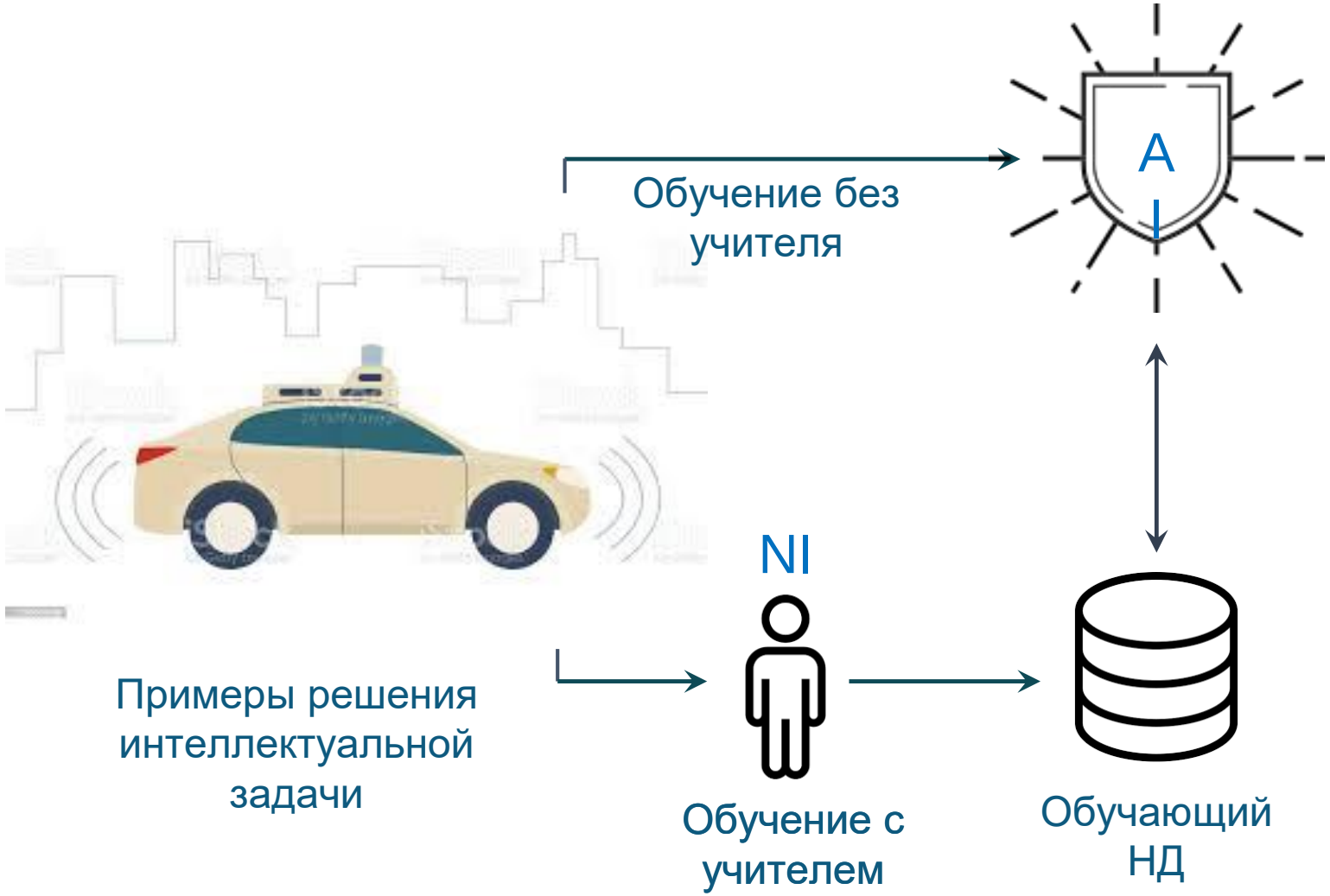
НАУЧНО-МЕТОДИЧЕСКИЕ ОСНОВЫ СТАНДАРТИЗАЦИИ И ОЦЕНКИ СООТВЕТСТВИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Сергей Гарбук, председатель Технического комитета по стандартизации №164 «Искусственный интеллект»

РСТ | РОССИЙСКИЙ ИНСТИТУТ СТАНДАРТИЗАЦИИ

2024: ИИ – ОБРАБОТКА ДАННЫХ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ



Алгоритм системы ИИ принципиально не обладает полной понятностью (объяснимостью) для человека

Плохо предсказуемое поведение системы ИИ в реальных условиях эксплуатации, отсутствие в поведении систем «здравого смысла», подверженность воздействию т.н. «состязательных» атак на исходные данные

НЕКОРРЕКТНАЯ РАБОТА АЛГОРИТМОВ ИИ НАБЛЮДАЕТСЯ ПРИ ОПРЕДЕЛЁННЫХ (СЛОЖНО ПРЕДСКАЗУЕМЫХ):

- условиях эксплуатации (сочетаниях параметров внешней среды и объекта измерения)

- небольших (не значительных с точки зрения здравого смысла человека) неумышленных или умышленных искажениях исходных данных, подаваемых на вход алгоритма ИИ

- характеристиках наборов данных, используемых для дообучения алгоритмов ИИ на стадии их эксплуатации

АСПЕКТЫ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ С ИИ

Техническая надежность	• Аккредитованные лаборатории по проведению испытаний на устойчивость к климатическим, механическим и иным воздействиям • КГВС «Мороз-7», «Климат-8» и др.
Информационная безопасность	• Система сертификации на соответствие требованиям в области защиты информации • Национальные стандарты и руководящие документы ФСБ и ФСТЭК России
Импортонезависимость	• Реестр отечественного ПО, Минцифры России • Реестр радиоэлектронной продукции российского происхождения, Минпромторг России
Функциональная корректность	• Общие подходы к оценке качества программных систем, не учитывающие особенности систем с ИИ • Организации по оценке соответствия отсутствуют

СТАНДАРТЫ ЖИЗНЕННОГО ЦИКЛА ТЕХНИЧЕСКИХ СИСТЕМ

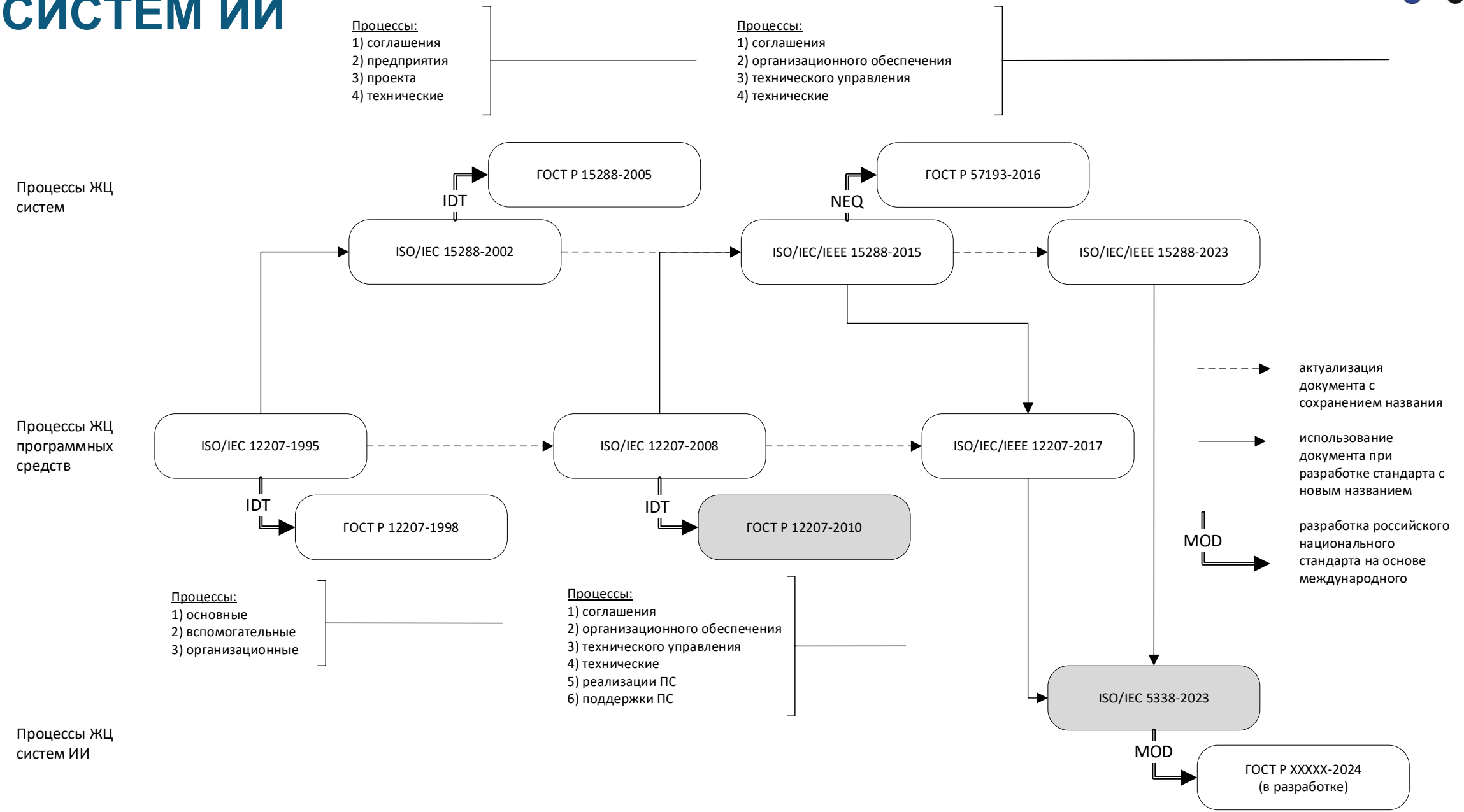
Стандарты, устанавливающие последовательность реализации стадий ЖЦ:

