ОТЗЫВ

официального оппонента на диссертационную работу

Кузнецовой Оксаны Игоревны,
выполненную на тему «Конструирование экстремально мультистабильных хаотических систем и их использование для преобразования информации» и представленную к защите на соискание ученой степени кандидата физико-математических наук по специальности 1.2.2. Математическое моделирование, численные методы и комплексы программ

1. **Структура и объем диссертации.** Диссертация состоит из введения, 4-х глав, заключения, списка литературы и 2-х приложений. Полный объем работы составляет 124 страницы, включает в себя 105 рисунков и 6 таблиц. Список литературы содержит 124 источника.

2. **Актуальность исследования.** В последние десятилетия всё большее количество информации необходимо передавать по каналам связи. Эта информация представляет собой мультимедийные данные, такие как текст, аудио, видео, изображения и другие. Шифрование мультимедийных данных представляет собой преобразование исходных данных в нечитаемую форму так, что злоумышленник не сможет извлечь из неё какую-либо значимую информацию. Для решения подобного рода задач хорошо себя зарекомендовали алгоритмы шифрования на основе хаоса. В последние годы возрос интерес к хаотической криптографии из-за быстрого роста и развития теории хаоса. Более широкое использование хаоса в шифровании мультимедиа мотивировано хаотическими свойствами, такими как сложная динамика, детерминированное поведение, эргодичность, непериодичность, псевдослучайность и высокая чувствительность к начальным условиям и параметрам системы. По сравнению с традиционными методами шифрования, теория хаоса основана на генерировании последовательности шифрования, а не на алгоритме, и генерирует высокослучайную последовательность на основе правильного выбора хаотической системы. Это делает хаотическое шифрование мультимедиа гораздо более безопасным и эффективным, чем традиционные схемы шифрования.

При передаче информации возникает необходимость преобразования аналоговых сигналов в цифровые и наоборот. Например, микросхеме АЦП обычно

требуется неотрицательный аналоговый сигнал в качестве входного сигнала. Естественный вопрос заключается в том, как лучше всего модифицировать биполярный сигнал в дифференциальной хаотической системе, чтобы сделать его однополярным. Оказалось, что добиться этого можно путем реализации процедуры «усиления смещения» (offset boosting). Усиление смещения является очень важной проблемой в хаотических системах, поскольку оно дает инженеру прямой способ преобразовать биполярный хаотический сигнал в униполярный. Существует несколько известных способов организации процедуры усиления смешения: самовоспроизводство аттракторов, удвоение числа аттракторов, введение в систему мемристора. Цель всех этих методов – генерирование на базе исходной хаотической системы новой системы, обладающей аттракторами, расположенными «нужным образом» в её фазовом пространстве.

Настоящая диссертационная работа посвящена разработке новых методов конструирования экстремально мультистабильных хаотических систем на основе систем в форме Лурье. Предлагаемые методы реализуют различные процедуры усиления смещения, а построенные системы допускают их использование в компьютерной криптографии. Поэтому тематику работы Кузнецовой Оксаны Игоревны следует, несомненно, признать **актуальной**.

3. **Научная новизна результатов и выводов.** Работа носит междисциплинарный характер. Для решения поставленных задач требуется комплексное применение математических методов моделирования объектов и явлений в комплексе с разработкой, обоснованием и тестированием эффективных вычислительных методов с применением современных компьютерных технологий, с привлечением математического моделирования, функционального анализа, дискретной и вычислительной математики, дифференциальных уравнений. Все это является предметом исследования в рамках специальности 1.2.2. Математическое моделирование, численные методы и комплексы программ. Анализ заявленной научной новизны и положений, выносимых на защиту, после тщательного изучения научного текста диссертационной работы позволяет согласиться со всеми ее пунктами. Приведу ниже некоторые суммарные результаты, обладающие новизной. Предложен метод конструирования однопараметрических систем-хамелеонов в

