ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к проекту предварительного национального стандарта «Искусственный интеллект. Техническая структура федеративной системы машинного обучения» (ITU-T F.748.13 (2021), Technical framework for a shared machine learning system, MOD)

1. Основание для разработки проекта стандарта

Проект предварительного национального стандарта ПНСТ «Искусственный интеллект. Техническая структура федеративной системы машинного обучения» разработан в соответствии с Государственным контрактом (Заказчик – Росстандарт) и Программой национальной стандартизации Российской Федерации на 2023 год. Шифр темы: 1.11.164–1.259.23.

2. Краткая характеристика объекта и аспекта стандартизации

Объектом стандартизации являются роли, технические требования и требования по безопасности для федеративной системы машинного обучения, а также описывает технические архитектуры, функциональные компоненты и процедуры обработки федеративной системы машинного обучения при централизованном и децентрализованном режимах работы.

3. Технико-экономическое, социальное или иное обоснование целесообразности разработки стандарта на национальном уровне

В федеративных системах машинного обучения (SML-системах) несколько участников совместно используют зашифрованные данные и/или обмениваются параметрами моделей с целью обеспечить безопасность данных и защиту персональных данных. Чтобы обеспечить наиболее эффективное использование данных, зашифрованные данные каждой стороны и/или предоставленные ею параметры моделей собираются и используются для обучения модели федеративного машинного обучения. Модели федеративного машинного обучения продолжают обучаться в интересах само-оптимизации, а участники или иные лица, авторизованные на доступ к модели, могут вводить

информацию для получения результатов или прогнозов на основе совместно используемых значений. Федеративные системы машинного обучения могут, например, применяться (не ограничиваясь ими) в мультимедийных и игровых приложениях (media applications).

Федеративные системы машинного обучения позволяют ряду сторон использовать для обучения моделей систем машинного обучения данные, имеющиеся в их распоряжении, не раскрывая при этом друг другу самих данных. Данная особенность полезна в ситуациях, когда требуется обеспечить защиту содержащейся в данных конфиденциальной информации и особенно персональных данных.

4. Сведения о соответствии проекта предварительного национального стандарта техническим регламентам Евразийского экономического союза, федеральным законам, техническим регламентам и иным нормативным правовым актам Российской Федерации, которые содержат требования к объекту и/или аспекту стандартизации

Настоящий предварительный стандарт разрабатывается в соответствии с требованиями Федерального закона от 29.06.2015 № 162 «О стандартизации в Российской Федерации» и соответствует техническим регламентам Евразийского экономического союза и законодательству Российской Федерации.

5. Сведения о соответствии проекта предварительного национального стандарта международному стандарту, региональному стандарту, региональному своду правил, стандарту иностранного государства и своду правил иностранного государства, иному документу по стандартизации иностранного государства и о форме применения данного документа как основы для разработки проекта предварительного национального стандарта Российской Федерации, а в случае отклонения от международного стандарта, регионального стандарта, регионального свода

правил, стандарта иностранного государства и свода правил иностранного государства, иного документа по стандартизации иностранного государства – мотивированное обоснование этого решения и/или иные сведения о научно-техническом уровне проекта предварительного национального стандарта

Проект предварительного стандарта является измененным по отношению к международному документу ITU-T F.748.13 (2021) «Искусственный интеллект. Техническая структура федеративной системы машинного обучения» (Technical framework for a shared machine learning system). В проект стандарта включены дополнительные по отношению к международному стандарту ITU-T F.748.13 (2021) определения и положения из международного стандарта ИСО/МЭК 22989 «Информационные технологии. Искусственный интеллект. Понятия и терминология искусственного интеллекта» (ISO/IEC 22989:2022 «Information technology — Artificial intelligence — Artificial intelligence concepts and terminology»). Это позволяет гармонизировать данный документ с принятыми ранее национальными стандартами и предварительными национальными стандартами в области ИИ.

6. Сведения о проведённых научно-исследовательских работах, технических предложениях, опытно-конструкторских, опытно-технологических и проектных работах, а также аналитических работах, послуживших основой для разработки первой редакции проекта национального стандарта

Проект национального стандарта разработан на основе выполненных научно-исследовательских работ в рамках проекта «Мониторинг и стандартизация развития и использования технологий хранения и анализа больших данных в цифровой экономике Российской Федерации», реализуемого Центром компетенций НТИ по направлению технологиям хранения и анализа больших данных Московского государственного университета имени

М.В.Ломоносова совместно с Институтом развития информационного общества.

7. Сведения о наличии в Федеральном информационном фонде стандартов переводов международных, региональных стандартов, стандартов и сводов правил иностранных государств, на которые даны нормативные ссылки в стандарте, использованном в качестве основы для разработки проекта национального стандарта Российской Федерации

Проект стандарта использует утверждённые действующие национальные стандарты, идентичные международным и региональным стандартам, либо имеющиеся в Федеральном информационном фонде стандартов переводы соответствующих стандартов.

8. Сведения о взаимосвязи проекта национального стандарта с проектами или действующими в Российской Федерации другими национальными и межгосударственными стандартами, сводами правил, а при необходимости также предложения по их пересмотру, изменению или отмене (одностороннему прекращению применения на территории Российской Федерации межгосударственных стандартов)

Проект стандарта взаимосвязан со следующими документами национальной системы стандартизации:

- ПНСТ 553–2021 Информационные технологии. Искусственный интеллект. Термины и определения.

9. Перечень исходных документов и другие источники информации, использованные при разработке стандарта, в том числе информацию об использовании документов, относящихся к объектам патентного или авторского права

При разработке проекта предварительного национального стандарта были учтены:

– ПНСТ 553–2021 Информационные технологии. Искусственный интеллект. Термины и определения.

10. Сведения о технических комитетах по стандартизации, в областях деятельности которых возможно пересечение с областью применения разрабатываемого проекта национального стандарта (далее - технических комитетах по стандартизации в смежной области деятельности)

Смежные технические комитеты по стандартизации, в предметных областях которых возможно пересечение с областью применения разрабатываемого проекта национального стандарта, отсутствуют.

11. Сведения о разработчиках стандарта

Проект предварительного национального стандарта разработан Научно-образовательным центром компетенций в области цифровой экономики Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В.Ломоносова» (МГУ имени М.В.Ломоносова) и Обществом с ограниченной ответственностью «Институт развития информационного общества» (ИРИО).

Контактная информация

Электронная почта:
standards@iis.ru
bigdata-wg02@digital.msu.ru
Номер телефона: +7 (495) 912-22-29; +7 (915) 140-42-04

Руководитель разработки

Председатель совета директоров

Института развития информационного общества Ю. Е. Хохлов

Исполнитель А.А. Храмцовская