АННОТАЦИЯ

диссертационной работы Бакировой Гульназ Сайлауовны «Разработка моделей и методов с применением федеративного машинного обучения», представленной на соискание степени доктора философии (PhD) по ОП: 8D06102 – «Компьютерная и Программная Инженерия»

Актуальность темы исследования. Образовательная среда переходит в эпоху глобальной цифровизации, поэтому в этой области идет устойчивое развитие инструментов анализа распределенных и конфиденциальных данных, в связи с этим идет активный рост научного и практического интереса к методам федеративного машинного обучения. Ужесточение требований к защите конфиденциальных данных при сборе больших обьемов информации ограничивает возможности централизованной обработки. Сохранение конфиденциальности данных, отражающие учебную активность, поведенческие характеристики и психоэмоциональное состояние студентов, собираемых в современных образовательных системах, являются особенно важной задачей.

Потенциал федеративного обучения при работе с распределенными данными подтверждаются результатами зарубежных исследований. Точность моделей, которая сопоставляется с централизованным обучением, обеспечивается базовым механизмом федеративной агрегации. Нестабильная сходимость и снижение качества глобальной модели характеризуется в условиях несбалансированных и гетерогенных данных, что отражено в исследованиях. В научной литературе предложены усовершенствованные схемы федеративного обучения для преодоления упомянутых ограничений. Подходы, основанные на серверной оптимизации, направлены на повышение устойчивости и ускорение сходимости процесса обучения и методы, использующие проксимальную регуляризацию, позволяют ограничить расхождение локальных моделей и стабилизировать обучение в условиях гетерогенности данных. Возможность достижения высокой точности без передачи исходных данных между клиентами отражены в дополнительных исследованиях в области горизонтального федеративного обучения.

Вопросам защиты персональных данных уделяется особое внимание в научной литературе. Федеративное обучение является одним из наиболее перспективных методов для образовательных и социальных систем, при этом позволяя комбинировать аналитическую эффективность и соблюдение требований информационной безопасности.

Анализ исследований показал, что в области федеративного обучения большинство работ преимущественно ориентировано на дифференцируемые модели и нейросетевые архитектуры. Применение федеративных подходов к

недифференцируемым алгоритмам машинного обучения, в частности к ансамблевым моделям типа Random Forest. Разработка методов федеративной агрегации, основанных на статистических представлениях локальных моделей, остаются недостаточно изученными. Практическая реализация для анализа психоэмоционального состояния студентов, основанных на реальных гетерогенных данных образовательных учреждений, имеет ограниченное количество упоминаний в научной литературе.

Задача разработки и практическая реализация методов федеративного машинного обучения для недифференцируемых моделей для анализа распределенных конфиденциальных данных студентов является актуальной. Решением данной задачи является обеспечение высокого уровня защиты персональной информации, повышение устойчивости и качества глобальных моделей в условиях гетерогенных данных, развитие цифровой трансформации образовательной среды и внедрение интеллектуальных аналитических систем при строгом соблюдении требований информационной безопасности.

Целью диссертационного исследования является разработка моделей и методов федеративного машинного обучения и их практическая реализация для анализа распределенных конфиденциальных данных при обеспечении требований защиты персональной информации и устойчивости обучения в условиях гетерогенных данных.

Задачи исследования:

1. Реализовать систему сбора, предварительной обработки и согласования признакового пространства распределенных данных студентов.
2. Разработать методы федеративной агрегации для недифферецируемых ансамблевых моделей на основе статистических представлений локальных моделей.
3. Разработать архитектуру федеративного машинного обучения для анализа распределенных конфиденциальных данных с локальной обработкой информации без передачи исходных данных на сервер.
4. Провести экспериментальную оценку эффективности, устойчивости и сходимости разработанных моделей в условиях гетерогенных non-IID данных.

Обьектом исследования является образовательная среда, в которой формируются и используются распределенные конфиденциальные данные студентов для анализа и прогнозирования их психоэмоционального состояния с применением методов федеративного машинного обучения.

Предметом исследования являются методы и алгоритмы федеративного машинного обучения, предназначенные для анализа и прогнозирования психоэмоционального состояния студентов на распределенных и гетерогенных данных при обеспечении конфиденциальности информации.

Методы исследования:

1. Методы системного анализа и проектирования при разработке архитектуры федеративной обучающей системы и веб-платформы.

2. Методы предварительной обработки и преобразования данных: очистка, валидация, обработка аномалий, кодирование признаков и преобразование временных характеристик.

3. Методы ансамблевого и федеративного машинного обучения, основанные на агрегировании статистических представлений локальных моделей.

4. Методы математической статистики и вычислительного эксперимента для оценки качества, устойчивости и сходимости глобальной модели.

