ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.1.120.01,
созданного на базе
Федерального государственного бюджетного учреждения науки
Институт системного программирования им. В.П. Иванникова
Российской академии наук
Министерства науки и высшего образования РФ
по диссертации на соискание ученой степени кандидата наук

аттестационное дело № _____

решение диссертационного совета от 27 ноября 2025 года № 2025/26

О присуждении Ширяеву Егору Михайловичу, гражданину РФ, ученой степени кандидата физико-математических наук.

Диссертация «Математическая модель, методы и алгоритмы эффективной реализации искусственных нейронных сетей, сохраняющих конфиденциальность» по специальности 2.3.5 – «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей» принята к защите 19 сентября 2025 года (протокол № 2025/15) диссертационным советом 24.1.120.01, созданным на базе Федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ведомственная принадлежность: Министерство науки и высшего образования РФ; адрес: 109004, г. Москва, ул. А. Солженицына, дом 25), создан Приказом Минобрнауки России о советах по защите докторских и кандидатских диссертаций от 2 ноября 2012 г. № 714/нк.

Соискатель Ширяев Егор Михайлович, 16 января 1998 года рождения.

В 2022 году соискатель окончил Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет». В 2025 году соискатель окончил аспирантуру Федерального государственного автономного

образовательного учреждения высшего образования «Северо-Кавказский федеральный университет».

Работает старшим преподавателем в Федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет» на факультете математики и компьютерных наук имени профессора Н.И. Червякова, кафедре вычислительной математики и кибернетики (ведомственная принадлежность: Министерство науки и высшего образования РФ).

Диссертация выполнена в Федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет» на факультете математики и компьютерных наук имени профессора Н.И. Червякова, кафедре вычислительной математики и кибернетики (ведомственная принадлежность: Министерство науки и высшего образования РФ).

Научный руководитель – доктор физико-математических наук, доцент, Бабенко Михаил Григорьевич, Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет», факультет математики и компьютерных наук имени профессора Н.И. Червякова, заведующий кафедрой вычислительной математики и кибернетики.

Официальные оппоненты:

1. Петровский Михаил Игоревич, кандидат физико-математических наук, доцент, Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет им. М.В. Ломоносова», факультет вычислительной математики и кибернетики, доцент кафедры интеллектуальных информационных технологий,
2. Фёдоров Роман Константинович, доктор технических наук, доцент, Федеральное государственное бюджетное учреждение науки

Институт динамики систем и теории управления имени В.М. Матросова Сибирского отделения Российской академии наук, отделение информационных технологий и систем, заведующий лабораторией комплексных информационных систем,

дали положительные отзывы о диссертации.

Ведущая организация Федеральное государственное автономное образовательное учреждение высшего образования «Южный Федеральный Университет», г. Ростов-на-Дону в своем положительном заключении, подписанном Угольницким Геннадием Анатольевичем, доктором физико-математических наук, профессором, заведующий кафедрой прикладкой математики и программирования, института математики, механики и компьютерных наук имени И. И. Воровича, указала, что диссертационная работа содержит новые научные результаты, имеющие существенное значение для науки и практики.

Соискатель имеет 66 опубликованных работ, в том числе по теме диссертации опубликовано 29 работ, из них в рецензируемых научных изданиях опубликовано 4 работы.

Все изложенные в диссертационной работе результаты получены лично автором. Из результатов работ, выполненных коллективно, в диссертацию включены только полученные непосредственно автором. В опубликованных работах автором рассмотрены модели распределенных вычислений, а именно облачных и туманных вычислений, проанализированы и обозначены их уязвимости с точки зрения безопасности; проанализирована безопасность «Умных городов», уточнены требования к безопасности; исследованы методы машинного обучения и искусственных нейронных сетей; исследованы вычислительные характеристики гомоморфных шифров, а также методы повышения их эффективности; проведены исследования искусственных нейронных сетей, сохраняющих конфиденциальность, на базе гомоморфных шифров, разработан метод умножения матриц, сохраняющий

конфиденциальность входных данных, характеризующийся меньшим потреблением памяти и меньшей вычислительной сложностью, достигаемыми путем сокращения количества гомоморфных операций. Разработан комплекс программ для разработки и исследования сверточных нейронных сетей, сохраняющих конфиденциальность, с применением схем полностью гомоморфного шифрования.

