Observatoire ARGA

МЕЖДУНАРОДНЫЙ АНАЛИТИЧЕСКИЙ ДОКЛАД

Исследование №17

Международные стандарты оценки соответствия, сертификации и аккредитации

AI Assurance: доказательственная надёжность, аккредитационный статус и пределы взаимного признания

Организация: Observatoire ARGA

Русская версия

21 rue de l’Aviation, 64600 Anglet, France

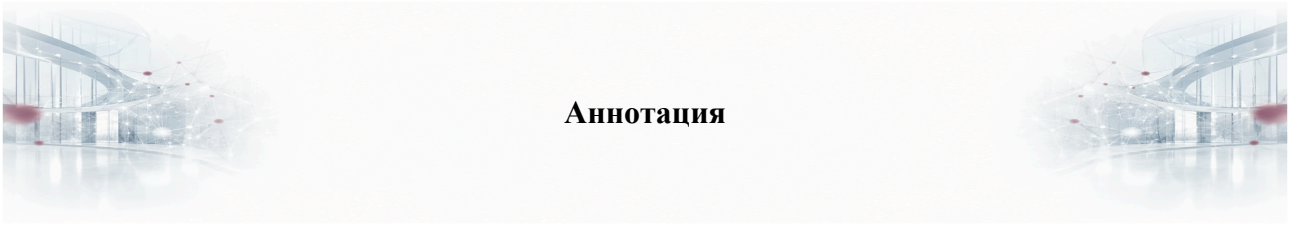
info@argaobservatory.org | www.argaobservatory.org

21 октября 2026 года

Содержание

Аннотация — 3
Научные основания и исследовательский дизайн — 4
1. Предмет AI Assurance и исследовательский вопрос — 6
2. Терминология и система уровней оценки — 8
3. Объект подтверждения и карта утверждений — 11
4. Доказательственная архитектура AI Assurance — 13
5. Институциональная инфраструктура качества — 16
6. ISO/IEC 42001:2023: система менеджмента ИИ — 18
7. ISO/IEC 42006:2025: качество органа сертификации AIMS — 19
8. ISO/IEC 17021-1:2015 и методология сертификационного аудита — 21
9. ISO/IEC 17065:2012: сертификация продукта, процесса или услуги — 23
10. Лабораторные испытания, ISO/IEC 17025 и техническая неопределённость — 25
11. ISO/IEC 17029:2019 и специальная проверка заявлений — 27
12. ISO/IEC 17011 и аккредитация органов оценки соответствия — 29
13. Глобальная система взаимного признания: переход 2026 года — 31
14. Европейское аккредитационное пространство: Regulation 765/2008 и EA MLA — 33
15. EU AI Act: редакция 2026 года и календарь применения — 35
16. Классификация высокорисковых систем и выбор маршрута — 37
17. Annex VI: внутренний контроль без нотифицированного органа — 40
18. Annex VII: участие нотифицированного органа и техническое досье — 41
19. Нотифицированные органы: назначение, компетентность и контроль — 43
20. Гармонизированные стандарты, общие спецификации и презумпции — 45
21. Декларация ЕС, сертификат и маркировка CE — 47
22. Техническая документация, система качества и прослеживаемость — 48
23. Проектирование технических испытаний и границы статистики — 50
24. Предвзятость, основные права и оценка воздействия — 53
25. Робастность, кибербезопасность и внешние зависимости — 55
26. Генеративный ИИ, модели общего назначения и специфика оценки — 57
27. Непрерывный мониторинг, существенные изменения и отзыв — 59
28. Великобритания: регулируемый рынок AI Assurance и UKAS — 61
29. США: NIST, добровольные рамки и отраслевой контекст — 63
30. Сингапур и инструменты AI Verify — 65
31. ОЭСР, должная осмотрительность и негосударственные стандарты — 67
32. Закупка AI Assurance и проверка контрагентов — 70
33. Конфиденциальность, персональные данные и доступ к модели — 72
34. Отраслевые сценарии: банки, санкции, международное сотрудничество — 74
35. Кейс-стади: юридический помощник и пределы сертификации — 76
Проверка достаточности условного досье юридического помощника — 77
36. Предлагаемая институциональная программа Observatoire ARGA — 78

37. Заключение и пределы международного взаимного признания — 80
Приложение 1. Паспорт утверждения и результата AI Assurance — 82
Приложение 2. Протокол проверки подлинности и области сертификата — 84
Приложение 3. Карта регуляторного маршрута по AI Act (редакция 2026) — 86
Приложение 4. Функциональная карта стандартов ISO/IEC и источников ЕС — 88
Приложение 5. Модельный протокол испытания санкционных совпадений — 89
Приложение 6. Статистическая неопределённость: воспроизводимые учебные расчёты — 90
Приложение 7. Реестр доказательств для ограниченного независимого анализа — 91
Приложение 8. Образец ограниченного экспертного заключения — 93
Приложение 9. Договорные условия для внешней оценки ИИ — 94
Приложение 10. Форма оценки независимости исполнителя — 96
Приложение 11. Программа мониторинга сертификата и триггеры переоценки — 98
Приложение 12. Проект институциональных предложений Observatoire ARGA — 100
Приложение 13. Проект универсального паспорта AI Assurance — 102
Приложение 14. Матрица принятия решений по сертификатам и свидетельствам — 103
Приложение 15. Рабочий протокол правовой квалификации по EU AI Act — 104
Приложение 16. Матрица независимости и контроля качества оценочной команды — 105
Приложение 17. Контрольный протокол для AI-систем санкционного скрининга — 106
Приложение 18. Технический протокол для генеративного юридического помощника — 107
Приложение 19. Договорное приложение о воспроизводимости и хранении доказательств — 109
Приложение 20. Программа документального мониторинга после AI Assurance — 110
Практический указатель рекомендаций — 111
Источники и указатель оснований — 113



Аннотация

Доклад исследует, какие доказательства позволяют обоснованно подтвердить конкретное свойство ИИ и какой юридический смысл имеет полученное подтверждение. AI Assurance рассматривается как совокупность исследовательских и организационных процедур с различными предметами: процесс управления, техническое свойство системы, отдельное заявление или компетентность оценщика. Центральный результат — методика проверки соответствия между обещанием, фактически исследованным объектом и допустимым выводом. Она объединяет метрологию, статистику, теорию управления качеством и сравнительный правовой анализ. [M1–M2]

Нормативная часть разграничивает аудит, испытание, верификацию, сертификацию, аккредитацию и нотификацию, а также рассматривает редакцию AI Act 2026 года и стандарты оценки соответствия. Научно-методологическая часть раскрывает, как определить измеряемое свойство, учесть неопределённость, проверить правило решения и оценить устойчивость классификации свидетельств. Для практического применения разработан

разбор условного досье юридического помощника: сертификат системы менеджмента сопоставляется с техническим испытанием, заявлением о качестве ссылок и границами предполагаемого использования. [1–8; 21–28; 32; M1–M2]

Основной вывод: пригодность заверения устанавливается по содержательной связи между критерием, методом и решением. Документ об организации процессов не подтверждает автоматически качество каждого ответа; успешный тест отдельной функции не устанавливает законность всего применения. Для ARGA предлагается исследовательская программа проверки достаточности свидетельств, включающая независимую квалификацию материалов, правило обращения с противоречиями и пилотную проверку воспроизводимости экспертного вывода.

Область, метод и ограничения

Доклад рассматривает состояние общедоступных нормативных и институциональных источников по состоянию на 21 октября 2026 года. Нормы ЕС анализируются по консолидированному акту на 27 июля 2026 года и официальным карточкам статей; профессиональные стандарты ISO/IEC - по опубликованным описаниям их предмета и статуса. Полные платные тексты стандартов не получались; поэтому ни одна таблица настоящего доклада не выдаёт авторскую методику за дословное воспроизведение пункта стандарта. Правовые последствия конкретного сертификата устанавливаются с учётом категории системы и применимых законов. [1-3,21-31]

Содержательные модели, условные числовые примеры, анкеты и формы являются разработанными в рамках настоящего исследования методическими инструментами. Они не свидетельствуют о реальном прохождении ARGA аккредитации, о заключённых договорах с сертификационными органами либо о фактическом тестировании обозначенных моделей. Выводы следует использовать как основу консультаций после внутреннего согласования и актуализации соответствующего права на дату подачи.

Научные основания и исследовательский дизайн

Научная задача assurance состоит в обосновании перехода от наблюдения к решению. Метрология помогает определить измеряемое свойство и процедуру; статистика оценивает неопределённость наблюдений; теория управления качеством связывает проверку с воспроизводимым процессом; институциональный анализ исследует компетентность и независимость оценщика. Правовая методология устанавливает юридическое значение результата. Их функции разделены, чтобы формальный статус документа не подменял проверку его содержания. [M1–M2]

Основание	Исследовательская задача	Результат в досье
Метрология	Определить свойство, метод и условия наблюдения	Паспорт измеряемого параметра
Статистика	Проверить знаменатель, зависимость и неопределённость	Расчёт и пределы статистического вывода
Управление качеством	Установить, действует ли заявленная процедура	Связь документа с записями исполнения

Основание	Исследовательская задача	Результат в досье
Институциональный анализ	Проверить компетентность и влияние интересов	Обоснованная область доверия к оценщику
Сравнительное право	Установить применимость статуса и процедуры	Отдельное заключение о юридическом значении

Операционное определение достаточности

В предлагаемой методике доказательства достаточны для данного утверждения, если определены объект и критерий, материалы пригодны для проверки, существенные противоречия разрешены, а язык вывода не выходит за исследованную область. Это авторское рабочее определение для анализа досье. Оно не заменяет специальные правила формальной схемы соответствия и не делает достаточность универсальным числовым показателем.

Определение параметра предшествует измерению. «94% правильных ссылок» может означать долю ссылок среди всех ссылок, долю ответов без ошибки либо долю досье без неверной существенной ссылки. Перевод одного показателя в другой без исходных данных недопустим. В паспорт включают единицу анализа, знаменатель, правила существенности и условия, при которых случай признаётся неопределённым.

Правило решения и неопределённость

JCGM 106 рассматривает связь неопределённости измерения и оценки соответствия [M2]. Для предлагаемого исследования это основание требовать явного правила решения до получения результата. Правило должно объяснять, как сопоставляются оценка и порог, какие риски ошибочного допуска и отказа учитываются и когда применяется исход «данных недостаточно». Конкретный порог определяется назначением и полномочиями владельца процедуры.

Статистическая неопределённость не охватывает все дефекты исследования. Дополнительно проверяют полноту входных данных, пригодность эталона, соответствие среды и независимость наблюдений. Узкий интервал вокруг смещённой оценки не делает свидетельство достаточным. При существенном дефекте измерения сначала исправляют метод либо сужают утверждение, а не увеличивают число повторов той же непригодной процедуры.

Исследовательские вопросы пилота

Пилот должен проверить, повышает ли структурированный паспорт утверждения воспроизводимость экспертной квалификации по сравнению с обычным чтением комплекта документов. Единицей анализа служит досье; исходами — пропуск существенной подмены предмета, необоснованное положительное заключение и мотивированное расхождение экспертов. Время работы является дополнительной характеристикой и не заменяет качество квалификации.

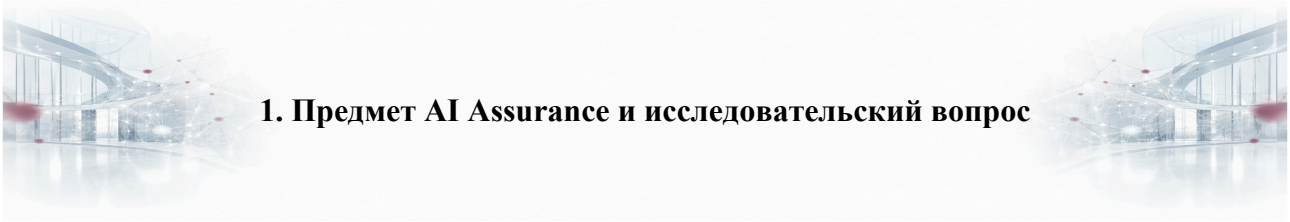
Для сравнительного дизайна предлагаются комплекты сопоставимой сложности, распределение порядка работы и сокрытие подготовленного эталонного разбора от оценщиков. Повторное чтение того же комплекта может дать эффект обучения; его следует

учитывать либо использовать разные, заранее сопоставленные наборы. Эталонная группа сохраняет основания своего решения и допускает несколько обоснованных ответов там, где вопрос действительно неоднозначен.

Условия научной проверки результата

Проверяется устойчивость вывода к изменению состава досье, наличию противоречивого приложения и сокрытию рекламных признаков поставщика. Если квалификация меняется после удаления логотипа при неизменных содержательных данных, требуется разбор влияния репутационного сигнала. Для положительного результата важна возможность другого специалиста восстановить основания решения без устного пояснения автора.

Результаты пилота не распространяются на все процедуры сертификации: перенос ограничен составом документов, подготовкой экспертов и задачами, исследованными в программе. В настоящем докладе представлены проект проверки и условный разбор. Доказательство преимуществ предлагаемой методики потребует выполнения описанного исследования, регистрации отклонений и независимой оценки полученных материалов.



1. Предмет AI Assurance и исследовательский вопрос

1.1. Гарантия как обоснованное утверждение

Исследуемое заверение представляется как проверяемое утверждение об определённом объекте. Вместо «помощник надёжен» требуется указать функцию, версию, состав входных материалов и критерий: например, долю досье, в которых все существенные ссылки подтверждены первичными документами. Отдельно устанавливают, каким действием вправе воспользоваться адресат результата. Это позволяет проверить, совпадает ли область коммерческого обещания с областью выполненного исследования.

Обоснованное доверие строится от проверяемого тезиса к доказательству, а не от внешне убедительного документа к тезису. Следует устанавливать, кому адресован результат: заказчику при выборе поставщика, регулятору, аудитору группы компаний, покупателю услуг или потенциально затронутому лицу. Для каждого адресата меняется необходимая детализация. Даже безупречный формальный сертификат системы менеджмента может мало сообщать о поведении одной модели на редкой группе входных данных.

1.2. Четыре границы заверения

Сначала фиксируется техническая граница: включены ли модель, правила предобработки, база поиска, интерфейс, человек, принимающий решение, и внешний API. Затем функциональная граница: какие решения охвачены и в каких случаях результат может быть использован. Третья - нормативная граница: применяется ли добровольная схема или установленная законом оценка. Четвёртая - временная: на какой версии и данных проводилась проверка и какие изменения делают её устаревшей.

Ошибка возникает, когда заключение об одном уровне распространяют на другой. Испытание устойчивости распознавания документа не удостоверяет правомерность использования биометрии; сертификация процедур хранения информации не доказывает отсутствие незаконных оснований обработки. Поэтому карта объёма составляет часть результата и должна быть доступна вместе с выводом.

1.3. Что является доказательством, а что маркетинговым сигналом

Копия рекламной брошюры, слово «ISO compliant» и свидетельство о прохождении курса не равны сертификату. Подлинный документ оценивают по выдающему органу, идентификатору, статусу, предмету, применяемой схеме и прослеживаемости к аккредитационному реестру. Результаты испытаний исследуются отдельно: входные данные, правила разметки, код, версии, квалификация экспертов и неопределённость имеют значение даже при наличии знака признания.

Для публичного использования целесообразно вводить правило: каждое упоминание сертификации сопровождается ссылкой на доступное для проверки свидетельство и узкой формулировкой его значения. Иначе читатель может неверно заключить, будто орган сертификации удостоверил весь продукт или выполнение всех требований права ЕС.

Практический контрольный список

1. Назвать одно измеримое утверждение и того, кто будет полагаться на результат.

2. Определить версию, контекст использования, период наблюдения и исключения.

3. Разделить доказательство процедуры, доказательство результата и доказательство правовой квалификации.

Иллюстративный пример

Юридический помощник верно ссылается на документы в 94 из 100 проверенных ответов: такое число характеризует только выборку, метод оценки и версию, а не «юридическую точность» любых будущих ответов.

Операционное определение достаточного заверения

Степень достаточности заверения должна определяться не престижностью исполнителя, а последствиями ошибочного вывода. При использовании ИИ для сортировки открытых новостей достаточно иной глубины исследования, чем для решения о закрытии банковского счёта или сообщения полиции об установленной идентичности лица. В чувствительном случае необходимо проверить не только среднее качество модели, но и механизм отказа от ответа, доступность вторичной проверки, устойчивость к плохо документированным именам и возможность восстановления всех значимых входов и действий. В решении о применении результата следует зафиксировать, какое остаточное сомнение принято и кто имеет полномочия его принять. [39,44]

Для экспертного заключения полезно использовать «паспорт утверждения». Он связывает предмет заверения, заинтересованное лицо, категорию риска, применённый критерий, идентификатор проверенной версии, среду испытаний, ограничения выборки, статус независимости оценщика и срок актуальности. Такая структура защищает от неявного

перехода от фразы «пройден набор тестов» к заявлению «система безопасна». Положительный результат без ясного перечня исключений неполон: получатель не способен понять, какие вопросы эксперт вовсе не изучал.

Особая проблема возникает при комбинировании отдельных оценок. Отчёт по кибербезопасности API, сертификат корпоративного менеджмента и тест качества распознавания не образуют автоматически единое заключение о правомерности итогового решения. Для объединённого вывода необходима явная логика перехода между свидетельствами и независимая проверка допущений о взаимодействии компонентов. Это относится и к результатам субподрядчиков, которые могут иметь разные сроки наблюдения и разные версии объектов.

Практический разбор 17.01

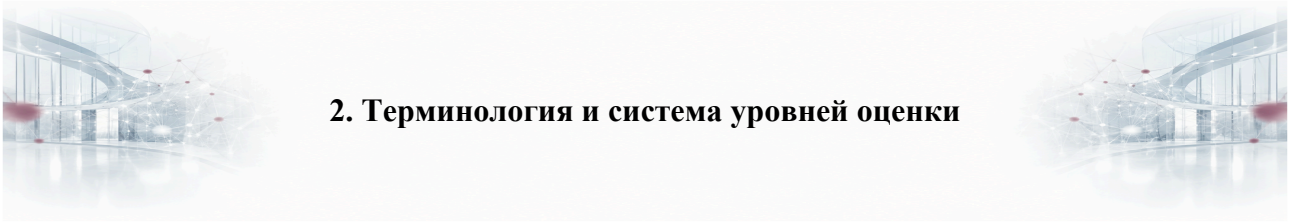
Рекомендация: Уточнять предмет заверения

Условный пример: Клиент просит подтвердить безопасность всего продукта по результату проверки цитат.

Разбор: Испытание цитирования касается одного свойства и не охватывает безопасность действий.

Практические действия: Руководитель формулирует отдельные утверждения о цитатах, данных и действиях; назначает свидетельства для каждого.

Критерий результата: Заключение содержит проверенные свойства и исключённые области.



