Технический Комитет 164

Национальная система оценки соответствия в области искусственного интеллекта: состояние и перспективы развития

XXX Юбилейный Форум «Технологии и Безопасность»
Конференция «Искусственный интеллект: вызовы и возможности»
11 февраля 2025 г.

Технологии ИИ на основе методов машинного обучения

Примеры решения интеллектуальной задачи

Обучение без учителя

AI

NI

Обучение с учителем

Обучающий НД

Высокая универсальность подхода

Алгоритмы системы ИИ позволяют решать задачи в условиях отсутствия объяснимой модели наблюдаемого объекта/процесса

Плохо предсказуемое поведение и отсутствие гарантий функциональной корректности систем ИИ при высоком субъективном правдоподобии результатов

Риски применения ИИ с неподтвержденной функциональной корректностью

Риски несоответствия характеристик ИИ установленным функциональным требованиям	Категория заинтересованной стороны	
	Акторы ИИ	Третьи лица
1 Угрозы жизни и здоровью людей, экологические угрозы	1.1 Потребители, разработчики и поставщики (собственная безопасность, дополнительные требования гос. регуляторов)	1.2 Общество в целом и регуляторы (безопасность общества и окружающей среды)
2 Угрозы информационной безопасности	2.1 Поставщики данных для обучения и тестирования ИИ, органы по оценке соответствия (конфиденциальность используемых данных)	2.2 Общество в целом и государственные регуляторы (защита персональных данных)
3 Нарушение этических и других норм «мягкого» права	Нет	3.2 Общество в целом (социальная приемлемость создания и применения ИИ)
4 Неопределенные потребительские свойства, не влияющие непосредственно на безопасность жизни и здоровья людей, экологическую безопасность	4.1 Потребители (функциональные характеристики, определяющие возможность применения ИИ по назначению), разработчики и поставщики (характеристики конкурентоспособности ИИ)	Нет

Национальная система оценки соответствия в области искусственного интеллекта

Росстандарт

ТК164 — Технический Комитет 164

72 организации-члена

ГОСТ Р, ПНСТ

Утверждено 156 стандартов

Перспективная программа стандартизации по приоритетному направлению «Искусственный интеллект»

Комплекс национальных стандартов в области ИИ

Информационный портал www.tc164.ru

Потребители и регуляторы ИИ

СДС «Интеллометрика»

Допущено 4 органа по оценке соответствия

Разработчики ИИ

Структура технического комитета ТК164 (2025)

Секретариат ТК 164 (71)
ФИЦ «Информатика и управление» РАН

ПК 01 «Искусственный интеллект в здравоохранении» (24)
Научно-практический клинический центр диагностики и телемедицины (Ю.А. Васильев)

РГ по разработке дорожной карты стандартов ИИ в здравоохранении (33)
(НПКЦ ДТ ДЗМ, А.В. Владзимирский)

ПК 02 «Данные» (61)
МГУ им. М.В. Ломоносова, ИРИО (Ю.Е. Хохлов)

ПК 03 «Искусственный интеллект в дорожно-транспортном комплексе» (29)
ФАУ «РОСДОРНИИ» (А.Д. Журавлев)

