Санкт-Петербургский
Федеральный исследовательский центр
Российской академии наук

КОНСОРЦИУМ
ИССЛЕДОВАНИЙ
БЕЗОПАСНОСТИ
ТЕХНОЛОГИЙ
ИСКУССТВЕННОГО
ИНТЕЛЛЕКТА

От угроз к доверию: подход к формированию и поддержанию реестра доверенных технологий ИИ

Андрей Чечулин
МЦЦК, НИЛ ПКБ
СПб ФИЦ РАН

О себе

Должности:

- Руководитель **Международного центра цифровой криминалистики** СПб ФИЦ РАН
- Доцент **ФБИТ**, Университет ИТМО

Опыт:

- Проекты для компаний HP, Fsecure, Газинформсервис, Huawei и др.
- Проекты по прикладному использованию ИИ для задач информационной безопасности
- Судебные и досудебные экспертизы
- Расследование инцидентов безопасности
- Участник консорциума исследований безопасности технологий ИИ

К.т.н., доцент **Чечулин Андрей Алексеевич**

Хронология понятия доверия

10 октября 2019 г. - Указ Президента РФ № 490
Утверждена *Национальная стратегия развития искусственного интеллекта на период до 2030 года*, где в разделе III закреплены принципы:

- **Безопасность**: недопустимость использования ИИ для умышленного причинения вреда, предупреждение и минимизация рисков негативных последствий.
- **Прозрачность**: объяснимость работы ИИ и процесса достижения им результатов, недискриминационный доступ пользователей к информации о применяемых алгоритмах.

1 марта 2021 г. - Введение ГОСТ Р 59276-2020
Стандарт *«Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения»* определяет:

- Понятие доверия к ИИ как уверенность в способности системы выполнять возложенные задачи с требуемым качеством.
- Классификацию факторов, влияющих на доверие, и способы его обеспечения на различных стадиях жизненного цикла ИИ-систем.

26 октября 2021 г. - Принятие Кодекса этики в сфере ИИ
Кодекс устанавливает этические принципы для участников отношений в сфере ИИ, включая:

- **Человекоцентричность**: приоритет прав и свобод человека при разработке и применении ИИ.
- **Прозрачность и объяснимость**: необходимость обеспечения понятности работы ИИ-систем для пользователей.
- **Ответственность**: разработчики и пользователи ИИ несут ответственность за последствия его применения.

5 июля 2023 г. - Постановление Правительства РФ № 1161
«О перечне критических технологий Российской Федерации»

- Искусственный интеллект включён в **обновлённый перечень критических технологий**, утверждённый постановлением Правительства.
- Технологии ИИ признаны имеющими **стратегическое значение для безопасности и суверенитета страны**.

15 февраля 2024 г. - Указ Президента РФ № 124
Внесены изменения в Указ № 490 и Национальную стратегию развития ИИ, включая:

- **Целевой показатель**: к 2030 году уровень доверия граждан к технологиям ИИ должен вырасти до 80%.
- Усиление требований к прозрачности и объяснимости работы ИИ, а также доступу к информации о применяемых алгоритмах.
- Акцент на недопустимость использования ИИ в целях умышленного причинения вреда и минимизацию рисков негативных последствий.

2025 г. - Разработка методических рекомендаций по оценке доверия к ИИ
Минцифры России разрабатывает методические рекомендации, включающие:

- **Показатели доверия**: надежность, безопасность, объяснимость, соответствие нормативным требованиям.
- **Методики оценки**: процедуры валидации, верификации, аудита и мониторинга ИИ-систем.

Что такое доверенный ИИ?

ГОСТ Р 59276-2020. Национальный стандарт российской федерации. Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения.

