ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора физико-математических наук Ильина Вячеслава Анатольевича на диссертацию Бабенко Михаила Григорьевича «Математические модели, методы и алгоритмы обработки зашифрованных данных в распределенных средах», представленную на соискание ученой степени доктора физико-математических наук по специальности 2.3.5 (05.13.11) «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей».

Диссертационное исследование М.Г. Бабенко было направлено на решение проблемы надежности систем хранения и обработки конфиденциальных данных в распределенных (облачных) гетерогенных вычислительных средах. Для обеспечения надежности облачных сервисов стандартно используется гомоморфное шифрование, что позволяет обрабатывать данные без предоставления к ним прозрачного (прямого) доступа к ним. Однако для применения метода гомоморфного шифрования в облачных средах серьезным ограничением является высокая вычислительная сложность современных прикладных алгоритмов. Актуальность диссертационного исследования М.Г. Бабенко высока в силу взрывного увеличения сложности и технического разнообразия алгоритмов, на которых строятся современные прикладные пакеты и сервисы для исполнения в распределенных средах разных архитектур и типов. Отметим, что (практически) все прикладные решения, используемые в практике распределенных сред, основаны на парадигме облачных вычислений, которая появилась еще в середине 00-х годов. Все это определяет высокую степень стартовых неопределенностей для создания системы надежности хранения и обработки конфиденциальных данных в таких вычислительных средах.

Научная новизна и теоретическая значимость полученных в ходе диссертационного исследования М.Г. Бабенко результатов связаны с многоуровневостью системы обработки данных, разработанной в рамках мультиоблачного метода обработки данных под управлением адаптивной распределенной службы хранения, основанной на избыточной системе остаточных классов с возможностью параллельной обработки данных. Отметим следующие два базовых оригинальных результата, полученные в ходе выполнения диссертационной работы:

- доказана теорема об условиях отсутствия критических ядер, которая позволила получить эффективные позиционные характеристики чисел;
- решена проблема аппроксимации функции определения знака числа и интерполяции функции ранга числа.

Научная значимость полученных результатов подтверждается их цитированием в международных наукометрических системах: почти 1200 ссылок в Google Scholar и более 500 ссылок в Scopus.

Практическая значимость полученных результатов связана с возможностью серьезного повышения эффективности разрабатываемых систем распределенной обработки конфиденциальных данных с использованием гомоморфных вычислений.

Такие системы были разработаны в рамках ряда научно-технических работ, выполненных при поддержке Министерства науки и высшего образования РФ, Российского научного фонда, Российского фонда фундаментальных исследований и Совета по грантам Президента Российской Федерации.

Представленные в диссертации результаты опубликованы в 89 статьях, из них 36 статей вышли в журналах, индексируемых в международных наукометрических базах WOS и Scopus. Остальные 53 работы опубликованы в сборниках трудов профильных российских и международных конференций. По результатам диссертации получено 26 Свидетельств о государственной регистрации программ для ЭВМ.

Обоснованность и достоверность научных положений и выводов диссертационной работы М.Г. Бабенко подтверждается корректным применением классических методов исследования, хорошо проверенных в обширной научной литературе, строгим математическим доказательством теоремы и научно обоснованным анализом эффективности разработанных моделей и алгоритмов. Все полученные результаты поучили хорошее согласование в проведенных численных экспериментах.

Диссертация включает в себя Введение, шесть Глав, Заключение, список Литературы из 374 наименований и два Приложения. Общий объем диссертации 415 страниц, в том числе 321 страница основного текста, включающего 42 рисунка и 35 таблиц.

Во Введении обоснована актуальность диссертационной работы, сформулированы цель исследования и поставленные задачи, научная новизна и практическая значимость полученных результатов. Даны формулировки положений, выносимых на защиту.

В первой Главе представлен обзор литературы в части угроз информационной безопасности в распределенных средах хранения и обработки данных. Акцент поставлен на проблемы, влияющие на эффективность вычислений и планирования облачных ресурсов, а также на возможные подходы к повышению эффективности гомоморфных вычислительных операций.