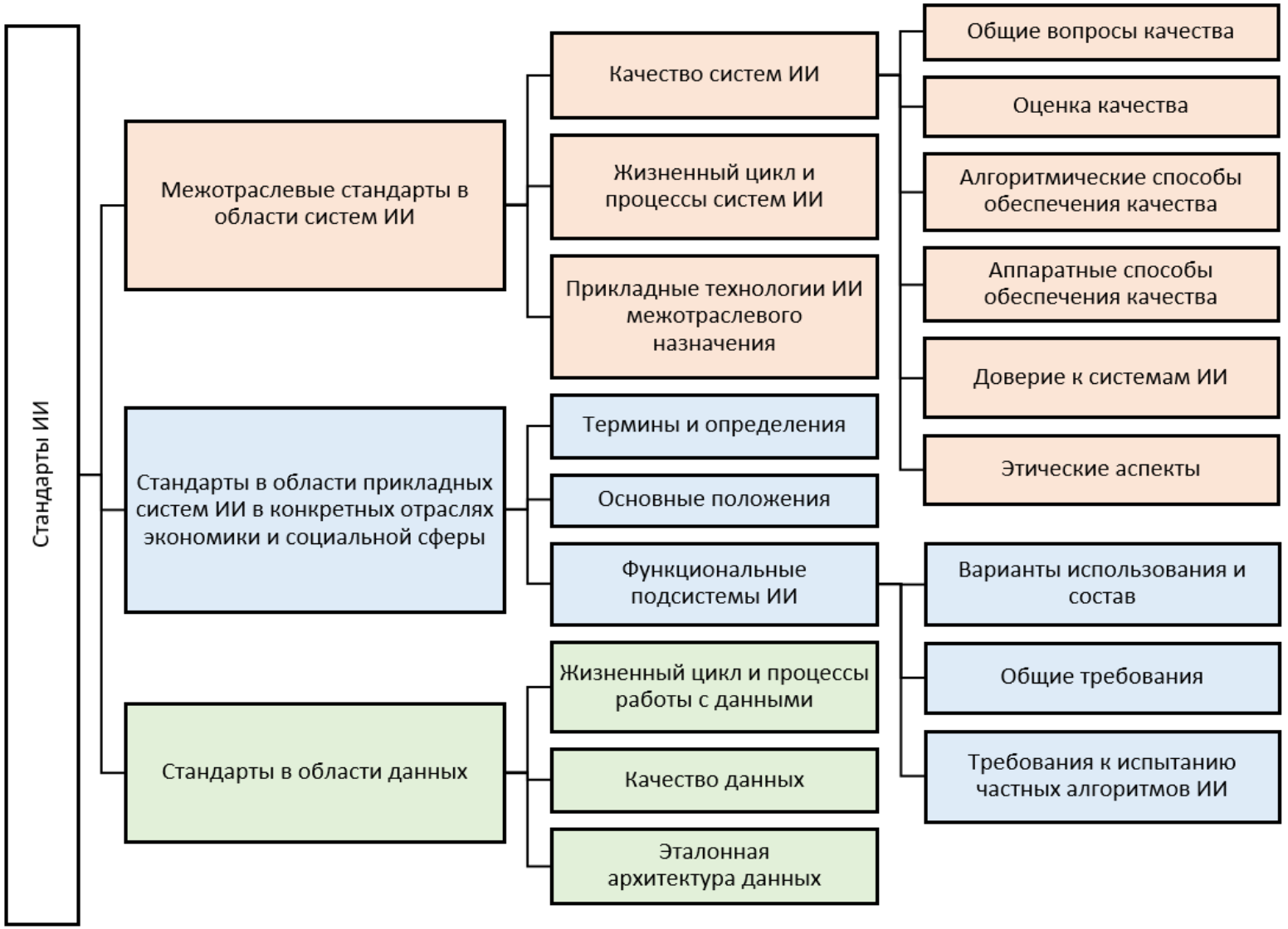
РГ по разработке дорожной карты стандартов ИИ на транспорте (13)
(Российский университет транспорта, С.В. Жанказиев)

ПК 04 «Искусственный интеллект на железнодорожном транспорте»
Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте (А.Е. Хатламаджиян)

Отраслевые РГ по применению технологий ИИ

№	Область	Ведущая организация	Смежные ТК
1	Здравоохранение	НПКЦ диагностики и телемедицины Депздрава Москвы	ТК 011 «Медицинские приборы, аппараты и оборудование» ТК 436 «Управление качеством медицинских изделий» ТК 468 «Информатизация здоровья»
2	Образование	ВолГУ	ТК 461 «Информационно-коммуникационные технологии в образовании (ИКТО)»
3	Гражданская авиация	Союз авиапроизводителей России	ТК 323 «Авиационная техника» ТК 363 «Радионавигация»
4	Специализированная техника	Ассоциация Росспецмаш	ТК 267 «Строительно-дорожные машины и оборудование» ТК 284 «Тракторы и машины сельскохозяйственные»
5	Дорожно-транспортный комплекс	РОСДОРНИИ	ТК 056 «Дорожный транспорт» ТК 057 «Интеллектуальные транспортные системы» ТК 278 «Безопасность дорожного движения» ТК 418 «Дорожное хозяйство»
6	Станкоинструментальная промышленность	Институт стандартизации, СТАНКИН	ТК 070 «Станки»
7	Средства измерений и неразрушающий контроль	ВНИИМ им. Менделеева	ТК 053 «Основные нормы и правила по обеспечению единства измерений» ТК 371 «Неразрушающий контроль»
8	Сельское хозяйство	Федеральный научный агроинженерный центр ВИМ	ТК 284 «Тракторы и машины сельскохозяйственные»
9	Технические средства охраны	НИЦ «Охрана» Росгвардии	ТК 234 «Системы тревожной сигнализации и противокриминальной защиты»
10	Следственная деятельность	Московская академия СКР	ТК 134 «Судебная экспертиза»
11	Промышленность	Федеральный центр прикладного развития ИИ	

Комплекс национальных стандартов в области ИИ



Межотраслевые стандарты

- Требования к аппаратным и программно-алгоритмическим средствам, используемым для создания доверенных систем ИИ