- *3.3 доверие к системе искусственного интеллекта: Уверенность потребителя, и при необходимости, организаций, ответственных за регулирование вопросов создания и применения систем искусственного интеллекта, и иных заинтересованных сторон в том, что система способна выполнять возложенные на нее задачи с требуемым качеством.*
- *3.4 доверенная система искусственного интеллекта: Система искусственного интеллекта, в отношении которой потребитель и, при необходимости, организации, ответственные за регулирование вопросов создания и применения систем искусственного интеллекта, проявляют доверие.*

Указ Президента РФ от 15 февраля 2024 г. № 124
«О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. № 490»

- ц) доверенные технологии искусственного интеллекта - технологии, отвечающие стандартам безопасности, разработанные с учетом принципов объективности, недискриминации, этичности, исключающие при их использовании возможность причинения вреда человеку и нарушения его основополагающих прав и свобод, нанесения ущерба интересам общества и государства.".

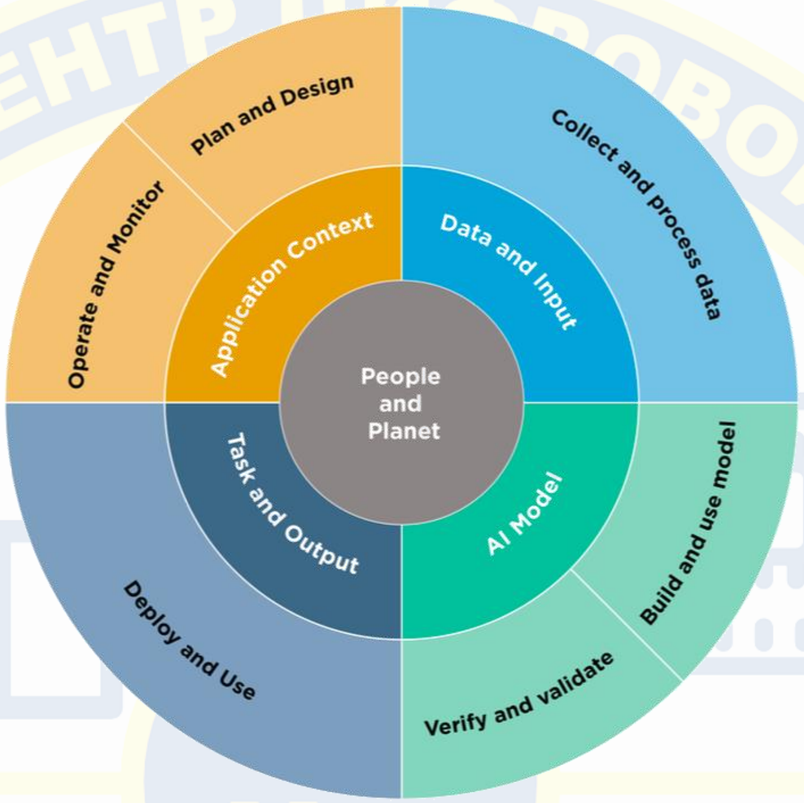
Элементы и жизненный цикл

Элементы

1. Данные
2. Модель
3. Алгоритмы
4. Программное обеспечение
5. Инфраструктура

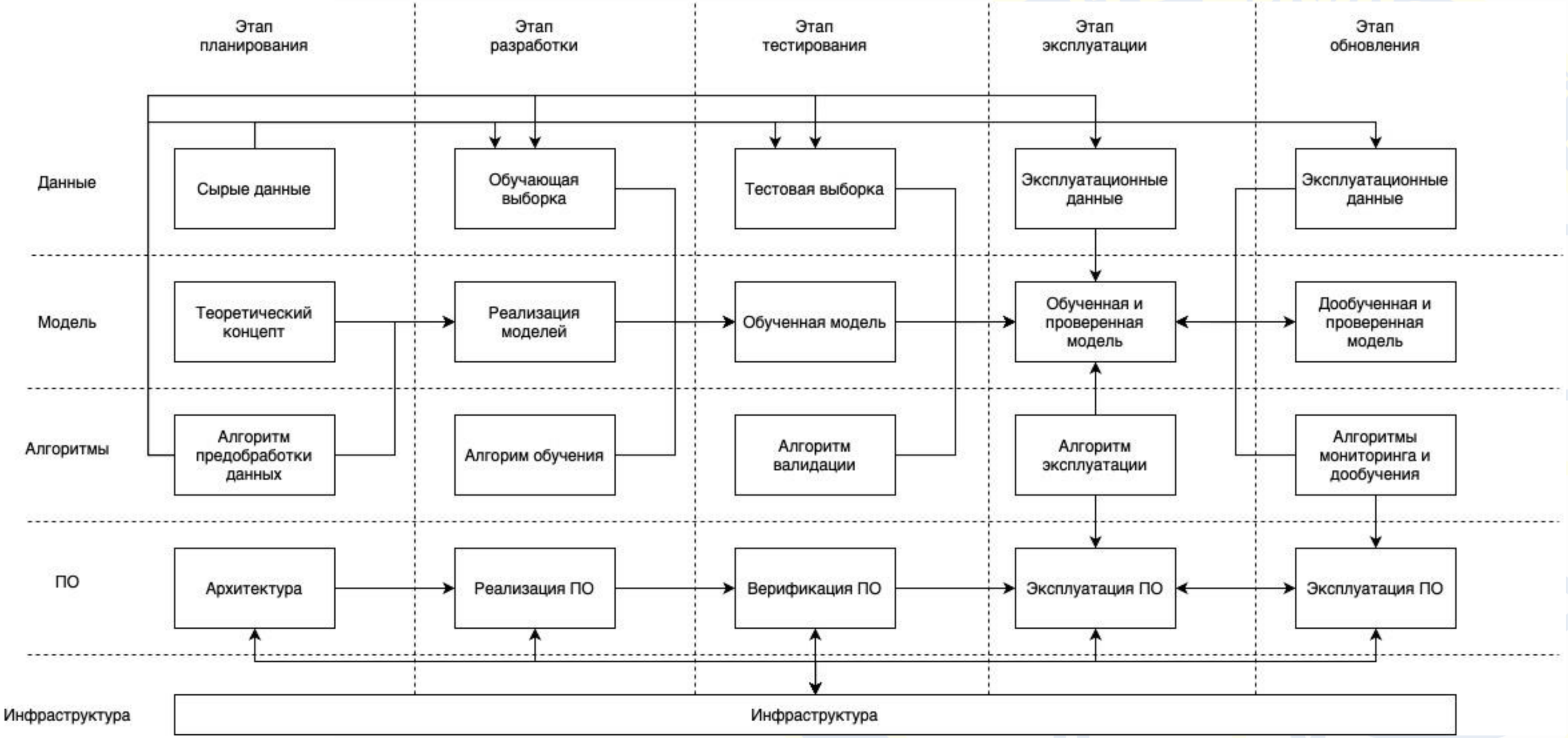
Жизненный цикл

1. Планирование и подготовка данных
2. Разработка
3. Тестирование
4. Эксплуатация
5. Обновление



NIST AI 100-1. Artificial Intelligence Risk Management Framework (AI RMF 1.0).

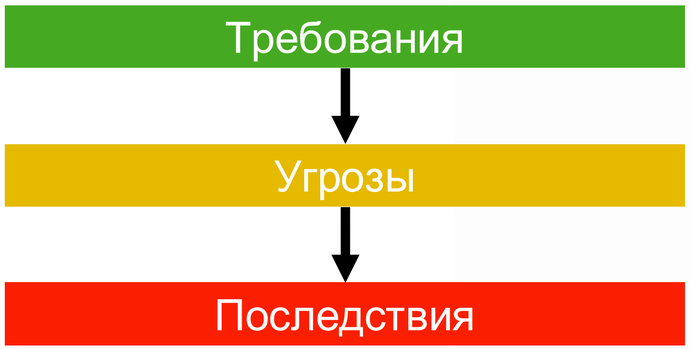
Взаимодействие элементов системы ИИ



Угрозы ИИ

Последствия

1. Целостность (корректность результатов)
2. Конфиденциальность (разглашение информации)
3. Доступность (работоспособность)
4. Доверенность (доверие к результату)



Риски (NIST AI Risk Management Framework)

Правильность и надёжность (Valid & Reliable)