форме Лурье, то есть систем, которые обладают самовозбуждающимися или скрытыми аттракторами в зависимости от значений, принимаемых параметром. Предложен метод конструирования n-мерных мегастабильных хаотических систем, обладающих 1-D, (n-1)-D решеткой аттракторов на основе систем в форме Лурье. Разработан метод конструирования n-мерных мегастабильных систем, обладающих n-D решеткой хаотических аттракторов. В диссертации впервые построена система четвертого порядка с 4-D решеткой хаотических аттракторов. Разработан и реализован в виде комплекса программ в пакете вычислений MATLAB алгоритм преобразования информации, передаваемой по каналам связи, на основе сконструированных в диссертации мегастабильных систем, обладающих хаотическими аттракторами, с помощью которого маскируются такие виды информации как текст, изображение в градациях серого, цветное изображение, аудиоинформация и видеоинформация.

4. **Соответствие паспорту научной специальности.** Область исследования и содержание диссертации соответствуют пунктам: 1. Разработка новых математических методов моделирования объектов и явлений. 2. Разработка, обоснование и тестирование эффективных вычислительных методов с применением современных компьютерных технологий. 3. Реализация эффективных численных методов и алгоритмов в виде комплексов проблемно-ориентированных программ для проведения вычислительного эксперимента. 5. Разработка новых математических методов и алгоритмов валидации математических моделей объектов на основе данных натурного эксперимента или на основе анализа математических моделей. 1.1.2. Дифференциальные уравнения и математическая физика (физико-математические науки) паспорта научной специальности 1.2.2. Математическое моделирование, численные методы и комплексы программ (физико-математические науки).

5. **Теоретическая и практическая ценность результатов.** Соискателем сделан существенный вклад в постановку и разработку новых аналитико-численных методов конструирования однопараметрических систем-хамелеонов, а также мегастабильных хаотических систем, допускающих потенциальное использование в маскировке информации, представленной в виде текста, изображений, аудио и видеоинформации,

или создании сигналов нужной полярности. Собственное теоретическое значение имеют и результаты многочисленных расчетов и анализа поставленных задач. Разработанный математический аппарат, алгоритмы, программное обеспечение, методики имеют универсальный характер и широкий спектр применения в различных инженерных приложениях, таких как использование хаотических систем в криптографии, для организация безопасной связи. Разработанные математические методы и программы, а также полученные численные результаты могут быть использованы специалистами в области теории хаоса, теории нелинейных колебаний, радиофизики, а также различных организациях, например, на кафедре прикладной математики и системного анализа Саратовского государственного технического университета имени Гагарина Ю.А., на кафедре динамического моделирования и биомедицинской инженерии Саратовского национального исследовательского государственного университета имени Н.Г. Чернышевского, в лаборатории теоретической нелинейной динамики Саратовского филиала Института радиотехники и электроники имени В.А. Котельникова РАН

6. **Апробация работы и полнота опубликованных результатов.** По теме диссертации опубликована 21 работа. Основные положения рецензируемой работы в достаточной мере опубликованы в рецензируемых научных журналах и изданиях, включая публикации из перечня ВАК Минобрнауки, в журналах, индексируемых в базе Scopus, в материалах ряда Международных и Всероссийских конференций и получены 2 свидетельства о государственной регистрации программы для ЭВМ.

7. **Диссертация и автореферат** написаны понятным научным языком, имеются некоторые замечания, которые будут изложены ниже. Содержание диссертации полно и подробно раскрывает постановку, методы и результаты решения рассмотренных задач с подробным анализом. Оформление диссертации и автореферата в основном соответствует существующим требованиям. Основные результаты опубликованы в рецензируемых изданиях в количестве, значительно превышающем требования для кандидатских диссертаций, указанных в пункте 9 «Положения о порядке присуждения ученых степеней ВАК РФ».