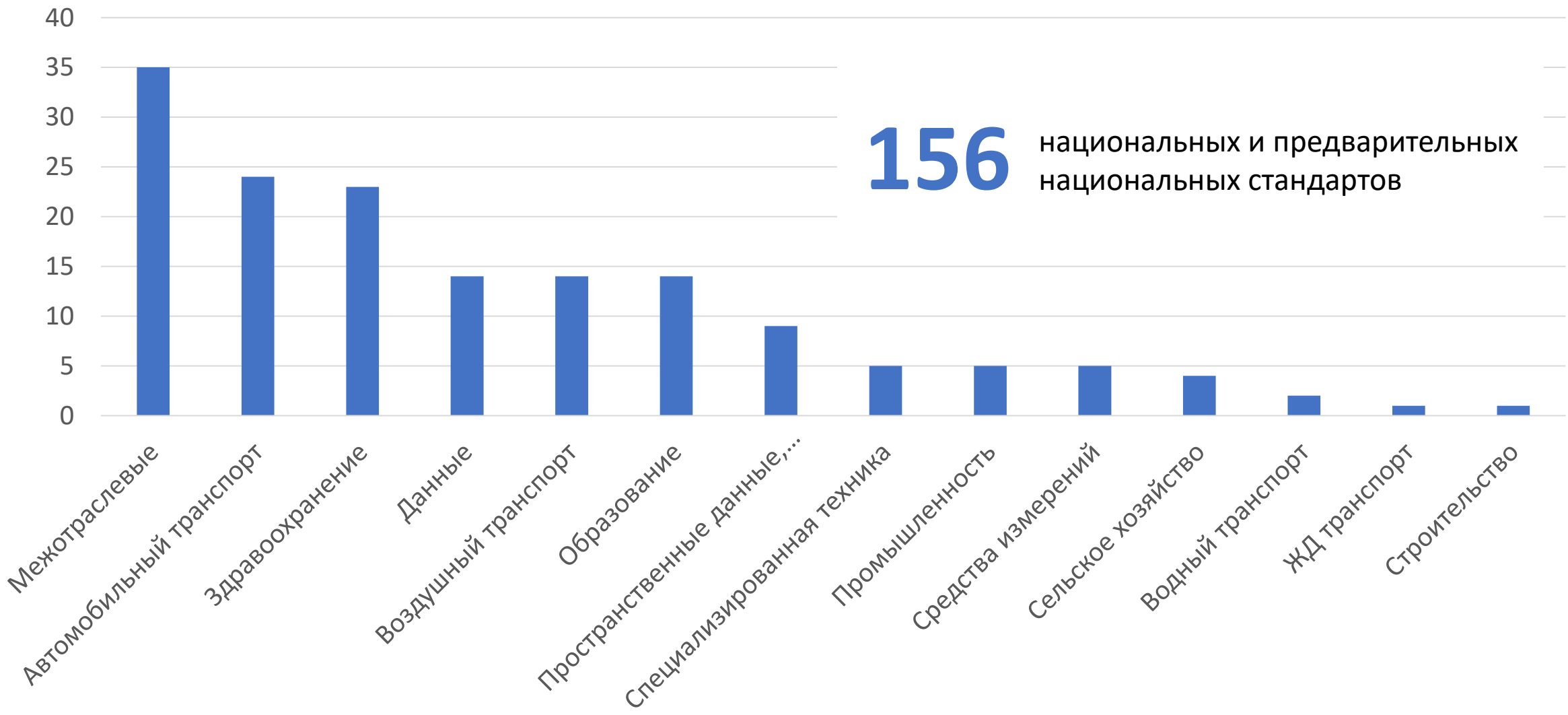
Отраслевые стандарты

- Требования к унифицированным процедурам оценки качества прикладных систем ИИ

Данные

- Требования к данным, используемым для создания доверенных систем ИИ

Комплекс национальных стандартов



156 национальных и предварительных национальных стандартов

Система добровольной сертификации «Интеллометрика»

Зарегистрирована Росстандартом в едином реестре систем добровольной сертификации 26.12.2023 (№ РОСС RU.В2915.04ВШЭ0)

Заявители

Руководящий орган

Наблюдательный совет

Комиссия по допуску участников СДС

Апелляционная комиссия

Транспорт

РОСДОРНИИ

НАМИ

ГЭТ Электротранспорт Санкт-Петербурга

НИИАС

Средства видеоаналитики

open{code:} открытый код

Образование

Интеллектуальное СИ

ВНИИМ 1842

Сельское хозяйство

ВИМ Федеральный центр

Следственная деятельность

Московская академия Следственного комитета имени А.Я. Сухарева

Специализированная техника

РОССПЕЦМАШ

ДСТ УРАЛ

Розничная торговля

РУС СОФТ

АЙТИЛЛЕКТ Инструменты для бизнеса

*перечень органов по оценке соответствия не является исчерпывающим

Правила функционирования СДС «Интеллометрика»

Зарегистрированы Росстандартом в едином реестре систем добровольной сертификации 26.12.2023, свидетельство № РОСС RU.В2915.04ВШЭ0

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

СИСТЕМА ДОБРОВОЛЬНОЙ СЕРТИФИКАЦИИ В СФЕРЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА «ИНТЕЛЛОМЕТРИКА» (СДС «ИНТЕЛЛОМЕТРИКА»)

УТВЕРЖДАЮ

Ректор НИУ ВШЭ

_____Н.Ю. Анисимов

«21» декабря 2023 г.