Научная новизна исследования заключается в том, что:

1. Разработан и реализован подход к модификации и расширению федеративного машинного обучения для недифференцируемой ансамблевой модели Random Forest Regression на основе замены классической агрегации параметров модели на агрегирование статистических представлений локальных моделей, а именно векторов важностей признаков, что обеспечивает устойчивость процесса обучения в условиях гетерогенных non-IID распределенных данных.

2. Разработаны модели и методы федеративного машинного обучения для анализа распределенных конфиденциальных данных, обеспечивающие локальную обработку информации, устойчивость глобальной модели и сохранение конфиденциальности данных при работе в реальных условиях распределенной образовательной среды.

3. Предложена архитектура федеративного обучения, обеспечивающая формирование глобальной модели на основе локальных обновлений без передачи исходных данных клиентов на сервер, что позволяет соблюдать требования конфиденциальности и защиты персональной информации.

Теоретическая значимость исследования: изучение вопросов распределенного анализа данных на основе теории машинного обучения. Мы применили FedAvg, FedOpt, FedProx в качестве алгоритмов федеративного обучения на децентрализованных наборах данных и Random Forest Regression в качестве ансамблевой модели машинного обучения для предсказаний, а также классические методы статистического анализа, и предварительная обработка данных являются ключевыми методами, которые применялись в исследовании. Работа шла по стандартным шагам машинного обучения от подготовки данных до оценки результатов. Реализовано было на языке Python с использованием библиотек sckit-learn, pandas, NumPy matpotlib инструменты, которые упростили проведение экспериментов и сделали визуализацию наглядной.

Практическая значимость исследования: исследование направлено на развитие и расширение методов федеративного машинного обучения за счет разработки и реализации подхода, адаптированного для недифференцируемой ансамблевой модели Random Forest Regression. В работе предложена замена классической агрегации параметров модели на агрегирование статистических представлений локальных моделей в виде

векторов важностей признаков, что обеспечивает устойчивость процесса обучения в условиях гетерогенных (non-IID) распределенных данных.

Разработана архитектура федеративного обучения, позволяющая формировать глобальную модель на основе локальных обновлений без передачи исходных данных клиентов на сервер, что обеспечивает соблюдение требований конфиденциальности и защиты персональной информации.

Основные положения, выносимые на защиту:

- Разработана и реализована архитектура федеративного машинного обучения для анализа распределенных и конфиденциальных данных студентов, обеспечивающая обучение локальных моделей без передачи исходной информации на сервер и соответствующая требованиям защиты персональных данных.
- Выполнена адаптация алгоритмов федеративного обучения FedAvg, FedOpt, FedProx к недифференцируемой модели Random Forest Regression путем замены агрегации весов на агрегацию статистических представлений – векторов важностей признаков, что позволило обеспечить устойчивость обучения при гетерогенных (non-IID) данных.
- Проведен сравнительный анализ эффективности алгоритмов федеративной агрегации на реальных распределенных данных, отражающих психоэмоциональное состояние студентов, показавший, что FedProx обеспечивает наибольшую стабильность при non-IID распределениях, а FedOpt ускоряет сходимость глобальной модели.

В ходе диссертационного исследования были получены следующие научные результаты, которые определяют его научную новизну:

- Реализована система сбора, предварительной обработки и согласования признакового пространства распределенных данных студентов.
- Разработаны методы федеративной агрегации для недифференцируемых ансамблевых модели на основе статистических представлений локальных моделей.
- Разработана архитектура федеративного машинного обучения для анализа распределенных конфиденциальных данных с локальной обработкой информации без передачи исходных данных на сервер.
- Проведена экспериментальная оценка эффективности, устойчивости и сходимости разработанных моделей в гетерогенных (non-IID) данных.

Основные результаты работы были представлены и обсуждены на семинарах кафедры «Компьютерная инженерия» АО МУИТ (2022–2026 гг.), университете Tenaga Nasional Малайзия (2024–2026 гг.). По теме диссертации опубликованы 8 публикаций: 1 статья - в изданиях, индексируемых в базе Web of Science и Scopus; 4 статьи - в журналах, рецензируемом Комитетом по обеспечению качества в сфере науки и высшего образования МНВО РК, 2 статьи - в Международном Журнале Информационных и Коммуникационных технологий, Спецвыпуск. 1 статья - в Вестнике КазНТУ, Computing & Engineering.

1. Бакирова Г. С., Бектемысова Г. У., Нор'ашикин Бинти Али. Federated Machine Learning for Monitoring Student Mental Health in Kazakhstan. International Journal of Advanced Computer Science and Applications. E-ISSN: 2156-5570 P-ISSN: 2158-107X. Volume 16 Issue 10. 2025. стр. 212–220. CiteScore - 2. Наивысший процентиль–47%. Квартиль - Q3. DOI: https://doi.org/doi:10.14569/IJACSA.2025.0161022

2. Бакирова Г. С., Бектемысова Г. У. Анализ алгоритмов федеративного обучения. Вестник КазАТК, Вестник Казахской Академии Транспорта и Коммуникации им. М.Тынышпаева, ISSN 2790-5802, - Том 131 №2, -2024г. С.: 297-304 DOI: https://doi.org/10.52167/1609-1817-2024-131-2-297-304.