8. **Достоверность и обоснованность положений, выводов и рекомендаций.** Приведенные в диссертационном исследовании теоретические результаты получены

на основе корректного применения качественной теории дифференциальных уравнений, методов нелинейной динамики, прикладной математики, компьютерного и математического моделирования, численных методов. Для проведения численного эксперимента использованы апробированные методики.

Полученные результаты в определенной мере обобщают теоретические результаты, полученные ранее другими авторами.

9. Замечания по содержанию диссертации и ее оформлению. Недостатков, ставящих под сомнение справедливость какого-либо результата, в диссертации не обнаружено. Тем не менее, есть некоторые замечания по диссертационной работе Кузнецовой Оксаны Игоревны, как по оформлению, так и по существу работы.

1. Обширный подробный обзор литературы приведен в первой главе. Практически все ссылки приведены без указания имен авторов работ, что затрудняет чтение. Было бы логичнее у ссылок ставить фамилии первого автора работы.
2. Глава 1 излишне перегружена справочной информацией, приведены широко известные теоремы и определения. На мой взгляд, можно было ограничиться ссылками. Хотелось бы, чтобы автор пояснил целесообразность такого изложения и подхода. Часть теорем и определений снабжены ссылками, а часть приведены без ссылок, и из текста не ясно эти теоремы и определения сформулированы автором работы или нет. Например, Определение 1.10. [21] имеет ссылку, а определения 1.15, 1.14 приведены без ссылки и т.д., если это сформулировал автор работы, то об этом надо написать, к Теореме 1.1. эти же замечания можно применить и т. д. по тексту.
3. Для вычисления спектра показателей Ляпунова существуют эффективные методы, и подходы: алгоритм Бенеттина, якобиана, Кантца, Розенштейна, Сато, Вольфа. На странице 27, приведена таблица Таблица 1.6.1. (Знаки показателей Ляпунова и соответствующий им тип решений) при этом каким методом происходило вычисление не сказано. И только на странице 35, Таблица 1.7.1.1 автор пишет, что был применен алгоритм Бенеттина. Хотелось бы что бы автор пояснил, почему был выбран алгоритм Бенеттина? Известно, что все перечисленные методы дают приближенное значение. На мой взгляд, для

верификации результатов целесообразно проводить вычисление показателей Ляпунова, как старшего показателя, так и спектра показателей Ляпунова разными методами, что позволит обеспечить достоверность результатов.

4. На стр. 84 автор пишет «……численным интегрированием, например, методом Рунге-Кутта с адаптированным шагом, удается обнаружить только решение x = 0, y = 0, z = z(0) −2t …….» Хотелось бы, чтобы автор пояснил какого порядка был применен метод Рунге-Кутта, и чем обусловлен этот выбор.
5. Автором были зарегистрированы два программных комплекса: Программа для шифрования информации с использованием мегастабильной системы с 2-D полосой скрытых аттракторов. №2022666310 и Программа для шифрования информации с использованием мегастабильной системы с 4-D решеткой хаотических аттракторов №2022666309. К сожалению, в диссертации вообще нет их описания, их функционала, структуры, не приведены блок схема. Не описано, какие программные модули разработаны и реализованы. Хотя из диссертации ясно, что программный комплекс разработан, о чем говорят нетривиальные полученные результаты.
6. На мой взгляд сквозная нумерация рисунков и таблиц не целесообразна (например, Рис. 4.2.2.11.), и только затрудняет прочтение.

Заключение по диссертации. Указанные замечания, высказанные в отзыве, не снижают общего научного уровня работы. Диссертация в целом хорошо структурирована и оформлена, материал изложен ясно. По каждой главе и работе в целом сделаны четкие выводы. Чувствуется высокая квалификация автора и его научная зрелость.

Все выносимые на защиту научные положения сформулированы правильно и обоснованно. Многочисленные высокого качества графики и рисунки хорошо иллюстрируют основные результаты работы и защищаемые положения. Автор умеет дать простую физическую и математическую интерпретацию полученным результатам. Все основные научные результаты опубликованы как самим автором, так и в соавторстве с научным руководителем. Автореферат дает исчерпывающее представление о содержании диссертации.