1. Надежность (Safe)
2. Безопасность и устойчивость (Secure & Resilient)
3. Объяснимость и интерпретируемость (Explainable & Interpretable)
4. Приватность (Privacy-Enhanced)
5. Сбалансированность (Fair – With Harmful Bias Management)

Понятность (Accountable & Transparent)

Примеры угроз

Целостность (корректность результатов)
Конфиденциальность (разглашение информации)
Доступность (работоспособность)
Доверенность (доверие к результату)

	Планирование	Разработка	Тестирование	Эксплуатация	Обновление
Данные	**Сырые данные**	**Обучающая выборка**	**Тестовая выборка**	**Эксплуатационные данные**	**Эксплуатационные данные**
	Внедрение ложных данных	Отравление данных	Подмена тестовых данных	Манипулирование данными (Adversarial examples)	Введение ложных данных для переобучения
	Утечка исходных данных	Утечка персональных данных	Утечка тестового набора	Утечка данных пользователей	Утечка данных обновления
	Недоступность источников данных	Некорректная обучающая выборка	Потеря доступа к тестам	Утрата источника данных	Нарушение процесса сбора данных
	Использование предвзятых данных	Использование устаревших данных	Использование несоответствующих тестов	Неверный ввод данных	Использование несоответствующих данных
Модель	**Теоретический концепт**	**Реализация моделей**	**Обученная модель**	**Обученная и проверенная модель**	**Дообученная и проверенная модель**
	Выбор уязвимой архитектуры	Вредоносный код в модели	Модификация параметров модели	Изменение параметров модели	Внедрение вредоносных параметров
	Кража предварительных моделей	Кража обученной модели	Кража весов модели	Извлечение внутренней логики модели	Утечка обновлённых параметров
	Потеря проектной документации	Уязвимости в библиотеках	Удаление модели злоумышленниками	Атака на API модели	Сбой при обновлении модели
	Манипуляция рекомендациями	Ошибки реализации	Понижение качества обучения	Некорректные результаты работы модели	Понижение качества из-за неправильного обновления
Алгоритмы	**Предобработка данных**	**Обучение**	**Валидация**	**Эксплуатация**	**Мониторинг и дообучение**
	Некорректная обработка данных	Манипуляции градиентным спуском	Манипуляция метриками	Нарушение алгоритма обработки данных	Ошибки в алгоритмах мониторинга
	Отсутствие анонимизации	Извлечение данных обучения	Утечка данных валидации	Перехват запросов к модели	Утечка данных мониторинга
	Нехватка ресурсов	Сбой процесса обучения	Атаки на процесс проверки	Сбой в работе интерфейса API	Вывод из строя системы мониторинга
	Нарушение структуры данных	Некорректная настройка гиперпараметров	Использование ложных метрик	Вывод ложных результатов	Неправильный результат на основе устаревшей модели
ПО	**Архитектура**	**Реализация**	**Верификация**	**Эксплуатация**	**Эксплуатация**
	Ошибки в проектировании логики	Ошибки компиляции	Введение некорректных данных для проверки	Изменение функциональности ПО	Изменение функциональности ПО
	Утечка технической документации	Доступ к внутренним данным	Утечка данных тестирования	Утечка данных через ПО	Утечка данных через ПО
	Использование уязвимого фреймворка	Перегрузка системы	Блокировка процесса верификации	DDoS-атака на ПО	DDoS-атака на ПО
	Выбор неподходящей архитектуры	Использование недоверенных библиотек	Ошибки в процессе проверки	Устаревшая версия ПО	Устаревшая версия ПО

Решение – создание реестра

Цель: обеспечение доверия, прозрачности, надёжности и безопасности технологий ИИ, используемых в ГИС и КИИ за счет стандартизированного доступа к проверенным решениям.

Форма реализации: государственная информационная система — централизованная цифровая платформа, обеспечивающая:

- регистрацию;
- верификацию;
- тестирование;
- мониторинг ИИ-технологий.

Функции Реестра:

- формирование каталога проверенных технологий ИИ;
- подтверждение соответствия стандартам доверия;
- проведение тестирования моделей на киберполигоне;
- ведение банка данных угроз и уязвимостей:
- обеспечение взаимодействия с госорганами и системами.