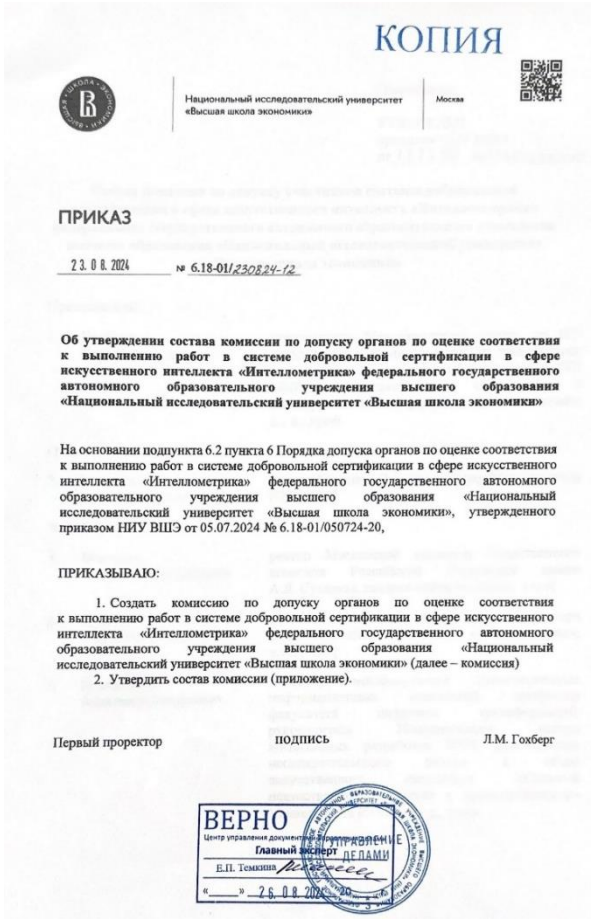
ПРАВИЛА ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ДОБРОВОЛЬНОЙ СЕРТИФИКАЦИИ В СФЕРЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА «ИНТЕЛЛОМЕТРИКА»

Правила предназначены для применения всеми участниками системы и другими заинтересованными юридическими и физическими лицами.

Устанавливают:

1. Объекты оценки соответствия
2. Организационную структуру и функции участников
3. Принципы функционирования системы
4. Правила и порядок проведения работ по сертификации
5. Требования к экспертам и испытателям системы

Первое заседание комиссии по допуску участников СДС «Интеллометрика». 23.08.2024



КОПИЯ

Национальный исследовательский университет «Высшая школа экономики» Москва

ПРИКАЗ

23.08.2024 № 6.18-01/230824-12

Об утверждении состава комиссии по допуску органов по оценке соответствия к выполнению работ в системе добровольной сертификации в сфере искусственного интеллекта «Интеллометрика» федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет «Высшая школа экономики»

На основании подпункта 6.2 пункта 6 Порядка допуска органов по оценке соответствия к выполнению работ в системе добровольной сертификации в сфере искусственного интеллекта «Интеллометрика» федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет «Высшая школа экономики», утвержденного приказом НИУ ВШЭ от 05.07.2024 № 6.18-01/050724-20,

ПРИКАЗЫВАЮ:

1. Создать комиссию по допуску органов по оценке соответствия к выполнению работ в системе добровольной сертификации в сфере искусственного интеллекта «Интеллометрика» федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет «Высшая школа экономики» (далее – комиссия)
2. Утвердить состав комиссии (приложение).

Первый проректор подпись Л.М. Гохберг

ВЕРНО Главный эксперт Е.П. Темкина

Участие в голосовании приняли 12 из 12 членов Комиссии

Кворум по всем вопросам повестки имеется

Решение о допуске принимается путем открытого голосования 2/3 голосов от числа членов Комиссии

О допуске организаций к выполнению работ в СДС «Интеллометрика»

допущен в качестве **органа по сертификации** **область допуска:** интеллектуальные средства измерений и системы контроля на их основе *12 из 12 проголосовали «ЗА»*	допущен в качестве **испытательной лаборатории** **область допуска:** системы автоматического контроля выбросов вредных веществ с применением искусственного интеллекта *12 из 12 проголосовали «ЗА»*	допущен в качестве **испытательной лаборатории** **область допуска:** строительно-дорожная техника *11 из 12 проголосовали «ЗА»*	допущен в качестве **испытательной лаборатории** **область допуска:** средства видеонаблюдения *12 из 12 проголосовали «ЗА»*