Оценивая работу в целом, считаю, что диссертация является законченной научно-квалификационной работой, выполненной соискателем самостоятельно и на достаточно высоком уровне. Работа основана на большем объеме полученных численных и теоретических результатов, и вносит существенный вклад в теорию и практику математического моделирования и численных методов.

Таким образом, диссертационная работа Кузнецовой Оксаны Игоревны «Конструирование экстремально мультистабильных хаотических систем и их использование для преобразования информации», представленная на соискание ученой степени кандидата физико-математических наук соответствует специальности 1.2.2. Математическое моделирование, численные методы и комплексы программ имеет важное научное и прикладное значение, соответствует требованиям «Положения о присуждении ученых степеней», утвержденного постановлением Правительства Российской Федерации N 842 от 24.03.2013 года (в редакции от 07.07.2021 года), а ее автор, Кузнецова Оксана Игоревна, заслуживает присуждения ей ученой степени кандидата физико-математических наук по указанной специальности.

Официальный оппонент,
профессор кафедры «Прикладная математика и системный анализ», ФГБОУ ВО «Саратовский государственный технический университет имени Гагарина Ю.А.»,
доктор физико-математических наук (05.13.18 и 01.02.04), профессор

Крысько Антон Вадимович
21.02.2024

Адрес: 410054, г. Саратов, ул. Политехническая, д. 77
Служебный телефон:
+7 (845) 299-88-11,
+7 (845) 225-33-96,
anton.krysko@gmail.com
https://sstu.ru/.

Подпись д.ф.-м.н., профессора
Антона Вадимовича Крысько
заверяю
Ученый секретарь Ученого совета
СГТУ им. Гагарина Ю.А.

Потапова А. В.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Рязанский государственный университет имени С.А. Есенина»

Отзыв

официального оппонента на диссертацию

Кузнецовой Оксаны Игоревны

«Конструирование экстремально мультистабильных хаотических систем и их использование для преобразования информации»,

представленную на соискание ученой степени кандидата физико-математических наук по специальности 1.2.2. Математическое моделирование, численные методы и комплексы программ

Открытие нерегулярных колебаний в детерминированных динамических системах различной природы стало одной из крупнейших научных сенсаций второй половины XX века, вызвавшей громадный поток теоретических и экспериментальных работ. На протяжении многих лет усилия исследователей были направлены на выяснение причин и механизмов возникновения детерминированного хаоса, а также на решение проблем борьбы с хаосом и синхронизации колебаний хаотических систем. Однако со временем стало понятно, что благодаря своей высокой чувствительности к начальным условиям и значениям параметров, хаотические системы могут быть чрезвычайно полезными в приложениях, требующих использования систем высокой сложности. Одним из таких приложений является защита мультимедийных данных (текст, аудио, видео, изображения), передаваемых по каналам связи, от попыток несанкционированного доступа со стороны злоумышленника. Поэтому в последние годы многие исследователи сосредоточились на искусственном конструировании новых хаотических систем, которые допускают потенциальное использование для решения задач маскировки информации и обеспечения безопасной связи. Наиболее перспективными здесь оказались эксремально мультистабильные системы, то есть системы, обладающие бесконечным числом сосуществующих хаотических аттракторов, как самовозбуждающихся, так и скрытых.

В диссертационной работе О.И. Кузнецовой решается **актуальная** задача разработки новых методов конструирования мегастабильных систем, содержащих счетное множество сосуществующих хаотических аттракторов. Все предложенные в диссертации методы основываются на использовании автономных систем в форме Лурье. Такие системы, в частности, являются

математическими моделями систем автоматического управления, теория нелинейных колебаний которых детально изучена с разных точек зрения. Например, известны критерии существования у таких систем циклов первого и второго рода, найдено множество систем, обладающих хаотическими аттракторами. Наконец, именно для систем в форме Лурье впервые разработаны численно-аналитические методы поиска скрытых аттракторов, бассейны притяжения которых, в отличие от бассейнов притяжения самовозбуждающихся аттракторов, не пересекаются с малыми окрестностями состояний равновесия системы.