Что включается в Реестр:

- наборы данных
- модели
- ПО (библиотеки, фреймворки и др.)

Критерии включения технологии ИИ в Реестр: технология ИИ должна соответствовать следующим **ключевым характеристикам доверия**:

- **безопасность** – соответствие требованиям защиты информации (в том числе 149-ФЗ, 187-ФЗ, ГОСТ Р 58412, ГОСТ Р 56939 и др.).
- **надёжность** – устойчивость к сбоям, корректность выполнения задач в штатных и стрессовых условиях.
- **прозрачность** – документированность процессов разработки, обучения, внедрения, описание архитектуры и ограничений.
- **этичность и законность** – отсутствие вреда человеку и обществу, соблюдение прав, исключение дискриминации.
- **соответствие нормативам** – выполнение стандартов и методик, утверждённых Минцифры РФ.

Но как быть, когда требования по доверенности для разных областей применения различаются?

Решение – балльная система оценки

Для наборов данных

Группа угроз	Угрозы	Связанные критерии оценки
1. Надёжность и достоверность источников	Внедрение ложных данных; Неверный ввод данных; Отравление данных; Подмена тестовых данных; Внедрение ложных данных для переобучения	1. Владелец; 5. Аудит данных
2. Прозрачность и доступность данных	Недоступность источников данных; Утрата источника данных; Потеря доступа к тестам; Нарушение процесса сбора данных	2. Прозрачность источников; 5. Аудит данных
3. Конфиден-циальность и защита информации	Утечка исходных данных; Утечка персональных данных; Утечка тестового набора; Утечка данных пользователей; Утечка данных обновления	3. Соответствие нормативным требованиям
4. Репрезен-тативность и релевантность данных	Использование предвзятых данных; Некорректная обучающая выборка; Использование несоответствующих тестов; Использование несоответствующих данных	4. Репрезен-тативность данных
5. Актуальность и своевременность	Использование устаревших данных	2. Прозрачность источников; 4. Репрезен-тативность данных
6. Угрозы, связанные с атакующими воздействиями	Манипулирование данными (adversarial examples)	5. Аудит данных

1. Владелец.
- **Плохо.** Владелец неизвестен, нет лицензий, нет истории успешных проектов.
- **Средне.** Владелец известен, но без подтвержденных аудитов или лицензий.
- **Хорошо.** Владелец, имеющий историю надежных поставок данных, аудиты, сертификаты и лицензии.

2. Прозрачность источников (открытость, доступность исходных наборов данных)
- **Плохо.** Источники данных неизвестны, данные могли быть получены незаконно.
- **Средне.** Источники известны, но не открыты для проверки.
- **Хорошо.** Полная прозрачность источников, есть возможность повторного сбора данных.

3. Соответствие нормативным требованиям (GDPR, ФЗ-152, ISO 27001 и др.)
- **Плохо.** Данные явно нарушают нормативные требования, возможны юридические риски.
- **Средне.** Данные частично соответствуют нормам, но без официального подтверждения.
- **Хорошо.** Полностью соответствуют нормам, есть юридические обоснования и сертификаты.

4. Репрезентативность данных (насколько набор данных соответствует задаче, вариативность данных).
- **Плохо.** Данные не соответствуют задаче, предусмотренной в условиях эксплуатации, или имеют значительные пробелы.
- **Средне.** Данные частично покрывают задачу, но есть недостаток примеров или смещенности.
- **Хорошо.** Набор данных полноценно и равномерно покрывает все необходимые сценарии, предусмотренной в условиях эксплуатации.

5. Аудит данных.
- **Плохо.** Данные не проверялись.
- **Средне.** Данные прошли проверку на автоматизированном полигоне.
- **Хорошо.** Данные проверены сертифицированной лабораторией или в органе по сертификации.

Каждый набор данных оценивается по шкале от 0 до 2 на основе перечисленных критериев.