3. Бакирова Г. С., Бектемысова Г. У. Сравнительный анализ алгоритмов объединенного машинного обучения. Scientific Journal of Astana IT University. ISSN (P): 2707-9031 ISSN (E): 2707-904X, Volume 17, March 2024, P.:57-67. DOI: https://doi.org/doi:10.37943/17BVCN7579

4. Бакирова Г. С., Бектемысова Г. У., Ермуханбетова Ш., Шынторе Г. А., Умуткулов Д. Б., Мангышева Ж. С. Анализ актуальности и перспективы применения федеративного обучения. Вестник НИА РК, №2(92), 2024, С.: 56–65 DOI: https://doi.org/10.52167/1609-1817-2024-131-2-297-304

5. Бектемысова Г. У., Ахмер Е. Ж., Сабденов А., Бакирова Г. С., Разработка модели для классификации документа (на примере паспортов). Вестник КазАТК, Вестник Казахской Академии Транспорта и Коммуникации им. М.Тынышпаева, ISSN 2790–5802, - Том 136 №1, -2025г. -С. 393–401 DOI: https://doi.org/10.52167/1609-1817-2025-136-1-393-401

6. Бакирова Г. С., Бектемысова Г. У. Обзор о распределенном и федеративном машинном обучении для моделей больших данных. Международный Журнал Информационных и Коммуникационных технологий, Спецвыпуск 2023. ISSN 2708–2032 (print) ISSN 2708–2040 (online), Спецвыпуск 2023. стр. 89-96. https://ydf.iitu.edu.kz/files/26-37-PB.pdf

7. Бакирова Г.С., Бектемысова Г.У. Analysis of probable threats in the use of federated learning and their protection methods . Международный Журнал Информационных и Коммуникационных технологий, Спецвыпуск 2024. ISSN 2708–2032 (print) ISSN 2708–2040 (online), стр. 64-69. https://ydf.iitu.edu.kz/files/%D0%A1%D0%BF%D0%B5%D1%86%D0%B2%D1%8B%D0%BF%D1%83%D1%81%D0%BAYDF2024.pdf

8. Бакирова Г.С., Бектемысова Г.У, Шайкемелов Г. Applications in federated machine learning. Вестник КазНТУ, Computing & Engineering, Том 1 №3, - 30.09. 2023г. С.: 25-28, DOI: https://doi.org/10.51301/ce.2023.i3.05

9. Бакирова Г. С., Бектемысова Г. У. Свидетельство на право охраны программы для ЭВМ № 62530 Республики Казахстан. Система анализа для выявления признаков психоэмоционального выгорания студентов с использованием методов федеративного обучения. заявка 26.09.2025; публикация 30.09.2025.

Результаты. В процессе работы над исследованием изучены актуальные подходы федеративного машинного обучения, уделено особое внимание алгоритмам FedAvg, FedOpt, FedProx, учитывая вопросы устойчивости и

сходимости моделей при гетерогенных (non-IID) распределенных данных. Анализ научных публикаций показал, что федеративное обучение является перспективным инструментом для обработки конфиденциальной информации, однако его применение к недифференцируемым моделям остается недостаточно изученным.

Архитектура федеративного обучения для анализа распределенных данных, которая отражает психоэмоциональное состояние студентов, была разработана и реализована в рамках исследования. Рассмотрим более подробно архитектуру, которая состоит из локальных моделей, обучающиеся на стороне клиентов, с применением Random Forest Regression, которая обеспечивает высокую точность прогнозирования и устойчивость к шуму данных и глобальных моделей, обучающиеся на стороне сервера, что означает серверная часть выполняет агрегацию без доступа к исходным данным.

Сбор данных осуществлялся через веб-платформу, которую отправляли всем клиентам, в течение 2 месяцев с 1 сентября по 30 октября. Информационная база включала данные о питании, физической активности, сна и отдыха, психоэмоционального состояния, а также временные и идентификационные атрибуты. Данные собирались от нескольких учебных заведений, что позволило смоделировать условия реальной гетерогенности. Предварительная подготовка данных включала очистку некорректных записей, фильтрацию выбросов, преобразование временных признаков в числовой формат и кодирование категориального идентификатора student_id методом One-Hot Encoding. Мы провели проверку согласованности признакового пространства между локальными наборами данных, которые необходимы для корректной федеративной агрегации.