2. Терминология и система уровней оценки

2.1. Самооценка, аудит, испытание и независимая проверка

Самооценка может быть полезной для непрерывного контроля, но при ней заказчик одновременно является источником данных и заинтересованным в результате лицом. Аудит проверяет соответствие установленным критериям на основе совокупности свидетельств. Испытание ставит технический эксперимент с заранее известной процедурой. Верификация оценивает истинность сформулированного утверждения; валидация - обоснованность утверждения применительно к предполагаемому использованию. Эти действия могут сочетаться, но они не синонимы. [27-28,39]

Условное испытание точности модели не воспроизводит комплексный аудит управления рисками. В свою очередь, проверка наличия процедуры мониторинга не заменяет фактическое измерение ложных совпадений. Рабочее дело должно содержать отдельные выводы по операционным процессам, техническим характеристикам, законности и независимости процедуры.

2.2. Сертификация и аккредитация

Сертификат сообщает о результате оценки определённого объекта по определённой схеме. Аккредитация оценивает компетентность и беспристрастность самого органа, который

проводит испытания, инспекции, валидацию или сертификацию. Например, аккредитация органа сертификации систем менеджмента по применимой области не делает автоматически аккредитованной каждую его дополнительную услугу. [23-25]

Компетентность специалиста, признание профессиональной квалификации, членство в ассоциации и нотификация для конкретной процедуры ЕС требуют отдельных оснований. По этой причине неверно заменять проверку области аккредитации вопросом «какой у компании логотип на сайте». Область действия и действующий статус всегда важнее оформления.

2.3. Нотификация и правовая презумпция

Нотификация означает допуск органа для определённых функций по специальному правовому режиму ЕС. Она не тождественна добровольной аккредитации: ст. 28-31 AI Act предусматривают отдельную роль компетентных властей и процедуру сообщения Комиссии. Наличие аккредитации может быть основанием для нотификации, но отсутствие её не всегда полностью исключает возможность представления альтернативных доказательств компетентности. [9-12]

Презумпция соответствия гармонизированному требованию возникает не из публикации стандарта ISO как таковой. Требуется соблюдение условий специальной нормы и, в рассматриваемом европейском механизме, публикация ссылки на гармонизированный стандарт в Официальном журнале ЕС в объёме, охватывающем соответствующее требование. [7]

Практический контрольный список

1. Указать тип документа: отчёт испытаний, заключение аудитора, сертификат или аккредитация.

2. Назвать орган, давший признание, и программу, в рамках которой он действовал.

3. Проверить, нет ли недопустимого перехода от добровольной схемы к обязательному правовому статусу.

Матрица А. Тип результата и его правовой смысл

Вид	Что подтверждает	Чего не подтверждает
Внутренний аудит	Наблюдение определённых критериев и контроль собственных процессов	Независимое государственное признание
Лабораторное испытание	Измеренные свойства по методу и в обозначенной области	Законность любого использования
ISO/IEC 42001	Систему менеджмента ИИ в заявленной области	Качество и безопасность всех отдельных продуктов
Аккредитация CAB	Компетентность оценщика по определённой области	Обязательную пригодность любого выданного им документа

Вид	Что подтверждает	Чего не подтверждает
Нотификация EU AI Act	Официальную компетенцию органа по обозначенной процедуре	Полномочия вне предмета нотификации
EU Declaration of Conformity	Ответственное заявление поставщика по специальному режиму	Внешнюю сертификацию при внутреннем маршруте

Реестр видов свидетельств и запрет подмены статусов

В каждом деле следует ввести четыре отдельных поля: тип выполняемой деятельности, статус её исполнителя, юридическое основание применения результата и конкретная область фактической проверки. Например, лаборатория может иметь аккредитацию на испытание определённого класса свойств, но её заключение об ином свойстве не становится аккредитованным из-за логотипа на первой странице. Точно так же сертификат системы менеджмента охватывает определённый организационный контур, а не все продукты юридического лица без исключения. [23-28]

Если заказчик требует «независимую сертификацию искусственного интеллекта», исполнитель должен ещё до заключения договора перевести эту формулу на язык проверяемых требований. Следует спросить, нужна ли оценка управленческих процессов, метрически установленное качество продукта, вывод по специальному правовому режиму или независимое подтверждение заявления поставщика. Только после ответа можно выбрать орган, аккредитационную область, схему и подходящие критерии. Иначе заказчик оплачивает документ, который может быть безупречен формально, но бесполезен для его действительной цели.

В справке для руководства рекомендуется сохранять исходную терминологию стороны и рядом помещать её квалификацию. Так, «сертификат доверенного ИИ» следует описывать как частное коммерческое утверждение до получения номера схемы, критериев и компетентного органа. Это не обвинение в недобросовестности: ошибка нередко возникает из-за упрощения маркетингового языка. Но для юридического использования упрощение недопустимо.

Практический разбор 17.02

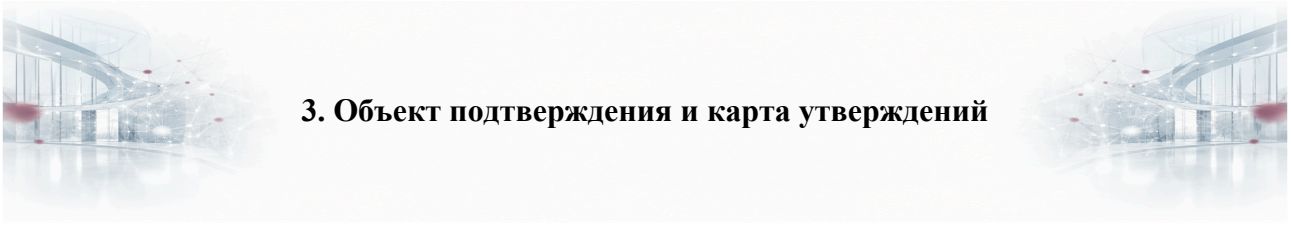
Рекомендация: Разделять испытание и сертификацию

Условный пример: Поставщик называет внутренний тест сертификатом соответствия.

Разбор: Название не подтверждает процедуру и полномочия выдавшего лица.

Практические действия: Закупщик запрашивает схему, критерии, исполнителя и область; описывает документ по фактическому содержанию.

Критерий результата: В реестре указан действительный вид документа без расширительного названия.



3. Объект подтверждения и карта утверждений

3.1. Система менеджмента и конкретный продукт

ISO/IEC 42001:2023 устанавливает рамку организационного управления ИИ. Объектом может быть система менеджмента организации, которая внедряет ИИ, разрабатывает его либо предоставляет AI-услуги. Сертификат такой системы свидетельствует о соответствии системы управления в заявленной области. Он не гарантирует точность каждой модели и не превращается в сертификат безопасности любого алгоритма поставщика. [21,48]

Для конкретного продукта потребуются отдельные, ориентированные на его свойства доказательства: версионное описание, функциональное назначение, реалистичные сценарии, результаты испытаний и юридическая карта. Техническое тестирование продукта может поддерживать систему менеджмента, но не является её полной заменой; аналогично качественный корпоративный процесс не исправляет критическую ошибку конкретной конфигурации.

3.2. Фрагментация объекта в цепочке ИИ

Поставщик фундаментальной модели предоставляет доступ по API, интегратор добавляет поиск по внутреннему архиву, заказчик устанавливает правила доступа, а сотрудники используют результат в оценке клиента. На практике каждое звено контролирует только часть поведения системы. Общая фраза «сертифицированный AI» стирает эту разницу и создаёт недопустимое расширение ответственности.

Для каждого элемента цепочки необходимо определить контролирующее лицо, применяемую версию, доказательство контроля, зависимость от третьих лиц и условия перепроверки. Если внешняя модель меняется без уведомления, прежнее испытание интеграции может потерять доказательную силу даже без обновления пользовательского интерфейса.

3.3. Коммерческое утверждение и проверяемая граница

Формулировки «этичный», «объективный», «безопасный» и «соответствующий всем международным стандартам» редко пригодны для заверения без декомпозиции. Следует запросить определение используемых терминов, метод измерения, порог приемлемости и документ о согласовании риска. При отсутствии такой информации вывод может ограничиться указанием непроверяемости исходного заявления.

Отдельный риск представляет сертификат, область которого сформулирована слишком широко или наоборот неполно: «AI services» не раскрывает, включены ли обучение моделей, поддержка клиентов, обработка медицинских данных или субподрядные процессы. Проверять следует точную область, указанную в действующем приложении к сертификату.

Практический контрольный список

1. Создать карту компонентов и внешних зависимостей с владельцами изменений.

2. Разложить рекламные заявления на утверждения и проверяемые показатели.

3. Установить границы применимости результата к каждой версии и предметной области.

Разделение обязанностей в многоуровневой системе

Область заверения следует задавать через архитектурную схему и реестр отношений с поставщиками. В гибридной системе могут одновременно существовать поставщик общей модели, провайдер облачного исполнения, владелец корпоративного поиска, интегратор правил, конечный оператор и субъект, принимающий значимое решение. У каждого отдельные возможности контроля. Если лицо владеет только подсистемой поиска, оно не вправе подтверждать неизменность внешней модели. Если внешний сервис хранит запросы, внутренний сертификат организации не доказывает режим фактического хранения этих записей. [21,22,49]

Приложение к договору должно содержать версии моделей и компонентов, точки перехода данных, перечень субподрядчиков, обязательства по уведомлению об изменении API, возможность получения журналов, условия экстренного отключения и требования к повторной проверке. Для моделей, работающих по постоянно обновляемым подпискам, особенно важно отличать зафиксированную версию от услуг с неограниченным изменением параметров. Заявление о неизменной области сертификата при реально неуправляемом обновлении представляет доказательственный риск.

Практическая карта утверждений делается в двух измерениях: строки показывают свойства системы, столбцы показывают элементы её цепочки. Ячейка заполняется лишь при наличии конкретного ответственного лица и доступного свидетельства. Пустая ячейка не означает отсутствия риска; она обозначает пробел в контроле. Это позволяет на ранней стадии определить, где необходимы дополнительные полномочия или ограничение планируемого использования.



Рисунок 17.1. Границы заявления о соответствии. Четыре самостоятельные границы из раздела 1.2. Изменение одной из них может потребовать пересмотра заверения.

Практический разбор 17.03

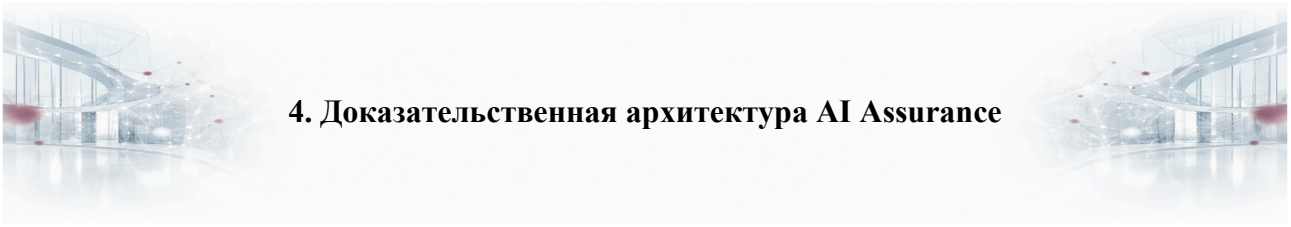
Рекомендация: Создавать паспорт каждого утверждения

Условный пример: Заявление о 95 процентах точности не содержит знаменателя.

Разбор: Это могут быть ссылки, ответы или досье; их доли несопоставимы.

Практические действия: Аналитик запрашивает единицу учёта, исходные количества, версию и область применения.

Критерий результата: Показатель можно пересчитать и связать с проверенным назначением.



4. Доказательственная архитектура AI Assurance

4.1. От критериев к цепочке подтверждения

Для каждого утверждения составляется карта обоснования: точная формулировка, объект и версия, источник критерия, способ наблюдения, исходные данные, правило решения и допустимая область применения. В карту включают также обстоятельство, при котором утверждение должно быть отклонено или сужено. Документирование этой связи делает возможной содержательную рецензию: специалист проверяет не количество приложений, а пригодность каждого свидетельства для конкретного вывода.

Различные свидетельства могут дополнять друг друга только при объяснимой связи с утверждением. Для заявления об исполнении процедуры нужны записи фактического применения; для заявления о качестве ответа — соответствующее испытание; для заявления о юридическом статусе — документ компетентного органа и проверка его области. Три документа, пересказывающие один отчёт поставщика, не образуют три независимых подтверждения. Происхождение сведений и общие зависимости указываются в карте.

4.2. Качество исходных материалов и воспроизводимость

Воспроизводимость технического свидетельства требует исходных ответов, идентификаторов задач, конфигурации системы и процедуры оценивания. Исследователь должен восстановить знаменатель и объяснить каждое исключение. Если из 100 заданий в отчёт попали 94 успешных ответа, необходимо установить судьбу остальных шести: ошибки, отказы, технические сбои или исключения по протоколу приводят к различным выводам. Повторный расчёт по сохранённым материалам предшествует оценке переносимости результата. [39–41]

Если существует ограничение доступа к исходному коду или обучающим данным, это не следует скрывать. Можно провести независимое функциональное тестирование или оценку процессов при достаточной прозрачности границ. Однако заключение обязано прямо говорить, какие свойства не были проверены из-за отсутствия доступа.

4.3. Выводы и степень уверенности

Для анализа отдельного утверждения предлагаются пять статусов: подтверждено в указанной области; подтверждено частично с перечислением границ; опровергнуто наблюдением, несовместимым с критерием; доказательств недостаточно; не исследовалось. Частичное подтверждение не используют как неопределённый компромисс: должно быть ясно, какая часть установлена и какая остаётся открытой. Для схемы с собственными категориями решений применяется её терминология, а исследовательская карта объясняет основания этого решения.

В юридически чувствительной сфере желательно фиксировать компетенцию подписанта. Технический специалист может оценить воспроизводимость процедуры, но вывод о юридической применимости конкретного режима требует правовой квалификации. Подпись одного человека под обоими видами выводов должна сопровождаться объяснением необходимых компетенций.

Практический контрольный список

1. Отделять наблюдение от интерпретации и рекомендации.

2. Для каждого существенного отрицательного вывода отмечать объём проверенных материалов.

3. Не употреблять «полностью соответствует», если использовалась ограниченная выборка или недоступный компонент.

Матрица B. Выбор инструментов для доказательств

Контрольный вопрос	Основной вид доказательства	Предостережение
Есть ли управленческая процедура?	Документы, назначенные роли, журнал решений	Документ может не исполняться
Работает ли модель на заданном корпусе?	Версионный протокол испытания, эталон, матрица ошибок	Не распространять на все данные
Компетентен ли независимый оценщик?	Реестр аккредитации, область, персонал	Проверять именно данную услугу
Существуют ли права затронутого лица?	Описание обжалования, реальные кейсы, нормативный анализ	Не достаточно интерфейсного уведомления
Сохраняется ли качество при изменении?	Реестр версий, регрессионные тесты, договор с API	Один исходный тест устаревает

Доказательственное досье и архитектура опровержения

Проверка достаточности включает попытку найти противоречие между заявлением и материалами. Исследователь сопоставляет заявленную функцию с областью сертификата, пересчитывает ключевую метрику, проверяет исключённые случаи и выбирает трудный

пример, способный изменить заключение. Обнаруженное противоречие не устраняется голосованием или ссылкой на репутацию поставщика. Оно разрешается новым доказательством, сужением утверждения либо фиксацией недостаточности имеющихся сведений.

Следует документировать отрицательные доказательства. Если журнал не содержит искомого события, эксперт должен знать срок его хранения, полноту выгрузки, систему синхронизации времени, фильтры и вероятность потери записи. Только после этого можно отличить «события не было» от «след события не найдено». Аналогично отсутствие найденных инцидентов в открытых источниках не исключает инцидентов, которые не публиковались либо описывались иными терминами.

Для существенных выводов рекомендуется двухступенчатая проверка: автор формирует вывод и список ссылок на исходные артефакты; независимый рецензент пытается повторить переход от материалов к заключению без участия автора. Если рецензенту необходимо устное пояснение, в тексте или в реестре имеется пробел. При работе с чувствительными данными повторяемость может достигаться через псевдонимизированные контрольные записи, контрольные суммы и документированные процедуры доступа, без распространения полного закрытого массива.

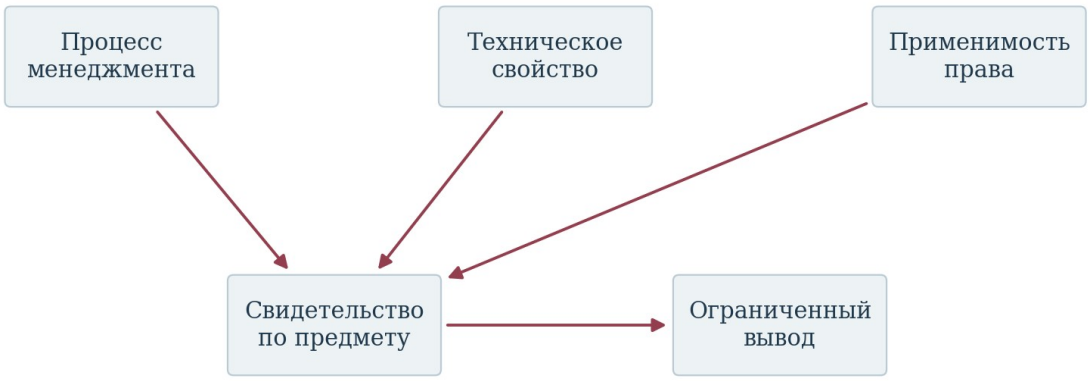


Рисунок 17.2. Что подтверждают разные свидетельства. Сертификат менеджмента, техническое испытание и юридическая квалификация имеют разные предметы. Их нельзя подменять друг другом.

Практический разбор 17.04

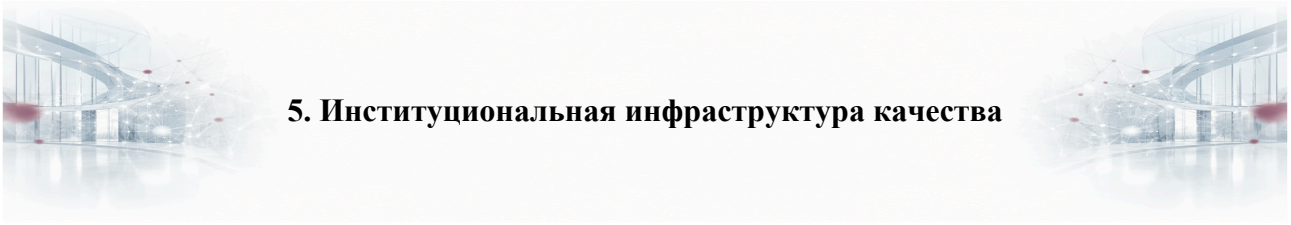
Рекомендация: Проверять достаточность всей цепочки свидетельств

Условный пример: К сертификату менеджмента приложены тест другой версии и недатированное описание процесса.

Разбор: Свидетельства не относятся к одному объекту; их сумма не подтверждает текущую сборку.

Практические действия: Эксперт связывает каждое утверждение с версией и датой; пробелы оформляет запросом дополнительных материалов.

Критерий результата: Для непокрытого свойства сохранён вывод о недостаточности данных.