Оценка доверия к данным:

$D = (w_{d1} C_{d1} + w_{d2} C_{d2} + w_{d1} C_{d3} + w_{d4} C_{d4} + w_{d5} C_{d5})$

где:
- C_{d1} – характеристика владельца данных [0-2],
- C_{d2} – характеристика прозрачности источников [0-2],
- C_{d3} – характеристика соответствия нормативным требованиям [0-2],
- C_{d4} – характеристика репрезентативности данных [0-2],
- C_{d5} – характеристика аудита данных [0-2],
- w_{d1} , w_{d2} , w_{d3} , w_{d4}, w_{d5} – весовые коэффициенты критериев [0..1], при этом $w_{d1} + w_{d2} + w_{d3} + w_{d4} + w_{d5} = 1$

Результат:
- **Уровень [0–1)**: низкий уровень доверенности, неизвестное происхождение, отсутствие проверок, высокий риск использования.
- **Уровень [1–2)**: средний уровень доверенности, проверка проводилась, но не хватает сертификации и независимого тестирования.
- **Уровень 2**: максимальная доверенность, полная сертификация, независимая проверка, подтвержденное соответствие стандартам.

Решение – балльная система оценки

Для моделей

Группа угроз	Угрозы	Связанные критерии оценки
1. Уязвимости проектирования	Выбор уязвимой архитектуры; Кража предварительных моделей; Потеря проектной документации	1. Владелец; 2. Доступность кода и структуры модели
2. Вредоносная реализация	Вредоносный код в модели; Внедрение вредоносных параметров	2. Доступность кода и структуры модели; 5. Устойчивость к атакам
3. Нарушение конфиденциальности	Кража обученной модели; Кража весов модели; Извлечение внутренней логики модели; Утечка обновлённых параметров	1. Владелец; 4. Соответствие нормативным требованиям
4. Уязвимости компонентов	Уязвимости в библиотеках; Удаление модели злоумышленниками; Атака на API модели; Сбой при обновлении модели	3. Оценка функциональной корректности; 5. Устойчивость к атакам
5. Ошибки и непредсказуемое поведение	Ошибки реализации; Понижение качества обучения; Некорректные результаты работы модели; Понижение качества из-за неправильного обновления	3. Оценка функциональной корректности; 6. Надежность и предсказуемость работы

1. Владелец.
- **Плохо.** Владелец неизвестен, нет лицензий, нет истории успешных проектов.
- **Средне.** Владелец известен, но без подтвержденных аудитов или лицензий.
- **Хорошо.** Владелец, имеющий историю надежных поставок моделей, аудиты, сертификаты и лицензии.

2. Доступность кода и структуры модели
- **Плохо**. Модель закрытая, неизвестны алгоритмы.
- **Средне**. Описание модели частично доступно, но код закрыт.
- **Хорошо**. Полная документация и открытый код.

3. Оценка функциональной корректности.
- **Плохо**. Модель не проверялись или проверялась только разработчиком.
- **Средне**. Модель прошла проверку на автоматизированном полигоне.
- **Хорошо**. Модель проверены испытательной лабораторией или в органе по сертификации.

4. Соответствие нормативным требованиям
- **Плохо**. Модель явно нарушает нормативные требования, возможны юридические риски. Или не проверялась.
- **Средне**. Модель частично соответствуют нормам, но без официального подтверждения.
- **Хорошо**. Модель полностью соответствует нормам, есть юридические обоснования и сертификаты.

5. Устойчивость к атакам
- **Плохо**. Модель не проверялись или проверялась только разработчиком.
- **Средне**. Модель прошла проверку на автоматизированном полигоне.
- **Хорошо**. Модель проверены испытательной лабораторией или в органе по сертификации.

6. Надежность и предсказуемость работы
- **Плохо**. Результаты нестабильны, модель работает непредсказуемо.
- **Средне**. Модель прошла проверку на автоматизированном полигоне.
- **Хорошо**. Модель проверены испытательной лабораторией или в органе по сертификации.

Каждая модель оценивается по шкале от 0 до 2 на основе перечисленных критериев.