Наиболее значимые работы по теме диссертации:

1. Shiriaev E. Comparative analysis of homomorphic encryption algorithms based on learning with errors / M. G. Babenko, E. I. Golimblevskaia, E. M. Shiriaev // Труды института системного программирования РАН. – 2020. – Т. 32, № 2. – С. 37-51.

2. Shiriaev E. A survey on multi-cloud storage security: threats and countermeasures / E. S. Bezuglova, E. M. Shiriaev, M. G. Babenko, [et al.] // Computational Technologies. – 2023. – Vol. 28, no. 1. – P. 72-80.

3. Shiriaev E. Analytical Review of Confidential Artificial Intelligence: Methods and Algorithms for Deployment in Cloud Computing / E. M. Shiriaev, A. S. Nazarov, N. N. Kucherov, & M. G. Babenko// Programming and Computer Software. – 2024. – Vol. 50, no. 4. – P. 304-314.

4. Shiriaev E. High-Speed Convolution Core Architecture for Privacy-Preserving Neural Networks / M. A. Lapina, E. M. Shiriaev, M. G. Babenko, & I. Istamov // Programming and Computer Software. – 2024. – Vol. 50, no. 6. – P. 417-424.

5. Shiriaev E. An efficient method for comparing numbers and determining the sign of a number in RNS for even ranges / A. Tchernykh, M. Babenko, E. Shiriaev, [et al.]. // Computation. – 2022. – Vol. 10, no. 2. – P. 17.

6. Shiriaev E. DT-RRNS: Routing protocol design for secure and reliable distributed smart sensors communication systems / A. Gladkov, E. Shiriaev, A. Tchernykh, [et al.] // Sensors. – 2023. – Vol. 23, no. 7. – P. 3738.

7. Shiriaev E. A Comparative Study of Secure Outsourced Matrix Multiplication Based on Homomorphic Encryption / M. Babenko, E. Golimblevskaia, A.

Tchernykh, E. Shiriaev, [et al.] // Big Data and Cognitive Computing. – 2023. – Vol. 7, no. 2. – P. 84.

8. Shiriaev E. Data Storage with Increased Survivability and Reliability Based on the Residue Number System / N. Kucherov, M. Babenko, E. Shiriaev, N. V. Hung //Advances in Systems Science and Applications. – 2024. – Vol. 24. – no. 02. – P. 166-186.

9. Shiriaev E. Reliablity and Security for Fog Computing Systems / E. Shiriaev, T. Ermakova, E. Bezuglova, [et al.] // Information. – 2024. – Vol. 15, no. 6. – P. 317.

Выбор официальных оппонентов и ведущей организации обосновывается их компетентностью и достижениями в данной отрасли науки, наличием публикаций в сфере исследований, соответствующей теме диссертации, и способностью определить научную и практическую ценность диссертации.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- разработана функция активации с обучаемыми коэффициентами, позволяющая повысить долю верных классификаций моделей искусственных нейронных сетей, сохраняющих конфиденциальность в среднем на 1.5% по сравнению с функциями, реализованными в других решениях с использованием гомоморфных шифров;
- модифицирован метод гомоморфного матричного умножения для проектирования искусственных нейронных сетей, сохраняющий конфиденциальность, уменьшая вычислительную сложность алгоритма с $O(n^4)$ до $O(n^2)$ в векторных операциях;
- разработан комплекс программ и алгоритмов для проектирования и исследования приближенных функций активации, позволяющий построить модель искусственной нейронной сети, сохраняющей конфиденциальность под конкретную задачу, повысить эффективность построенной модели, а также расширить область применения для решения прикладных задач, требующих сохранения конфиденциальности.