- ГОСТ 34.601–90 АС. Стадии создания
- ГОСТ РВ 15.004-2004 Система разработки и постановки продукции на производство. Военная техника. Стадии жизненного цикла изделий
- ГОСТ Р 56135-2014 Управление жизненным циклом продукции военного назначения. Общие положения
- ГОСТ Р 53791-2010 Ресурсосбережение. Стадии жизненного цикла изделий производственно-технического назначения. Общие положения
- ГОСТ Р 60.0.0.6—2023 Роботы и робототехнические устройства. Жизненный цикл. Основные положения

Стандарты системной инженерии, задающие исчерпывающий перечень процессов ЖЦ без определения очередности и обязательности их реализации:

- ISO/IEC/IEEE 15288:2015 Systems and software engineering — System life cycle processes и производные стандарты в области ЖЦ систем
- ISO/IEC 12207:2008 System and software engineering – Software lifecycle processes и производные документы в области ЖЦ программных средств\
- ISO/IEC 5338-2023 Information technology — Artificial intelligence — AI system life cycle processes

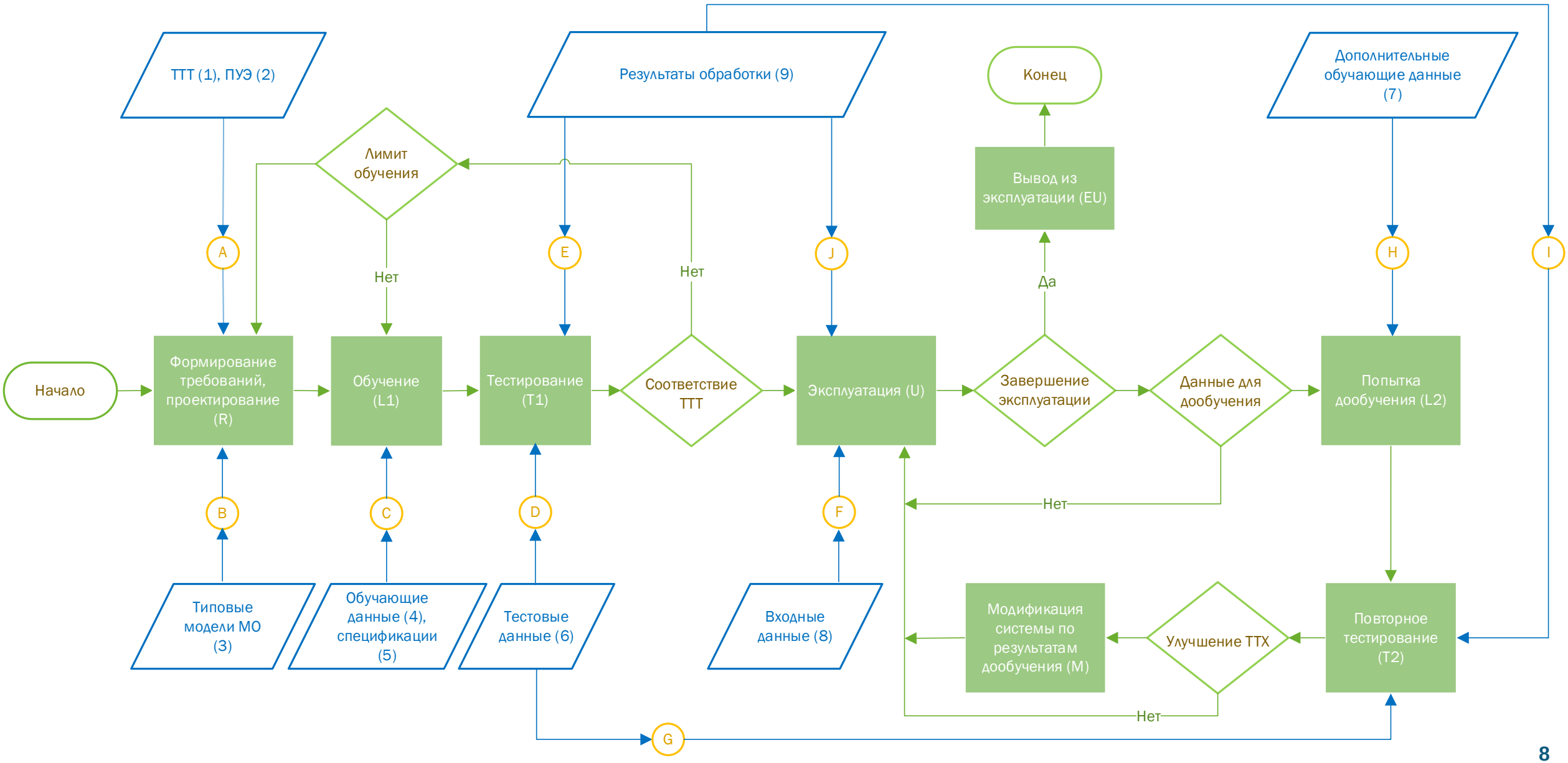
СТАНДАРТЫ ЖЦ СИСТЕМ, ПРОГРАММНЫХ СРЕДСТВ И СИСТЕМ ИИ



ОСОБЕННОСТИ И МОДЕЛЬ ЖЦ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В соответствии с моделью ЖЦ		В соответствии с ISO/IEC/IEEE 5338-2023	
№	Содержание	№	Содержание
1	Обязательность этапа обучения	5	Принципиальная необходимость использования представительных НД для обучения, тестирования, верификации и валидации СИИ. Определение поведения моделей МО не путем программирования (“not programmed”), а методом изучения на основе данных
2	Неполная интерпретируемость и отсутствие строгих доказательств функциональной корректности алгоритмов МО	4	Принципиальный вероятностный характер поведения СИИ, наличие ограничений на применение формальных методов при верификации корректности моделей МО
		6	Важное значение знаний, определяющих корректность моделей МО
		8	Возможное снижение доверия к СИИ на основе алгоритмов МО, связанное с их меньшей предсказуемостью, понятностью и объяснимостью поведения по сравнению с системами обработки данных, основанных на интерпретируемых знаниях
3	Возможность дообучения СИИ на стадии эксплуатации	1	Необходимость мониторинга возможных изменений в поведении контролируемого объекта в процессе применения СИИ
		3	Итерационное уточнение требований и поведенческих сценариев СИИ, в том числе – при возникновении непредвиденных ситуаций в процессе их эксплуатации
4	Важность социальной приемлемости применения	7	Необходимость информирования пользователей о возможных рисках применения СИИ для предотвращения избыточного и неоправданного доверия к ним, в том числе – при попытке использования систем для замены человека
5	Необходимость сопоставления с интеллектуальными способностями человека	2	Необходимость контроля качества СИИ, обладающих автономностью, сопоставимой с поведением человека и способных нанести существенный ущерб окружающим
6	Рост конфиденциальности данных в процессе эксплуатации СИИ	-	-

МОДЕЛЬ ЖИЗНЕННОГО ЦИКЛА СИСТЕМЫ ИИ



СООТВЕТСТВИЕ ЭТАПОВ ЖЦ В РАЗНЫХ НОРМАТИВНЫХ ДОКУМЕНТАХ И ПРЕДЛОЖЕННОЙ МОДЕЛИ

Стадии ЖЦ СИИ	ГОСТ 34.601–90 АС	ГОСТ РВ 15.004-2004	ГОСТ Р 56135-2014	ГОСТ Р 53791-2010	ГОСТ Р 60.0.0.6—2023
R: формирование требований и проектирование	- формирование требований к АС; - разработка концепции АС; - техническое задание; - эскизный проект	исследование и обоснование разработки	- создание научно-технического задела; - формирование концепции образца ПВН (аванпроект)	- обоснование разработки; - разработка ТЗ	1: обоснование разработки и формирование исходных требований; 2: проектирование (разработка); 3: изготовление (производство)
$L1$: обучение	- технический проект; - рабочая документация	- разработка; - производство	- разработка; - производство	- проведение ОКР; - производство и испытания	
$T1$: тестирование	ввод в действие	эксплуатация изделий	эксплуатация		4: контроль (приемка)
$L2$: дообучение	не предусматривается, т.к. не относится к созданию АС			использование (эксплуатация)	5: эксплуатация
$T2$: повторное тестирование					
U: эксплуатация					
EU: вывод из эксплуатации			утилизация	ликвидация (с избавлением от отходов путем их утилизации и/или удаления)	7: утилизация
M: модификация по результатам дообучения	сопровождение АС	капитальный ремонт (для изделий, подлежащих капремонту)	капитальный ремонт (при необходимости)	модернизация	6: ремонт (модернизация)