5. Институциональная инфраструктура качества

5.1. Цепочка участники - критерии - решение

Стандартизирующая организация разрабатывает документ, но обычно не выдаёт сертификат на его основе. Орган по оценке соответствия осуществляет предусмотренную процедурой проверку; орган по аккредитации подтверждает компетентность этого оценщика в определённой области; регулирующий орган устанавливает обязательные последствия отдельных процедур. В зависимости от сектора несколько ролей могут быть распределены иначе, но их смешение недопустимо. [19,21-28]

При проверке провайдера необходимо проследить цепочку от проверяемого утверждения до реального субъекта, который вправе или способен его подтвердить. Международный стандарт и аккредитация полезны только в рамках такой цепочки, а не в качестве универсального символа добросовестности.

5.2. Объективность и конкурирующие интересы

Отношения оценщика с разработчиком могут повлиять на выбор тестов и пороги, даже если открытого финансового конфликта нет. Проблему представляют участие в разработке системы, обещание результата до начала работы, премия за выдачу положительного отчёта и зависимость от постоянных контрактов одного клиента. Система управления беспристрастностью должна не только декларироваться, но и содержать оценку угроз и принятые меры. [12,22-24]

Процедуры нотификации и аккредитации выстраиваются вокруг независимой компетенции; внешняя исследовательская проверка должна исходить из сопоставимого принципа, не присваивая формального статуса. Для ARGA это означает отдельную проверку конфликтов интересов при составлении заключений, которые планируется представить регуляторам.

5.3. Контроль статуса публичных заявлений

На сайте организации могут одновременно присутствовать аккредитованная лаборатория, неаккредитованный консалтинг, обучение персонала и платные услуги добровольной оценки. Разумный пользователь не может считать их одним видом официального признания. Следует запросить номер аккредитации, название области, стандарты, перечень адресов и дату последней актуализации.

Даже если несколько компаний входят в одну группу, аккредитация конкретного юридического лица не переносится автоматически на аффилированные организации. Аналогично логотип международного соглашения о взаимном признании не должен сопровождать заключения, выходящие за область аккредитации.

Практический контрольный список

1. Верифицировать юридическое лицо, а не только торговое наименование.

2. Проверить раздельные услуги и области действия аккредитации.

3. Зафиксировать результат проверки статуса на конкретную дату.

II. МЕЖДУНАРОДНЫЕ СТАНДАРТЫ

Три линии контроля и условия организационной независимости

Независимость проверяющего должна анализироваться по всей цепочке: выбор методики, получение данных, установление порогов, интерпретация исключений, утверждение заключения и возможность публикации. Внешний подрядчик не является автоматически независимым, если его вознаграждение зависит от получения положительной отметки или если проверяемый субъект может запретить раскрывать существенные отрицательные находки. Для таких ситуаций нужны заранее согласованные условия о недопустимости редактирования профессионального вывода заказчиком. [22,23,28]

Практически полезно разграничивать внутренний контроль владельца процесса, внутренний аудит функции риска и внешнее подтверждение по специально согласованным критериям. Ни одна линия не является универсальной заменой других: разработчик лучше знает технологию, но имеет заинтересованность; внешний орган обладает дистанцией, но может не получить достаточного доступа; надзорная власть оценивает вопросы законности, которые не всегда являются предметом сертификата. Поэтому матрица обязанностей должна содержать отдельную строку для эскалации разногласий между линиями.

При выборе эксперта разумно получить декларации о финансовых, трудовых, семейных и подрядных отношениях, сведения о прежних консультационных услугах, структуру принятия решений и процедуру отстранения проверяющего. Не каждый возможный конфликт требует автоматического отказа, но каждый существенный конфликт должен быть оценён с точки зрения угрозы беспристрастности и доступности защитных мер. Декларация, подписанная только при заключении договора, без повторной проверки в ходе проекта недостаточна.

Практический разбор 17.05

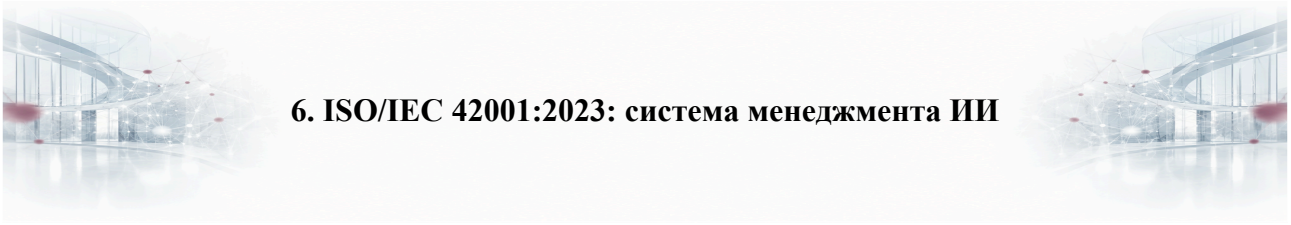
Рекомендация: Проверять каждого участника цепочки качества

Условный пример: Орган сертификации ссылается на аккредитатора, но не указывает область признания.

Разбор: Существование организации не подтверждает конкретную компетенцию.

Практические действия: Ответственный сверяет орган, область, срок и схему с первичными реестровыми сведениями.

Критерий результата: Сохранена проверяемая цепочка статуса для нужного вида оценки.



6. ISO/IEC 42001:2023: система менеджмента ИИ

6.1. Предмет стандарта и правовой статус

ISO/IEC 42001:2023 описывает создание, поддержание и постоянное улучшение системы менеджмента искусственного интеллекта. Он адресован организациям, участвующим в разработке, предоставлении и использовании ИИ, и служит структурой для распределения ролей, процессов и мер управления. По открытой карточке ISO его предмет - система менеджмента, а не выдача оценки конкретной модели или передача регулятору права контроля. [21]

Стандарты систем менеджмента применимы на добровольной основе, если специальное правило или договор не делает их исполнение обязательным в конкретном отношении. Даже после внедрения стандарта сертификация остаётся отдельным решением; организация может вести работоспособную систему менеджмента без сертификата, а сертификат не устраняет самостоятельных обязанностей по закону. [48]

6.2. Практическая оценка области AIMS

Предмет сертификации разумно сопоставлять с бизнес-процессами: инвентаризация AI-систем, изменение моделей, закупка внешних сервисов, контроль данных, ответственность подразделений, обучение сотрудников, управление жалобами и документирование инцидентов. При этом лабораторная оценка конкретного ответа модели выходит за пределы простой проверки того, что процессы предусмотрены.

Если сертифицирована «разработка IT-решений», недостаточно считать включёнными все процессы рискованного применения. Важно проверить буквальный текст области сертификата, функции исключённых филиалов и ответственность облачного поставщика. При приобретении одного продукта клиенту может понадобиться не только сертификат компании, но и продуктовые протоколы испытаний.

6.3. Что сертификат 42001 не должен обещать

Из сертификата AIMS нельзя механически вывести соответствие GDPR, EU AI Act, правилам санкционного мониторинга или специальным требованиям медицинского изделия. Он является частью комплаенс-доказательств и может подтверждать организационную зрелость, но правовая квалификация и соответствие конкретной системы требуют других материалов. [1,17,21]

Корректное утверждение в договоре: «система менеджмента организации сертифицирована в заявленной области». Некорректное: «все решения компании одобрены международным регулятором и могут применяться без дополнительной проверки». Правило полезно и для закупок, и для публикации заключений, и для рассмотрения претензий о вводящем в заблуждение маркетинге.

Практический контрольный список

1. Прочитать дословную область сертификации и исключения.

2. Соотнести AIMS с фактическими процессами разработки, внедрения и эксплуатации.

3. Отдельно запросить продуктовые тесты и применимую нормативную карту.

Проверка сертификата AIMS по содержанию

Для ISO/IEC 42001 ключевой вопрос состоит не в том, сколько моделей использует организация, а какие процессы управленческой системы охвачены областью сертификации. В одном юридическом лице разработка, продажа и эксплуатация могут быть распределены между подразделениями и территориями. Поэтому при закупке необходимо запросить приложение с областью, перечень охваченных площадок, сведения о выдавшем органе и действующий статус сертификата. На основании одного публичного логотипа нельзя установить, что конкретная услуга входит в область AIMS. [21,23,48]

Свидетельством функционирования системы менеджмента могут быть реестр ИИ, политика ответственности, записи об оценке воздействия, журналы изменения моделей, решения по непринятым рискам, процедуры мониторинга и доказательства работы механизма исправления ошибок. Но наличие этих документов не доказывает эффективность каждой процедуры. Для независимого анализа важно выбрать выборку реальных решений: кто обнаружил отклонение, кто разрешил его, были ли затронутые лица уведомлены, менялся ли критерий после появления неблагоприятных результатов.

Особый риск связан с термином «сертифицированная модель». Правомерно указать, что организация сертифицировала AIMS в определённой области; неправомерно без отдельного основания распространять такой вывод на точность, безопасность, отсутствие дискриминации или правовую квалификацию каждого продукта. В отчётах ARGA целесообразно сохранять исходную формулировку сертификата и рядом делать короткую заметку о её пределах.

Практический разбор 17.06

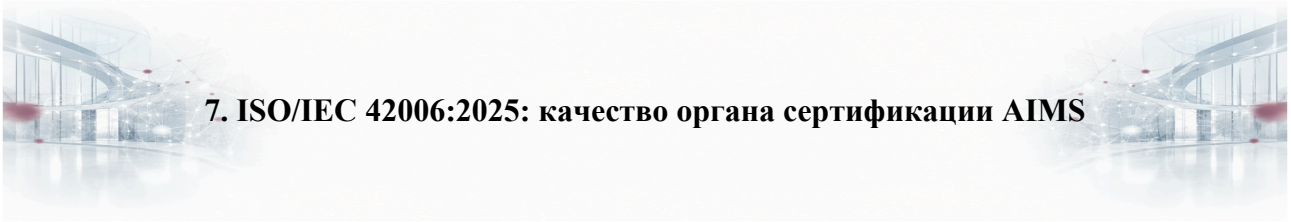
Рекомендация: Отделять систему менеджмента от качества ответа

Условный пример: Поставщик показывает сертификат AIMS после обнаружения вымышленной ссылки.

Разбор: Организационный процесс сам по себе не подтверждает отсутствие ошибок продукта.

Практические действия: Оценщик учитывает сертификат как отдельное свидетельство и назначает техническую проверку ссылок.

Критерий результата: Технический вывод опирается на испытания конкретной версии.



7. ISO/IEC 42006:2025: качество органа сертификации AIMS

7.1. Специальное дополнение к ISO/IEC 17021-1

В июле 2025 года опубликован ISO/IEC 42006, посвящённый органам аудита и сертификации систем менеджмента ИИ. Открытая карточка ISO описывает его как дополнительные требования к ISO/IEC 17021-1, необходимые из-за специфических AI-рисков, качества данных, этики, прозрачности и компетенции. Использование 42006 не отменяет базовые требования к беспристрастности и процессам органа сертификации. [22-23]

Практическая ценность новой редакции состоит в стандартизированном языке для оценки «проверяющего». Клиенту уже недостаточно спрашивать, обучен ли аудитор общим правилам систем менеджмента. Требуется понимать, способен ли оценщик разобраться в архитектуре ИИ, организационном контуре, границах данных и роли человека при принятии решений.

7.2. Компетентность, состав команды и надзор

AI Assurance требует сочетания знаний об управлении системами, технической оценке моделей, защите данных и отраслевом использовании. Само наличие специалиста с техническим сертификатом не означает способность квалифицировать право ЕС; наличие юриста не заменяет статистическую проверку выборки. Орган оценки должен определить необходимые компетенции и обеспечить их практическое присутствие, а не условную подпись в итоговом отчёте.

При аккредитационной проверке интересуют не только резюме сотрудников, но и то, как орган назначает команды, контролирует независимость, обеспечивает доступ к экспертной помощи и принимает решения. Отчёт о сертификации требует документированной связи между наблюдениями аудиторов и заключением компетентного решающего лица.

7.3. Пределы переносимости 42006

ISO прямо указывает, что 42006 может использоваться внутри более широких схем оценки продуктов, процессов или услуг на базе ISO/IEC 17065, но это не превращает сертификат менеджмента в сертификат продукта. Для такой схемы необходимы самостоятельные критерии, предмет и процедура. [22,25]

В частности, проверка AIMS разработчика биометрии не позволяет заявлять, что специальная процедура Annex VII уже выполнена. Применяется отдельный режим нотификации, роли и доступ к доказательствам. Ошибку «42006 = право выдавать сертификаты по AI Act» следует исключать в любых инструкциях и маркетинговых текстах.

Практический контрольный список

1. Запросить применимую аккредитационную область органа, а не только ссылку на 42006.

2. Оценить AI-специфические компетенции команды и право органа подписывать документ.

3. Сверить тип сертификата с типом заявленного объекта.

Компетентность органов AIMS и раздельность решений

ISO/IEC 42006:2025 адресует требования к органам, которые аудируют и сертифицируют AIMS, дополняя ISO/IEC 17021-1; по открытой карточке ISO это самостоятельный опубликованный стандарт, а не проект. При оценке компетентности следует анализировать не только общий опыт аудитора в системах менеджмента, но и способности команды работать с системным риском ИИ, данными, программным обеспечением, эксплуатацией, правами человека и границами корпоративной ответственности. Именно сочетание компетенций снижает вероятность формального аудита без анализа реальных воздействий. [22,23]

При сложной инфраструктуре сертификатор может привлекать предметных экспертов, однако их участие не должно размывать ответственность за аудиторское решение. Заказчику важно установить, кто оценивает технические отчёты, кто отвечает за беспристрастность, кто принимает решение о сертификации и как рассматриваются жалобы. Профессиональная биография консультанта или публикация собственной программы обучения не служит достаточным доказательством статуса органа сертификации.

Особенно полезно отличать область компетентности от области коммерческого предложения. Орган может рекламировать широкий портфель AI Assurance, при этом его аккредитация распространяется на узкую схему AIMS. Результаты за её пределами могут оставаться услугами, но заказчик должен понимать их статус и не описывать их как аккредитованную сертификацию. Это различие следует отражать в закупочной документации и в финальном отчёте.

Практический разбор 17.07

Рекомендация: Проверять компетентность сертификационной команды

Условный пример: Аудит сложного языкового инструмента проводит команда без профильного опыта.

Разбор: Формальное назначение не гарантирует понимания исследуемого процесса.

Практические действия: Заказчик запрашивает матрицу компетенций и рецензирование спорных технических вопросов.

Критерий результата: Существенные вопросы рассмотрены специалистом с подтверждённой компетенцией.

8. ISO/IEC 17021-1:2015 и методология сертификационного аудита

8.1. Процедуры, беспристрастность и решение

ISO/IEC 17021-1:2015 адресован органам, которые проводят аудит и сертификацию систем менеджмента. Открытое описание подтверждает акцент на компетентности, последовательности и беспристрастности. В AIMS-сфере это стандарт общего слоя, к которому добавляется AI-специфика 42006. [23]

При подготовке к проверке важно различать независимость сборщика фактов и независимость решения о сертификации. Отделение функций уменьшает риск, когда вывод принимается лицом, заинтересованным в коммерческих отношениях с клиентом. Для заказчика значима также возможность жалобы и контроля состояния сертификата после первоначальной оценки.

8.2. Наблюдение, выборка и несоответствия

Сертификационный аудит использует выборку процессов и доказательств: невозможно каждую минуту контролировать все решения организации. По этой причине описание метода выборки должно учитывать критичность процесса, число площадок, частоту изменений и историю инцидентов. Положительный результат в отношении выборки не означает математической гарантии отсутствия неизвестных нарушений.

Для AI-систем несоответствие может быть организационным (нет назначенного владельца риска), процедурным (изменения не утверждаются), доказательственным (отсутствует требуемый журнал) или техническим (система даёт опасный результат). Доклад предлагает разделять эти виды вместо объединения в одну категорию «AI risk».

8.3. Интегрированные системы менеджмента

Компании могут совмещать управление ИИ с информационной безопасностью и качеством. Такая интеграция уменьшает дублирование ролей и отчётности, но не позволяет автоматически переносить сертификацию одного стандарта на другой. У каждой программы остаются свои критерии и документальный след.

При закупке важно спросить, кто отвечает за интерфейс между ИИ и информационной безопасностью: разграничение прав доступа, обучение персонала, хранение журналов и реагирование на обнаруженный вывод модели. Фраза «у нас уже есть ISO 27001» не доказывает, что оценены последствия ошибочного финансового или правового заключения.

Практический контрольный список

1. Описать программу аудита и независимость принятия решения.

2. Выделить процессы высокого риска для расширенной выборки.

3. Развести документальное несоответствие и эмпирическую ошибку модели.

Сертификационный цикл и подтверждение действия контроля

Стандарт ISO/IEC 17021-1 касается органа, который сертифицирует системы менеджмента, и предусматривает системный подход к беспристрастности и компетентности. В технической части доклада целесообразно исследовать операционный цикл AIMS, а не подменять его разовой демонстрацией политики. При аудите полезны сведения о первоначальной проверке, корректирующих действиях, надзорных оценках и переоформлении в пределах применимой схемы; конкретные периодичности нужно проверять по правилам сертификатора и схемы, а не предполагать для всех одинаковую. [23,22]

Для компаний, одновременно сертифицирующих качество, безопасность информации и управление ИИ, возможен интегрированный аудит общих процессов, но результаты должны

быть разнесены по требованиям. Общая процедура управления документами не свидетельствует сама по себе о полноценной оценке ошибок генеративной модели, а стандарт информационной безопасности не заменяет оценки последствий алгоритмического решения. Совместное использование свидетельств допустимо лишь при документированной карте покрытия.

Если обнаружены существенные несоответствия, вывод не должен сводиться к отметке «исправлено». Следует установить причину, охват затронутых систем, временные меры, проверку эффективности и остаточное воздействие на пользователей. Для целей сравнительного исследования ARGA рекомендует хранить историю изменения статуса, а не одну фотографию сертификата в момент закупки.

Практический разбор 17.08

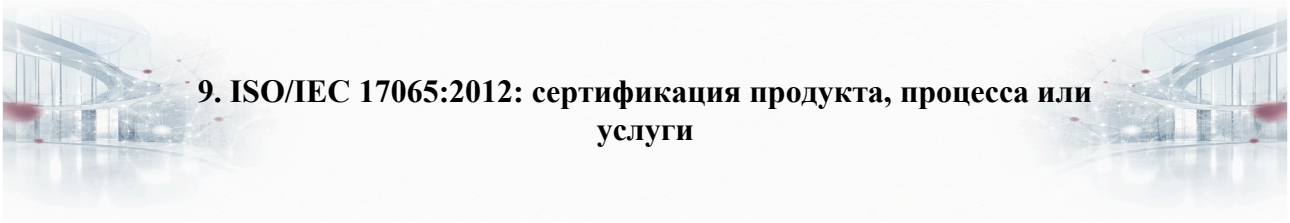
Рекомендация: Проверять фактическое выполнение аудиторской программы

Условный пример: В плане заявлены интервью операторов, но в досье есть только ответы руководства.

Разбор: Описанный процесс не подтверждён независимыми наблюдениями исполнения.

Практические действия: Рецензент сопоставляет программу, выборку записей и выполненные действия; фиксирует непокрытые участки.

