естественный вопрос: а какими свойствами должно обладать хаотическое отображение, чтобы обеспечить прежде всего устойчивость схемы шифрования для криптоанализа? Изначальная предпосылка заключается в том, что динамические системы, демонстрирующие хаотическое поведение, обладают высокой чувствительностью к изменению начальных условий (стартовой точки для итераций) и изменению параметров отображения. Так, незначительное изменение начальных условий ведет к существенно новой орбите (траектории) отображения. Изменение же параметра отображения

приводит к изменению всех его характеристик, включая вид инвариантного распределения, значения показателя Ляпунова, значений собственных чисел ассоциированного с отображением оператора линейного оператора Перрона-Фробениуса и т.п.

Вариация стартовой точки и правила изменения параметров отображения можно произвести в рамках различных вариантов. И определенное сочетание значений стартовой точки и последовательности изменения параметров – это ключ, который может и должен использоваться при построении схем кодирования. Кроме того, выбор самого отображения может привести к интересным особенностям схемы кодирования.

***Метод исследовании*** **–** аналитический и компьютерный анализ особенностей поведения хаотических отображений, позволяющих использовать их для целей криптографической защиты как с позиции их общих свойств, так и с учетом их индивидуальных особенностей, что позволило бы максимально затруднить криптографический анализ шифротекста любым разработанным методом – методом тотального перебора вариантов на компьютерах с самыми мощными вычислительными возможностями (с учетом возможной организации параллельных вычислений на компьютерах с многоядерными процессорами), методами статистического и корреляционного анализа зашифрованного текста и пр.

Ясно, что параллельно с детальной разработкой системы *зашифрования* должна быть определена и методика *расшифрования* передаваемой информации; выявлена степень влияния на них случайных возмущений; исследованы преимущества и недостатки схемы и другие сопутствующие вопросы.

В качестве конкретных отображений для построения криптографических схем в выпускной квалификационной работе используются ***одномерное отображение Гаусса***, определенное на единичном интервале, и ***двумерное отображение пекаря***, заданное на единичном квадрате. Инвариантные плотности для этих отображений имеют аналитические выражения для инвариантных плотностей, а отображение пекаря обладает и уникальными траекторными особенностями.

***Задачами ВКР*** являются:

1) построение общей схемы кодирования на базе одномерного отображения;

2) адаптация этой схемы для отображения Гаусса;

3) исследование эффективности криптографической схемы на базе отображения Гаусса;

4) аналитическое и численное выявление траекторных особенностей одномерного дискретного отображения Гаусса, способствующие его использованию в криптографических схемах;

5) аналитическое и численное выявление траекторных особенностей двумерного дискретного, сохраняющего меру отображения пекаря, способствующие его использованию в криптографических схемах. Под траекторными особенностями отображения пекаря мы будем понимать его обратимость, возможность соотнесения с авторегрессионной системой, циклические траектории отображения.

В качестве ***выносимых на защиту научных результатов*** выносятся примененные приемы изучения и трактовка траекторных свойств отображения Гаусса и пекаря, а также и алгоритмы использования как ядра хаотической схемы кодирования информации для защиты от несанкционированного доступа к ней.

## СТРУКТУРА И СОДЕРЖАНИЕ РАБОТЫ

Во **введении** сформулированы аспектные характеристики выпускной квалификационной работы – ее цель и задачи, теоретическая и прикладная значимость, новые результаты.

**В главе 1** рассмотрены особенности кодирования символов на основе одномерного хаотического отображения Гаусса как дискретной хаотической системы. Выявлены. Свойства криптографической системы при использовании в общем алгоритме: а) разбиения, совпадающего с фундаментальными интервалами отображения Гаусса; б) разбиения с интервалами равной длины. Составлена программа кодирования символов. Проведено сравнение результатов кодирования, полученных на основе двух типов разбиения единичного отрезка, на котором определено отображение Гаусса.

Для проверки криптостойкости метода были исследованы и построены некоторые характеристики, в частности, распределение числа итераций) и средняя длительность итерационной фазы при кодировании больших сообщений (1000 символов), состоящих из одинаковых символов (рис. 1–3).

