БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра биомедицинской информатики

Аннотация к дипломной работе

«Разработка методов федеративного обучения для агрегации нейросетевых моделей в условиях приватности медицинских изображений»

Зеленковский Виктор Петрович

Научный руководитель – кандидат технических наук, доцент, доцент кафедры биомедицинской информатики ФПМИ Ковалёв В. А.

Минск, 2024

Реферат

Дипломная работа, 40 страниц, 24 рисунка, 11 формул, 7 источников

Ключевые слова: ФЕДЕРАТИВНОЕ ОБУЧЕНИЕ, АГРЕГАЦИЯ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ, ГЛУБОКИЕ НЕЙРОННЫЕ СЕТИ, КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ, МЕДИЦИНСКИЕ ИЗОБРАЖЕНИЯ.

Объектом исследования является агрегация нейросетевых моделей.

Предметом исследования являются методы федеративного обучения.

Целью работы является исследование существующих и разработка новых методов федеративного обучения, позволяющих сохранить конфиденциальность данных при агрегации глубоких нейросетевых моделей.

В ходе работы были изучены существующие методы федеративного обучения и выявлены их недостатки, не позволяющие агрегировать модели машинного обучения в условиях конфиденциальности медицинских изображений. Разработаны 2 подхода федеративного обучения, позволяющие агрегировать нейросетевые модели различной архитектуры с сохранением приватности обучающего набора данных.

Полученную в результате работы методы можно использовать для агрегации нейросетевых моделей в условиях конфиденциальности обучающего набора данных, в том числе медицинских изображений.

Abstract

Diploma thesis, 40 pages, 24 figures, 11 formulas, 7 sources.

Keywords: FEDERATED LEARNING, AGGREGATION OF MACHINE LEARNING MODELS, DEEP NEURAL NETWORKS, DATA PRIVACY, MEDICAL IMAGES.

The object of research is an aggregation of neural network models.

The subject of study is methods of federated learning.

The aim of this work is to research of existing and develop of new methods of federated learning, allowing to preserve data confidentiality in the aggregation of deep neural network models.

In the course of the work, the existing methods of federated learning were studied and their disadvantages were identified, which do not allow aggregating machine learning models in conditions of confidentiality of medical images. 2 approaches of federated learning have been developed that allow aggregating neural network models of various architectures while maintaining the privacy of the training dataset.

The resulting methods can be used to aggregate neural network models in conditions of confidentiality of the training data set, including medical images.