ТРЕБОВАНИЯ В ОБЛАСТИ ЦЕЛОСТНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИОННЫХ КОМПОНЕНТ СИИ

Требования целостности

- Репрезентативность (объём и вариативность) и точность обучающих и тестовых НД
- Отсутствие преднамеренных и естественных искажений входных данных
- Предотвращение преднамеренного внесения изменений (уязвимостей) в обучающие и тестовые НД

Требования конфиденциальности

- Предотвращение доступа к НД злоумышленников и других заинтересованных лиц (например, доступ разработчиков к тестовым НД)
- Предотвращение компрометации данных в результате недооценки уровня их конфиденциальности на этапе разработки СИИ

ТРЕБОВАНИЯ К ИНФОРМАЦИОННЫМ КОМПОНЕНТАМ (ФАКТОРЫ КАЧЕСТВА) СИИ

Информационная компонента	Причины, связанные с нарушением целостности n-й компоненты	Причины, связанные с нарушением конфиденциальности n-й компоненты
1. Функциональные характеристики (ФХ)	$i1$ Неполный набор, некорректные пороговые значения и весовые коэффициенты	$c1$ Компрометация ФХ (для систем безопасности и др., предполагающих возможность активного противодействия)
2. Предусмотренные условия эксплуатации (ПУЭ)	$i2$ Неполный перечень факторов эксплуатации, расхождение реальных условий эксплуатации с ПУЭ	$c2$. Компрометация ПУЭ (для систем безопасности)
3. Типовые модели МО, эталонные архитектуры	$i3$ Манипуляции с моделями: размещение злоумышленниками в открытом доступе моделей МО с программными закладками, реализующими НДВ	$c3$ Извлечение моделей: нарушение конфиденциальности сведений о моделях МО, использованных при разработке СИИ
4. Обучающие НД	$i4$ Манипуляции с обучающими НД: «атаки отравления» (poisoning), каузативные (causative) атаки	$c4$ Извлечение сведений об обучающих НД с целью повышения эффективности реализации атак на СИИ и извлечения сведений о объектах, данные которых использовались при обучении СИИ
5. Спецификации требований к моделям МО	$i5$ Неполные и искаженные спецификации, обусловленные заблуждениями относительно законов и закономерностях, присущих предметной области	$c5$ Использование злоумышленниками спецификаций для реализации атак, противоречащих принятым интерпретируемым моделям
6. Тестовые НД	$i6$ Искажение тестовых НД, низкая репрезентативность, смещённость тестовых НД	$c6$ Извлечение сведений о тестовых НД заинтересованными лицами (например, недобросовестными разработчиками)
7. Данные для дообучения СИИ	$i7$ Смещение обучающего НД вследствие эксплуатации в однотипных условиях	$c7$ Компрометация сценариев применения (для ВВСТ, систем безопасности)
8. Исходные данные	$i8$ Прямые манипуляции с входными данными, «состязательные примеры», непрямые манипуляции (воздействие на входы сенсоров СИИ)	$c8$ Извлечение исходных данных: «атаки инверсии модели» (model inversion)
9. Результаты обработки	$i9$ Искажение результатов обработки при их отображении, хранении, использовании в процессе тестирования СИИ и т.п.	$c9$ Извлечение выходных данных: «атаки инверсии модели» (model inversion), подмена результатов тестирования для завышения возможностей или дискредитации СИИ

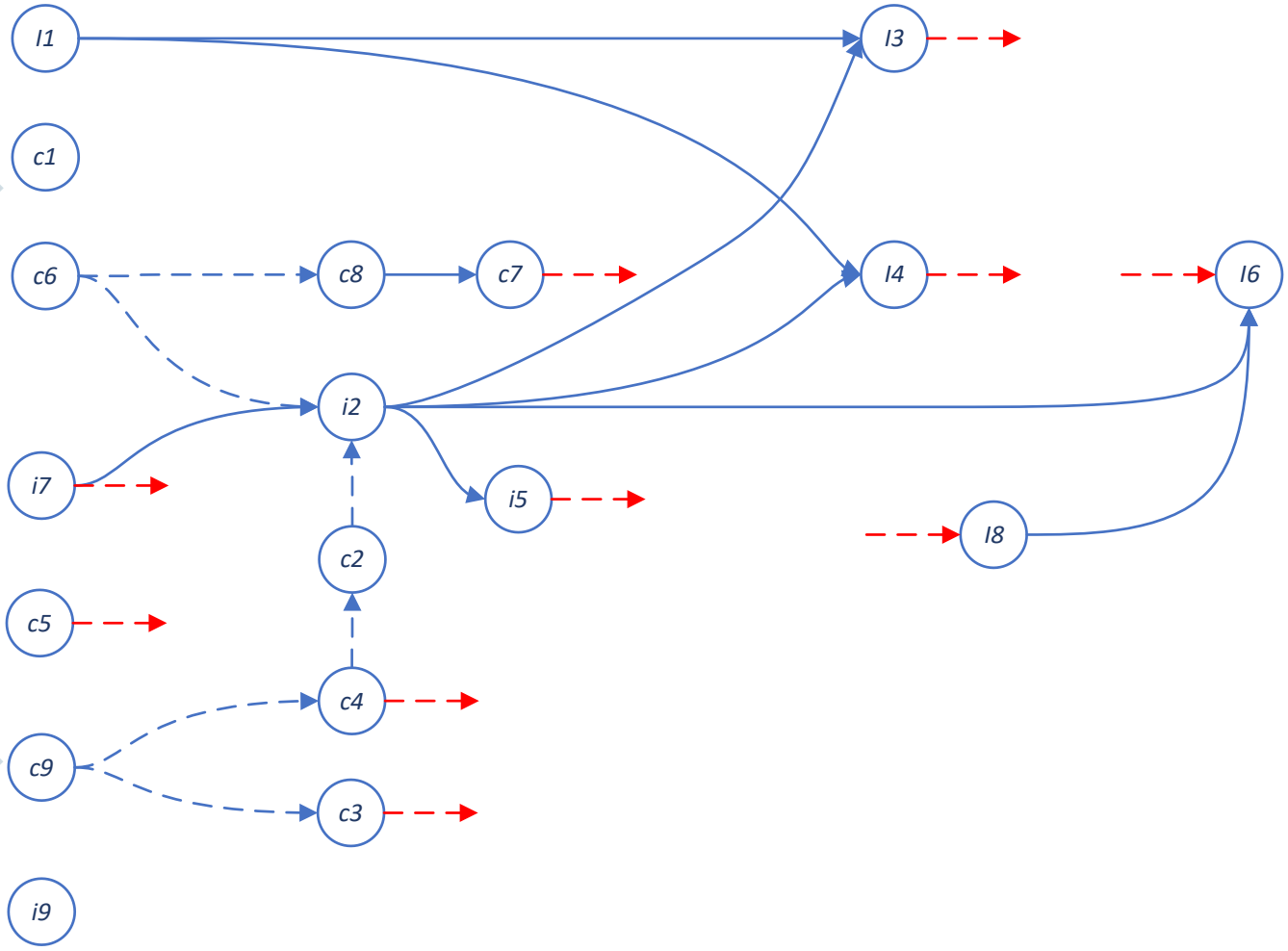
НЕГАТИВНЫЕ ЭФФЕКТЫ, ОБУСЛОВЛЕННЫЕ ФАКТОРАМИ КАЧЕСТВА СИИ

Нарушения функциональности

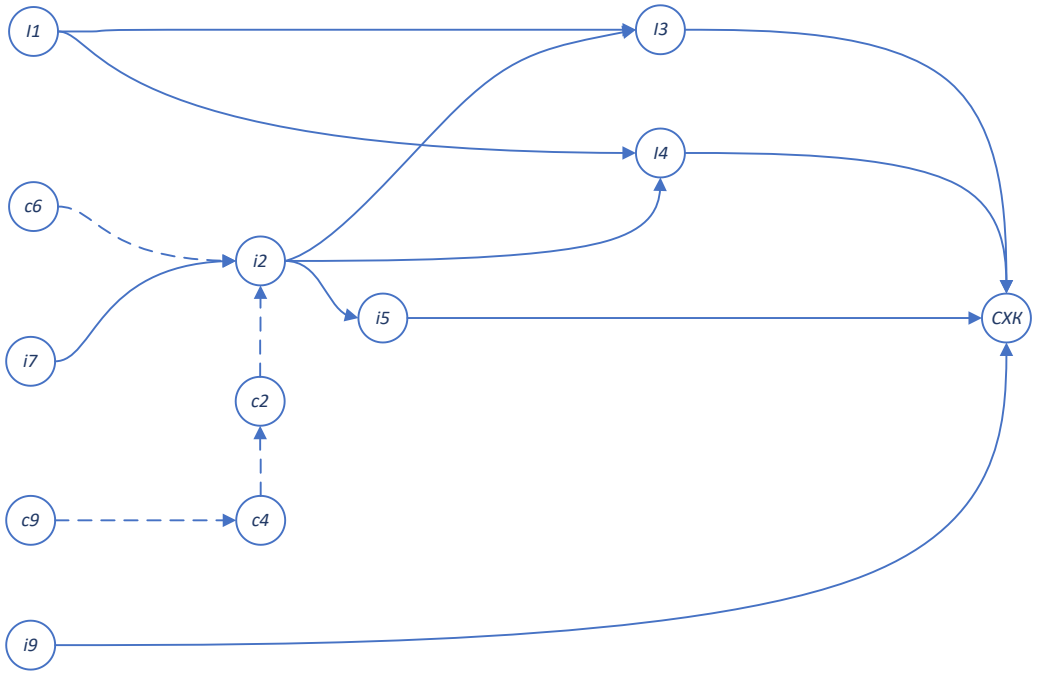
- 1. Деградация функциональных характеристик СИИ
- 2. Рост погрешности оценки функциональных характеристик