Оценка доверия к моделям:

$M = (w_{m1} C_{m1} + w_{m2} C_{m2} + w_{m1} C_{m3} + w_{m4} C_{m4} + w_{m5} C_{m5} + w_{m6} C_{m6})$

где:
- C_{m1} – характеристика владельца ПО [0-2],
- C_{m2} – характеристика доступности кода и логики работы [0-2],
- C_{m3} – характеристика устойчивости к атакам [0-2],
- C_{m4} – характеристика соответствия нормативным требованиям [0-2],
- C_{m5} – характеристика устойчивости к атакам [0-2],
- C_{m6} – характеристика надежности и предсказуемости работы [0-2],
- w_{m1} , w_{m2} , w_{m3} , w_{m4} , w_{m5} , w_{m6} – весовые коэффициенты критериев [0..1], при этом $w_{m1} + w_{m2} + w_{m3} + w_{m4} + w_{m5} + w_{m6} = 1$

Результат:
- **Уровень [0–1)**: низкий уровень доверенности, неизвестное происхождение, отсутствие проверок, высокий риск использования.
- **Уровень [1–2)**: средний уровень доверенности, проверка проводилась, но не хватает сертификации и независимого тестирования.
- **Уровень 2**: максимальная доверенность, полная сертификация, независимая проверка, подтвержденное соответствие стандартам.

Решение – балльная система оценки

Для ПО

Группа угроз	Угрозы	Связанные критерии оценки
1. Ошибки проектирования и архитектуры	Ошибки в проектировании логики; Выбор неподходящей архитектуры	1. Владелец; 2. Доступность кода и логики работы
2. Нарушения конфиденциальности	Утечка технической документации; Доступ к внутренним данным; Утечка данных тестирования; Утечка данных через ПО	2. Доступность кода и логики работы; 4. Соответствие нормативным требованиям
3. Уязвимости реализации и библиотек	Использование уязвимого фреймворка; Использование недоверенных библиотек; Перегрузка системы	1. Владелец; 3. Устойчивость к атакам
4. Проблемы валидации и проверки	Ошибки компиляции; Введение некорректных данных для проверки; Ошибки в процессе проверки; Блокировка процесса верификации	3. Устойчивость к атакам; 5. Возможность защиты модели
5. Угрозы в эксплуатации	Изменение функциональности ПО; DDoS-атака на ПО; Устаревшая версия ПО	3. Устойчивость к атакам; 4. Соответствие нормативным требованиям

1. Владелец.
- **Плохо.** Владелец неизвестен, нет лицензий, нет истории успешных проектов.
- **Средне.** Владелец известен, но без подтвержденных аудитов или лицензий.
- **Хорошо.** Владелец, имеющий историю надежных поставок ПО, аудиты, сертификаты и лицензии.

2. Доступность кода и логики работы
- **Плохо.** Код закрыт, нет информации о внутренней логике работы.
- **Средне.** Код частично открыт, но важные компоненты скрыты.
- **Хорошо.** Полностью открытый исходный код, доступный для аудита.

3. Устойчивость к атакам
- **Плохо.** ПО не проверялось или проверялась только разработчиком.
- **Средне.** ПО прошло проверку на автоматизированном полигоне.
- **Хорошо.** ПО проверено испытательной лабораторией или в органе по сертификации.

4. Соответствие нормативным требованиям
- **Плохо.** ПО явно нарушает нормативные требования.
- **Средне.** ПО частично соответствуют нормам, но без официального подтверждения.
- **Хорошо.** ПО полностью соответствует нормам, есть обоснования и сертификаты.

5. Возможность защиты модели.
- **Плохо.** ПО принимает любые данные без проверки.
- **Средне.** Есть минимальные механизмы валидации, но они не защищают от атак.
- **Хорошо.** Встроенные механизмы защиты от атакующих данных и некорректных входных данных.

Каждый экземпляр ПО оценивается по шкале от 0 до 2 на основе перечисленных критериев.