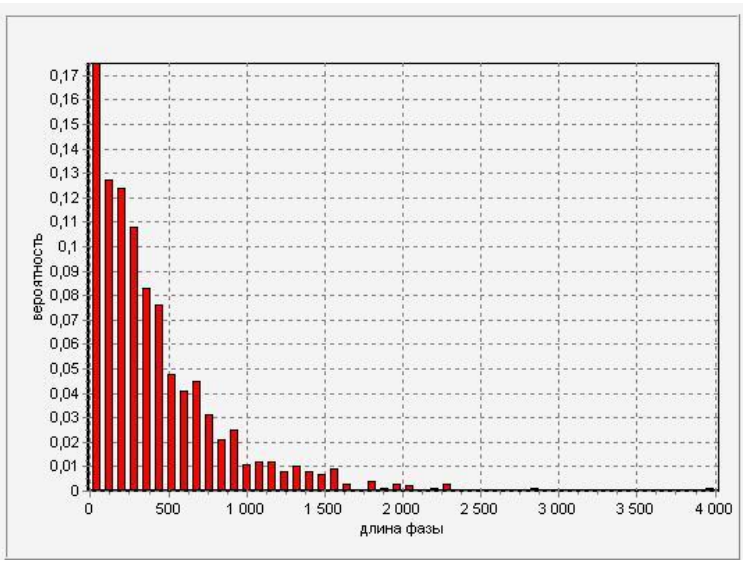


Рис. 1. Распределение чисел итераций для символа на начальном интервале. Средняя длительность – порядка 400 итераций.

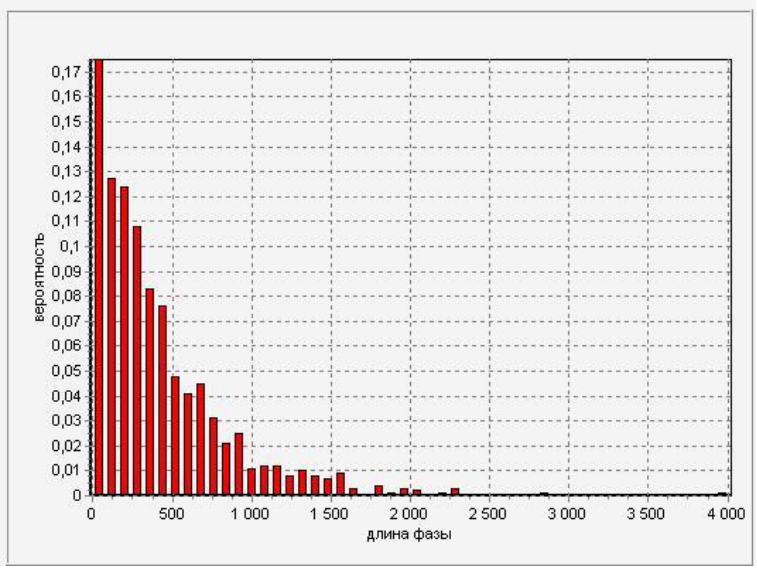


Рис. 2. Распределение чисел итераций для символа на конечном интервале, Средняя длительность – порядка 45000 итераций.

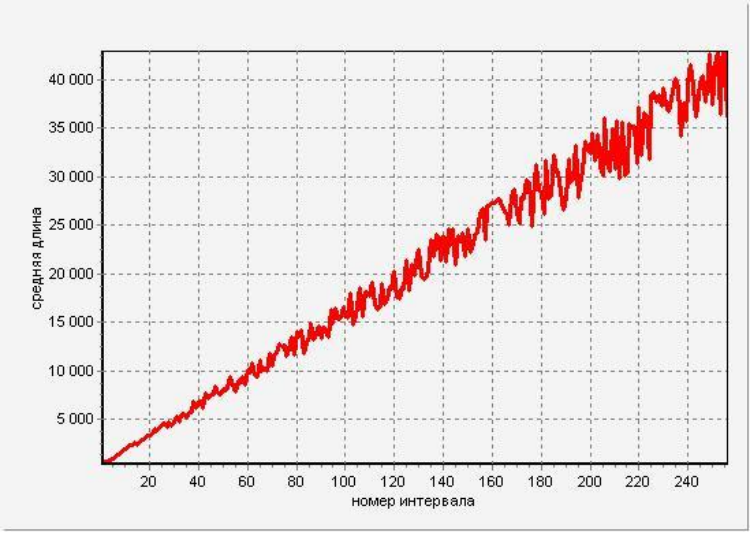


Рис. 3. Распределение средней длительности итераций в зависимости от номера интервала.