Одним из результатов диссертации, представленным в ее первой главе, является метод конструирования однопараметрических систем-хамелеонов, основанный на использовании упомянутого метода поиска скрытых аттракторов. Такие системы при различных значениях параметра демонстрируют либо самовозбуждающиеся, либо скрытые аттракторы. Среди приведенных в диссертации примеров сконструированных автором систем-хамелеонов наиболее интересным представляется пример системы, в которой при различных значениях параметра присутствуют как самовозбуждающиеся хаотические аттракторы, так и бесконечное число скрытых аттракторов-близнецов.

Весьма интересными представляются подходы к конструированию мегастабильных систем, предложенные автором во второй главе. Первый подход предлагает использовать для этой цели известные системы в форме Лурье, содержащие самовозбуждающиеся или скрытые аттракторы, например, известную систему Чуа. Путем замены нелинейности в такой системе на периодическую функцию система трансформируется в систему с угловой координатой, имеющую счетное число аттракторов-клонов.

Второй подход базируется на возможности путем неособого линейного преобразования трансформировать систему в форме Лурье в систему каскадного типа (jerk-систему). Такая система является смещаемой по переменным (*variable-boostable system*). После специально подобранной замены некоторых переменных в новой системе на периодические функции этих переменных удается сконструировать новую динамическую систему, которая содержит многомерную решетку хаотических аттракторов. При этом аттракторы в новой системе могут оказаться скрытыми, хотя в исходной системе аттрактор был самовозбуждающимся. Предложенный метод генерирования систем с многомерной решеткой хаотических аттракторов проиллюстрирован рядом примеров. Тот факт, что все аттракторы решетки являются хаотическими, подтверждается вычислением их показателей Ляпунова и фрактальной размерности по формуле Каплана-Йорке.

Разработанные во второй главе диссертации **новые** оригинальные методы позволяют на основе n-мерной системы в форме Лурье сконструировать мегастабильную систему, содержащую (n-1)-D решетку хаотических аттракторов. Однако синтез этих методов, как продемонстрировано в главе 3, предоставляет возможность конструирования n-мерной системы с n-D решеткой хаотических аттракторов. В этой главе

впервые построена система четвертого порядка с 4-D решеткой хаотических аттракторов.

В главе 3 также построена гладкая система третьего порядка без состояний равновесия и аналитическими решениями, на основе которой сконструирована новая система с разрывной нелинейностью, содержащая 2-D полосу скрытых аттракторов с размерностью Ляпунова "почти 3".

В заключительной главе диссертации продемонстрировано ее **прикладное значение**. Мегастабильные системы, сконструированные в третьей главе, применяются для организации безопасной связи в системах коммуникаций. При этом используется известная стратегия адаптивной синхронизации хаотических систем. Показано, что разработанная на основе этой стратегии схема маскировки эффективно защищает передаваемую информацию, что продемонстрировано на различных примерах информации, представленной в виде текста, цветных и черно-белых изображений, а также аудио и видеосигналов. На программы для ЭВМ, оформленные по результатам исследования, получены 2 свидетельства о государственной регистрации.

Все результаты диссертации опубликованы в профильных научных изданиях (в том числе, две статьи в журналах, индексируемых в базе Scopus, пять публикаций в изданиях, индексируемых в базе Scopus и рекомендованных ВАК), для совместных публикаций указан личный вклад автора диссертации.

По содержанию работы имеется несколько замечаний редакционного характера.