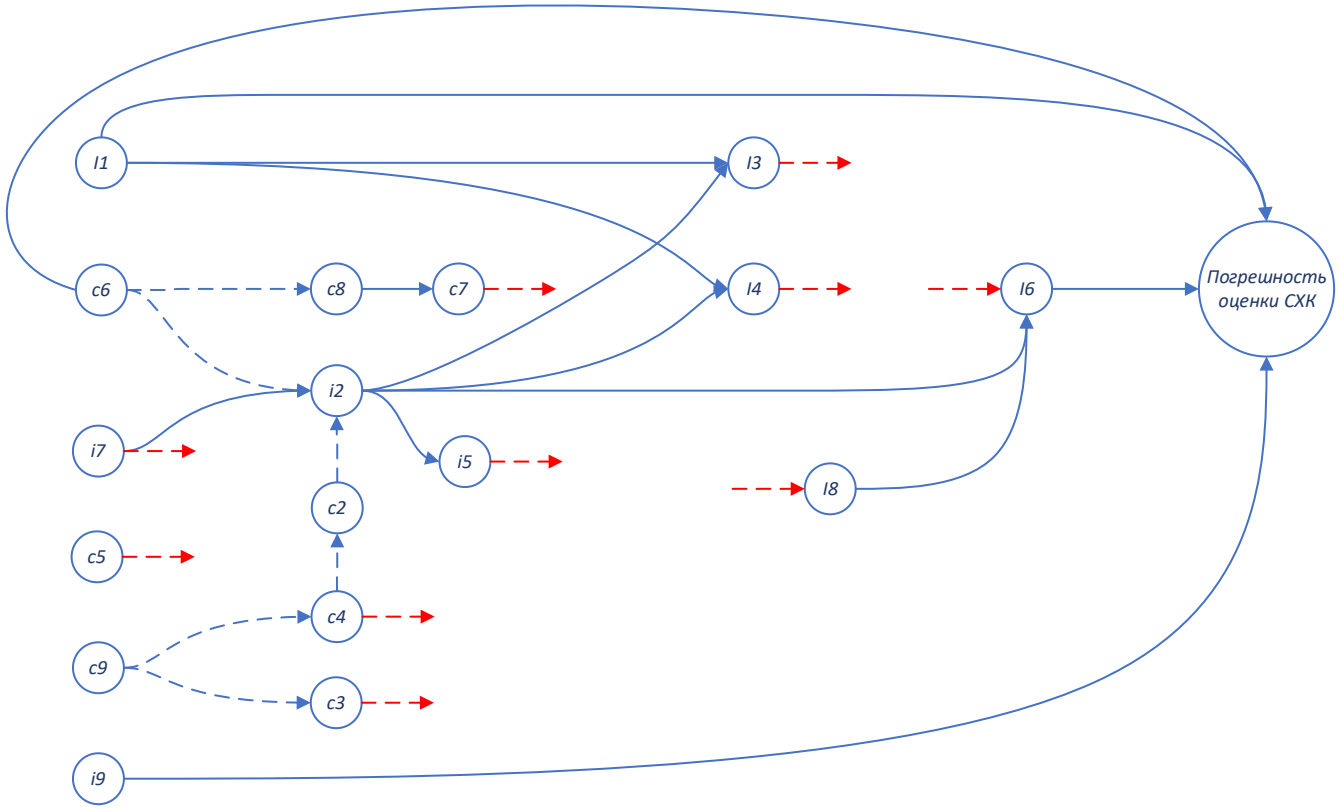
Нарушения конфиденциальности

- 3. Компрометация данных о СИИ
- 4. Компрометация данных третьих лиц, использованных при создании СИИ



ДЕГРАДАЦИЯ СУЩЕСТВЕННЫХ ХАРАКТЕРИСТИК КАЧЕСТВА И ВОЗРАСТАНИЕ ПОГРЕШНОСТИ ИХ ОЦЕНИВАНИЯ

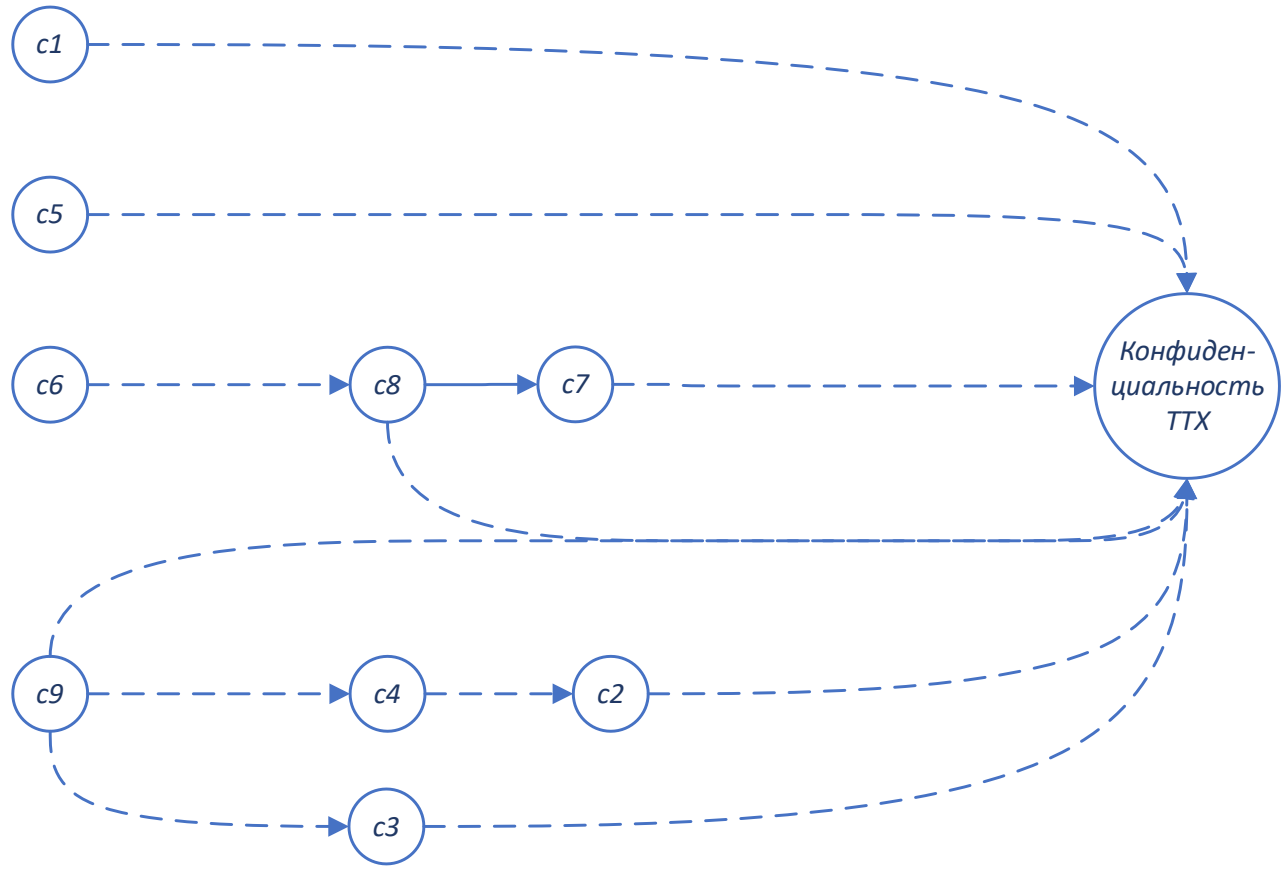


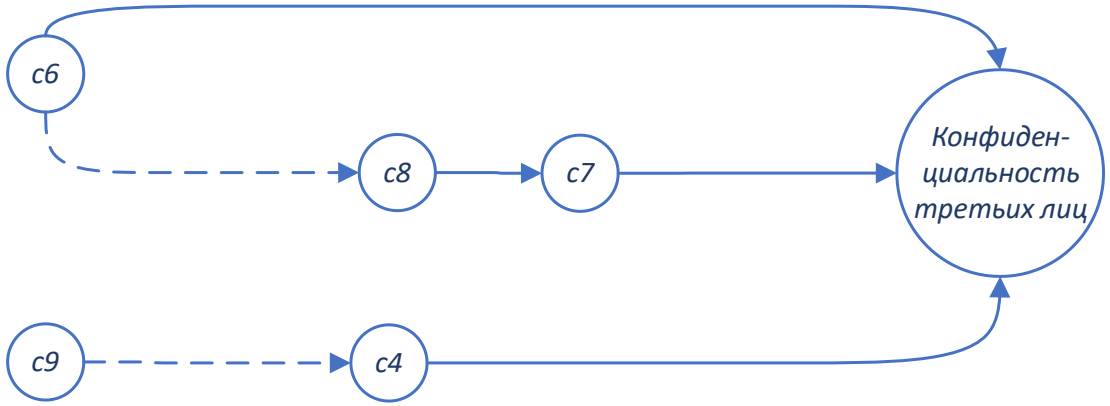


1. ФХ
2. предусмотренные условия эксплуатации
3. типовые модели МО, эталонные архитектуры
4. обучающие НД
5. спецификации требований к моделям МО
6. тестовые НД
7. данные для дообучения
8. исходные данные
9. результаты обработки