Из графиков видно, что среднее число итераций значительно зависит от номера интервала (отличие на два порядка). Это может дать информацию об исходном файле при криптоанализе, так как кодам в данном случае можно сопоставить с большой вероятностью небольшую группу интервалов, для которой характерно это значение.

Данный факт привел к изменению исходного алгоритма, и вместо разбития области определения отображения Гаусса на интервалы по точкам разрыва, отрезок $(0,1)$ разбивается на равные интервалы, общее количество которых совпадает с длиной алфавита, то есть общим количеством символов в ключе. На рис. 4 и 5 приведены распределения числа итераций и средняя длительность итерационной фазы для модифицированного метода.

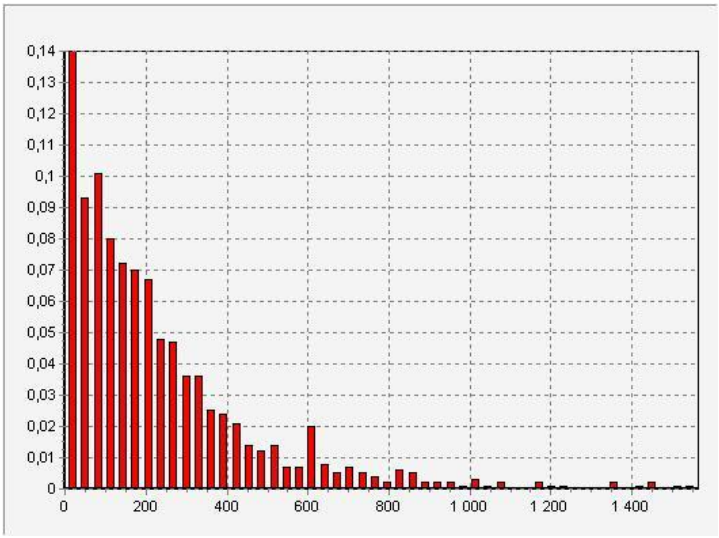


Рис. 4. Распределение чисел итераций, средняя длительность находится в пределах 200-300 итераций. Модифицированный метод

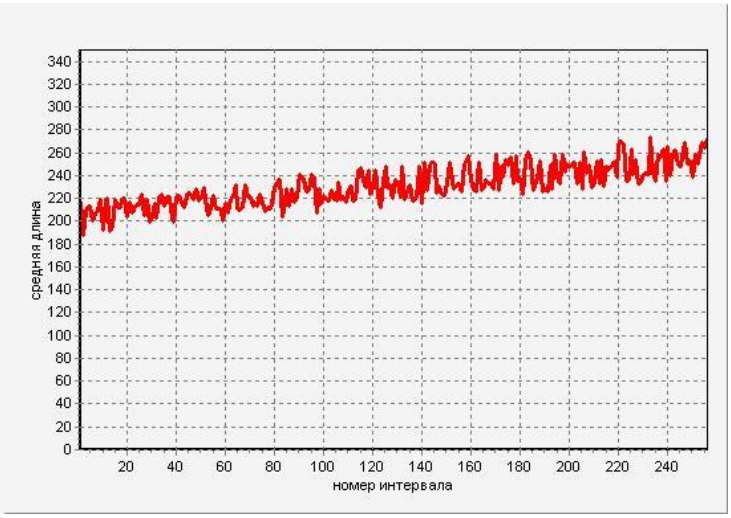


Рис. 5. Распределение средней длительности итераций в зависимости от номера интервала. Модифицированный метод.

Из графика на рис. 5 видно, среднее число итераций зависит от номера интервала гораздо слабее, чем в случае разбиения единичного интервала на бесконечное число фундаментальных интервалов для отображения Гаусса. Поскольку распределение возможных чисел итераций для всех интервалов перекрывает весь диапазон средних значений, то возможности для определения конкретного символа при криптоанализе заметно снижается.

**В главе 2** изучены трансформационные свойства отображения пекаря. Проанализированы система разностных уравнений для отображения пекаря, особенности хаотического перемешивания, представление итераций в двоичной системе; получены точные выражения для периодических орбит отображения; выявлен характер обратимости отображения пекаря.

**В главе 3** разработан алгоритм кодирования на базе отображения пекаря с учетом свойств отображения, изученных в главе 2 и проведен статистический анализ результатов кодирования.