Система автоматического контроля выбросов на основе ИИ получила первый сертификат соответствия

Axioma

Предиктивная система автоматического контроля и мониторинга эмиссий

Орган по сертификации

ВНИИМ 1842

Правообладатели системы

НОРНИКЕЛЬ

НОРСОФТ

ЦИФРОВЫЕ КОРПОРАТИВНЫЕ ТЕХНОЛОГИИ

СИСТЕМА ДОБРОВОЛЬНОЙ СЕРТИФИКАЦИИ В СФЕРЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА «ИНТЕЛЛОМЕТРИКА»

Зарегистрирована Федеральным агентством по техническому регулированию и метрологии 26.12.2023 регистрационный № РОСС RU.В2915.04ВЩЭ0

СЕРТИФИКАТ СООТВЕТСТВИЯ

№ ОС/1-001-2024 от 03 декабря 2024 г.

Срок действия: бессрочно

ОРГАН ПО СЕРТИФИКАЦИИ

Измерительные информационные системы и Системы контроля ($И^2С^2К$) ФГУП «ВНИИМ им. Д.И.Менделеева», г. Санкт-Петербург

ПРОДУКЦИЯ

Предиктивная система автоматического контроля выбросов «Axioma»

код ОКПД2: *62.01.29, 26.51.5*
код ТН ВЭД: -

СООТВЕТСТВУЕТ ТРЕБОВАНИЯМ

ГОСТ Р 71561-2024 Средства измерений на основе искусственного интеллекта. Состав, структура и области применения. Основные положения
ГОСТ Р 59898-2021 Оценка качества систем искусственного интеллекта. Общие положения

ПРАВООБЛАДАТЕЛЬ

Общество с ограниченной ответственностью «Норсофт» (ООО «Норсофт»), г. Москва, ИНН 7743395841, ОГРН 1227700685431
Общество с ограниченной ответственностью «Цифровые корпоративные технологии» (ООО «ЦКТ»), г. Санкт-Петербург, ИНН 7813664900, ОГРН 1227800100021

ИЗГОТОВИТЕЛЬ

Общество с ограниченной ответственностью «Цифровые корпоративные технологии» (ООО «ЦКТ»), г. Санкт-Петербург, ИНН 7813664900, ОГРН 1227800100021

Руководитель органа по сертификации — Р.А.Родин

М.П.

Унификация методов и средств испытаний алгоритмов ИИ

универсальные классы интеллектуальных задач

- в рамках универсальных классов интеллектуальных задач к испытаниям алгоритмов ИИ предъявляются схожие требования