Критерий результата: Каждый существенный этап имеет запись выполнения либо обоснованное ограничение.



9. ISO/IEC 17065:2012: сертификация продукта, процесса или услуги

9.1. Отличие продуктовой схемы

ISO/IEC 17065:2012 относится к органам, которые сертифицируют продукцию, процессы и услуги. Здесь исходным объектом выступает не вся система менеджмента компании, а предмет, определённый схемой: например, конкретная версия системы, вид функции, доступная конфигурация или технология испытания. Схема должна содержать измеримые требования, правила принятия решения и надзора. [25]

Для AI Assurance это особенно важно, потому что типичный продукт обновляется быстрее, чем корпоративные процедуры. Если сертификат распространяется лишь на фиксированную модель, его маркетинговое использование после значительного обновления без новой оценки может создать ложное впечатление непрерывного подтверждения.

9.2. Схема сертификации и её владелец

Нельзя путать стандарт, устанавливающий компетентность органа, с техническим стандартом, задающим требования к продукту. ISO/IEC 17065 сам по себе не определяет общую «проходную оценку» качества ИИ. Такая оценка возникает из конкретной схемы и установленных в ней критериев. Две добросовестные программы могут использовать разные свойства и пороги, а их сертификаты не обязательно эквивалентны.

Заказчику стоит запросить текст схемы, основание выбранных порогов, перечень допустимых отклонений, правила о новых версиях и порядок жалоб. В AI-сфере особенно нужны определения данных, сценариев отказа и роли человеческого контроля: без них публичный знак остаётся слишком абстрактным.

9.3. Статус редакции 2026 года

По открытой карточке ISO на октябрь 2026 года доступен проект ISO/IEC FDIS 17065 новой редакции; действующей опубликованной редакцией в каталоге остаётся ISO/IEC 17065:2012. Текст проекта нельзя выдавать за вступившие в действие обязательные требования. [25-26]

Договоры и заключения должны фиксировать год редакции и дату её проверки. Если впоследствии будет опубликован пересмотренный стандарт, организация отдельно определяет переходный период и требования своей аккредитационной программы. Автоматически объявлять прежние сертификаты недействительными также нельзя.

Практический контрольный список

1. Установить предмет и версию продукта, отражённые в сертификате.

2. Получить схему оценки, её критерии и основания для повторного испытания.

3. Не ссылаться на FDIS как на опубликованный стандарт.

Критерии продуктовой схемы и проблема обещанного качества

Сертификация продукта, процесса или услуги строится вокруг схемы, которая должна определять объект, набор требований, допустимые методы оценки, порядок принятия решения и надзор. ISO/IEC 17065:2012 задаёт требования к деятельности соответствующих органов; при этом обсуждаемая в 2026 году новая редакция находится на стадии FDIS и не должна выдаваться за вступивший в силу стандарт. До её публикации ссылки в действующих схемах нужно проверять по конкретной нормативной редакции. [25,26]

Для ИИ значение схемы особенно велико: одна и та же модель может иметь высокое качество на массовом наборе тестов и недопустимое число ошибок в редкой, но юридически критичной подгруппе. Поэтому программа продуктовой оценки должна определять происхождение тестовых сценариев, критические пороги, способ построения статистического интервала, роль человеческого оператора и последствия существенного обновления. Широкая формула «проверка этичности» без таких элементов плохо воспроизводима.

Если продукт поставляется как сервис, нужно отдельно описать изменение модели в эксплуатации и наличие доступа к контрольным версиям. Положительный сертификат, полученный на старой конфигурации, не обязан покрывать новую; вопрос решается по соответствующей схеме. Закупщик должен получить условия приостановления, расширения и отзыва подтверждения. Это особенно важно там, где поставщик периодически подменяет базовую модель без изменения названия коммерческой услуги.

Практический разбор 17.09

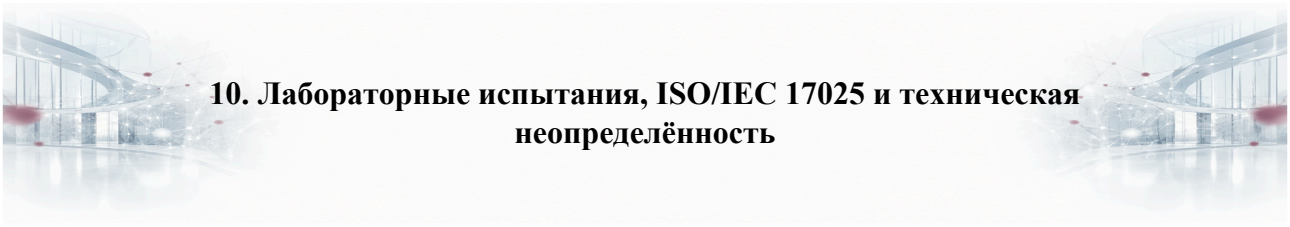
Рекомендация: Указывать объект продуктовой схемы

Условный пример: Сертификат относится к модулю поиска, а реклама распространяет его на весь помощник.

Разбор: Состав продукта шире сертифицированного объекта.

Практические действия: Эксперт сопоставляет область схемы с архитектурой продукта и корректирует внешнее заявление.

Критерий результата: Непроверенные модули явно исключены из заявления.



10. Лабораторные испытания, ISO/IEC 17025 и техническая неопределённость

10.1. Компетентность лаборатории не равна универсальности метода

ISO/IEC 17025:2017 задаёт требования к компетентности, беспристрастности и устойчивой работе испытательных и калибровочных лабораторий. Для AI-оценки это полезная инфраструктура, когда существует конкретный метод испытания. Но сертификат лаборатории по одной области не даёт ей универсального полномочия оценивать любую модель, а область аккредитации может описывать ограниченные типы испытаний. [27]

Юридически чувствительный заказчик должен установить, покрывает ли аккредитация именно нужный показатель. Например, аккредитация по измерениям кибербезопасности не подразумевает без дополнительного основания оценку справедливости кадровых решений или точности перевода юридических документов.

10.2. Испытание, эталон и репрезентативность

Результат испытания зависит от набора входных задач, способа формирования правильного ответа, повторений и независимости тестовых данных от обучающих. Если тестовый корпус составлен разработчиком и хорошо известен модели, высокое качество может отражать подгонку. Требуется отличать валидирующую выборку разработчика от внешней, заранее закрытой контрольной выборки.

При сравнении моделей следует обеспечить одинаковые правила запроса, инструменты, ограничения времени и критерии выставления оценки. Особенно нежелательно применять к одному провайдеру ручную коррекцию ответов, а к другому полностью автоматический подсчёт. Такой дизайн нарушает сопоставимость даже без намерения исказить итог.

10.3. Неопределённость и предел вывода

При обследовании 100 задач нельзя с высокой точностью предсказать вероятность редких сбоев в миллионах будущих случаев. Статистические интервалы следует сообщать с размером выборки, определением успеха и методологией расчёта. Точность числа «96,8%» может быть иллюзорной, если сами разметчики расходятся в определении верного ответа.

Отдельно рассматриваются систематические ошибки: непропорционально лёгкие вопросы, невидимые пропуски данных и исключение неудобных сценариев. Увеличение выборки уменьшает случайную погрешность, но не исправляет систематическую нерепрезентативность. Поэтому независимый методический контроль должен предшествовать выдаче итогового результата.

Практический контрольный список

1. Сверить аккредитационную область лаборатории с конкретным тестом.

2. Зафиксировать происхождение эталонного набора и возможное пересечение с обучением.

3. Описать неопределённость и исключённые группы сценариев.

Испытания и допустимость вывода о редких событиях

Аккредитованная лаборатория демонстрирует компетентность по определённой области, но даже безупречный протокол не переносит автоматически свойства испытанной выборки на всю будущую эксплуатацию. Для ИИ критичны происхождение данных, актуальность распределения входов, процедура разметки и правила обработки неоднозначных случаев. ISO/IEC 17025 используется для оценки компетентности лаборатории, но само измерение необходимо обосновать для конкретной задачи. [27,39]

В задачах санкционного скрининга высокая совокупная точность может скрывать неудовлетворительное обнаружение редких истинных совпадений или невыносимую нагрузку ложных тревог. Проверку целесообразно строить на слоях: обычные имена, транслитерация, альтернативный порядок компонентов имени, неполные даты рождения, псевдонимы и записи с ошибками. В каждом слое фиксируется размер выборки, правило установления истины и независимость разметчиков. Результаты разных слоёв нельзя без объяснения смешивать в один общий процент.

При небольшом числе наблюдений необходимо давать интервал неопределённости и предупреждать о невозможности надёжно оценить редкие ошибки. Например, отсутствие ошибок в ста проверках не доказывает нулевую вероятность ошибки в реальном использовании. В приложениях следует использовать воспроизводимые учебные расчёты и чётко отделять их от эмпирических данных реальных систем.

Практический разбор 17.10

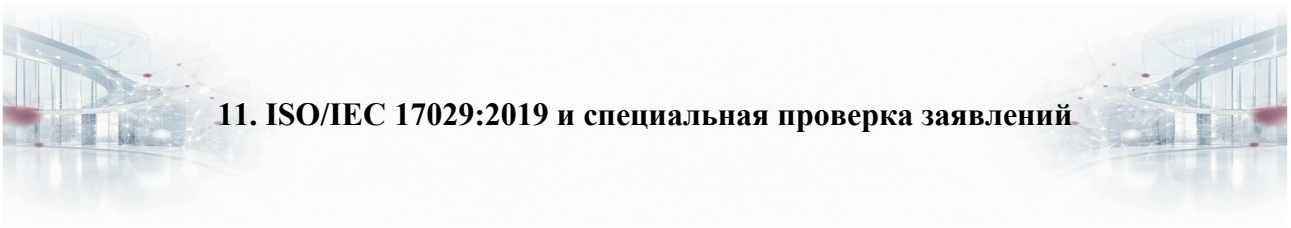
Рекомендация: Учитывать неопределённость у порога

Условный пример: Рабочий критерий пилота требует не менее 95 успешных досье из 100; получено 94.

Разбор: Порог не достигнут; округление и последующая смена правила скрывают исход.

Практические действия: Аналитик применяет утверждённое правило, показывает неопределённость и направляет систему на доработку.

Критерий результата: Решение соответствует первоначальному критерию без округления в пользу допуска.



11. ISO/IEC 17029:2019 и специальная проверка заявлений

11.1. Верификация, валидация и формулировка утверждения

Открытая карточка ISO/IEC 17029:2019 различает проверку истинности утверждения (verification) и подтверждение правдоподобности утверждения применительно к предполагаемому будущему использованию (validation). Стандарт адресован органам оценки соответствия, работающим по специально установленным программам. По нему нельзя делать вывод, что любая независимая проверка программного обеспечения уже является верификацией в формальном смысле. [28]

Для AI Assurance рационально формулировать отдельные claims: «доля несанкционированных обращений к защищённым данным не превышает значение по протоколу», «модель проходит тест на конкретные классы уязвимостей», «выборка санкционных совпадений сформирована без включения обучающих примеров». Чем уже заявление, тем легче установить его пределы и повторить процедуру.

11.2. Программы как источник требований

ISO/IEC 17029 не заменяет предметную программу, определяющую тип свидетельств, пороги и содержание заключения. Отчёт, обещающий «верифицировать прозрачность», должен сначала определить, что означает прозрачность: доступность документации, право пользователя на объяснение, воспроизводимость входных данных либо открытость архитектуры модели. Это разные свойства с разными субъектами и правовыми последствиями.

В случае сложных организационных претензий полезно совместить документальную и эмпирическую проверки: проверить, существует ли процесс уведомления, и установить на контрольных сценариях, исполняется ли он. Но такая комплексная оценка должна быть прямо заявлена в программе, иначе читатель ошибочно приписывает результату несуществующий охват.

11.3. Независимость сообщения о результатах

Существенна проверка того, кто выбирает формулировку публичного заявления. Если клиент заказывает «подтверждение, что продукт этичен», но не разрешает исследовать жалобы пострадавших пользователей, исходное утверждение следует сузить либо отказаться от вывода. Утверждение должно соответствовать объёму исследованного материала, а не маркетинговой цели.

Для ARGA рационально отделить подготовку доказательственной записки от формального заявления о верификации: пока нет подтверждённой области аккредитации и программы, допустим лишь исследовательский отчёт с описанием работы и ограничений. Институциональный статус нельзя создавать стилем документа.

Практический контрольный список

1. Формализовать исходное заявление без ценностных лозунгов.

2. Привязать его к проверяемой программе и измеримому свойству.

3. Указать, даёт ли результат самостоятельное заверение или только экспертную оценку.

Верификация заявлений и пригодность будущего применения

Подтверждение того, что заявленная численная характеристика была достигнута на конкретном наборе, отличается от оценки того, имеет ли эта характеристика достаточное значение для реального использования. В первой ситуации проверяется утверждение о прошлом измерении; во второй требуется обоснование пригодности для заданной цели, где имеют значение возможные пользователи, контекст эксплуатации и тяжесть ошибок. Это практическое разграничение совместимо с публично описанной направленностью ISO/IEC 17029, хотя не заменяет чтения полного текста стандарта и требований конкретной программы. [28]

Заявление «модель обнаруживает 99 процентов опасных случаев» не поддаётся серьёзной проверке без определения опасного случая, состава набора, способа образования доли, численности наблюдений, исключений и периода. Если оценщик получает тестовые данные от разработчика, следует отдельно оценить риск утечки примеров в обучение и возможность независимого воспроизведения. Там, где прямая передача исходного массива невозможна, используют независимую генерацию контрольных случаев и журналирование испытаний в контролируемой среде.

В отчёте полезно оставлять два результата: подтверждён ли исходный тезис на проверенных материалах и допустимо ли использовать его для конкретного внешнего решения. Второй результат может быть отрицательным даже при положительном первом. Такое разделение предотвращает расширительное толкование формально верного протокола.

Практический разбор 17.11

Рекомендация: Проверять проверяемое заявление отдельно

Условный пример: Компания заявляет, что все источники ответа проверены человеком.

Разбор: Подпись на итоговом документе не показывает проверку каждой ссылки.

Практические действия: Верификатор выбирает ответы, сопоставляет ссылки с журналом и интервьюирует проверяющих.

Критерий результата: Вывод ограничен проверенной процедурой и выявленной долей подтверждений.



12. ISO/IEC 17011 и аккредитация органов оценки соответствия

12.1. Кого и за что аккредитуют

ISO/IEC 17011:2017 охватывает компетентность, последовательность работы и беспристрастность органов аккредитации, которые оценивают другие органы оценки соответствия. Аккредитация говорит о способности учреждения проводить конкретную категорию работ в конкретной области, но не переносит права на все возможные услуги учреждения. [24]

Для клиента особое значение имеет разница между аккредитацией лаборатории, аккредитацией сертификационного органа и формальным признанием отдельных схем. Даже один национальный орган аккредитации может вести эти направления по различным программам и выносить разные решения об областях применения.

12.2. Область и статус на дату обращения

Проверка начинается не с отсканированной копии свидетельства, а с действующего реестра аккредитующего органа. Обычно необходимо сопоставить номер, полное юридическое наименование, филиал, область, стандарт и статус: действителен, ограничен, приостановлен, прекращён. Истекшая дата не всегда исчерпывает вопрос при изменении схемы, но игнорировать её нельзя.

Следует оценить, распространяется ли действие на конкретные площадки или удалённые подразделения. Если испытания выполняет субподрядчик, нужно установить, кем подтверждена его компетентность и под чьей ответственностью подписан отчёт. Иначе цепочка доказательств прерывается между названием сертификационной группы и реальным исполнителем.

12.3. Пропорциональное использование аккредитации

Аккредитация повышает доверие к процедуре проверки, но не исключает содержательных ошибок конкретного отчёта. Рецензент всё равно оценивает постановку вопроса, дизайн испытания и логическую силу вывода. Если орган аккредитован, но его программа не проверяет требуемую характеристику ИИ, наличие статуса не исправляет дефект предмета.

Отсутствие аккредитации также не означает, что исследовательский анализ бесполезен или незаконен. Важно честно обозначить статус работы. В профильных задачах ARGA допустимы экспертные обзоры нормативных режимов и анализ представленных доказательств, пока они не выдаются за официальную сертификацию.

Практический контрольный список

1. Выполнить прямую реестровую проверку выдавшего аккредитацию органа.

2. Сопоставить заявленный вид услуги с приложением об области аккредитации.

3. Отделить статус компетентности исполнителя от доказательств качества результата.

Проверка области аккредитации по состоянию на конкретную дату

При аккредитации оценке подлежит компетентность органа, выполняющего определённые работы, а не потребительское качество любого товара с его знаком. Регламент 765/2008 определяет европейскую инфраструктуру национальной аккредитации; ISO/IEC 17011 описывает компетентность органов аккредитации. На практике основное доказательство находится в действующем публичном статусе и области, а не в случайной копии свидетельства. [19,24]

По каждому сертификату закупщик должен документировать официальное наименование органа, правовое лицо, адрес и филиалы, актуальный номер аккредитации, точно охваченные схемы, ограничения и временные приостановления. Особенно важно различать наличие статуса на дату выдачи сертификата и на дату проверки. При расхождении данных следует сохранить дату обращения в реестр и запросить пояснение органа аккредитации, а не принимать коммерческое письмо продавца как окончательное доказательство.

Если признание основано на международной договорённости, этого ещё недостаточно для вывода об обязательном признании результата местным регулятором. Необходимо сопоставить категорию процедуры, область действующего MRA, специальные требования внутреннего права и круг адресатов документа. Для юридического досье корректнее формула «имеется аккредитация в такой-то области; правовые последствия в выбранной юрисдикции устанавливаются отдельно», чем обещание автоматической трансграничной силы.

Практический разбор 17.12

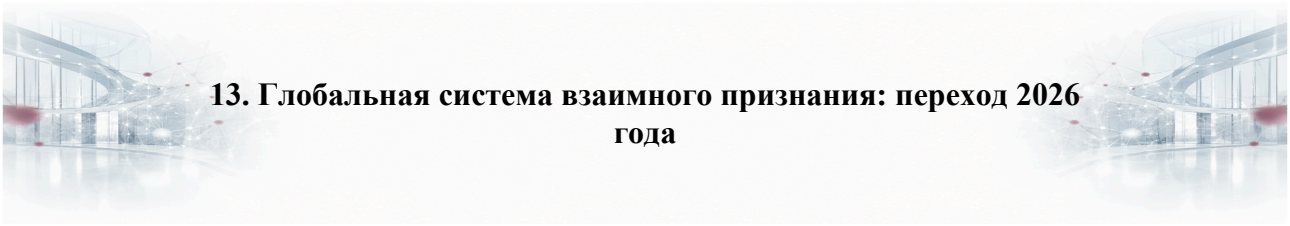
Рекомендация: Проверять область аккредитации

Условный пример: Лаборатория аккредитована для одного вида испытаний и предлагает другой.

Разбор: Общий статус не распространяется автоматически на новую методику.

Практические действия: Закупщик проверяет приложение с областью и требует отдельного обоснования новой процедуры.

Критерий результата: В договоре различены работы в области аккредитации и вне неё.