Необходимо отметить интересные особенности отображения пекаря в применении к задачам хаотического кодирования. Особенности схемы кодирования сообщений на основе отображения пекаря определяются рассмотренными выше свойствами этого отображения. А именно явным образом учитываются три факта. Во-первых, отображение обладает, по существу, единственной компонентой, «ответственной» за хаос (это сдвиг Бернулли, реализуемый по координате $x$). Во-вторых, инвариантным распределением отображения является равномерное распределение. Названные два свойства ценны для процесса шифрования дискретного сигнала. На стадии расшифровки переданного сообщения оказывается незаменимым такое свойство отображения, как его обратимость.

Рассмотрим процесс кодирования сигналов более подробно. Предполагается, что нужно зашифровать сообщение, состоящее из последовательности дискретных (цифровых) отсчетов $s_i$, $i = 1, 2, \ldots$ (аналоговый сигнал предварительно квантуется и нормируется). Процесс кодирования будет состоять из $n$

применений отображения пекаря, начальными данными для каждого цикла итераций (рассмотрим, к примеру, цикл с номером $k$) будут значения $(x_0^{(k)}, y_0^{(k)} = s_k)$.

Почему мы говорим о повторяющихся итерациях отображения с различными начальными условиями? Полезную информацию мы передаем начальному значению по координате $y$. В принципе, в качестве другой координаты – координаты $x_0^{(k)}$ можно взять любое значение, равномерным образом выбранное из единичного интервала. Если теперь осуществить процесс итераций на основе отображения пекаря, состоящий из $m^{(k)}$ шагов, то оба начальных значения $(x_0^{(k)}, y_0^{(k)} = s_k)$, естественно, претерпят соответствующие изменения, причем траектория точки будет заполнять единичный квадрат. При этом в силу эргодичности отображения можно ожидать, что эта траектория в среднем не будет иметь «излюбленных» мест для посещения на единичном квадрате. Остановив процесс итераций через $m^{(k)}$ шагов, переходим к преобразованиям следующей пары координат $(x_0^{(k+1)}, y_0^{(k+1)} = s_{k+1})$, осуществляемой в процессе $m^{(k+1)}$ шагов.

Данная процедура повторяется $n$ раз, по числу дискретных отсчетов в шифруемой последовательности.

В силу обратимости отображения в указанном выше смысле, зная количество проделанных итераций, можно восстановить каждую стартовую пару значений. Если же не знать числа проделанных итераций, то определение начальных значений становится затруднительным и требующим огромного числа переборов с целью определения искомой пары $(x_0^{(k)}, y_0^{(k)} = s_k)$. Несанкционированная дешифровка может быть еще более затруднена, если выбор начальных значений $x_0^{(k)}$ и числа итераций отображения $m^{(k)}$ подчинен дополнительным ключам.

Результаты статистической обработки результатов кодирования показаны на рис. 6.

Ожидаемые результаты кодирования – приближенное к равномерному распределение значений координаты $y_n$ для любого начального значения $x_0$. Полезным сигналом, как говорилось, является величина $y_0$. В процессе итераций происходит ее преобразование; «сигнал» передается в форме $y_N$.

