Отзыв официального оппонента

на диссертацию Алхуссайн Амани **«Вероятностный анализ стойкости защиты информации методом целочисленного расщепления символов»**, представленную к защите в диссертационном совете ПДС 0200.006 при федеральном государственном автономном образовательном учреждении высшего образования «Российский университет дружбы народов имени Патриса Лумумбы» на соискание ученой степени кандидата физико-математических наук по специальности 1.2.3 — Теоретическая информатика, кибернетика.

Актуальность темы диссертационной работы. Диссертационная работа Алхуссайн Амани посвящена исследованию новой теоретико-методологической и практической концепции расщепления как одной из систем защиты информации при её хранении и передаче. Защита информации при ее хранении и передаче по каналам связи, несомненно, является важной прикладной задачей.

Все современные подходы так или иначе используют методы модулярной арифметики, однако подход Алхуссайн Амани лежит в стороне от проторенных дорог. В его основе оригинальная идея – использование новой операции модулярной арифметики, названной в тексте «расщеплением». Это понятие, вообще говоря, не связано с защитой информации и может быть рассмотрено само по себе как интересная алгебраическая конструкция, возникшая, вероятно, как математическая модель эволюции популяций. Вопрос о том, как эта операция может использоваться для защиты передачи информации по каналу связи ранее исследован не был, а между тем использование нестандартных конструкций сулит занимательные преимущества при шифровании информации.

Характеристика содержания диссертационной работы. Диссертация состоит из Введения, четырех глав, Заключения и двух приложений. Во Введении сформулирована цель диссертации – разработка новой теоретико-методологической и практической концепции расщепления как одной из систем защиты информации при её хранении и передаче. Обоснована актуальность выбора темы, дан обзор литературы и сформулированы 4 положения, вынесенные на защиту.

Первая глава носит вводный характер. В ней вводятся основные подходы к защите информации, перечисляются их основные преимущества и недостатки. Представлен обзор работ о теоретической стойкости шифров по К. Шеннону, описаны работы по использованию метода гаммирования и шифра Вернама, указана их применимость, перечислены присущие им достоинства и недостатки.

Во второй главе введено понятие целочисленного расщепления целого числа по базе, в качестве которой может выступать другое целое число или несколько чисел. Фактически введено отображение, которое ставит в соответствие целому числу последовательность чисел, длина которой называется уровнем расщепления. Хотя операция целочисленного расщепления весьма

близка к моделям эволюции, используемым в генетическом алгоритме Дж. Холланда, ранее она не была описана и исследована. Доказанные во второй главе теоремы позволяют утверждать, что, при соблюдении указанных в тексте условий, целочисленное расщепление заданного числа может быть вычислено без деления на нуль и, обратно, по заданному расщеплению числа можно однозначно восстановить само число. Все это, разумеется, при известной базе. Доказанные в тексте теоремы выполнены в рамках модулярной арифметики, носят конструктивный характер и составляют 2-е положение, выносимое на защиту.

В третьей главе предложена схема применения целочисленного расщепления для защиты передачи текста. Ключевым моментом для дешифрации текста, зашифрованного при помощи целочисленного расщепления, является отыскание уровня расщепления. При шифровании каждый символ заменяется на последовательность символов, длина которой совпадает с уровнем расщепления. Поэтому длина зашифрованного текста делится на уровень расщепления, что позволяет без труда найти его в том случае, когда длина текста известна. По этой причине эффективное применение целочисленного расщепления для защиты текста возможно лишь в том случае, когда длина текста неизвестна. Именно такая ситуация возникает при непрерывной передаче информации, которая и рассматривается в третьей главе. Таким образом, предложен «новый метод защиты текстовой информации путем применения целочисленного расщепления, основанного на принципах модульной арифметики, позволяющий представить целое число по базе другого целого в виде последовательности k целых чисел, построенных по определенному правилу», что составляет 1-ое положение, выносимое на защиту.

В этой главе описана модель и алгоритмическая реализация системы защиты передачи текстовой информации, основанная на операции модулярного расщепления и приведены иллюстрации работы метода защиты информации на основе символьного расщепления (3-е положение, выносимое на защиту). Приведен вероятностный анализ математической модели символьного расщепления, в центре которого доказательство асимптотической стойкости предлагаемого метода защиты информации (4-е положение, выносимое на защиту).

В четвертой главе дается сравнение предложенного метода с известными схемами защиты, использующими гаммирование, со схемой Вернама, а также с указанными ранее традиционными методами защиты, применяющими операции модулярной арифметики, с целью выделения достоинств предлагаемого метода защиты. Здесь же приведены иллюстрации работы метода защиты информации на основе символьного расщепления.

В Заключении приводятся основные результаты, полученные в диссертационной работе.