13. Глобальная система взаимного признания: переход 2026 года

13.1. Новый участник после IAF и ILAC

С 1 января 2026 года начала работу Global Accreditation Cooperation Incorporated, объединив институциональные функции IAF и ILAC и запустив собственное многостороннее соглашение о признании (MRA). Этот факт подтверждён официальным сообщением ILAC и пресс-релизом переходного периода. Указывать IAF и ILAC как действующие независимые центры новой глобальной системы без оговорки о переходе было бы устаревшим описанием. [37-38]

При этом документы и марки прежних механизмов сохраняют значение в рамках предусмотренных переходных правил. Для проверки реального сертификата необходимо учитывать дату его выдачи, область признания и актуальные правила использования знака. Недопустимо механически объявлять все документы с прежней аббревиатурой недействительными с января 2026 года.

13.2. Предмет международного признания

Смысл MRA состоит в доверии к компетентности аккредитующих органов и результатам аккредитованных органов оценки соответствия в пределах признанных областей. Это не глобальный договор, который отменяет национальные законы о допуске AI-систем к рынку. Даже международно признаваемый отчёт испытаний не освобождает поставщика от специфической процедуры нотификации ЕС, если она юридически требуется. [19,35-38]

Отдельная категория проблем возникает при сравнении разных схем. Два органа могут быть членами одного признанного сообщества аккредитации, однако тестировать разные свойства, разные версии и по разным порогам. Взаимное признание компетентности оценщика не означает эквивалентности измеренного объекта.

13.3. Практическая проверка сертификата из третьей страны

Сначала проверяется подлинность и статус сертификата. Затем - область аккредитации органа, а не только аккредитующего учреждения. Следующий шаг - охватывает ли MRA соответствующую категорию работ и применима ли в стране назначения норма о признании. В конце выполняется содержательное сопоставление критериев: технические характеристики, права человека, требования к данным и доказательственная форма.

Для проекта в сфере международного финансового контроля экспортируемый сертификат AIMS может стать фактором оценки поставщика, но не заменить местную оценку обработки данных, санкционных списков и процедур обжалования. Такое сочетание международной

инфраструктуры качества и национальных требований лучше отражает реальные возможности трансграничного AI Assurance.

Практический контрольный список

1. Учитывать новую Global Accreditation Cooperation Incorporated MRA с 01.01.2026.

2. Разделять признание аккредитованного отчёта и правовое разрешение на применение продукта.

3. Проверять область и переходные правила для старых маркировок.

Переход 2026 года: непрерывность и ограничения признания

С 1 января 2026 года Global Accreditation Cooperation Incorporated (Global ACI) объединила функции международных систем IAF и ILAC и начала работу с общей многосторонней договорённостью MRA. Этот переход подтверждён сообщениям организаций системы аккредитации и не означает одномоментного исчезновения всех прежних маркировок: предусмотрены переходные условия их использования. При проверке документа 2025 года важно не признавать его недействительным только из-за прежнего знака, но и не считать знак достаточным доказательством действующего статуса. [37,38]

Международное признание должно проверяться по конкретному виду деятельности. Результат лабораторного испытания, сертификат менеджмента и продуктовый сертификат могут попадать в разные области признания. Само участие аккредитационного органа в глобальной организации не гарантирует, что каждая его программа включена в признанный объём. Проверяющий должен установить область органа, применимую к данной схеме и конкретному документу, на дату выдачи и на дату оценки.

Для юридического анализа требуется отдельная граница: международная доверительная инфраструктура облегчает принятие результатов, но не отменяет обязательных требований внутреннего права, публично-правовых разрешений или компетенции органов ЕС. В закупочных условиях рекомендуются специальные положения о предоставлении статуса аккредитации и его обновлении, а в публичных заявлениях — запрет выражения «признаётся во всех странах» без указания конкретного правового механизма.

Практический разбор 17.13

Рекомендация: Не приравнивать взаимное признание к разрешению применения

Условный пример: Иностранный отчёт принимается партнёром как техническое свидетельство.

Разбор: Принятие отчёта не решает вопрос национального допуска продукта.

Практические действия: Юрист отдельно проверяет режим использования и требования местного адресата.

Критерий результата: Запись о признании не содержит необоснованного разрешения эксплуатации.

14. Европейское аккредитационное пространство: Regulation 765/2008 и EA MLA

14.1. Специальная юридическая архитектура ЕС

Регламент (ЕС) № 765/2008 формирует правовую основу аккредитации в ЕС. Согласно официальным материалам European co-operation for Accreditation, статья 11 касается признания эквивалентности услуг национальных органов, успешно прошедших оценку в системе EA, и результатов организаций, аккредитованных ими в релевантной области. [19,35-36]

Для пользователя это означает более сильный юридический контекст признания, чем простая договорная ссылка на зарубежный сертификат. Однако акт не стирает границы областей компетентности и не является универсальной лицензией на использование любой AI-модели. Правовой эффект оценивается вместе с профильным отраслевым законодательством.

14.2. Марка EA MLA и проверка области

В 2025 году EA объявила о специальной марке MLA; обновления 2026 года касались расширения регистрации знака. Материалы EA указывают, что его использование должно быть связано с национальным знаком аккредитации и не выходить за признанную область. Одного изображения марки на рекламной странице недостаточно, если нельзя установить действующую область, в которой выдан документ. [35-36]

Верификация должна включать реестр национального органа, область аккредитации CAB и категорию услуг, на которую распространяется EA MLA. Для организационного решения крайне важно, чтобы этот анализ сохранялся в деле как отдельная запись. Иначе через год невозможно будет восстановить, какое признание существовало на дату закупки.

14.3. Пределы признания в отношении AI Act

Даже европейский аккредитованный орган сертификации ISO/IEC 42001 не становится нотифицированным органом AI Act автоматически. Нотификация осуществляется по статье 28-31 Регламента и конкретным видам оценки; при этом аккредитация может использоваться в доказательственной базе компетентности. [9-12]

Следовательно, договор с «европейским аккредитованным партнёром» не заменяет проверку NANDO/применимого официального списка уполномоченных органов, их области и конкретной процедуры. Особенно серьёзным является риск смешения сертификации менеджмента с технической оценкой биометрической системы.

Практический контрольный список

1. Установить правовую базу национального органа аккредитации.

2. Проверить действующую область EA MLA, указанную для вида оценки.

3. Нотификацию по AI Act подтверждать отдельно.

III. ЕВРОПЕЙСКИЕ ПРАВОВЫЕ МЕХАНИЗМЫ

Территориальная специфика европейской системы

В Европейском союзе аккредитация связана с правовой конструкцией Регламента (ЕС) №765/2008, в которой действуют национальные аккредитационные органы и механизм взаимного доверия к результатам. Добровольное международное признание и европейская система EA MLA связаны институционально, однако правовые последствия необходимо оценивать именно по соответствующему акту и области оценочной деятельности. Упоминание знака EA MLA без проверки конкретной области ничего не доказывает о правовом статусе AI-системы. [19,35,36]

В европейской закупке важны как минимум три самостоятельных документа: подтверждение действующей области аккредитации органа, документ результата оценки и юридическое обоснование того, что применённая схема подходит для соответствующего режима. Если AI Act предусматривает внутренний контроль, получение необязательного сертификата не создаёт дополнительной законной обязанности; если закон требует участия компетентного нотифицированного органа, обычная добровольная сертификация не закрывает это требование.

При трансграничном сравнении следует описывать не «ЕС признаёт сертификат X», а проверяемую цепочку: национальный аккредитационный орган, область EA MLA, полномочия органа оценки, вид результата и релевантная норма ЕС. Такое изложение пригодно для договоров, регуляторных консультаций и анализа доказательств. Оно также позволяет быстро обнаружить случаи использования настоящих, но не относящихся к делу сертификатов.

Практический разбор 17.14

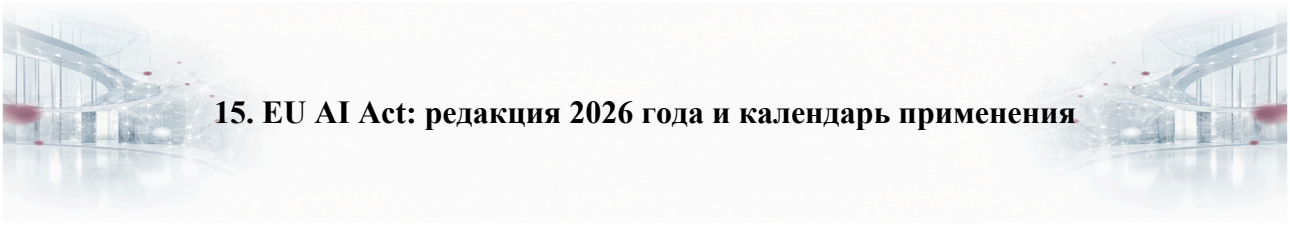
Рекомендация: Проверять конкретную область европейского признания

Условный пример: Поставщик ссылается на европейскую сеть, не показывая нужную область соглашения.

Разбор: Членство и охват определённого результата различаются.

Практические действия: Эксперт проверяет участника, область и применимость к типу выданного документа.

Критерий результата: Ссылка на признание сопровождается конкретным подтверждением охвата.



15. EU AI Act: редакция 2026 года и календарь применения

15.1. Консолидированный текст вместо исторических презентаций

В июле 2026 года принят Регламент (ЕС) 2026/1744, изменивший отдельные положения AI Act, включая сроки применения требований к высокорисковым системам. Официальный AI Act Service Desk показывает консолидированный текст на 27 июля 2026 года с пометками изменённых норм; общая дата применения 2 августа 2026 года сохранена, но не должна распространяться на все группы обязанностей. [1-3]

Согласно обновлённой статье 113, разделы 1-3 главы III для систем, отнесённых к высокому риску на основании Annex III, применяются с 2 декабря 2027 года; для систем по статье 6(1) и Annex I - с 2 августа 2028 года. Этот календарь принципиально влияет на утверждение о готовности к обязательной оценке соответствия и сроки закупки услуг.

15.2. Неприменимость одного срока ко всему регулированию

Некоторые запреты и общие нормы применяются с февраля 2025 года, специальные положения о GPAI и институциональные главы - с августа 2025 года; отдельные обновлённые запреты будут применяться с декабря 2026 года. Поэтому фраза «до 2028 года у ИИ нет никаких обязательств» юридически неверна. Также продолжают действовать GDPR, отраслевые нормы и договорные обязательства. [1,3]

Для работы с конкретным AI-продуктом обязательна таблица применения на дату: категория, юрисдикция, роль лица, наличие переходного правила, действующие нормы и предстоящие обязанности. Такая таблица позволяет избежать двух ошибок: требовать ещё не наступившую процедуру как формально обязательную либо пропустить уже действующее требование.

15.3. Планирование аккредитации и задержка стандартизации

Перенос дат связан, среди прочего, с задержкой готовности гармонизированных стандартов и органов контроля. Он не означает, что подготовка оценщиков и разработчиков не нужна до новой даты. Организации продолжают проектировать документацию, схемы испытаний, внутреннюю ответственность и инфраструктуру аккредитации. [2-3]

Для ARGA целесообразно использовать этот период для аналитических предложений о составе доказательственных досье и минимальном языке ограничения сертификатов. Такие предложения могут быть направлены на правовую определённость, но не должны представляться как утверждённый Европейской комиссией обязательный стандарт.

Практический контрольный список

1. Проверять сроки по редакции 27.07.2026, а не по первоначальной версии 2024 года.

2. Разводить сроки для Annex III и Annex I.

3. Не делать вывод об отсутствии иных действующих обязательств из переноса high-risk требований.

Точность дат и последствия реформы AI Act

Дата публикации акта, дата его вступления в силу и дата применения конкретной обязанности не тождественны. Регламент (ЕС) 2026/1744 изменил AI Act с 27 июля 2026 года; по обновлённой статье 113 соответствующие положения о высокорисковых системах Annex III применяются с 2 декабря 2027 года, а для категории Annex I — со 2 августа 2028 года. При этом отдельные разделы, включая некоторые требования к поставщикам моделей общего назначения, имеют иные даты. Универсальная фраза «весь AI Act вступает в силу с августа 2026 года» вводит адресата в заблуждение. [1-3]

Любая таблица обязанностей должна содержать пять признаков: роль стороны, территориальная связь, конкретная категория системы, номер статьи и дату начала применения. К ним рекомендуется добавлять статус возможных переходных правил и предмет уже действующих обязанностей. Консультационную позицию нельзя строить на устаревшем графике, даже если он по-прежнему воспроизводится в презентациях профессиональных ассоциаций и на сайтах консультантов.

Реальный проект может одновременно подпадать под GDPR, отраслевое банковское регулирование и уже применимые положения AI Act, тогда как часть требований высокорискового режима ещё не начала действовать. Отсрочка одной группы норм не означает освобождения от остального права. Для ARGA принципиально отделять действующее обязательство, ожидаемое обязательство и добровольную меру подготовки; такие статусы должны отмечаться прямо в каждом заключении.

Практический разбор 17.15

Рекомендация: Вести календарь обязанностей по каждому назначению

Условный пример: Один продукт применяется в нескольких секторах с различными режимами.

Разбор: Одна общая дата в презентации может скрыть уже действующие обязанности.

Практические действия: Юрист составляет календарь по роли, назначению и применимому акту; дату сверяет перед внешним использованием.

Критерий результата: У каждой обязанности указаны субъект, основание и проверенная дата.

16. Классификация высокорисковых систем и выбор маршрута

16.1. Категория системы не определяет маршрут автоматически

Статья 43 устанавливает разные маршруты для систем, подпадающих под отдельные категории Annex III, и для систем, являющихся компонентами или продуктами согласно Annex I. Нельзя утверждать, что каждая high-risk AI-система требует участия внешнего нотифицированного органа. Для большинства категорий, указанных в пунктах 2-8 Annex III, основной маршрут - процедура внутреннего контроля по Annex VI. [4-6]

Для пункта 1 Annex III, относящегося к определённым биометрическим применениям, возможность выбора между внутренним контролем и нотифицированным органом зависит от

применения соответствующих гармонизированных стандартов или общих спецификаций. При их отсутствии либо неполном применении предусмотренная статья 43 процедура требует вовлечения нотифицированного органа с учётом специальных правил.

16.2. Перекрытие с отраслевым законодательством

Системы по Annex I следуют соответствующим процедурам законодательства о продукции, включая предусмотренный AI Act слой требований. После изменений 2026 года специальное правило статьи 43(3) уточняет, что само наличие high-risk компонента ИИ не создаёт неизбежной обязанности внешней оценки, если применимый секторный акт предусматривает законную возможность внутреннего пути при выполнении условий. [1,4]

Квалификация должна учитывать продукт целиком: медицинское изделие, машина, транспортная система, цифровой компонент и его функция безопасности могут иметь разные правовые входы. Сводить всю матрицу к вопросу «есть ИИ - нужен аудит» означает игнорировать структуру гармонизационного права ЕС.

16.3. Алгоритм предварительного выбора

Сначала определяется применимость EU AI Act к участнику и системе. Затем проверяется, является ли применение запрещённым либо высокорисковым, и на каком основании. Далее устанавливается соответствующее секторное право и дата наступления специальных обязанностей. Только после этого выбирается Annex VI, Annex VII или специальная процедура, предусмотренная отраслевым законодательством. [1,4-6]

Результат предварительной юридической оценки следует оформлять не как окончательный сертификат, а как карту регуляторного маршрута с возможными альтернативами и открытыми вопросами. Если существенные сведения отсутствуют, решение остаётся условным и требует проверки производителем или компетентным органом.

Практический контрольный список

1. Уточнить Annex I против Annex III, а не ограничиваться словом high-risk.

2. Проверить особую ветку биометрии и наличие применимых гармонизированных стандартов.

3. Для совмещённого продукта установить специальный секторный маршрут.

Матрица C. Маршруты оценки в ЕС

Сценарий	Вероятный маршрут	Что ещё выяснить
Annex III, пункты 2-8	Annex VI, внутренний контроль [4-5]	Дата вступления в применение; роль поставщика
Annex III, пункт 1, биометрия	Annex VI или VII по условиям статьи 43	Наличие и применение стандартов или общих спецификаций
Annex I, секторное изделие	Секторная процедура с требованиями AI Act	Конкретный режим изделия и опция без третьей стороны

Сценарий	Вероятный маршрут	Что ещё выяснить
GPAI-модель как таковая	Специальная глава V	Имеются ли системные риски; не смешивать с Annex VII
Обычный добровольный AI-сервис	Выбор вида assurance по целям	Отраслевое право и режим данных

Двухступенчатое решение о категории и процедуре

Первый этап — квалификация системы по функции и сфере воздействия. Следует установить, связана ли она с продуктом, регулируемым в Annex I, либо с категориями Annex III, учесть исключения и указать, кто действительно выступает поставщиком системы. Второй этап — определение процедуры оценки в соответствии со статьёй 43, включая специальные правила для биометрической категории и продукционного законодательства. Пропуск первого этапа часто приводит к ложному выбору дорогостоящей третьесторонней процедуры там, где право требует внутреннего контроля, либо к обратной ошибке. [1,4]

Для систем Annex III в областях 2–8 статья 43 предусматривает внутренний контроль без нотифицированного органа. Для пункта 1 Annex III возможен выбор в зависимости от применения гармонизированных стандартов или общих спецификаций, а при определённых условиях требуется Annex VII. Отдельный маршрут действует для систем, охваченных отраслевыми актами из раздела A Annex I. Поэтому простой вопрос «высокий риск или нет?» не определяет закупку сертификационной услуги.

Предварительная карта должна содержать конкурирующие основания классификации и объяснение, почему отвергнут альтернативный маршрут. Это особенно важно для систем, объединяющих биометрию, кадровые решения и работу с регулируемым оборудованием. В итоговом юридическом выводе допустимо указать, что по неполной информации процедура пока не установлена. Подмена этого вывода коммерческим удобством создаёт больший риск, чем честно обозначенный пробел.

Практический разбор 17.16

Рекомендация: Обосновывать классификацию до выбора процедуры

Условный пример: Систему предварительного поиска документов называют высокорисковой без анализа назначения.

Разбор: Техническая сложность сама по себе не определяет маршрут.

Практические действия: Юрист описывает фактическое применение и проверяет критерии классификации по источникам доклада.

Критерий результата: В досье есть мотивированное решение о маршруте и открытых вопросах.

17. Annex VI: внутренний контроль без нотифицированного органа

17.1. Содержание внутренней процедуры

Приложение VI предусматривает проверку поставщиком системы управления качеством по статье 17, анализ технической документации на соответствие применимым требованиям и сверку процессов разработки и пострыночного мониторинга с зафиксированными документами. Эта процедура называется conformity assessment, несмотря на отсутствие обязательного независимого внешнего оценщика в соответствующем маршруте. [5,17-18]

Качественный внутренний контроль может привлекать внешнего консультанта или лабораторию, но юридическая ответственность поставщика не исчезает. Контрактная помощь не изменяет того, кто составляет декларацию ЕС и несёт ответственность за указанные в ней утверждения.

