ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к первой редакции проекта национального стандарта ГОСТ Р «Искусственный интеллект. Оценка робастности нейронных сетей. Часть 2. Методология использования формальных методов» (ISO/IEC 24029-2:2023 Artificial intelligence (AI) — Assessment of the robustness of neural networks — Part 2: Methodology for the use of formal methods, IDT)

1. Основание для разработки проекта стандарта

Проект национального стандарта ГОСТ Р «Искусственный интеллект. Оценка робастности нейронных сетей. Часть 2. Методология использования формальных методов» разработан в соответствии с Государственным контрактом (Заказчик – Росстандарт) и Программой национальной стандартизации Российской Федерации на 2023 год.

Шифр темы: 1.11.164-1.265.23.

2. Краткая характеристика объекта и аспекта стандартизации

Объектом стандартизации являются критерии, применимые для оценки робастности нейронных сетей и способы проверки нейронных сетей с помощью формальных методов на каждой стадии жизненного цикла ИИ-системы.

Аспектом стандартизации является методология использования формальных методов оценки свойств робастности нейронных сетей. Основное внимание уделяется тому, как выбирать и применять формальные методы, а также управлять ими для подтверждения свойств робастности.

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

Целесообразность разработки проекта национального стандарта объясняется тем, что технологии искусственного интеллекта являются особо

важными и перспективными инструментами для реализации разного рода задач во многих отраслях экономики. В настоящем стандарте представлены критерии, применимые для оценки робастности нейронных сетей и определены способы проверки нейронных сетей с помощью формальных методов на каждой стадии жизненного цикла ИИ-системы. При использовании формальных методов могут возникнуть сложности с точки зрения масштабируемости, однако они по-прежнему применимы ко всем типам нейронных сетей, выполняющих различные задачи с несколькими типами данных. Формальные методы уже давно используются в традиционных программных системах, однако их применение по отношению к нейронным сетям началось сравнительно недавно и все еще является активной областью исследований.

Настоящий стандарт направлен на то, чтобы помочь разработчикам ИИ, которые используют нейронные сети и перед которыми стоит задача оценить их робастность на соответствующих стадиях жизненного цикла ИИ-системы.

Благодаря установлению единой терминологии и набора понятий для таких систем, настоящий проект предоставляет основу для ясного объяснения как систем, так и различных соображений, касающихся их проектирования и использования.

4. Сведения о соответствии проекта 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

Проект национального стандарта разработан 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 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 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 национального стандарта

Проект национального стандарта является идентичным международному стандарту ИСО/МЭК 24029-2:2023 «Искусственный интеллект (ИИ). Оценка робастности нейронных сетей. Часть 2. Методология использования формальных методов» (ISO/IEC 24029-2:2023 «Artificial intelligence (AI) — Assessment of the robustness of neural networks — Part 2: Methodology for the use of formal methods», IDT).

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

Аналогичных работ при разработке настоящего проекта национального стандарта не проводилось.

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:

− ГОСТ Р 70462.1-2022/ISO/IEC TR 24029-1-2021 Информационные технологии. Интеллект искусственный. Оценка робастности нейронных сетей. Часть 1. Обзор (ISO/IEC TR 24029-1:2021, Artificial Intelligence (Al) — Assessment of the robustness of neural networks — Part 1: Overview, IDT).

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 национального стандарта были учтены:

– ИСО/МЭК 22989:2022, Information technology — Artificial intelligence — Artificial intelligence concepts and terminology (Информационные технологии. Искусственный интеллект. Термины и определения)

– ИСО/МЭК 23053:2022, Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) (Экосистема разработки систем искусственного интеллекта (ИИ) с использованием машинного обучения (МО));

– ГОСТ 1.5—2001 Межгосударственная система стандартизации. Стандарты межгосударственные. Правила и рекомендации по межгосударственной стандартизации. Общие требования к построению, изложению, оформлению, содержанию и обозначению;

– ГОСТ Р 1.5—2012 Стандартизация в Российской Федерации. Стандарты национальные. Правила построения, изложения, оформления и обозначения;

– ГОСТ 1.3—2014 Межгосударственная система стандартизации. Стандарты межгосударственные. Правила разработки на основе международных и региональных стандартов;

– ГОСТ Р 1.7—2014 Стандартизация в Российской Федерации. Стандарты национальные. Правила оформления и обозначения при разработке на основе применения международных стандартов.

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)

Технические комитеты по стандартизации в смежной области деятельности отсутствуют.

11. Сведения о разработчиках стандарта

Проект национального стандарта разработан Обществом с ограниченной ответственностью «Институт развития информационного общества» (ИРИО).

Контактная информация

Электронная почта: standards@iis.ru

Номер телефона: +7 (495) 912-22-29

Руководитель разработки и исполнитель
Председатель совета директоров
Института развития информационного общества Ю.Е. Хохлов