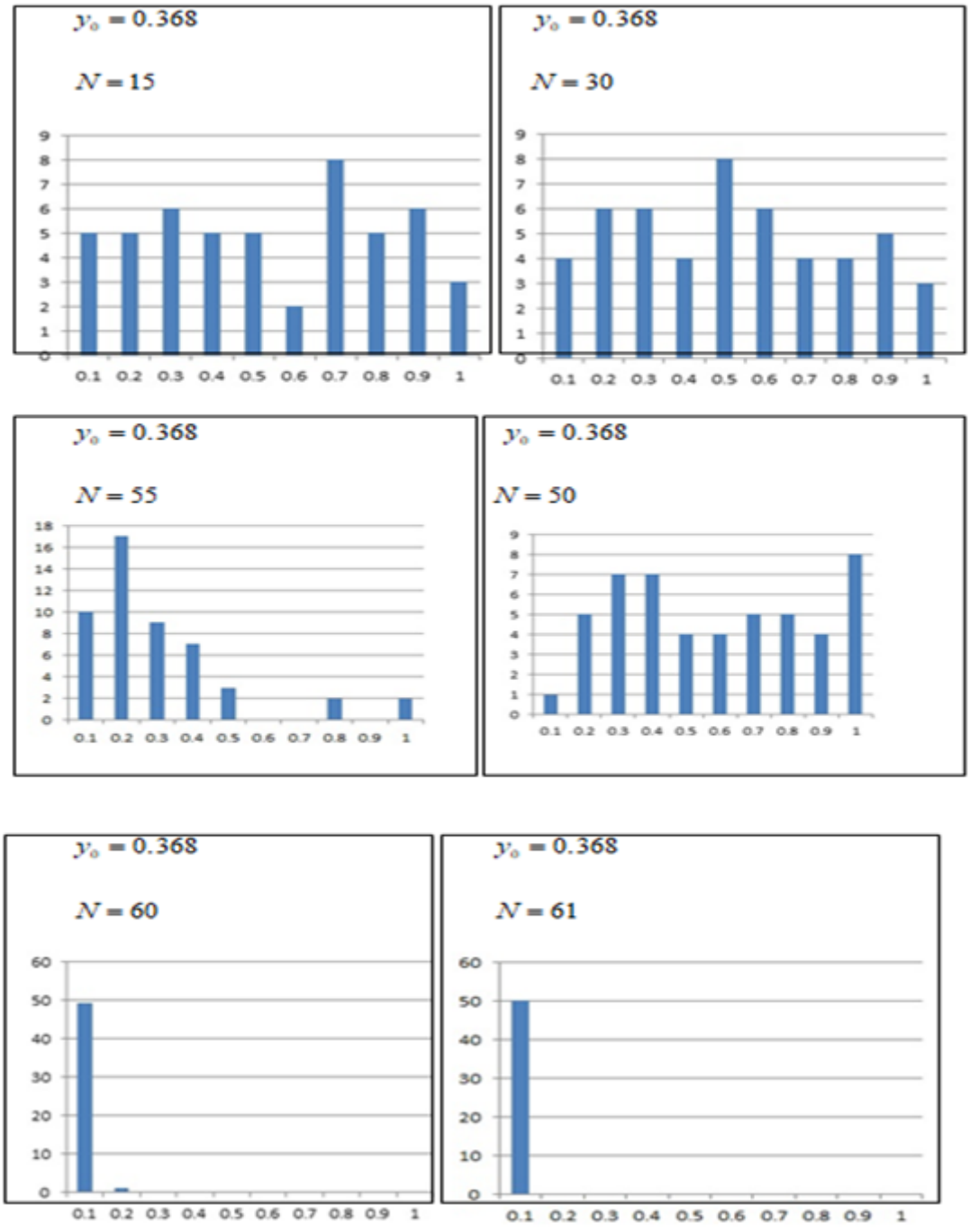


Рис. 6. Результаты статистической обработки результатов кодирования с использованием отображения пекаря

Были построены гистограммы распределения $y_N$ на интервалах (0, 0.1), (0.1, 0.2), …, (0.9, 1) при следующих вариациях данных:

1) для одного $y_0$ и разного количества итераций;

2) для разных $y_0$ и для разного количества производимых итераций. Число генерируемых $x_0$ было постоянным и равным 50 ($m$=50).

В **Заключении ВКР** сформулированы основные выводы по работе.

## ВЫВОДЫ

Применение схемы кодирования, построенной на основе естественных интервалов задания отображения Гаусса, не обеспечивает должной равномерности распределения кодовых значений, т.е. делает систему критичной для криптоанализа. Более приемлемый результат достигается с применением схемы кодирования на базе фиксированного числа интервалов. Эта схема показала свою работоспособность возможность вариабельности базовых отображений делает ее универсальной. Говоря несколько иначе, в схемах с одномерным отображением защита может повышаться посредством введения в ключ шифрования вида отображения.

Проанализирована принципиальная возможность использования отображения пекаря в схемах хаотического кодирования информации. Полезный сигнал соотносится с начальным значениям у-координаты, которая в процессе итераций «искажается» и передается. Восстановление истинного значения возможно благодаря обратимости отображения. Ключ шифра должен содержать число повторений отображения.

На основе анализа полученных гистограмм при кодировании с использованием двумерного отображения пекаря выяснилось следующее:

1) равномерность численных значений выходного сигнала зависит от числа итераций, что может быть связано с наличием машинных ошибок округления результатов и переходом на периодические орбиты;

2) для исключения эффектов машинной арифметики может быть предложено использование иных модификаций отображения пекаря – вместо двоичного сдвига Бернулли, согласно которому изменяется координата $x$ , использовать иные кусочно-линейные отображения (с различным числом и

направлением ветвей при сохранении модуля тангенса наклонов этих ветвей);

3) с той же целью может быть предложена разработка алгоритмов по принципам безошибочной машинной арифметики (работа с целыми числами);

4) таким образом, дальнейшее исследование алгоритма кодирования числовой информации на базе двумерного консервативного перемешивающего отображения пекаря представляется целесообразным.