17.2. Внутренний контроль и внешние доказательства

Поставщик может использовать лабораторные испытания, рецензии и аудиты сторонних организаций для укрепления собственного досье. Но эти документы следует оценивать по предмету. Если сторонний оценщик проверил качество набора данных, нельзя считать автоматически проверенным управление инцидентами или информационную безопасность. [5,18,27]

В случае последующего запроса надзора важна возможность восстановить доказательственную базу: версию модели, дату, условия, результаты, внутренний вывод и корректирующее действие. Для такой цели разумно вести единую матрицу требований и доказательств, а не набор разрозненных презентаций поставщика.

17.3. Предел самодекларации

Внутренняя оценка не равна признанию со стороны государственного органа. При этом она не становится автоматически менее законной только из-за отсутствия печати независимой организации, если закон выбрал такой маршрут. Нужно разделять юридическую достаточность предусмотренной процедуры и содержательную убедительность доказательств в конкретном споре.

Подход ARGA должен быть нейтрален к форме: проверять, соответствует ли процедура требуемому маршруту, и отдельно оценивать риск недостоверного самоподтверждения. Навязывание платного внешнего сертификата для каждой ситуации не обосновано текстом AI Act.

Практический контрольный список

1. Оценить соответствие документации Annex IV и управления по статье 17.

2. Сохранить след фактических проверок, а не только итоговую декларацию.

3. Отразить самостоятельную ответственность поставщика.

Внутренний контроль как полноценная система доказательств

Внутренняя процедура Annex VI не равна отсутствию оценки. Ответственность за подтверждение выполнения требований лежит на поставщике; соответствующая документация должна позволять восстановить критерии, систему управления качеством, результаты проверки, технические характеристики и основание декларирования соответствия. Заказчик, которому предъявляют только рекламную презентацию, не получает сведения, достаточные для понимания полноты внутренней процедуры. [5,17,18]

Внешний аудитор может помогать поставщику исследовать доказательства, но его добровольный отчёт не превращает процедуру Annex VI в обязательную сертификацию третьей стороны. В регуляторной переписке следует указывать правовой статус каждого элемента. Если специалист выявил несоответствие, необходимо различать методическое замечание, юридическое нарушение и ситуацию, когда информации недостаточно. В противном случае внутренний контроль может стать набором формальных отметок без пригодной базы для решения.

В практической программе ARGA предлагается предварительный аудит по модели «пробная регуляторная проверка»: независимая команда получает реестр системы, карту требований, выборку технических материалов и журнал устранения недостатков. Результатом является список подтверждённых и неподтверждённых тезисов, а не выданный ARGA сертификат. Это позволяет честно позиционировать исследовательскую услугу и не смешивать её со статусом нотифицированного органа.

Практический разбор 17.17

Рекомендация: Документировать внутренний контроль

Условный пример: Поставщик считает отсутствие внешнего органа отсутствием необходимости вести досье.

Разбор: Внутренний маршрут не устраняет потребность обосновать выполненную процедуру.

Практические действия: Ответственный собирает применимые требования, испытания, записи утверждения и версии документации.

Критерий результата: Рецензент восстанавливает основания внутреннего решения по досье.

18. Annex VII: участие нотифицированного органа и техническое досье

18.1. Две части процедуры

Annex VII предусматривает оценку системы управления качеством и технической документации конкретной системы, включая последующий надзор. Важны не только формально принятые инструкции, но и право компетентного оценщика получить необходимые сведения, запросить дополнительные испытания и мотивировать отказ. [6,17-18]

Содержание процедуры существенно отличается от добровольной сертификации AIMS. При проверке по Annex VII предмет, объём доступа, круг заявителей и форма результата определяются специальным нормативным актом. Превратить обычный отчёт о зрелости корпоративных процессов в документ такого режима задним числом невозможно.

18.2. Доступ к данным, моделям и коммерческая тайна

Приложение VII предусматривает при соблюдении условий необходимый доступ к обучающим, валидационным и тестовым данным; в исключительных предусмотренных случаях - к самой обученной модели и соответствующим параметрам. Одновременно учитываются safeguards по интеллектуальной собственности и коммерческой тайне. Это иллюстрирует, почему качественная оценка не сводится к чтению рекламных описаний. [6]

Для внешнего исследовательского договора аналогичный принцип реализуется через согласованную матрицу доступов: документы, API, анонимизированные корпуса, журналы и контролируемая среда. Следует избегать обязательства предоставить больше данных, чем оправдано законной целью, и не объявлять юридически невозможным аудит в случае разумной технической альтернативы.

18.3. Решение, надзор и существенные изменения

Annex VII описывает мотивированное решение и, при положительном результате, соответствующее свидетельство оценки технической документации; система управления качеством продолжает находиться под надзором. Последующие изменения продукта или системы управления могут потребовать дополнительной оценки. [6,13]

С практической точки зрения это означает необходимость версионного реестра. Если модель дообучена на новых источниках либо изменён модуль принятия решений, владелец должен оценить, затрагивает ли изменение ранее подтверждённые свойства. Без такого анализа публичная ссылка на исходное свидетельство может стать неполной.

Практический контрольный список

1. Разграничить оценку системы качества и проверку технической документации.

2. Зафиксировать законную модель доступа к закрытым данным и параметрам.

3. Установить критерии пересмотра при существенных изменениях.

Контроль документации при участии нотифицированного органа

Процедура Annex VII включает оценку системы управления качеством и оценку технической документации с участием нотифицированного органа в установленном объёме. Для ИИ на практике возникают вопросы доступа к исходным данным, критически значимым моделям, тестовой инфраструктуре и коммерческой тайне. При отсутствии подготовленного протокола доступа даже компетентная сторона может не получить достаточных материалов. Поэтому до начала процедуры необходимо согласовать безопасную среду, перечень доступных артефактов и пределы копирования. [6,12,18]

Защита секрета и право на независимую оценку не являются взаимоисключающими. Часть проверки может проводиться с контролируемым доступом, обезличенными выгрузками,

воспроизводимыми тестами и независимым хранением контрольных сумм. Однако если ограничения не позволяют подтвердить обязательное требование, честный результат — не сертификат «с оговоркой обо всём», а запрос дополнительных данных либо применение предусмотренных процедур отказа, приостановления и повторной оценки.

Отдельного контроля требуют изменения после первоначального решения. Если обновился алгоритм, состав обучающих данных, назначение продукта или интеграция с человеком, необходимо определить существенность изменения и условия новой оценки. Регистр таких решений полезно включать в пакет технической документации: он показывает, кто признал изменение несущественным, на каких основаниях и с какими обязанностями наблюдения.

Практический разбор 17.18

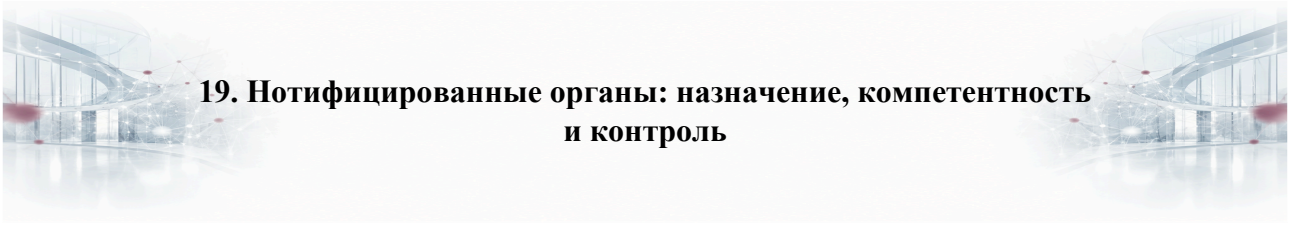
Рекомендация: Согласовывать объём внешней оценки

Условный пример: В договоре указан внешний орган, но не определены версии и изменения системы.

Разбор: Непонятно, какой объект должен быть оценён и что произойдёт после обновления.

Практические действия: Заказчик фиксирует объект, доступ, свидетельства и порядок сообщения изменений.

Критерий результата: Итоговый документ относится к согласованной версии и процедуре.



19. Нотифицированные органы: назначение, компетентность и контроль

19.1. Нотифицирующая власть и независимая компетенция

Каждое государство-член назначает или создаёт компетентный нотифицирующий орган, отвечающий за процедуры оценки, назначения, сообщения и мониторинга органов оценки соответствия по AI Act. Государство может поручить часть оценки национальному аккредитующему органу по Reg 765/2008, однако это не устраняет специальную процедуру публичного признания. [9]

Требования статьи 31 касаются организационной независимости, конфиденциальности, ресурсов, качества процессов и компетенции. В частности, предоставление консультаций, способных поставить под сомнение беспристрастность оценки, вызывает специальную проблему. Поэтому модель «мы разработали продукт, а затем как независимый орган сертифицировали его» не может считаться нейтральной без анализа конфликта интересов. [12]

19.2. Аккредитация как доказательство, а не синоним нотификации

По статье 29 заявление на нотификацию сопровождается необходимым подтверждением компетентности. Статья 30 предусматривает процедуру сообщения Комиссии и государствам-членам; наличие аккредитационного сертификата влияет на процесс, но при альтернативном документальном подтверждении применяются иные условия. Поэтому

вопрос решает конкретный статус нотификации, а не любой иностранный знак аккредитации. [10-11]

При проверке кандидата заказчику нужно установить его полномочия в отношении системы и вида процедуры. Общее указание «notified body» может относиться к другому секторному акту или к другому типу изделия. Для целей AI Act необходимо документальное подтверждение именно релевантной области.

19.3. Обжалование и информирование

Статья 44 предусматривает правила действия сертификатов нотифицированных органов и доступность процедуры обжалования их решений. Статья 45 требует определённых сообщений о выданных, отклонённых, ограниченных, приостановленных и отозванных документах. Это показывает, что сертификат - не бессрочная иммунитетная грамота, а элемент продолжающегося публично-правового контроля. [13-14]

Заинтересованное лицо должно иметь возможность отличить актуальный действующий результат от исторической записи. Для контрактов рекомендуется отдельное требование немедленно сообщать заказчику об ограничении, приостановлении либо изменении области подтверждения.

Практический контрольный список

1. Проверить нотифицирующую власть и точную область признания органа.

2. Выяснить наличие консультационного конфликта интересов.

3. Уточнить статус сертификата и механизмы уведомления об изменениях.

Компетенция нотифицированного органа и вопросы доверия

Нотификация по AI Act основана на специальной публично-правовой процедуре. Требуется установить компетентную нотифицирующую власть, заявленный и фактически предоставленный объём функций, а также соответствие требованиям к органам оценки соответствия. Сертификат ISO/IEC 42001 и аккредитация обычной лаборатории не подтверждают автоматически право действовать нотифицированным органом для иной процедуры. Для конкретного продукта нужен официальный источник статуса и области, а не только письмо продавца услуг. [9-12]

Когда назначение органа опирается на прежние полномочия в отраслевой гармонизации, необходимо проверить переходные особенности и пределы новой компетенции. Для решений, относящихся к праву ЕС, оценка должна учитывать изменённый в 2026 году текст, в том числе процедурные положения статьи 43, а не строиться на старой брошюре. При сомнении приоритет имеют действующие публичные данные компетентного органа и официальный текст нормы. [1,4]

Независимость предполагает также способность принимать неблагоприятные решения. Если коммерческая модель поставщика оценочных услуг ориентирована исключительно на выдачу положительных заключений, доверие к процедуре уменьшается. В закупочных документах следует потребовать механизм отвода эксперта, правила рассмотрения

конфликта интересов, пересмотра решений и жалоб. Но результат юридической оценки не должен подменять компетенцию самого нотифицированного органа.

Практический разбор 17.19

Рекомендация: Проверять назначение органа по нужному предмету

Условный пример: Исполнитель предъявляет полномочия по другому виду продукции.

Разбор: Статус в соседней сфере не подтверждает полномочия на требуемую работу.

Практические действия: Юрист сверяет запись назначения и область с предметом договора.

Критерий результата: Несоответствие устранено до начала процедуры либо выбран иной исполнитель.

20. Гармонизированные стандарты, общие спецификации и презумпции

20.1. Международный стандарт и гармонизация ЕС

Публикация международного ISO/IEC-стандарта не означает автоматического возникновения презумпции соответствия по AI Act. Статья 40 связывает такой эффект с гармонизированным стандартом или его частью, ссылка на который опубликована в Официальном журнале ЕС, и только в пределах охваченных требований. [7]

Практический вопрос состоит из трёх частей: существует ли ссылка в официальной публикации, к какому требованию она относится и покрывает ли выбранная реализация конкретную функцию системы. Инструмент сертификации должен делать эту связь прозрачной; общее утверждение «соответствует стандартам ISO, значит соответствует AI Act» является чрезмерным.

20.2. Общие спецификации по статье 41

Статья 41 разрешает Комиссии при предусмотренных обстоятельствах принимать общие спецификации, если гармонизированные стандарты отсутствуют, несвоевременны либо не решают требуемую задачу. Следование таким спецификациям может породить предусмотренную законом презумпцию в соответствующей части. При использовании альтернативного решения поставщик должен обосновать эквивалентный уровень выполнения применимых требований. [8]

Таким образом, общие спецификации - не произвольный список «рекомендаций экспертов», а особый акт в установленной процедуре. Их нельзя заменять частной сертификационной схемой только потому, что эта схема использует похожие слова: прозрачность, безопасность или контроль человека.

20.3. Карта стандартов и покрытие требований

Для целей закупки и правового заключения полезна двухмерная таблица: строки - юридические обязанности, столбцы - технические нормы, способы испытаний, документальные артефакты и исключения. Каждой клетке присваивается статус «покрыто»,

«частично», «не подтверждено», «не применяется». Это позволяет предотвратить ошибку, когда один общий сертификат используется для закрытия всего нормативного перечня.

Дополнительно следует фиксировать дату проверки гармонизированного статуса. Стандарты развиваются, а публикация новой редакции ISO и публикация ссылки на неё в Официальном журнале ЕС происходят не обязательно одновременно. В условиях активной стандартизации 2026 года эта дата имеет практическое значение.

Практический контрольный список

1. Искать запись о гармонизации именно в Официальном журнале ЕС.

2. Указывать охват презумпции по конкретному требованию.

3. Не представлять частную схему как общие спецификации статьи 41.

Стандартизация как доказательство соблюдения конкретного требования

Международное обозначение ISO/IEC и гармонизация стандарта в праве ЕС описывают разные статусы. ISO разрабатывает и публикует стандарты; презумпция соответствия требованиям специального акта ЕС зависит от условий соответствующей нормы, в том числе официальной публикации ссылки на гармонизированный стандарт в Официальном журнале ЕС и фактического охвата требования. Статья 40 AI Act не превращает автоматически любой стандарт ИИ в инструмент правовой презумпции. [7,20,21]

Практическая таблица покрытия должна связывать каждое обязательное требование с конкретным техническим документом, проверенной версией стандарта, отдельным испытанием и полученным результатом. Если стандартизация не закрывает вопрос объяснимости, соответствующий пробел не устраняется ссылкой на общую сертификацию системы менеджмента. Поставщик может продемонстрировать соответствие иными средствами при соблюдении применимого права, однако качество доказательств и допустимый маршрут процедуры следует устанавливать по закону, а не маркетинговому предложению.

Общие спецификации по статье 41 требуют отдельного анализа: их правовой эффект и условия применения не сводятся к статусу добровольного стандарта. При подготовке заключения нужно указать, используются ли опубликованные гармонизированные стандарты, общие спецификации, частные схемы или авторские методы. Если стандарт ещё находится в стадии FDIS, ссылка на него может иметь прогнозное либо методическое значение, но не должна маскировать его неопубликованный статус.

Практический разбор 17.20

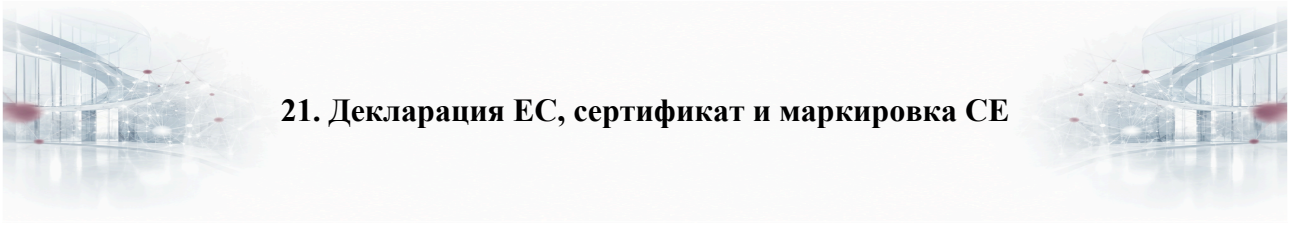
Рекомендация: Связывать стандарт с конкретным требованием

Условный пример: В карте соответствия один стандарт указан напротив всех требований.

Разбор: Общая ссылка скрывает непокрытые свойства и различия редакций.

Практические действия: Эксперт раскладывает требования по свидетельствам и отмечает пробелы покрытия.

Критерий результата: Каждое существенное требование имеет обоснованную связь со свидетельством.



21. Декларация ЕС, сертификат и маркировка CE

21.1. Разные документы в одной процедуре

Статья 47 AI Act предусматривает декларацию соответствия ЕС, которую составляет поставщик для соответствующей высокорисковой системы; предусмотрено содержание декларации и хранение документа. Статья 48 регулирует маркировку CE, в том числе цифровую форму и указание идентификационного номера нотифицированного органа, когда это применимо. [15-16,55]

Ни декларация, ни CE-маркировка не являются синонимами сертификата ISO/IEC 42001. Декларация выражает нормативную ответственность поставщика; сертификат, выданный нотифицированным органом по специальной процедуре, имеет иные основания; знак CE указывает на утверждаемое соответствие установленному режиму, а не на отсутствие любого риска при любом применении.

21.2. Проверка документа по существу

В декларации должны идентифицироваться модель, поставщик, применимое законодательство и использованные основания подтверждения. Если документ невозможно связать с версией системы, он мало полезен в случае спора о результатах. Особенно рискованно, когда декларация относится к другой модели или изменённой комплектации, но представляется как общий документ для нового продукта. [15,55]

Проверяющему необходимо сопоставить декларацию с техническим досье, логикой оценки риска и изменениями после выпуска. В случае участия нотифицированного органа проверяют его название, идентификатор и относящееся к данному продукту свидетельство. Значение имеет не только существование бумаги, но и её действующий предмет.

21.3. Использование знака в маркетинге

Поставщик не должен переносить значение CE-маркировки на свойства, не охваченные нормативным режимом. Например, отметка, связанная с одним изделием, не доказывает точность юридического помощника той же компании. Аналогично знак аккредитации сертификационного органа не является потребительской маркировкой качества любой модели.

Внутренняя проверка публичных заявлений должна отвечать: «какой документ», «к какому объекту», «на основании какого режима», «до какой даты» и «при какой конфигурации». Эти пять вопросов позволяют выявить большинство необоснованных переходов от частного свидетельства к глобальному обещанию безопасности.

Практический контрольный список

1. Не смешивать декларацию поставщика, сертификат нотифицированного органа и сертификат AIMS.

2. Сверять модель, версии, нормативные основания и срок действия.

3. Проверять правомерность использования знаков только в фактическом объёме.