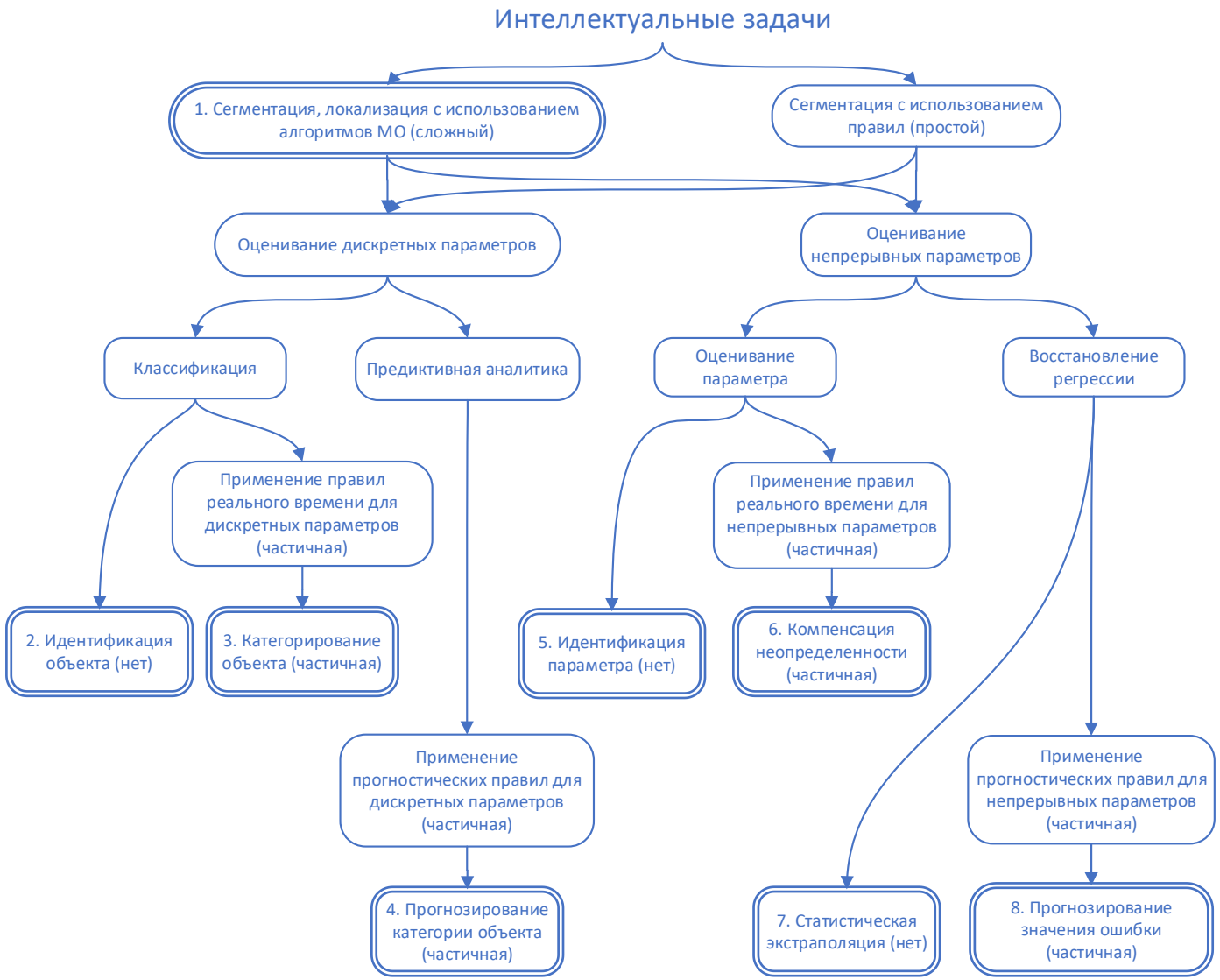
методические инструменты обеспечения репрезентативности тестовых НД

- требования к обоснованию необходимого объема и вариативности тестовых НД обеспечивают интерпретируемость результатов испытаний для предусмотренных условий эксплуатации

механизмы определения точности проведенных испытаний

- метрологические подходы к определению погрешностей оценки функциональных характеристик с учетом репрезентативности тестовых НД

Классификационные дескрипторы интеллектуальных функций



Основные:

$e_1^{\text{Кл}}$ (уровень сложности ОК) = {без сегментации (0); с сегментацией (1)}

$e_2^{\text{Кл}} = \left(\frac{T_P}{\tau_P} \lesseqgtr e_{2,max}^{\text{Кл}} \rightarrow \{0,1\}\right)$, сравнение коэффициента прогнозирования $\frac{T_P}{\tau_P}$ с порогом $e_{2,max}^{\text{Кл}} \rightarrow$ оценивание параметров: {текущих (0); прогнозных (1)}

$e_3^{\text{Кл}}$ (вид оцениваемых параметров объекта) = оценивание параметров: {дискретных (0); непрерывных (1)}

$e_4^{\text{Кл}}$ (наличие интерпретируемых правил) = модель идентификации объекта: {полностью не интерпретируемая (0); частично интерпретируемая (1)}

Дополнительные:

$e_1^{\text{Доп}} = \left(\frac{T_S}{\tau_S} \lesseqgtr e_{1,max}^{\text{Доп}} \rightarrow \{0,1\}\right)$, сравнение коэффициента динамичности $\frac{T_S}{\tau_S}$ с порогом $e_{1,max}^{\text{Доп}} \rightarrow$ обработка характеристик: {статических (0); динамических (1)}

$e_2^{\text{Доп}}$ (модальность входных данных) = {изображения (1); векторные описания (2); текст (3); таблицы (4); временные ряды (5); речь (6)}

$e_3^{\text{Доп}}$ (характер управления) = {непосредственное (1); локальное (2); глобальное (3); отложенное (4)}

Обеспечение репрезентативности тестовых НД

Существенные факторы эксплуатации

e_1

e_2

e_3

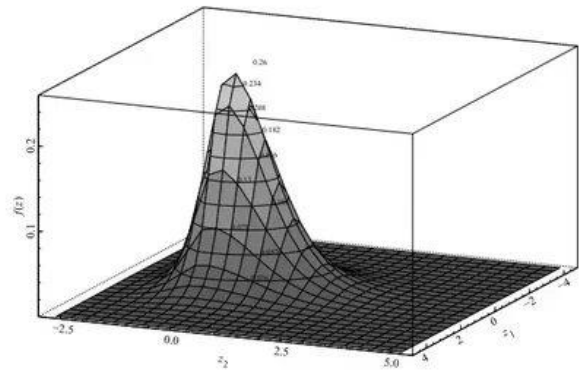
…

e_n

Выявляются внешние факторы, существенно влияющие на качество работы алгоритмов ИИ для заданной прикладной задачи (СФЭ)