Связи, присутствующие в СИИ со злоумышленником

КОМПРОМЕТАЦИЯ СВЕДЕНИЙ О СИИ И О ТРЕТЬИХ ЛИЦАХ





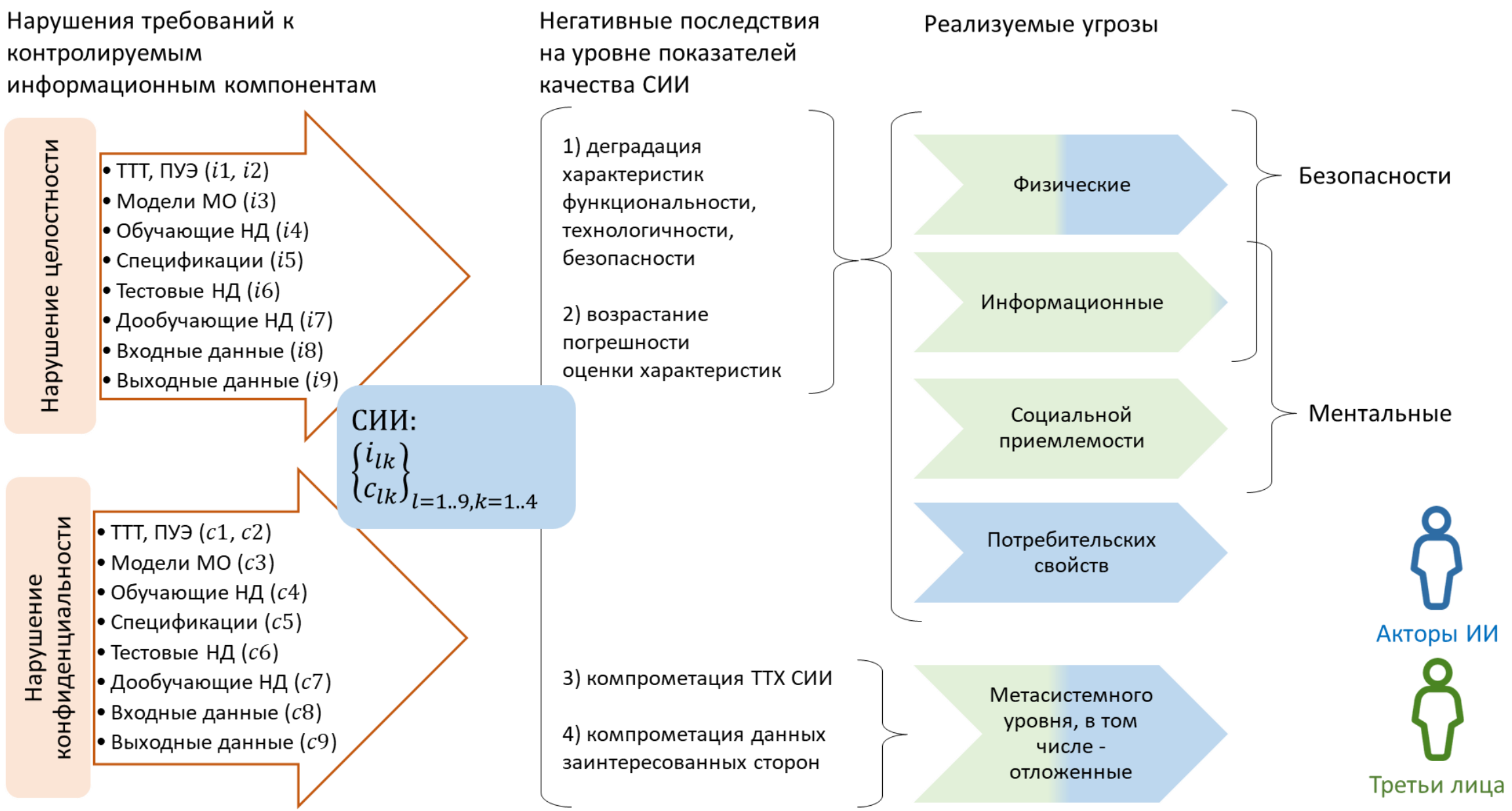
Связи, присутствующие в СИИ со злоумышленником

1. ФХ
2. предусмотренные условия эксплуатации
3. типовые модели МО, эталонные архитектуры
4. обучающие НД
5. спецификации требований к моделям МО
6. тестовые НД
7. данные для дообучения
8. исходные данные
9. результаты обработки

РИСКИ, ОБУСЛОВЛЕННЫЕ ДЕГРАДАЦИЕЙ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК ИИ

Вид угроз, обусловленных нарушением функциональной корректности СИИ	Категория заинтересованной стороны	
	Лица, непосредственно участвующие в создании и применении СИИ (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 в отношении заинтересованных сторон	Нет	2.2 Общество в целом и государственные регуляторы (защита персональных данных, предотвращение деструктивных информационно-психологических воздействий)
3 Нарушение этических и других норм «мягкого» права	Нет	3.2 Общество в целом (социальная приемлемость создания и применения СИИ)
4 Неопределенные потребительские свойства, не влияющие непосредственно на безопасность жизни и здоровья людей, экологическую безопасность	4.1 Потребители (функциональные характеристики, определяющие возможность применения СИИ по назначению), разработчики и поставщики (характеристики конкурентоспособности СИИ)	Нет

МОДЕЛЬ РИСКОВ ПРИ СОЗДАНИИ И ПРИМЕНЕНИИ СИИ



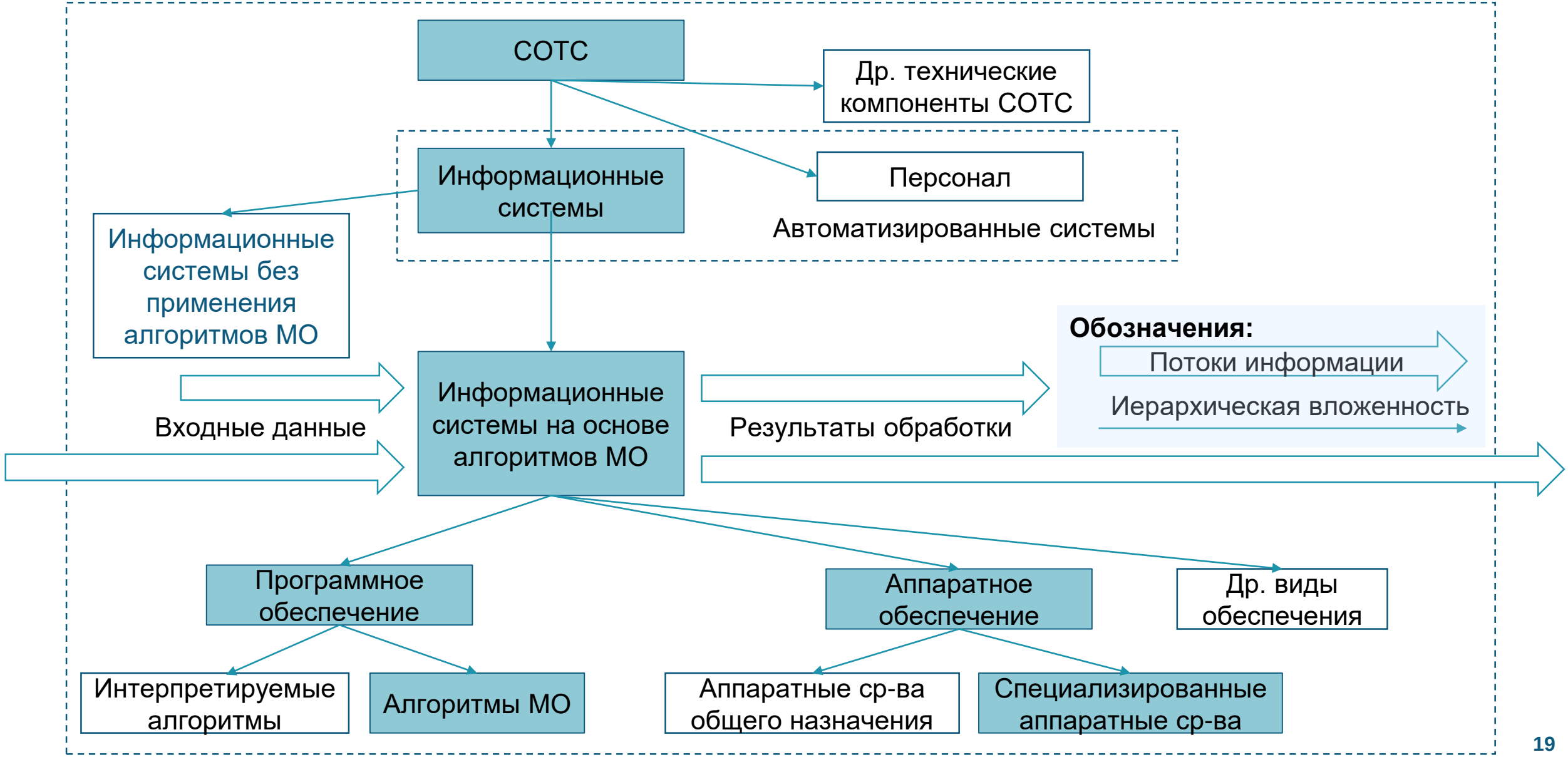
ПРЕДСТАВИТЕЛЬНЫЕ ИСПЫТАНИЯ ИИ

ОПРЕДЕЛЕНИЕ СОСТАВА СИСТЕМЫ ИИ В РАМКАХ СОТС

Принципы выделения минимальных уровней компонент, на которых полностью проявляются особенности реализации алгоритмов МО

- ясность и измеряемость показателей качества;
- соответствие устоявшимся понятиям и терминологии;
- возможность последующего уточнения, детализации;
- отсутствие перекрытия между используемыми показателями;
- выбор характеристик, позволяющих оценивать комплекс программ с позиции заказчика, пользователя, разработчика и управляющего проектом.