Цепочка от технического досье к маркировке CE

Маркировка CE является юридическим сигналом ответственности соответствующего субъекта за соблюдение применимых требований, а не знаком «безошибочного» поведения модели. Декларация соответствия ЕС, документы оценки и сертификат нотифицированного органа, если он предусмотрен, имеют разные функции. В системе закупки следует установить, кто подписал декларацию, какой продукт и версия в ней описаны, какие акты названы и существует ли предусмотренная процедура хранения документации. [15,16,55]

При совмещении нескольких режимов гармонизации может потребоваться рассмотрение требований различных актов, действующих для одной системы. Нельзя заключить, что наличие отметки CE на регулируемом оборудовании автоматически удостоверяет качество отдельно интегрированного генеративного помощника. Проверяется вся юридически значимая конфигурация и отдельные требования к используемому в ней ИИ. Изменение назначенного применения может влиять и на обязанности поставщика, и на документ, которым подтверждалось соответствие.

Для международного аналитического отчёта полезен отрицательный тест: что именно остаётся недоказанным даже при предъявлении документа? Это могут быть необязательные этические заявления, точность на определённой подгруппе, соответствие чужому национальному праву или актуальность версии после существенного обновления. Список таких пробелов нужен не для дискредитации CE, а для точного определения законной и доказательственной силы конкретного результата.

Практический разбор 17.21

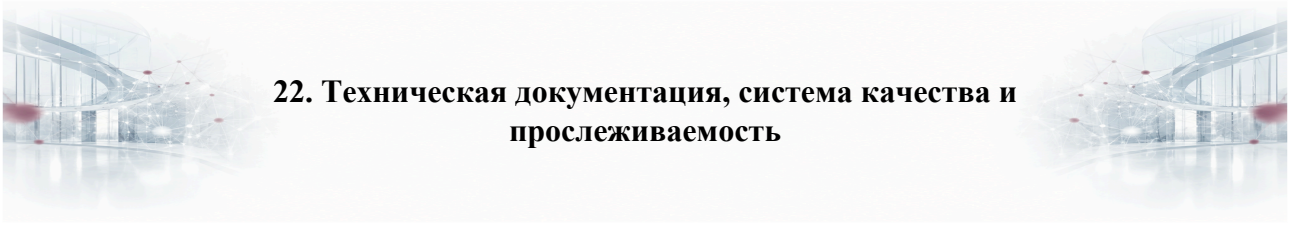
Рекомендация: Согласовывать декларацию и технический объект

Условный пример: Декларация описывает версию A, фактически поставляется версия B.

Разбор: Совпадение торгового названия не подтверждает идентичность объекта.

Практические действия: Ответственный сверяет идентификаторы, изменения и документы до внешнего заявления.

Критерий результата: Маркировка и сопровождающие сведения относятся к фактическому объекту.



22. Техническая документация, система качества и прослеживаемость

22.1. Архитектура документального досье

Приложение IV AI Act перечисляет содержание технической документации с учётом применимости: назначение системы, версии, взаимодействующие компоненты, используемая инфраструктура, разработка, тестирование и другие сведения. Статья 17 касается системы управления качеством. Эти два блока взаимосвязаны, но не взаимозаменяемы: документация продукта описывает объект, а организационные процедуры показывают, как он контролируется в течение жизненного цикла. [17-18]

Состав досье целесообразно закрепить до первого испытания. Если доказательства собираются только после обнаружения проблемы, появляется риск выборочного сохранения благоприятных результатов. Для каждого артефакта указываются источник, дата, ответственное лицо, версия и разрешённый режим раскрытия.

22.2. Происхождение данных и независимость записи

Материал об обучающих данных нужен в пределах применимых юридических оснований и фактического доступа. Достоверная оценка требует не просто слова «качественные», а сведений о происхождении, правомерности, пригодности, представительности и обновлениях данных. В ряде случаев коммерческая тайна ограничивает публичное раскрытие, но это не оправдывает отсутствие внутреннего следа управления и оценки.

Для данных санкционных или полицейских совпадений необходимо отделять авторитетный источник записи, извлечённую копию, нормализацию и алгоритмическое предположение об идентичности лица. Ошибка на одном этапе может привести к юридическому последствию, которое не исправляется высокой средней метрикой по другим стадиям.

22.3. Срок хранения и защита доказательств

Статья 18 AI Act устанавливает специальное правило хранения отдельных видов документов на установленный срок после размещения на рынке или ввода в эксплуатацию высокорисковой системы. Однако передача персональных данных, срок хранения конкретного рабочего массива и доступ аудитора также подчиняются самостоятельным требованиям о защите данных и конфиденциальности. [45]

Следует отделять постоянную обязанность сохранить нормативную техническую документацию от неоправданного хранения персональных данных из тестового корпуса. Допустимы псевдонимизация, ограниченный архив и проверяемые правила удаления копий при сохранении необходимого доказательственного следа.

Практический контрольный список

1. Связать каждое утверждение с конкретным элементом досье и его версией.

2. Развести регуляторный срок хранения и режим персональных данных.

3. Отслеживать происхождение сведений из внешних списков и баз.

IV. ТЕХНИЧЕСКАЯ И ДОКАЗАТЕЛЬСТВЕННАЯ ПРОВЕРКА

Сроки хранения, идентификация версии и след доказательства

Техническое досье должно позволять восстановить состояние системы, относительно которого сделано юридическое или инженерное утверждение. Для этого недостаточно файла с названием модели. В контрольный пакет разумно включать описание назначения, реестр компонентов, конфигурацию интерфейсов, происхождение данных, правила обработки результатов, сведения о тестовом окружении и таблицу исправления известных недостатков. При изменении внешней модели следует сохранять точный идентификатор установленной версии и условия её доступности. [17,18,45]

Поскольку документы могут одновременно содержать коммерческую тайну и персональные данные, нужен раздельный доступ к первичным материалам и к их доказательственным метаданным. Отчёт может хранить контрольные суммы и ссылки на закрытое хранилище вместо полной копии массива; рецензент должен понимать способ получения доступа и возможность независимой повторной проверки. Для согласования с GDPR и отраслевыми правилами задают назначение обработки, круг лиц, основание передачи и период хранения по конкретному виду записи, не утверждая, что AI Act автоматически разрешает любое использование данных.

Отдельным этапом является квалификация существенного изменения. Не всякая замена текстовой метки требует полной новой процедуры, но изменение модели, данных или области применения может нарушить предпосылки прежней проверки. Решение о необходимости новой оценки должно быть документировано ответственным лицом с сопоставлением исходных и новых рисков, а не оставлено только владельцу продукта или поставщику API.

Практический разбор 17.22

Рекомендация: Поддерживать прослеживаемость досье

Условный пример: Отчёт содержит ссылки на файлы, которые перезаписаны новой версией.

Разбор: Рецензент не может восстановить материалы, использованные при решении.

Практические действия: Хранитель фиксирует версии, контроль целостности и срок доступа; сохраняет исходные записи.

Критерий результата: Каждое существенное утверждение связано с доступной неизменной версией материала.

23. Проектирование технических испытаний и границы статистики

23.1. Тестовый дизайн до получения результата

План испытания начинается с определения измеряемого параметра. Для доли правильных ссылок необходимо уточнить, считаются ли все ссылки, только существенные ссылки или досье без единой неверной существенной ссылки. Эти параметры имеют разные знаменатели и разный смысл для пользователя. Затем фиксируются совокупность, отбор, эталон, правила отказов и пропусков, метод оценки неопределённости и решение у порога. Изменение определения после просмотра результата требует новой версии протокола.

Набор для настройки, независимый итоговый набор и диагностические сценарии выполняют разные функции. Первый помогает разработать систему и критерии; второй позволяет выполнить заранее определённую оценку; третий выявляет способы отказа. Результаты диагностического набора не подменяют оценку распространённости ошибок. Если испытание включено в формальную схему соответствия, правила схемы устанавливаются отдельно и имеют приоритет перед авторским примером доклада.

23.2. Precision, recall и юридическая цена ошибок

В задачах поиска совпадений ошибочная идентификация лица (false positive) и пропуск действительного совпадения (false negative) создают разные последствия. Утверждение «accuracy 99%» малоинформативно при сильном дисбалансе классов: модель, всегда отвечающая «совпадений нет», может получить высокую общую долю правильных ответов и быть непригодной для цели. Нужны матрица ошибок, правила порога и характеристика базовой распространённости класса.

В правоприменительной и финансовой сфере обязательно фиксируют действия после флага системы: это только рекомендация сотруднику, временная блокировка, сообщение в орган либо отказ клиенту? Даже одинаковая вероятность ошибки может быть приемлемой или недопустимой в зависимости от характера и обратимости решения.

23.3. Интервалы и нулевые наблюдения

Если в условной независимой выборке из 300 случаев не выявлено ни одного опасного сбоя, это не означает доказанного нулевого риска. При упрощённой биномиальной модели односторонняя верхняя 95-процентная граница вероятности события равна 1 - 0,05^(1/300), то есть приблизительно 0,99%. Для редкого события это важное ограничение даже при кажущемся безупречном испытании.

Модель независимых одинаково распределённых испытаний может не выполняться для серий связанных запросов к одной генеративной системе. Тогда формальное число не должно публиковаться без оговорки. Для проверок, где возможен тяжёлый вред одному лицу, статистику следует дополнять стресс-сценариями и правовым анализом процедуры вмешательства.

Правило решения при пограничном результате

В условной схеме критерий допуска установлен заранее: нижняя граница двустороннего 95%-го интервала Уилсона для доли успешных досье должна быть не ниже 90%. При 94 успехах из 100 интервал составляет примерно 87,5–97,2%, поэтому данных для предусмотренного положительного решения недостаточно. Этот результат не доказывает, что истинная доля успеха ниже 90%. В интервале не отражены автоматически нерепрезентативность набора, ошибочная разметка и зависимость досье; их оценивают отдельно. Порог и правило являются условиями учебной схемы, а не требованиями ISO или AI Act. [M2]

Практический контрольный список

1. Публиковать матрицу ошибок и знаменатели, а не один процент успеха.

2. Отмечать вероятность отбора сценариев и возможную систематическую предвзятость.

3. Чётко разграничивать результаты модели и последствия решения человека.

Протокол испытаний с заранее установленными порогами

Пороговое решение проверяют в двух плоскостях. Сначала устанавливают корректность расчёта при выбранной модели наблюдений. Затем исследуют устойчивость вывода к обоснованным изменениям разметки, учёту пропусков и исключению зависимых повторов. Если положительный итог появляется только после удаления неудобных наблюдений, это требует отдельного обоснования. План дополнительного набора данных определяется заранее: последовательное добавление случаев до первого благоприятного результата без соответствующего статистического дизайна не сохраняет смысл исходной процедуры.

При нескольких вариантах одного имени, повторах по одному клиенту или задачах из одного досье исследование имеет кластерную структуру. Объём доказательств нельзя оценивать только числом строк. Протокол указывает независимую единицу, число таких единиц и способ учёта вложенности. Если исходный отчёт не позволяет восстановить зависимость наблюдений, интервал из него не принимается как достаточное основание положительного заверения без дополнительной проверки.

Стресс-тесты должны изучать механизм сбоя: задержку поступления новых сведений, конфликт между реестрами, отсутствие уникального идентификатора, неожиданные символы, сбой внешнего API и некорректную реакцию человека на рекомендацию системы. Один показатель качества плохо отражает совокупность этих рисков. Результат представляется в виде набора метрик, классифицированных ошибок и формулировки о том, что исследование не охватывало. Если результаты невозможно повторить из сохранившихся материалов, обоснованность заверения ограничена независимо от красоты итогового процента.

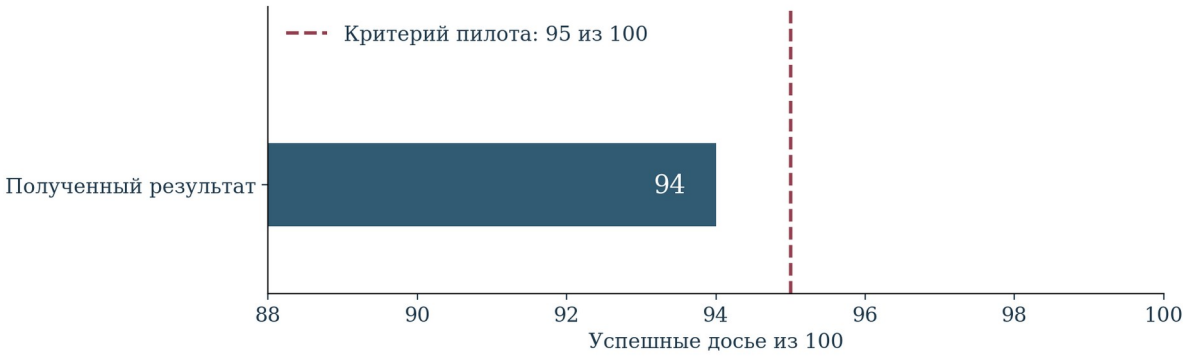


Рисунок 17.3. Пограничный результат и заранее установленный критерий. Условный пример практического разбора 17.10. Изображение показывает разницу в одно досье; горизонтальная шкала начинается с 88. Порог не меняется после испытания.

Практический разбор 17.23

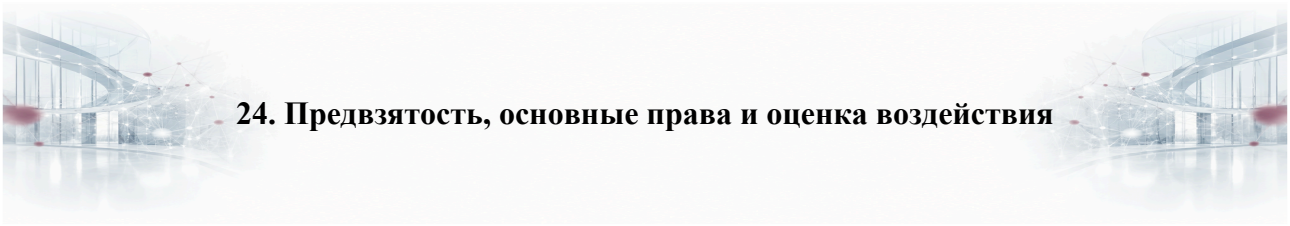
Рекомендация: Утверждать план испытаний заранее

Условный пример: После слабого результата исключили самые сложные досье.

Разбор: Показатель относится уже к другой совокупности и не отвечает исходному вопросу.

Практические действия: Статистик сохраняет первоначальный расчёт и отдельно анализирует изменение набора.

Критерий результата: Показаны все исключения и влияние каждого на решение.



24. Предвзятость, основные права и оценка воздействия

24.1. Групповые различия требуют предметной интерпретации

Разница в средних метриках между группами может отражать особенности тестовых данных, конфигурацию системы, неодинаковое качество первичных записей либо дискриминационный эффект. Универсального одного показателя «справедливости» не существует. Необходимо определить, какие группы юридически и фактически релевантны, какие характеристики допустимо обрабатывать и какую ошибку следует минимизировать. [29,39,44]

В рассмотрении кредитных или кадровых решений особенно важно различать статистическую корреляцию и вывод о правовой дискриминации. Последний требует проверки применимого права, контекста, возможных оправданий и процессуальных гарантий. Технический отчёт служит доказательством части обстоятельств, но не заменяет квалифицированный правовой вывод.

24.2. Оценка воздействия и пределы сертификата

ISO/IEC 42005:2025 посвящён оценке воздействия системы ИИ на людей, группы и общество на протяжении жизненного цикла. Подход полезен для выявления потенциальных негативных последствий, однако открытая карточка ISO не даёт оснований утверждать, что сам стандарт является сертификатом соблюдения всех прав человека. [29]

Статья 27 AI Act предусматривает специальную оценку воздействия на основные права для определённых участников и ситуаций, имеющую собственные условия применения. Организационная оценка по международному руководству и юридически требуемый процесс должны рассматриваться раздельно, хотя информация между ними может использоваться с соблюдением закона. [51]

24.3. Вовлечение затронутых сторон

Надёжная оценка воздействия невозможна только по тексту маркетинговой инструкции поставщика. Необходимо учитывать практическое использование, жалобы, возможность человеческого пересмотра и то, понимают ли затронутые люди причины неблагоприятного решения. Когда прямой контакт невозможен, следует обозначить это ограничение и использовать допустимые косвенные свидетельства.

Для ARGA особенно существенен принцип недопустимости автоматического переноса сомнительной записи из одной базы в другую. Человек должен иметь определённый путь

оспаривания, а проверка качества должна различать ошибку идентичности, ошибку интерпретации и ошибку правовой квалификации.

Практический контрольный список

1. Выбирать показатели с учётом последствий ошибок для разных групп.

2. Отделять техническую статистику от юридического заключения о дискриминации.

3. Проверять реальность каналов жалоб и человеческого пересмотра.

Основные права и качество средства исправления ошибки

Оценка предвзятости требует выяснить, какие лица и права затрагивает система. Для решения о занятости, доступе к банковской услуге и международном полицейском обмене одинаковая разница в метрике может иметь различные последствия. Поэтому статистические тесты должны дополняться картой принимаемых решений, степенью обратимости вреда, процедурой уведомления и доступностью эффективной проверки человеком. Простое равенство средних показателей не исключает систематической ошибки в редких, но критических случаях. [1,39,44,51]

При выборе групп для сравнения необходимо соблюдать право на защиту персональных данных и ограничения сбора чувствительной информации. Отсутствие допустимых групповых данных не позволяет заявлять отсутствие дискриминации; следует описать невозможность измерения и доступные альтернативные методы контроля. Если группа мала, узкий численный результат без интервала может создать ложную уверенность. Для практического заключения важно различать наблюдаемое расхождение, юридическую квалификацию и вывод о необходимости корректирующего действия.

Процедура рассмотрения жалоб должна быть действующей. Наличие кнопки «обжаловать» не доказывает независимый пересмотр, если тот же алгоритм автоматически утверждает первоначальный вывод. Нужно проверить возможность представления новых данных, компетенцию проверяющего лица, сроки, журнал исправлений и доступность обоснованного ответа. Для ARGA особенно важна проверка способности исправлять исходный идентификационный признак, а не только пересчитывать оценку на ошибочной исходной записи.

Практический разбор 17.24

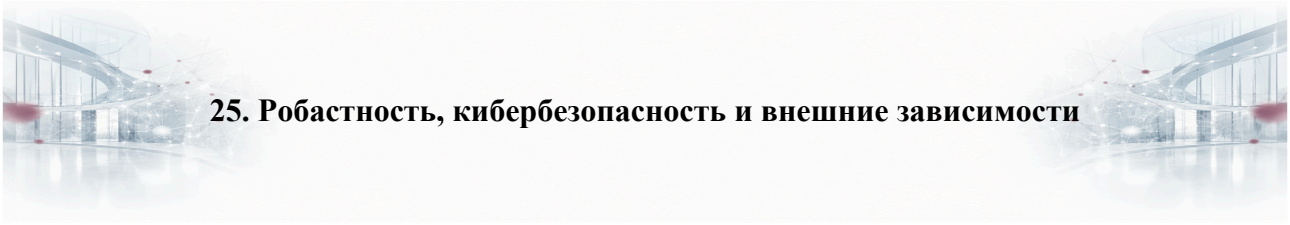
Рекомендация: Проверять воздействие на затронутых лиц

Условный пример: Система чаще отклоняет заявки с неполными цифровыми данными.