Оценка доверия к ПО:

$$S = (w_{s1}\, C_{s1} + w_{s2}\, C_{s2} + w_{s1}\, C_{s3} + w_{s4}\, C_{s4} + w_{s5}\, C_{s5})*3$$

где:
- C_{s1} – характеристика владельца модели [0-2],
- C_{s2} – характеристика доступности кода и структуры модели [0-2],
- C_{s3} – характеристика устойчивости к атакам [0-2],
- C_{s4} – характеристика соответствия нормативным требованиям [0-2],
- C_{s5} – характеристика валидации данных перед использованием [0-2],
- w_{s1} , w_{s2} , w_{s3} , w_{s4} , w_{s5} – весовые коэффициенты критериев [0..1], при этом $w_{s1} + w_{s2} + w_{s3} + w_{s4} + w_{s5} = 1$

Результат:
- **Уровень [0–1)**: низкий уровень доверенности, неизвестное происхождение, отсутствие проверок, высокий риск использования.
- **Уровень [1–2)**: средний уровень доверенности, проверка проводилась, но не хватает сертификации и независимого тестирования.
- **Уровень 2**: максимальная доверенность, полная сертификация, независимая проверка, подтвержденное соответствие стандартам.

Решение – балльная система оценки

Для систем, использующих элементы ИИ

Оценка (0–6)	Уровень доверия	Описание	Примеры
6	Максимальный	Использование в критических условиях без ограничений	Автопилоты, медицинские ИИ-диагносты, оборонные ИИ, системы управления КИИ
5	Повышенный	Допуск в автоматизированные системы с ограниченным ручным контролем	Финансовый скоринг, судебные ИИ, системы биометрической идентификации
4	Стандартный	Использование в некритичных прикладных задачах	ИИ-помощники в документообороте, персонализированное обучение
3	Ограниченный	Только в контролируемых средах, возможно с уведомлением пользователя	Рекомендательные системы, чат-боты, фильтрация контента
2-1	Эксперимен-тальный	Не использовать в продуктах системах	Исследовательские прототипы, тестовые sandbox-среды
0	Нулевой (запрещён)	Запрет на эксплуатацию до прохождения оценки и устранения уязвимостей	

Итог

Реестр доверенных технологий ИИ должен стать открытым каталогом, где:

- разработчики могут свободно вносить свои решения, получая объективную оценку доверенности;
- государственные организации и компании самостоятельно определяют минимально допустимый уровень доверенности при использовании решений в ГИС, КИИ и других критически важных системах;
- система автоматизированного тестирования обеспечивает прозрачность и объективность оценки технологий.

Каждая система оценивается по наименее доверенным экземплярам данных, моделей и ПО, которые в ней используются. Интегральная оценка выставляется по шкале от 0 до 6 на основе перечисленных ранее оценок.

Оценка доверия к системе:
Общий уровень доверия к реализации оценивается по шкале от 0 до 6 на основе доверия к элементам

$$TS = (w_d D + w_m M + w_s C) * 3$$

где:

- D – минимальная оценка доверия к данным
- M – минимальная оценка доверия к моделям
- S – минимальная оценка доверия к ПО
- w_d , w_m , w_s – весовые коэффициенты областей доверия [0..1], при этом $w_d + w_m + w_s = 1$

Результат:

- **Уровень [0–2):** низкий уровень доверенности, неизвестное происхождение, отсутствие проверок, высокий риск использования.
- **Уровень [2–4):** базовый уровень доверенности, проверка проводилась, но не хватает сертификации и независимого тестирования.
- **Уровень [4–6):** высокий уровень доверенности, проведены независимые тесты, верификация и аудит.
- **Уровень 6:** максимальная доверенность, полная сертификация, независимая проверка, подтвержденное соответствие стандартам.

Визуализация счастливого будущего

Санкт-Петербургский
Федеральный исследовательский центр
Российской академии наук

Контакты

Международный центр цифровой криминалистики

https://indiforce.ru

Россия, 199178, Санкт-Петербург,
14-я линия В.О., д.39
+7-(812)-328-7181

Руководитель МЦЦК СПб ФИЦ РАН

Андрей Чечулин

chechulin@indiforce.ru