Алгоритмы федеративного обучения FedAvg, FedOpt, FedProx были адаптированы к недифференцируемой модели Random Forest Regression путем замены агрегации весов модели на агрегацию статистических представлений, т.е. векторов важностей признаков, что позволяет сохранить математическую логику федеративного обучения и обеспечивает устойчивость глобальной модели.

Сравнительный анализ алгоритмов федеративной агрегации провели по регрессионным и классификационным метрикам. В результате показал, что обеспечивает базовый уровень качества и будет использоваться как эталон, при этом его сходимость ухудшается при выраженной гетерогенности данных, в свою очередь демонстрирует ускоренную сходимость за счет применения серверной оптимизации, но обеспечил наиболее стабильное обучение и минимальные колебания качества. Динамика точности и функции потерь глобальных моделей была проанализирована по раундам федеративного обучения. Все алгоритмы показывают устойчивый рост точности и монотонное снижение Centralized Loss, что демонстрирует корректную сходимость и отсутствие переобучения. Следовательно, цели и задачи диссертационного исследования были достигнуты и полученные результаты подтверждают эффективность применения адаптированных методов федеративного обучения для анализа психоэмоционального состояния

студентов на распределенных конфиденциальных данных и обладают как научной, так и практической значимостью.

В первой главе рассмотрены основные подходы к федеративному обучению и обоснован выбор синхронного горизонтального Cross-Silo федеративного обучения. Использование единого пространство признаков позволило корректно агрегировать локальные результаты без передачи исходных данных. Архитектура обеспечила устойчивую сходимость глобальной модели, сохранение конфиденциальности и эффективность обучения в условиях гетерогенных данных, что подтверждает применимость предложенного решения в образовательной среде.

Во второй главе рассмотрены алгоритмы и архитектуры федеративного обучения, показано, что базовые методы FedAvg и FedSGD, обеспечивают конфиденциальность данных, но теряют устойчивость при non-IID распределениях. В свою очередь FedOpt FedProx повышают стабильность и ускоряют сходимость за счет проксимальной регуляризации и серверной оптимизации. В результате выбор FedAvg, FedOpt и FedProx является наиболее сбалансированным решением для анализа распределенных конфиденциальных данных.

Третья глава посвящена описанию веб-платформы сбора данных о питании, физической активности, сне и психоэмоциональном состоянии студентов, а также использованию опросника Maslach Burnout Inventory (MBI) и его адаптации для исследования. Рассмотрены методы обработки non-IID данных, обеспечения конфиденциальности и математические модели анализа психоэмоционального состояния. Описаны алгоритмы прогнозирования выгорания, принципы кодирования данных и автоматизированного анализа факторов, влияющих на уровень выгорания. Также обозначены ограничения исследования и перспективы дальнейшего развития предложенного подхода.

В четвертой главе проведен сравнительный анализ алгоритмов федеративного обучения FedAvg, FedOpt и FedProx для прогнозирования психоэмоционального выгорания студентов. Показано, что FedAvg ограниченно эффективен при non-IID данных, тогда как FedOpt обеспечивает более быструю и устойчивую сходимость за счет серверной оптимизации, а FedProx повышает стабильность обучения посредством проксимальной регуляризации, но с более медленной сходимостью. В результате FedOpt выбран в качестве основного алгоритма, FedProx как устойчивое решение при высокой гетерогенности данных, а FedAvg используется в качестве базового эталона.

Пятая глава посвящена описанию веб-платформы для сбора данных о питании, физической активности, сне и психоэмоциональном выгорании студентов, а также анализу структуры и адаптации опросника Maslach Burnout Inventory (MBI). Рассмотрены методы обработки non-IID данных, обеспечения конфиденциальности и алгоритмы прогнозирования уровня выгорания. Описаны подходы к кодированию данных, автоматизированному анализу и выявлению факторов, влияющих на психоэмоциональное состояние, а также обозначены ограничения исследования и направления дальнейшего развития.

В главе «Заключение» показано, как реализована и исследована федеративная архитектура обучения для анализа психоэмоционального состояния студентов на распределенных конфиденциальных данных. Рассмотрено, что адаптация алгоритмов FedAvg, FedOpt и FedProx к недифференцируемой модели Random Forest Regression обеспечивает устойчивую сходимость глобальной модели в условиях non-IID данных. Полученные результаты подтверждают практическую применимость федеративного обучения в образовательной среде при сохранении конфиденциальности информации.

Личный вклад автора. Все основные результаты, описанные в диссертации, выполнены и собраны автором. Кроме того, основные результаты исследований, анализы, модели, программы созданы автором, выводы сделаны на основе результатов, полученных от работы и исследования PhD докторанта.

Структура и обьем работы. Диссертация включает введение, 5 основных глав, заключения и списка использованных источников. Полный обьем диссертации составляет 144 страницы, включая 46 иллюстраций и 14 таблиц. Список литературы содержит 105 наименований.