Таким образом, все 4 положения, вынесенные на защиту, были обоснованы в тексте диссертации.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации, их достоверность. Диссертация содержит ряд оригинальных теорем, доказательства которых были своевременно опубликованы в

рецензируемых журналах, что вполне подтверждает обоснованность результатов. Достоверность результатов вычислений по предложенным алгоритмам подтверждается совпадением результатов вычислений в тестовых примерах.

Теоретическая и практическая значимость работы. Теоретическая ценность полученных в диссертации результатов заключается в исследовании свойств новой операции – целочисленного расщепления по базе – в модулярной арифметике, и исследовании стойкости разработанной на ее основе схемы защиты передачи информации. Практическая значимость выполненной работы обусловлена тем, что в ней построена и реализована в виде комплекса программ новая математическая схема защиты информации при её передаче, которую можно использовать как основу для создания действующей программной системы.

Недостатки работы. В диссертации имеется ряд недостатков.

1. Отсутствует сравнительный анализ скорости работы предложенного алгоритма шифрования и других известных алгоритмов.
2. Не приведены детали программной реализации предложенного алгоритма. Отсутствует ссылка на исходный код программы.
3. Не ясен смысл стрелок, изображенных на рисунке 3.4 на странице 64.
4. Кривые, приведенные на рисунках 3.7 – 3.12, для наглядности имело смысл представить в логарифмическом масштабе.
5. На странице 93 приведено доказательство, что вероятность восстановления исходного текста монотонно убывает с ростом уровня расщепления. Однако в тексте не объяснено, почему вероятности стремятся именно к нулю, а не к некоторой константе.

Указанные недостатки не снижают общее положительное впечатление о диссертационной работе.

Заключение. Диссертационное исследование представляет собой законченное и самостоятельное научно-квалификационное исследование, в котором решена актуальная задача разработки новой теоретико-методологической и практической концепции расщепления как одной из систем защиты информации.

Диссертационное исследование соответствует паспорту специальности 1.2.3. Теоретическая информатика, кибернетика, а именно п.15 (Модели данных и новые принципы их проектирования), п.25 (Методы высоконадежной обработки информации и обеспечения помехоустойчивости информационных коммуникаций для целей передачи, хранения и защиты информации), п.26 (Теория надежности и безопасности использования информационных технологий) и п.29 (Теоретические основы программирования, создания программных систем для новых информационных технологий).

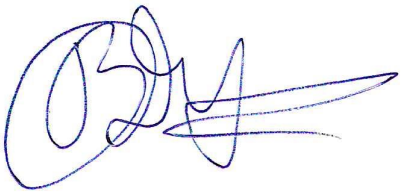
Полученные автором результаты достоверны, основные выводы и заключения обоснованы. Все положения, вынесенные на защиту, обоснованы в тексте диссертации. Автореферат

корректно отражает результаты диссертационного исследования. Основные научные результаты диссертации достаточно полно изложены в 24 статьях и докладах, в том числе 7 работ опубликовано в рецензируемых изданиях, рекомендованных перечнем ВАК, 6 работ опубликовано в изданиях, индексируемых в базе Scopus, получен 1 патент на изобретение.

На основании вышеизложенного считаю, что диссертационная работа «Вероятностный анализ стойкости защиты информации методом целочисленного расщепления символов» полностью соответствует требованиям п. 2.2 разделы II Положения о присуждении ученых степеней в ФГАУ ВО Российский университет дружбы народов, утвержденного Ученым советом РУДН, протокол № 12 от 23 сентября 2019 г., предъявляемых к диссертациям на соискание ученой степени кандидата физико-математических наук по специальности 1.2.3 — Теоретическая информатика, кибернетика, а ее автор — Алхуссайн Амани — степени кандидата физико-математических наук.

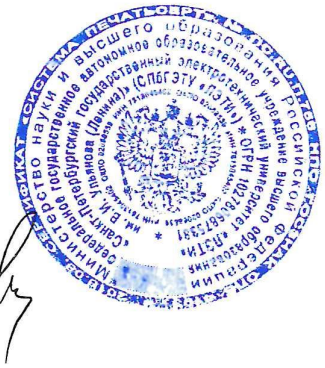
Официальный оппонент:
кандидат физико-математических наук (специальность 05.13.18. – «Математическое моделирование, численные методы и комплексы программ»),
доцент кафедры алгоритмической математики федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)»

Дужин Василий Сергеевич
« 5 » сентября 2023 г.



Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)»
197376, г. Санкт-Петербург, ул. Профессора Попова, д. 5, Россия
Тел.: +7 812 234-46-51
Электронная почта: vsduzhin@etu.ru

Подпись В.С. Дужина удостоверяю.



ПОДПИСЬ ЗАВЕРЯЮ
НАЧАЛЬНИК ОДС
Т.Л. РУСЯЕВА