СТРУКТУРА СЛОЖНОЙ ОРГАНИЗАЦИОННО ТЕХНИЧЕСКОЙ СИСТЕМЫ (СОТС)



РАСПРЕДЕЛЕНИЕ ПОКАЗАТЕЛЕЙ ПО УРОВНЯМ ИЕРАРХИИ СИИ

Начало таблицы

Показатели СИИ		Уровни компонент, на которых определены показатели*)					
		1	2	3	4	5	6
Целостность КИК	$i1$ (ТТТ СИИ)					■	
	$i2$ (ПУЭ)	■					
	$i3$ (типовые модели машинного обучения)		■	■			
	$i4$ (обучающие НД)		■				
	$i5$ (спецификации требований к моделям МО)	■					
	$i6$ (тестовые НД)	■					
	$i7$ (данные для дообучения СИИ)		■				
	$i8$ (исходные данные)		■	■			
	$i9$ (результаты обработки)		■	■			
Конфиденциальность КИК	$c1$ (ТТТ СИИ)					■	
	$c2$ (ПУЭ)					■	
	$c3$ (типовые модели машинного обучения)					■	
	$c4$ (обучающие НД)					■	
	$c5$ (спецификации требований к моделям МО)					■	
	$c6$ (тестовые НД)					■	
	$c7$ (данные для дообучения СИИ)					■	
	$c8$ (исходные данные)					■	
	$c9$ (результаты обработки)					■	

Конец таблицы

Показатели СИИ		Уровни компонент, на которых определены показатели*)					
		1	2	3	4	5	6
СХК	$f_Ф$ (характеристики назначения – функциональные)	■					
	$f_Э$ (характеристики назначения – эксплуатационные)		■	■			
	$f_Т$ (технологичность)		■	■			
	$f_Б$ (безопасность)					■	
Последствия	Деградация СХК (назначения и технологичности)		■	■			
	Повышение погрешности оценки СХК		■	■			
	Компрометация данных СИИ						■
	Компрометация данных третьих лиц						■
Риски	Физические					■	
	Информационные				■		
	Социальной приемлемости				■		
	Экономические		■	■			

*) Иерархические уровни, на которых определены показатели СИИ: 1 – алгоритмы МО; 2 – ПО, реализующее алгоритмы МО; 3 – аппаратные средства, реализующие алгоритмы МО; 4 – информационные системы; 5 – СОТС в целом; 6 – метасистема (система более высокого уровня по отношению к СОТС).

УНИВЕРСАЛЬНЫЕ КЛАССЫ ЗАДАЧ ИИ
(ПО АНАЛОГИИ С ЕСТЕСТВЕННЫМ ИНТЕЛЛЕКТОМ ЧЕЛОВЕКА)

СФЭ ПРИ ИСПЫТАНИЯХ АЛГОРИТМОВ РАСПОЗНАВАНИЯ ДОРОЖНЫХ ЗНАКОВ

номенклатура и типоразмеры номеров, 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

НАЦИОНАЛЬНАЯ СИСТЕМА ОЦЕНКИ СООТВЕТСТВИЯ В ОБЛАСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Росстандарт

ТК164 — Технический Комитет 164

ГОСТ Р, ПНСТ

Перспективная программа стандартизации по приоритетному направлению «Искусственный интеллект»

Комплекс национальных стандартов в области ИИ

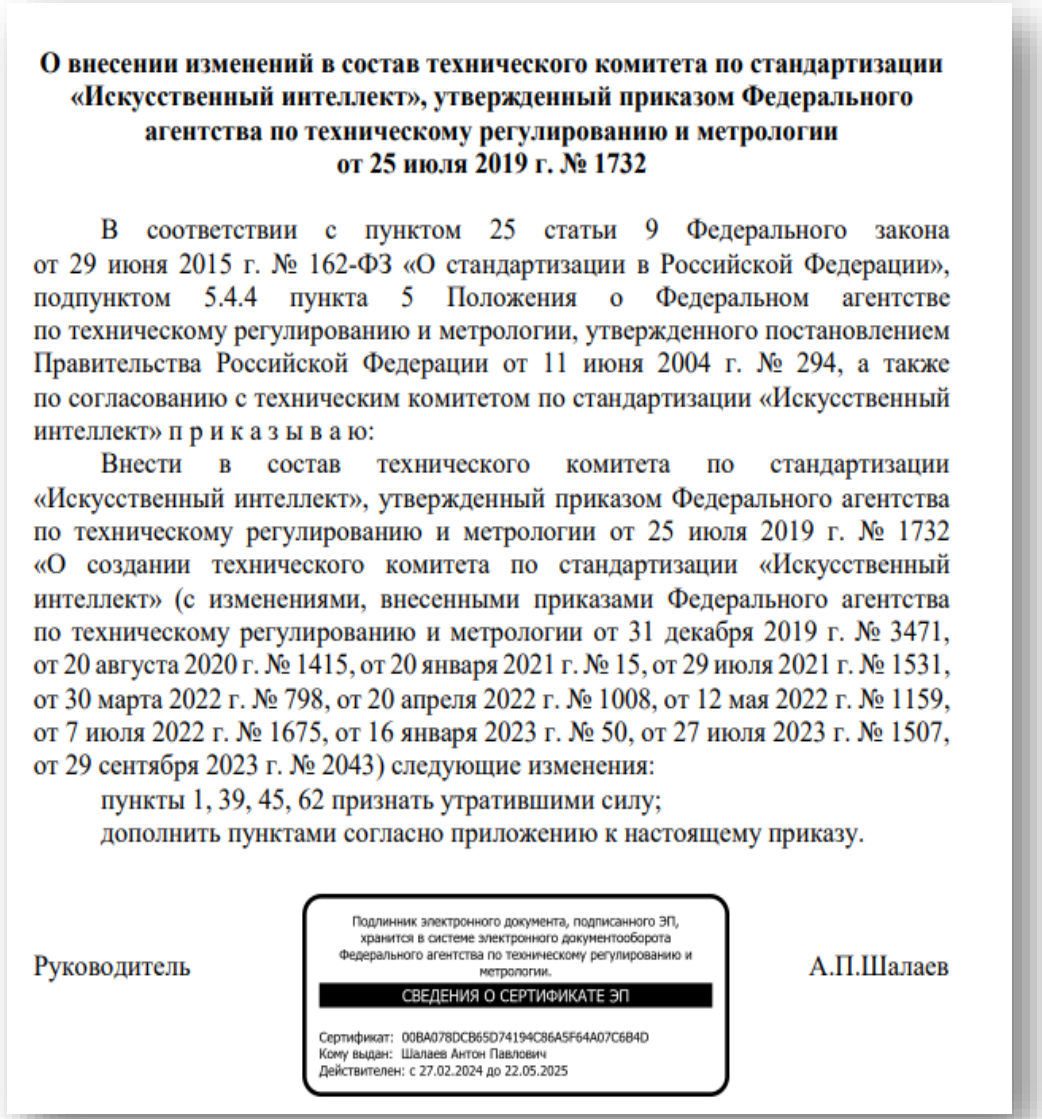
Информационный портал www.tc164.ru

Потребители и регуляторы ИИ

СДС «Интеллометрика»

Разработчики ИИ

СОСТАВ ТЕХНИЧЕСКОГО КОМИТЕТА (71 ОРГАНИЗАЦИЯ)



О внесении изменений в состав технического комитета по стандартизации «Искусственный интеллект», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 25 июля 2019 г. № 1732

В соответствии с пунктом 25 статьи 9 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации», подпунктом 5.4.4 пункта 5 Положения о Федеральном агентстве по техническому регулированию и метрологии, утвержденного постановлением Правительства Российской Федерации от 11 июня 2004 г. № 294, а также по согласованию с техническим комитетом по стандартизации «Искусственный интеллект» п р и к а з ы в а ю:

Внести в состав технического комитета по стандартизации «Искусственный интеллект», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 25 июля 2019 г. № 1732 «О создании технического комитета по стандартизации «Искусственный интеллект» (с изменениями, внесенными приказами Федерального агентства по техническому регулированию и метрологии от 31 декабря 2019 г. № 3471, от 20 августа 2020 г. № 1415, от 20 января 2021 г. № 15, от 29 июля 2021 г. № 1531, от 30 марта 2022 г. № 798, от 20 апреля 2022 г. № 1008, от 12 мая 2022 г. № 1159, от 7 июля 2022 г. № 1675, от 16 января 2023 г. № 50, от 27 июля 2023 г. № 1507, от 29 сентября 2023 г. № 2043) следующие изменения:

пункты 1, 39, 45, 62 признать утратившими силу;

дополнить пунктами согласно приложению к настоящему приказу.

