

ОТЗЫВ

официального оппонента

на диссертационную работу Ширяева Егора Михайловича
«Математическая модель, методы и алгоритмы эффективной реализации
искусственных нейронных сетей, сохраняющих конфиденциальность»,
представленную на соискание ученой степени кандидата физико-
математических наук по специальности 2.3.5 – Математическое и
программное обеспечение вычислительных систем, комплексов и
компьютерных сетей (физико-математические науки)

Актуальность темы. Диссертационная работа Ширяева Егора Михайловича посвящена разработке нейросетевых алгоритмов и методов, сохраняющих конфиденциальность. Для решения поставленной научной задачи диссертантом производится адаптация существующих моделей сверточных нейронных сетей с ограничениями, накладываемыми полностью гомоморфными шифрами.

Разработанные методы и алгоритмы для сверточных нейронных сетей позволяют производить конфиденциальную обработку данных на удаленных серверах. Диссертационная работа Ширяева Е.М. посвящена решению актуальной задачи исследования и разработки методов и алгоритмов искусственных нейронных сетей, сохраняющих конфиденциальность.

Научная новизна. Наиболее важными результатами, составляющими научную новизну диссертации, являются следующие:

- Методы и алгоритмы для проектирования слоев сверточной нейронной сети, сохраняющей конфиденциальность.
- Методы дистилляции и квантизации параметров для адаптации сверточных нейронных сетей к ограничениям гомоморфных шифров, позволяющие сократить потребление памяти и уменьшить время обработки данных.
- Методы полиномиальной аппроксимации популярных функций активации в сверточных сетях, позволяющие применять такие сети для обработки данных с использованием гомоморфных шифров.

Практическая значимость. В диссертации разработана математическая модель, методы и алгоритмы, позволяющие реализовывать модели сверточных нейронных сетей, сохраняющих конфиденциальность, для обработки входных данных в зашифрованном виде при решении задач классификации графических изображений.

Достоверность и обоснованность научных результатов. Все основные теоретические положения и выводы, сформулированные в диссертационной работе Ширяева Е.М., являются обоснованными. При получении основных теоретических положений автор использовал методы

математического анализа, теории чисел и численных методов. Все результаты подтверждаются проведенным сравнительным анализом разработанных методов и алгоритмов с общеизвестными. Математические выкладки выполнены с должной степенью строгости.

Рекомендации по использованию результатов диссертации сформулированы на основании совокупности полученных аналитических оценок, экспериментов и результатов моделирования, поэтому их обоснованность не вызывает сомнения.

Результаты диссертационного исследования прошли апробацию на конференциях и иных научных мероприятиях всероссийского и международного уровней, а также в 29 научных публикациях, среди которых 4 в рецензируемых журналах, рекомендованных ВАК, 8 публикаций, индексируемых в базах научных работ Scopus и Web of Science. Кроме того, получены 3 свидетельства о государственной регистрации программ для ЭВМ.

Содержание и структура диссертации. Диссертационная работа состоит из введения, 3-х глав, заключения и списка литературных источников. Общий объем диссертации 156 страниц, список используемой литературы содержит 186 источников.

В первой главе проведен анализ безопасности распределенных вычислительных систем и проведено выявление проблем конфиденциальности. Проведен обзор подходов на основе гомоморфных шифров, среди которых выбраны для исследования: TFHE, CKKS и BFV.

Во второй главе проведен анализ библиотек гомоморфного шифрования, по итогам которого для последующих исследований выбраны библиотеки TenSEAL и Concrete-ML. Изучены подходы к конфиденциальному матричному умножению. Сформулированы и доказаны утверждения о произведении зашифрованной матрицы на не зашифрованную, и об аппроксимации функций нейронными сетями. На основе полученных результатов предложена модификация гомоморфного умножения матрицы зашифрованных входов на открытую матрицу параметров, что позволило существенно сократить требования к памяти, понизить пространственную и вычислительную сложность. Проведено исследование методов квантизации и дистилляции для сверточных сетей, определены оптимальные параметры моделей. Показано, что схема BFV проигрывает схеме CKKS и в точности распознавания изображений, и по скорости обработки данных.

В третьей главе построены и формализованы математические модели сверточных нейронных сетей в открытом и конфиденциальном варианте с использованием аппроксимации полиномами классических функций активации, согласованных с ограничениями гомоморфных вычислений. Полученные модели образуют концептуальную и методическую основу для строгого анализа, сопоставления и верификации нейронных сетей сохраняющих конфиденциальность на базе схем CKKS и TFHE, включая

изучение баланса между точностью, устойчивостью и вычислительной сложностью. Экспериментально установлено, что при использовании приближенных функций активации модели на базе CKKS демонстрируют наивысшие показатели точности, тогда как конфигурации на TFHE нередко не достигают уровня точности выше 90% при заданных параметрах. Наилучший результат распознавания получен при использовании активации с обучаемыми коэффициентами в моделях CKKS. В совокупности это позволило построить модели нейронных сетей, сохраняющих конфиденциальность, оптимизированные под различные наборы данных и обеспечивающие требуемый баланс между точностью и скоростью обработки. Достигнутые результаты легли в основу программного комплекса для проектирования конфиденциальных сверточных нейронных сетей, который, в перспективе, расширяет область их применения за счет безопасной обработки чувствительных данных в общедоступных облачных и туманных вычислительных средах.

В заключении подведены итоги и обобщены результаты проведенных исследований.

Замечание по диссертации.

1. Для более ясного понимания ценности полученного результата не хватает обобщенной схемы ограничений, накладываемых гомоморфными шифрами и то, каким образом результаты, описанные в работе, позволяют их преодолеть.
 2. В автореферате не хватает подробного описания свойств и характеристик представляемого программного комплекса
 3. В работе указано, что все оценки использует эталонный набор данных рукописных цифр MNIST, однако нет явного описания процедур проведения экспериментов, включая алгоритм формирования проверочной выборки.
 4. Во второй главе представлено сравнение предложенных подходов с методом Halevi. Но при этом нет точной формулировки, какие изменения были в структуре нейронной сети, и проводилась ли экспериментальная оценка на базе тех же параметров набора MNIST.
 5. В работе представлена функция активации на основе полиномов с обучаемыми коэффициентами, но нет пояснения, за счет чего был получен высокий результат в точности по сравнению с полиномами наилучшего приближения Чебышева и почему этот подход не уступает существенно исходным, неаппроксимированным функциям активации.
 6. В работе имеются опечатки, не влияющие на общую научную значимость полученных результатов.
- Отмеченные недостатки не влияют на положительную оценку всех научных и практических результатов диссертации.

Заключение. Диссертация Ширяева Е.М., «Математическая модель, методы и алгоритмы эффективной реализации искусственных нейронных сетей, сохраняющих конфиденциальность» выполнена на актуальную тему, является законченной научно-квалификационной работой, обладает научной новизной и имеет практическую ценность. Автореферат отражает основные полученные научные результаты диссертационной работы.

Диссертационная работа отвечает требованиям ВАК РФ, предъявляемым к кандидатским диссертациям, её содержание соответствует паспорту специальности 2.3.5 – «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей», а ее автор, Ширяев Егор Михайлович, заслуживает присуждения ученой степени кандидата физико-математических наук по выше указанной специальности.

Официальный оппонент,
канд. физ.-мат. наук, доцент
доцент кафедры интеллектуальных
информационных технологий,
ФГБОУ ВО «МГУ им.
М.В. Ломоносова»

Петровский Михаил Игоревич

5.11.2025