Теоретическая значимость исследования обоснована тем, что:

- доказаны теорема об гомоморфном умножении зашифрованной матрицы на открытую матрицу с уменьшением сложности векторных операций с $O(n^4)$ до $O(n^2)$ и теорема об аппроксимации функций, имеющих конечное число разрывов первого рода;
- изучены и модифицированы методы сжатия искусственных нейронных сетей, такие как дистилляция и квантизация, их применимость для проектирования искусственных нейронных сетей, сохраняющих конфиденциальность с учетом ограничений гомоморфных шифров, что позволило с точки зрения дистилляции сократить потребление памяти примерно в 1500 раз, уменьшение времени обработки данных в среднем в 30 раз, при уменьшении доли верных классификаций от 0.5% до 1%, уменьшить потребления памяти при применении квантизации более чем в 3.5 раза и уменьшение времени обработки данных на 20% по сравнению с другими решениями с использованием гомоморфных шифров;
- раскрыты ограничения гомоморфных шифров, накладываемые на искусственные нейронные сети, сохраняющие конфиденциальность;
- проведена модернизация существующей математической модели искусственной нейронной сети, сохраняющей конфиденциальность на базе различных гомоморфных схем с учетом ограничений гомоморфных шифров.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

- разработанная математическая модель искусственной нейронной сети, сохраняющей конфиденциальность с учетом ограничений гомоморфных шифров, может быть применена при разработке других моделей машинного обучения, сохраняющих конфиденциальность;

- полученный метод гомоморфного матричного умножения может быть применен в различных системах, сохраняющих конфиденциальность использующих обработку данных, представленных в табличном виде;
- разработанный комплекс программ и алгоритмов для проектирования и исследования приближенных функций активации позволяет проводить исследования и тестирование моделей доверительного искусственного интеллекта на базе гомоморфных шифров с учетом их ограничений.

Оценка достоверности результатов исследования выявила, что:

- эффективность разработанных методов и алгоритмов подтверждается результатами математического моделирования;
- представленные теоремы имеют строгое доказательство и подтверждены в экспериментальном исследовании;
- установлена научная новизна, которая подтверждена сравнительным анализом на базе экспериментального исследования полученных результатов с существующими аналогами.

Личный вклад соискателя состоит в разработке метода умножения матриц, сохраняющего конфиденциальность входных данных, характеризующегося меньшим потреблением памяти и меньшей вычислительной сложностью, достигаемыми путем сокращения количества гомоморфных операций, в создании комплекса программ для разработки и исследования сверточных нейронных сетей, сохраняющих конфиденциальность, с применением схем ПГШ, в участии в проведенных научных экспериментах, в апробации результатов исследования, в формулировании и доказательстве теорем и интерпретации экспериментальных данных.

В ходе защиты диссертации были высказаны следующие критические замечания:

1. В работе нет сценариев атак на нейронные сети, сохраняющие конфиденциальность, и методов противодействия им.

2. В качестве критериев [эффективности] искусственных нейронных сетей, сохраняющих конфиденциальность, целесообразно было бы так же рассмотреть вычислительную безопасность.

3. В работе предложены методы проектирования нейронных сетей, сохраняющих конфиденциальность, однако, не исследован вопрос о применимости этих методов при проектировании больших языковых моделей, сохраняющих конфиденциальность. Сохраняется ли эффективность предложенных подходов при переходе к реальным, более масштабным задачам?

4. Часть представленных графиков (например, рис. 3.7-3.10) сложна для восприятия из-за перегруженности данными. Для улучшения наглядности целесообразно было бы вынести детализированные данные в дополнительные таблицы, размещённые в приложениях.

5. 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.

6. 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.

7. В работе представлена функция активации на основе полиномов с обучаемыми коэффициентами, но нет пояснения, за счет чего был получен результат в точности по сравнению с полиномами наилучшего приближения Чебышева и почему этот подход не уступает существенно исходным, не аппроксимированным функциям активации.

Соискатель Ширяев Егор Михайлович согласился с замечаниями, ответил на задаваемые ему в ходе заседания вопросы.

На заседании 27 ноября 2025 диссертационный совет принял следующее решение: за решение научной задачи, имеющей значение для развития методов разработки математического и программного обеспечения вычислительных

систем, комплексов и компьютерных сетей, присудить Ширяеву Е.М. ученую степень кандидата физико-математических наук по специальности 2.3.5 – «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей».

При проведении тайного голосования диссертационный совет в количестве 12 человек, из них 3 доктора наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 15 человек, входящих в состав совета, проголосовали: за – 12, против – 0, недействительных бюллетеней – 0.

Заместитель председателя диссертационного совета,
доктор физико-математических наук Белеванцев А. А.

Ученый секретарь диссертационного совета,
кандидат физико-математических наук Турдаков Д. Ю.

27 ноября 2025