## Список использованных источников


1. *Дмитриев А.С., Панас А.И.* Динамический хаос: новые носители информации для систем связи. – М.: Изд-во физ.-мат. лит, 2002. – 252 с.
2. *Владимиров С.* Н., *Измайлов И. В., Пойзнер Б. Н.* Нелинейно-динамическая криптология. Радиофизические и оптические системы. М. : ФИЗМАТЛИТ, 2009. 208 с.
3. *Шнайдер Б.* Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке Си. М.: Издательство ТРИУМФ, 2002. – 816 с.
4. *Lasota A., Mackey M.C.* Probabilistic properties of deterministic systems. Cambridge: Cambridge University Press, 1985.
5. *Аникин В.М., Голубенцев А.Ф.* Аналитические модели детерминированного хаоса. М.: ФИЗМАТЛИТ, 2007. – 328 с/
6. *Аникин В. М., Аркадакский С.С., Ремизов А. С.* Несамосопряженные операторы в хаотической динамике. Саратов: Изд-во Сарат. ун-та, 2015. 96 с.
7. *Baptista M.S.* Cryptography with chaos // Phys. Lett. 1998. V. A240. Pp. 50–54.
8. *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.
9. *Аникин В.М., Чебаненко С.В.* Хаотические отображения и кодирование информации: модификации исторически первого алгоритма // Гетеромагнитная электроника: Сб. науч. трудов / под ред. проф. А.В. Ляшенко. Вып. 9. Магнитоэлектроника. Микро- и анноструктуры. Прикладные аспекты. Проблемы физического образования. Саратов: Изд-во Сарат. ун-та, 2011. С. 81-95.
10. *Аникин В.М., Ноянова С.А., Чебаненко С.В.* Кодирование информации на базе отображения пекаря // Гетеромагнитная электроника. 2012. Вып. 12. С. 52 – 60.
11. *Арнольд В. И., Авец А.* Эргодические проблемы классической механики. Ижевск, РХД, 1999. 284 с.
12. *Табор М.* Хаос и интегрируемость в нелинейной динамике. М. : Эдиториал УРСС. 2001. 320 с.
13. *Хопф Э.* Эргодическая теория // УМН. 1949. Т. 4, вып. 1 (29). С. 113–182.

14. *Аникин В.М.* Отображение Гаусса: эволюционные и вероятностные свойства. Саратов: Изд-во Сарат. ун-та, 2007. – 80 с.

15. *Голубенцев А. Ф., Аникин В. М., Ноянова С. А.* Модификация отображения пекаря: особенности асимптотического поведения // Изв. вузов. Прикладная нелинейная динамика. 2004. Т. 12, № 3. С. 45 – 57.

16. *Морозов А. В., Пирожков М. А.* Отображение пекаря и его траектории // Актуальные проблемы гуманитарных и естественных наук. 2017. № 4–6. С. 7–13.

17. *Грегори Р., Кришнамурти Е.* Безошибочные вычисления. Методы и приложения. М. : Мир, 1988. 208 с.

18. *Gaspard P.* Diffusion, Effusion and Chaotic Scattering: An Exactly Solvable Liovillia Dynamics // J. Stat. Phys.1992.Vol 68, Nos 5/6. Pp. 673-747.

19. Kaufman Z., Szépfalusy P. Transient chaos and critical states in generalized baker map // J. Stat. Phys. 2000. V. 101. Nos. 1/2. Pp. 107-124.

20. Toroczkai Z., Károlyi, Péntek Á., Tél T. Autocatalytic reactions in systems with hyperbolic mixing exact results for active Baker map // J. Phys. A: Math. Gen. 2001. V. 34. Pp. 5215-5235.

21. Chernoff D. F., Barrow J. D. Chaos in the Mixmaster Universe // Phys. Rev. Letters. 1983. V.50. No. 2. Pp. 134-137.

22. Tracy M. M., Scott A. J. The classical limit for a class of quantum baker's maps // J. Phys. A: Math. Gen. 2002. V. 35. Pp. 8341-8360.