Руководитель А.П.Шалаев

Подлинник электронного документа, подписанного ЭП, хранится в системе электронного документооборота Федерального агентства по техническому регулированию и метрологии.

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 00BA078DCB65D74194C86A5F64A07C6B4D
Кому выдан: Шалаев Антон Павлович
Действителен: с 27.02.2024 до 22.05.2025

23.08.2023 г. – 67 организаций

29.09.2023 г. – 69 организаций:

- ФГБУ «ВНИИИМТ» Росздравнадзора
- СПб ГУП «ГОРЭЛЕКТРОТРАНС»

12.04.2024 г. – 69 организаций:

- ФГАУ «ФЦПР ИИ»
- ФГАОУ ДПО АСМС
- ООО НТП «Криптософт»

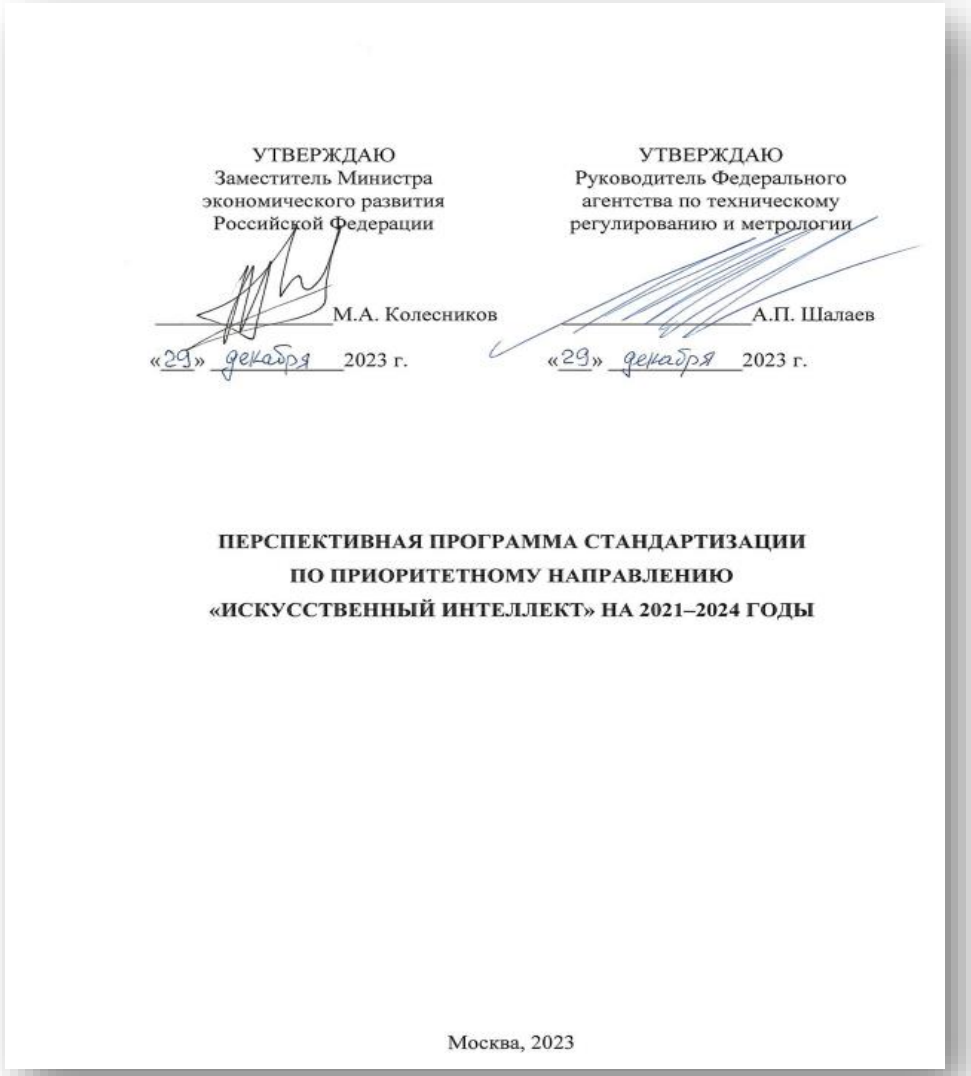
Перевели в ПК 02 «Данные»:

- ФГУП «СНПО «Элерон»
- ООО «РобоСиВи»
- ООО «Форексис»

28.07.2024 г. – 71 организация:

- ФГУП «РФЯЦ – ВНИИТФ им. академ. Е.И. Забабахина
- АО «НИИАС»

АКТУАЛИЗАЦИЯ ПЕРСПЕКТИВНОЙ ПРОГРАММЫ СТАНДАРТИЗАЦИИ ПО ПРИОРИТЕТНОМУ НАПРАВЛЕНИЮ «ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ»



УТВЕРЖДАЮ
Заместитель Министра
экономического развития
Российской Федерации

М.А. Колесников

«29» декабря 2023 г.

УТВЕРЖДАЮ
Руководитель Федерального
агентства по техническому
регулированию и метрологии

А.П. Шалаев

«29» декабря 2023 г.

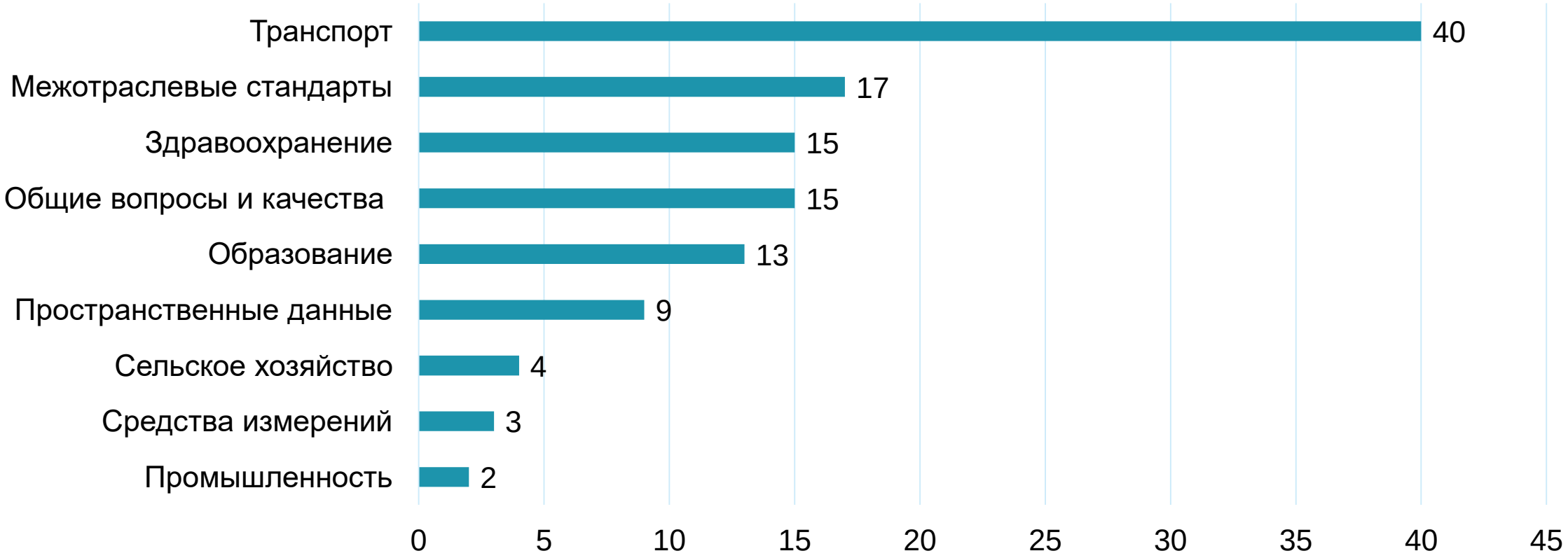
ПЕРСПЕКТИВНАЯ ПРОГРАММА СТАНДАРТИЗАЦИИ
ПО ПРИОРИТЕТНОМУ НАПРАВЛЕНИЮ
«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ» НА 2021–2024 ГОДЫ

Москва, 2023

29.12.2023 г. Минэкономразвития России и Росстандарт утверждена ППС по приоритетному направлению «Искусственный интеллект» на период 2021-2024 годов (далее – Программа) в обновленной редакции.

Разработка и актуализация Программы осуществляется в соответствии с результатом 5.2 «Разработка и актуализация комплекса стандартов в сфере ИИ», установленного в паспорте федерального проекта «Искусственный интеллект» национального проекта «Цифровая экономика Российской Федерации».