Предусмотренные условия эксплуатации

Делается предположение о законах распределения СФЭ в реальных (предусмотренных) условиях эксплуатации



Критерий представительности испытаний

$e_1 \in [x_1; x_2]$

…

$e_n \in [y_1; y_2]$

Статистические характеристики СФЭ для НД сравниваются с предусмотренными условиями эксплуатации

СФЭ при испытаниях алгоритмов распознавания дорожных знаков

номенклатура и типоразмеры знаков, подлежащих распознаванию

характеристики фона, количество одновременно наблюдаемых знаков

пространственное и радиометрическое разрешение средств видеонаблюдения

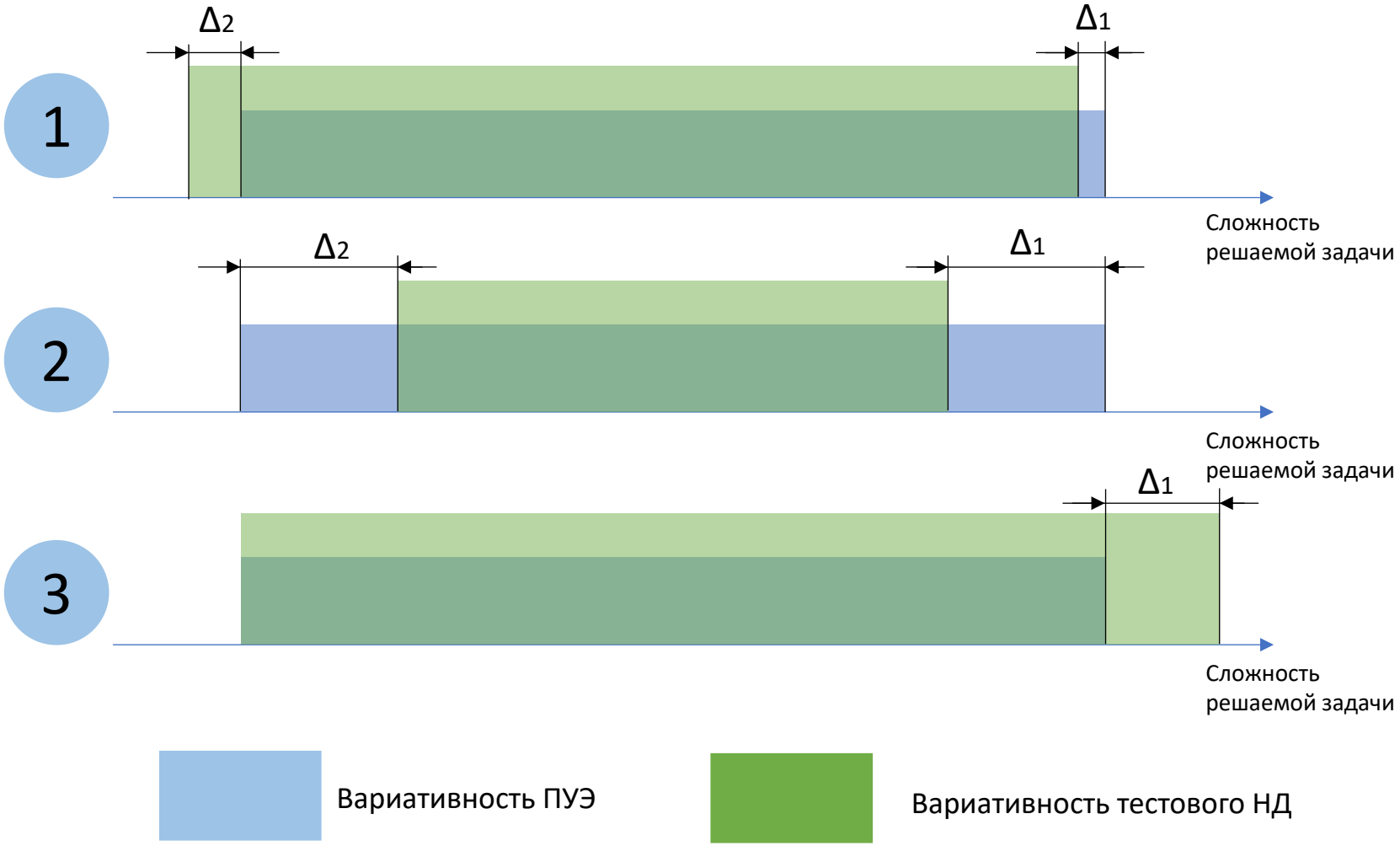
диапазон ракурсов и расстояний до знака, условия освещенности, скорость перемещения ТС относительно знака