1. В диссертации на стр. 20 в теореме 1.2 в условии 1 используется уравнение прямой, заданной в виде $\sigma + \chi(0)\varphi = 0$. Не совсем понятно, что понимается под множителем φ в этом уравнении.
2. На странице 7 автореферата при описании содержания второй главы не вводится определения хаотических систем, обладающих 1-D, $(n-1)-$D решеткой аттракторов.
3. Опечатки в автореферате, мешающие восприятию информации:
   а) на странице 8 в теореме 2 рассматривается функция $\varphi(\sigma)$ для системы (1), но при этом в самой системе (1) эта функция не задействована;
   б) на странице 8 в примере 2 вводится функция $g(\sigma) = \varphi(\sigma) - k\sigma$ не понятно какую структуру имеет функция $\varphi(\sigma)$.
   в) ведены обозначения для систем (1) и (3), но при этом пропущено обозначение (2);
   г) в примере 5 на станице 10 определяются координаты вектора c, как c_j, где $j = 1, \dots, 4$, но при этом сам вектор-столбец содержит координаты c_0, c_1, c_2, c_3;
4. Для преобразования информации в работе предлагается использовать аттракторы систем дифференциальных уравнений. Частным случаем

аттрактора является периодическое решение такой системы. Возникает вопрос о преимуществе использования аттракторов вместо стандартных периодических функций или непериодических решений систем дифференциальных уравнений.

5. При вычислении показателей Ляпунова по алгоритму Бенеттина результат зависит от выбора интервала времени, по истечении которого происходит пересчет вектора начальных условий, и числа шагов вдоль траектории. Целесообразно было бы указать параметры расчета, использованные в диссертации.
6. Анонсируя прием, применяемый для клонирования аттрактора системы каскадного типа в (n-1)-D решетку, автор пишет "Для этого необходимо сначала оценить размах аттрактора по осям, затем заменить переменные в системе на периодические функции этих переменных, период которых будет не меньше, чем размах аттрактора по соответствующим осям". Возникает вопрос: для замены годятся любые функции из описанного класса, или необходим некоторый специальный их выбор? Например, из каких соображений выбрана замена в разделе 2.3.1 на стр. 61?
7. В тексте диссертации не указано, какие начальные условия использовались при синхронизации систем (4.2.1)-(4.2.2) на стр. 92 и (4.3.1)-(4.3.2) на стр. 102.

Вышеозначенные замечания носят частный характер, и не влияют на общую положительную оценку работы.

Диссертация является законченной научно-квалификационной работой, выполненной на высоком математическом уровне. В работе содержатся новые научные результаты, имеющие практическое значение для разработки востребованных в приложениях мегастабильных хаотических систем. Данные результаты могут быть использованы, например, в курсе «Основы информационной безопасности» РГУ имени С.А. Есенина, а также специалистами в области динамического хаоса, математической кибернетики и защиты информации. Полученные результаты достоверны, выводы обоснованы. Работа прошла апробацию на конференциях различного уровня. Основные результаты диссертации в достаточной степени опубликованы в научной печати. Автореферат диссертации правильно и полностью отражает её содержание.

Считаю, что диссертация Кузнецовой Оксаны Игоревны «Конструирование экстремально мультистабильных хаотических систем и их использование для преобразования информации», соответствует специальности 1.2.2. Математическое моделирование, численные методы и комплексы программ, имеет важное научное и прикладное значение, соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата наук «Положения о присуждении ученых степеней», утверждённого постановлением Правительства РФ №842

от 24.09.2013 (в редакции от 26.10.2023), а ее автор заслуживает присвоения ей ученой степени кандидата физико-математических наук по указанной специальности.

Официальный оппонент:
кандидат физико-математических наук,
доцент кафедры математики
федерального государственного
бюджетного образовательного
учреждения высшего образования
«Рязанский государственный
университет имени С.А. Есенина» Харламова Анастасия Олеговна

Заверяю отзыв доцента кафедры математики Харламовой А.О.

Ученый секретарь РГУ имени С.А. Есенина Е.В. Корчагина

21.02.2024 г.

Адрес: 390000, г. Рязань, ул. Свободы, д.46
Телефон: 4(912)-97-15-25
E-mail: a.harlamova@365.rsu.edu.ru