УТВЕРЖДЕННЫЕ СТАНДАРТЫ ИИ (ОКТЯБРЬ 2024)



СИСТЕМА ДОБРОВОЛЬНОЙ СЕРТИФИКАЦИИ «ИНТЕЛЛОМЕТРИКА»

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

Транспорт

РОСДОРНИИ

НАМИ

ГЭТ Электротранспорт Санкт-Петербурга

РЖД НИИАС

Здравоохранение

ЦЕНТР ДИАГНОСТИКИ И ТЕЛЕМЕДИЦИНЫ

Образование

Промышленность

ФГАУ «ФЦПР ИИ»

Энергетика

МЭИ

Сельское хозяйство

ВИМ

Следственная деятельность

Московская академия Следственного комитета имени А.Я. Сухарева

Специализированная техника

РОССПЕЦМАШ

ДСТ УРАЛ

Розничная торговля

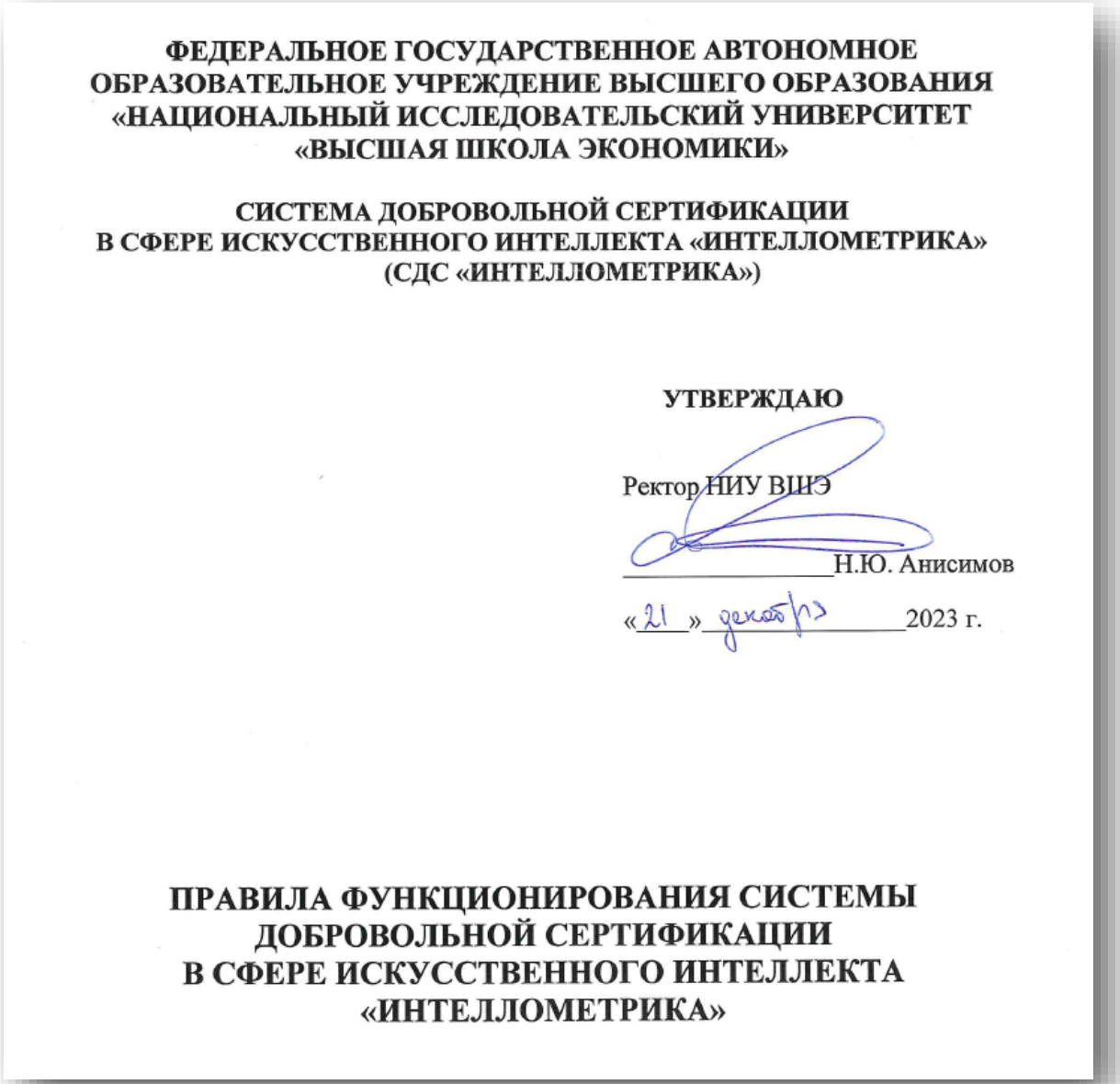
РУС СОФТ

АЙТИЛЛЕКТ Инструменты для бизнеса

*перечень органов по оценке соответствия не является исчерпывающим

ПРАВИЛА ФУНКЦИОНИРОВАНИЯ СДС «ИНТЕЛЛОМЕТРИКА»

Зарегистрирована Росстандартом в едином реестре систем добровольной сертификации 26.12.2023 (№ 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

УЧАСТИЕ В РАБОТАХ СДС «ИНТЕЛЛОМЕТРИКА»

Подготовка

Выявление объектов сертификации 1-ой очереди

Формализация областей допуска

Формирование частных методик испытаний ИИ

Заявка

Подготовка и направление в руководящий орган СДС «Интеллометрика» **заявки** на предоставление доступа к участию в работах СДС «Интеллометрика» в качестве **испытательной лаборатории** ИЛИ **органа по сертификации** и соответствующего комплекта документов

Допуск

Формирование комиссии по допуску участников СДС «Интеллометрика»

Проведение экспертизы (документарной и выездной) предоставленных заявителем документов на предмет соответствия критериям допуска

Выдача заявителю свидетельства о допуске к проведению работ в СДС «Интеллометрика»

Дальнейшая работа

Регулярный инспекционный контроль

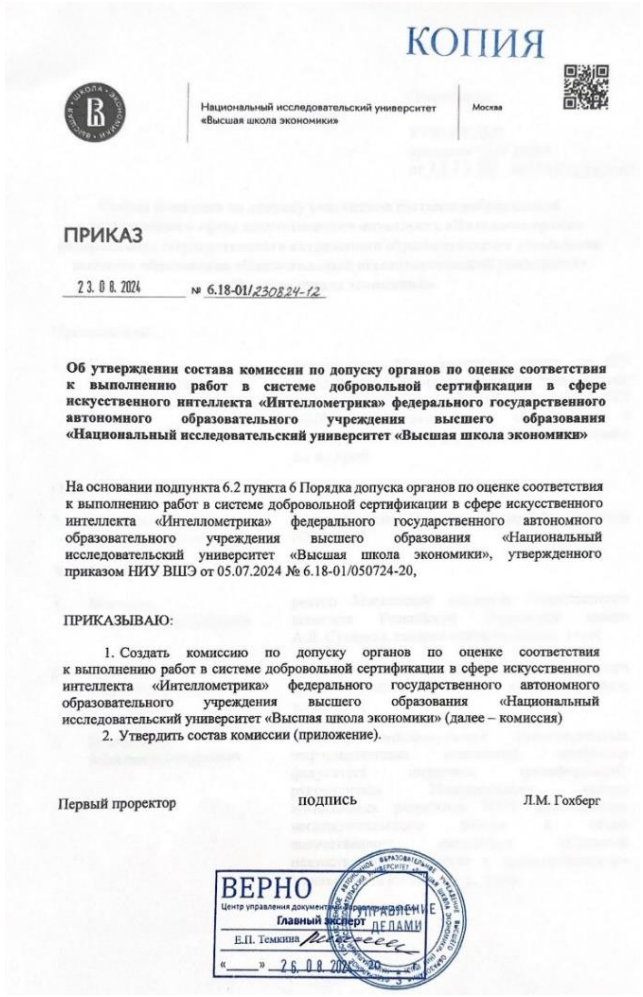
Ответственные

Заявитель + методическая поддержка РО СДС «Интеллометрика»

Заявитель

РО СДС «Интеллометрика»

ПЕРВОЕ ЗАСЕДАНИЕ КОМИССИИ ПО ДОПУСКУ УЧАСТНИКОВ СДС «ИНТЕЛЛОМЕТРИКА»



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
Центр управления документооборотом и делопроизводством
Главный эксперт
Е.П. Темкина
«23» 08 2024

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» (29.08.2024)

ВНИИМ 1842	ВНИИМ 1842	ДСТ УРАЛ	open{code:} открытый код
допущен в качестве **органа по сертификации** (1 год)	допущен в качестве **испытательной лаборатории** (1 год)	допущен в качестве **испытательной лаборатории** (1 год)	допущен в качестве **испытательной лаборатории** (6 мес.)
область допуска: интеллектуальные средства измерений и системы контроля на их основе	**область допуска:** системы автоматического контроля выбросов вредных веществ с применением искусственного интеллекта	**область допуска:** строительно-дорожная техника	**область допуска:** средства видеонаблюдения
12 из 12 проголосовали «ЗА»	*12 из 12 проголосовали «ЗА»*	*11 из 12 проголосовали «ЗА»*	*12 из 12 проголосовали «ЗА»*

СИИ С ГАРАНТИРОВАННОЙ ФУНКЦИОНАЛЬНОЙ КОРРЕКТНОСТЬЮ

- 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

www.tc164.ru