характеристики осадков, задымленности, загрязнений апертуры средств наблюдения, процент загрязнения и закрытия информативной части знака мешающими предметами

возможности злоумышленника по «отравлению» обучающих НД, возможности по реализации состязательных атак на АТС ИИ, возможности по нарушению целостности данных, поступающих от сенсоров, при применении АТС ИИ

Условия репрезентативности наборов данных (НД)

Репрезентативность НД: $\sigma = f(\Delta)$



НД достаточен с определенной погрешностью, провоцирует смещение результатов испытаний

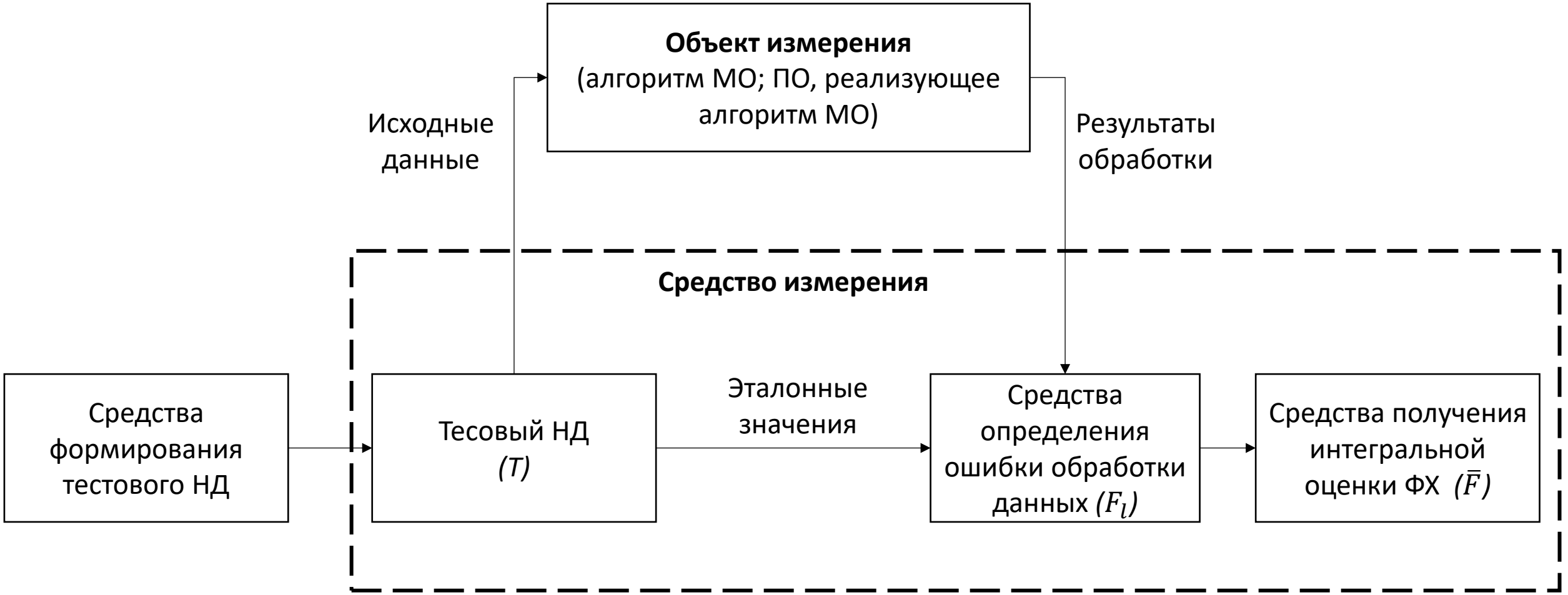
НД недостаточен, испытания нельзя считать представительными

НД избыточен, результаты испытаний могут дать заниженную оценку функциональной корректности

Схема измерительной задачи при оценивании функциональных характеристик систем ИИ на основе алгоритмов МО

*цветом выделены различные оценки погрешности измерения функциональных характеристик

Средство измерения функциональных характеристик (ФХ) алгоритма ИИ



ИИ с гарантированной функциональной корректностью

Для предусмотренных условий эксплуатации могут быть оценены:

- доверительные интервалы и вероятности прогнозирования погрешностей измерений для определенных условий проведения измерений
- предельные интегральные риски, связанные с некорректной работой системы ИИ
- ресурсы, необходимые злоумышленнику для успешного информационного воздействия на измерительную систему с алгоритмами ИИ (опционально, при наличии активного злоумышленника)

Технический Комитет 164

Спасибо за внимание

Гарбук Сергей Владимирович
председатель ТК164 «Искусственный интеллект»,
директор ВИНИТИ РАН

www.tc164.ru