Во второй Главе представлена модель высокопроизводительной вычислительно стойкой процедуры доступа, обеспечивающая высокий уровень безопасности и надежности в нестационарной облачной среде. Высокая производительность достигается за счет разработанных алгоритмов кодирования/декодирования, основанных на переходе к представлению в обобщенной позиционной системе счисления, нейронной сети конечного кольца и их эффективной программной реализации.

Третья Глава посвящена разработке алгоритмов определения знака числа для гомоморфных вычислений над кольцом вычетов. Проведен анализ существующих методов сравнения, основанных на вычислении позиционных характеристик. Предложена модифицированная диагональная функция, которая за счет

монотонности обеспечивает взаимно-однозначное соответствие числа и его позиционной характеристики.

В четвертой Главе приведены результаты исследования проблемы определения знака числа и сравнения чисел с помощью интерполяционных полиномов Лагранжа. Обоснована степень интерполяционного многочлена функции определения знака и сравнения чисел. Предложен модифицированный нейросетевой метод определения знака числа.

Пятая Глава посвящена вопросам вычисления ранга чисел, представленных в RNS. Приведены результаты исследования формы ранга числа, возможности представления ранга с помощью алгебраических многочленов. Предложен и математически обоснован метод вычисления ранга числа, основанный на функции ядра Акушского, не содержащий критических ядер. Предложенный метод имеет выигрыш в быстродействии над существующими методами, на основании него разработаны алгоритмы вычисления ранга числа, представленного в RNS.

Шестая Глава обобщает результаты, представленные в 2-5-х главах, в виде конфигурируемой масштабируемой двухуровневой пороговой структуры доступа с обратным распространением ошибки. Предлагаемая структура позволяет использовать гомоморфные вычисления, используя параллельную обработку данных с сохранением безопасности. В предложенной структуре реализованы эффективные алгоритмы кодирования и декодирования данных. Предложенная двухуровневая пороговая структура прошла сравнительную проверку на восьми облачных хранилищах данных.

Диссертация написана ясным языком, по главам и по диссертации сделаны обоснованные выводы. Автореферат правильно отражает содержание диссертации и полученные результаты.

Диссертация не лишена недостатков, которые относятся к форме представления, отметим следующие из них:

1) в конце каждой из шести глав даются выводы, объем которых неоправданно велик (до нескольких страниц). Почему-то, в этих выводах диссертант решил еще раз изложить содержание соответствующих глав. Оптимально было бы дать компактные формулировки основных результатов, представленных в этих главах, со ссылками на публикации, в которых они были представлены. Добавим, что нигде в диссертации не указано, в каких публикациях представлены те или иные полученные результаты;
2) в диссертации рефреном проходит терминологическая пара *гомоморфное шифрование – облачные среды*. Почему именно выбраны *облачные среды* в диссертации не разъяснено. Конечно, можно предполагать, что такой выбор связан с тем, что подавляющее количество приложений реализуется в облачных средах. Однако, было бы правильно, если где-то в диссертации было отдельно обсуждено какие технологические аспекты облачных вычислений необходимо было учитывать при решении тех или иных поставленных задач.

Отметим, при этом, что эти замечания не снижают общую высокую оценку диссертации.

В результате приходим к следующему заключению.

Диссертация Бабенко Михаила Григорьевича «Математические модели, методы и алгоритмы обработки зашифрованных данных в распределенных средах» является самостоятельным научным трудом, выполненном на высоком научном уровне, и является законченной научной работой. Сформулированная в диссертации цель и поставленные задачи имеют высокую научную актуальность, полученные научные результаты имеют практическое значение для решения широкого спектра задач по распределенной обработке конфиденциальной информации в центрах хранения и обработки данных облачных сред общего назначения. Диссертация М.Г. Бабенко соответствует требованиям п. 9 Положения ВАК о присуждении ученых степеней, а ее содержание соответствует паспорту специальности 2.3.5 (05.13.11) «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей». Таким образом, соискатель Бабенко Михаил Григорьевич заслуживает присвоения ученой степени доктора технических наук по специальности 2.3.5 (05.13.11) «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей».

Официальный оппонент:
Главный научный сотрудник
КК НБИКС-природоподобных технологий
ФГБУ Национальный исследовательский
центр «Курчатовский институт» (г. Москва),
доктор физ.-мат. наук

В.А. Ильин
22 ноября 2022 г.