Разбор: Проблема может касаться доступности процедуры, а не только средней точности.

Практические действия: Команда анализирует основания отказов и доступный ручной пересмотр; отдельно изучает группы сопоставимых заявок.

Критерий результата: Для спорного отказа доступен содержательный пересмотр по исходным сведениям.



25. Робастность, кибербезопасность и внешние зависимости

25.1. Устойчивость к разумно предсказуемым условиям

Стабильность AI-системы зависит от качества ввода, языка, оформления документа, шумов, изменений среды и попыток преднамеренно вызвать ошибку. Поэтому испытание на «типовых» документах не является достаточным для сервиса, который применяют к разноязычным именам, повреждённым файлам и неструктурированным архивам. Нужны модель угроз и документированный диапазон условий. [39-41]

При сравнении устойчивости следует фиксировать не только долю ошибок, но и характер деградации: может ли система отказаться от ответа, передать результат человеку, показать неопределённость или молча породить ложное фактическое утверждение. Для юридических и финансовых задач безопасный отказ иногда предпочтительнее уверенного вымысла.

25.2. Prompt injection и цепочка инструментов

Генеративный помощник, который читает внешние документы и вызывает программные инструменты, может принять враждебный текст из источника за распоряжение. Такой риск относится не только к качеству языковой модели, но и к настройкам разрешений, приоритетам инструкций, фильтрации содержания, журналированию и человеческому подтверждению действия.

В аудиторском деле нужно иметь ясную схему доверенных и недоверенных источников. Испытания проводят в изолированной среде с согласованным объёмом; результаты атакующей проверки описывают как выявленные особенности конфигурации, а не как универсальное доказательство способности нарушить любую систему.

25.3. Контроль поставщиков, облаков и обновлений

При внешнем API основной разработчик может изменять модель или инфраструктуру. Интегратор должен установить контрактный уровень контроля: уведомления о версиях, журнал несовместимых изменений, механизмы аварийного отключения и план обратимости. Без этого первоначальный отчёт может быть действителен только для короткого технического состояния.

Особое внимание уделяется трансграничной передаче сведений, правам доступа к данным клиента и ограничениям использования вводимых документов для обучения. Даже сертифицированная система менеджмента поставщика не позволяет предполагать, что конкретный договор обеспечивает необходимый режим конфиденциальности.

Практический контрольный список

1. Формировать модель угроз с учётом языковых и контекстных отклонений.

2. Проверять возможность безопасного отказа и ограничения действий инструментов.

3. Контрактно определить последствия скрытого изменения внешней модели.

Атаки на модель и зависимость от инфраструктуры

Для AI Assurance безопасность интерфейса недостаточна: необходимо оценивать цепочку загрузки данных, промпты, векторный поиск, инструменты агента, внешние плагины и полномочия доступа. Уязвимость может возникать при смешивании пользовательской инструкции с непроверенным фрагментом внешнего документа. В таком случае технически корректная модель выполняет ложный рабочий контекст. Предмет исследования — не абстрактная «защита от всех атак», а заранее определённый профиль угроз и доказательства того, какие атаки система обнаруживает, ограничивает и документирует. [39,40,43]

Испытания следует повторять на реалистичных сценариях: внедрение в документ скрытой инструкции, попытка извлечь клиентские данные, ошибочная выдача прав на создание письма, загрязнение поискового индекса и нарушение связи с внешней моделью. При этом критично не описывать опасные техники как универсальные рецепты, а оценивать наличие защитных слоёв и контролируемое поведение системы. Эксперт должен указывать применённую версию, число сценариев и остаточные уязвимости, поскольку смена модели и защиты быстро меняет результаты.

Сертификат управления информационной безопасностью или отдельная проверка проникновения могут служить частью свидетельств, но не заменяют исследования задач с вероятностным результатом. Для чувствительных юридических операций важны ограничения автономного выполнения действия: подготовка документа, проверка человеком и отправка должны иметь разные права и журнал. Это особенно существенно для агентных инструментов с доступом к почте, файлам и финансовым операциям.

Практический разбор 17.25

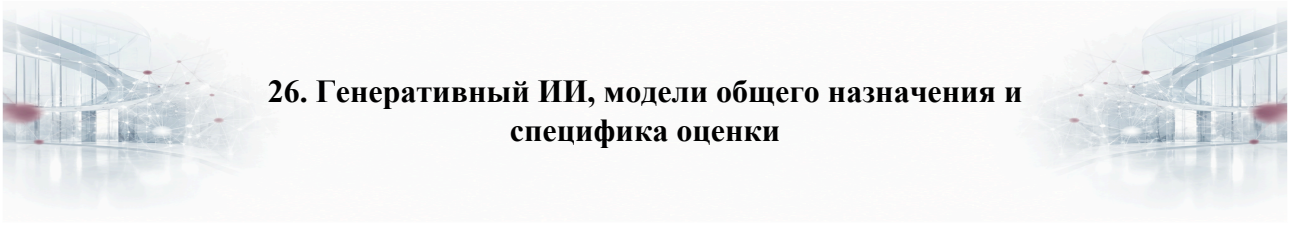
Рекомендация: Проверять внешние зависимости

Условный пример: После обновления библиотек помощник перестал корректно обрабатывать вложения.

Разбор: Прежние испытания не покрывают изменившуюся цепочку обработки.

Практические действия: Инженер фиксирует зависимости и проводит регрессию на сохранённых и новых допустимых файлах.

Критерий результата: Досье содержит версию зависимости и результаты повторной проверки.



26. Генеративный ИИ, модели общего назначения и специфика оценки

26.1. От способности модели к пригодности применения

Универсальная языковая модель может показывать высокие результаты на стандартном бенчмарке и при этом ошибаться на договоре с необычным правовым контекстом. Поэтому оценка базовой модели и оценка законченного продукта должны разделяться. Для второй необходимы документы пользователя, подключённые инструменты, правила обращения с источниками и процедурные последствия ответа. [39-41]

Пригодность модели для информационного поиска нельзя механически переносить на юридическое консультирование, медицинские решения или автоматический отказ клиенту. Именно применение определяет допустимый риск и требуемую доказательственную программу.

26.2. GPAI в праве ЕС

AI Act устанавливает самостоятельные обязанности поставщиков моделей общего назначения (GPAI), а для моделей с системным риском - дополнительный набор мер. Эти обязанности юридически не тождественны правилам оценки соответствия высокорисковых законченных AI-систем по Annex VI/VII. Наличие внешнего аудита провайдера не позволяет без проверки считать выполненной каждую норму о GPAI. [1,49-50]

Если интегратор использует GPAI-модель как компонент высокорискового сервиса, важно различать обязанности самого поставщика модели и обязанности поставщика законченной системы. Доступность информации об исходной модели становится вопросом цепочки ответственности, но не превращает всех участников в одного субъекта.

26.3. Нестабильность оценок и воспроизводимость

Параметры генерации, переключение модели и изменения внешнего поискового индекса способны изменять результат одного и того же запроса. Для заверения этого класса систем нужны повторения, журнал настроек и периодическая переоценка на независимых наборах. Если входящие материалы конфиденциальны, можно применять искусственные кейсы со специально размеченными ошибками без передачи реальных клиентских досье.

При публикации следует указывать, что оценки справедливы для заданных условий и времени. Утверждение «LLM не галлюцинирует» практически непроверяемо в абсолютном смысле; гораздо полезнее доля ответов с подтверждаемой цитатой на определённом корпусе, проверенная независимым рецензентом.

Практический контрольный список

1. Развести базовую модель GPAI и конечную прикладную систему.

2. Измерять качество в реальной конфигурации, включая инструменты и источники.

3. Привязать вывод к точной версии модели и правилам повторной оценки.

Особенность генеративной модели и ответственности интегратора

AI Assurance для модели общего назначения не равен проверке приложения, которое использует такую модель. Документация базового провайдера может быть надлежащей для его роли, но конкретный интегратор определяет источники корпоративного поиска, доступ сотрудников, шаблоны инструкций и допустимые внешние действия. Его заверение должно охватывать эти самостоятельные элементы. Соответствующие обязанности по AI Act различаются для поставщиков моделей GPAI и для поставщиков или операторов конечных систем; смешение ролей искажает правовую оценку. [1,49,50]

Для генеративного помощника тестирование требует фиксировать промпт, контекст поиска, температуру и иные существенные параметры, версию модели, доступные инструменты и эталон правильного ответа. Метрика «сходства с ответом эксперта» не всегда обнаруживает вымышленную правовую ссылку или пропуск процессуального срока. Для чувствительных досье разумно классифицировать ошибки по последствиям: неверная цитата, несуществующий источник, неподтверждённый факт, разглашение сведений, самостоятельное выполнение запрещённого действия. Каждый класс требует собственного порога допуска.

При использовании агентного ИИ необходимо оценивать полномочия, а не только текстовую генерацию. Даже корректный ответ может создать риск, если агент имеет право отправить письмо или изменить файл без подтверждения. Сингапурская рамка управления агентным ИИ 2026 года подчёркивает роль предварительных ограничений и значимых контрольных точек человека. Для ARGA это означает разделение функции анализа и функции юридически значимого действия. [43]

Практический разбор 17.26

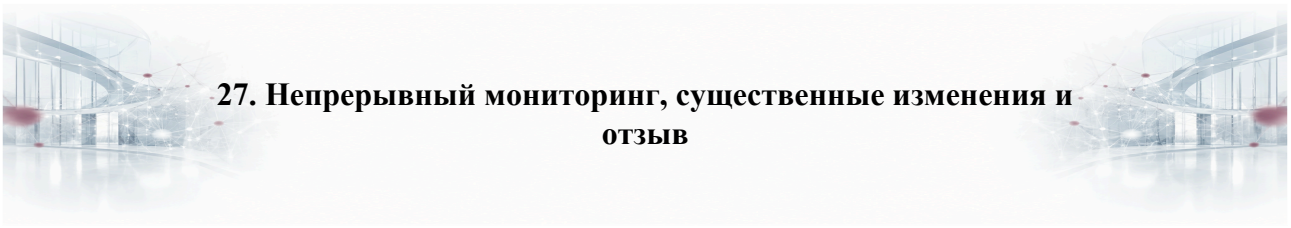
Рекомендация: Оценивать генеративный продукт в контексте использования

Условный пример: Базовая модель хорошо отвечает на общие вопросы, но ошибается на сканах клиента.

Разбор: Публичная оценка модели не характеризует качество извлечения документов в продукте.

Практические действия: Оценщик испытывает всю конфигурацию с поиском, OCR и человеческой проверкой.

Критерий результата: Вывод относится к продуктовой сборке и конкретному назначению.



27. Непрерывный мониторинг, существенные изменения и отзыв

27.1. Почему сертификат не бессрочная гарантия

Для систем ИИ дрейф данных, обновления внешнего поставщика, изменение языковой среды и рост числа пользователей могут повлиять на свойства после первоначальной оценки. В AI Act предусмотрены процедуры в отношении существенных изменений и пострыночного

мониторинга; нотифицированные сертификаты могут ограничиваться или отзываться при предусмотренных основаниях. [4,13,52]

Отдельная управленческая программа должна связывать факты изменения с решением: оставить подтверждение в силе, провести ограниченный повторный тест, расширить аудит или инициировать предусмотренную законом новую оценку. Порог пересмотра нельзя определять исключительно коммерческой стоимостью повторного испытания.

27.2. События, запускающие внеплановую проверку

Триггерами являются изменения модели, данных, назначения, группы пользователей, правил принятия решения, доступа к конфиденциальным сведениям или регуляторной классификации. Серьёзный инцидент требует оценки последствий, сохранения журналов и надлежащего уведомления, если этого требует применимое право. [52-53]

Организационная документация должна отличать горячее исправление от существенной модификации. Иногда блокировка опасного сценария не требует полной сертификации, но каждое исправление необходимо испытать на регрессию, чтобы не создать новую скрытую ошибку.

27.3. Статус результата и публичное обновление

Если орган отозвал сертификат, поставщик обязан скорректировать публичные заявления и информацию, предоставленную клиентам, в соответствии с законом и договором. Действующий контракт может предусматривать обязанность сообщать об ограничении статуса в определённый срок и право независимой перепроверки. При покупке критического AI-сервиса такие условия не менее важны, чем начальная копия сертификата.

Свидетельства предыдущих версий следует хранить как исторические документы с метаданными. Удаление истории после неудачной оценки разрушает доказательственную цепочку и затрудняет рассмотрение потенциальных жалоб. Одновременно нужно соблюдать минимизацию хранения персональных данных.

Практический контрольный список

1. Определить правовые и технические триггеры повторной оценки.

2. Описать действия при ограничении или отзыве подтверждения.

3. Сохранять историю выводов без необоснованного хранения клиентских данных.

V. СРАВНИТЕЛЬНАЯ И ИНСТИТУЦИОНАЛЬНАЯ ПРАКТИКА

Мониторинг как условие сохранения доказательственной силы

Однократный положительный тест быстро теряет ценность, когда меняется распределение данных, внешний провайдер или рабочий процесс. Поэтому в практической модели следует различать плановый мониторинг, повторную проверку после значимого изменения и расследование конкретного инцидента. Триггерами могут быть ухудшение точности на критической подгруппе, изменение источника данных, увеличение нагрузки ложных

совпадений, жалобы пользователей, обновление модели и обнаруженное нарушение ограничений доступа. [52,53]

Для каждого триггера нужен собственный маршрут: кто принимает сообщение, какой артефакт сохраняется первым, кто может остановить использование системы, какие лица уведомляются и в какой срок выполняется переоценка. Следует различать внутреннюю операционную остановку, приостановление сертификата компетентным органом и юридические меры по специальному регулированию. Это разные статусы, и ни один не должен предполагаться без соответствующего решения.

Рекомендуется хранить цепочку «обнаружение — верификация — коррекция — независимая повторная проверка — закрытие». Закрытие по факту изменения инструкции, без проверки эффективности, недостаточно. Для поставщиков чувствительных систем полезны обязательства об уведомлении заказчика не только о критическом киберинциденте, но и о существенной деградации метрик или прекращении применимости прежнего отчёта. В публичном заверении нужно указывать дату последнего подтверждённого статуса.

Практический разбор 17.27

Рекомендация: Пересматривать оценку после существенного изменения

Условный пример: Поставщик добавил автоматическую отправку уведомлений к ранее текстовому помощнику.

Разбор: Последствия изменились, поэтому прежний допуск не покрывает новую функцию.

Практические действия: Владелец проводит оценку изменения и отдельный тест полномочий до включения отправки.

Критерий результата: Новая функция имеет собственное мотивированное решение о допуске.

28. Великобритания: регулируемый рынок AI Assurance и UKAS

28.1. Политика доверенного внешнего подтверждения

Опубликованная DSIT 3 сентября 2025 года Trusted third-party AI assurance roadmap рассматривает развитие профессионального рынка внешних проверок ИИ, компетенций специалистов и процедур подтверждения качества. Документ описывает возможности, ограничения и потребность в стандартизации, а не вводит универсальный обязательный сертификат на все AI-системы в Великобритании. [32]

Подход полезен для сравнительного анализа: государство пытается повысить качество поставщиков assurance, не смешивая все отраслевые задачи в один документ. Для заказчика это подтверждает необходимость выбирать вид оценки по риску и назначению, а не по модному наименованию консалтингового продукта.

28.2. Аккредитация ISO/IEC 42001

15 января 2026 года UKAS объявил о первой аккредитации BSI для сертификации AI management systems по ISO/IEC 42001:2023. Это конкретный факт развития рынка

аккредитованной сертификации систем менеджмента ИИ, но не основание утверждать, что все системы, связанные с BSI, получили разрешение на юридически чувствительное применение. [33-34]

При выборе британского органа заказчику следует проверять область аккредитации и применимую схему. Британское решение также не заменяет требования о нотификации при соответствующем применении права ЕС. Трансграничное признание требует отдельного анализа юридической компетенции.

28.3. Вывод из британской модели

Великобритания разграничивает развитие рынка услуг assurance, профессиональные компетенции и инфраструктуру аккредитации. Такая модель открывает пространство для специализированной экспертной работы, особенно при правовой оценке AI-систем в регулируемых сферах, без немедленного создания единого «AI Safety Certificate» для всей экономики.

Для ARGA релевантны исследования качества доказательств, составление юридической карты и независимая экспертиза заявлений заказчика. До получения какой-либо специальной аккредитации эти услуги следует описывать как аналитические и экспертные, не используя термин «аккредитованная сертификация».

Практический контрольный список

1. Проверять утверждения о UKAS через официальный реестр и область аккредитации.

2. Разделять стратегию развития рынка и действующую юридическую обязанность.

3. Не переносить британское коммерческое признание на нотификацию ЕС.

Британская экосистема: доказательный продукт вместо абстрактного доверия

Британская модель AI Assurance развивается через сочетание отраслевых требований, профессиональной инфраструктуры аккредитации и опубликованных государственных дорожных карт. Документы DSIT о доверенной сторонней оценке полезны как описание политики развития рынка, но не следует автоматически считать их единым законом, который требует сертификации каждой AI-системы. Конкретный контракт и отраслевой режим определяют, какой тип доказательств действительно нужен заказчику. [32,33,34]

UKAS имеет значение как аккредитационный орган, однако его компетенция по отдельной программе оценивается по объявленной и действующей области. Даже первое выданное признание в направлении AIMS не означает наличия глобального полномочия выдавать сертификаты по всем AI-инструментам. При проверке британской компании нужно раздельно подтверждать статус аккредитации органа оценки, допустимую схему и соответствие оказанной услуги заявленному объёму.

Для международных организаций особенно полезна договорная дисциплина. Заказчик может предусмотреть доступ к независимым испытаниям, обязанность сохранять журналы, раскрытие конфликта интересов и пересмотр статуса после обновления модели, даже если специальное законодательство не требует конкретного сертификата. Но в отчёте ARGA такая договорная обязанность должна обозначаться как условие сторон, а не как автоматическое следствие британского публичного права.

Практический разбор 17.28

Рекомендация: Проверять местный предмет assurance

Условный пример: Британский отчёт предлагают как универсальное подтверждение для зарубежного заказчика.

Разбор: Процедура полезна как свидетельство, но её юридическое значение зависит от адресата.

Практические действия: Юрист сопоставляет назначение и критерии отчёта с местной задачей.

Критерий результата: Остаточные проверки перечислены до принятия результата.

29. США: NIST, добровольные рамки и отраслевой контекст

29.1. Добровольная рамка управления рисками

NIST AI Risk Management Framework 1.0 опубликована в январе 2023 года как добровольный, межотраслевой инструмент управления рисками. Она помогает организовать процессы идентификации, измерения и управления рисками, но не является федеральной лицензией или общенациональным сертификатом соответствия, выдаваемым всем AI-системам. [39]

Профиль для генеративного ИИ NIST AI 600-1 развивает подход применительно к характерным рискам генеративных моделей. В 2026 году NIST также указывает на работу по пересмотру AI RMF 1.0. Следовательно, при использовании этой рамки в договоре нужно

фиксировать версию и статус документа, не выдавая проект обновления за окончательный текст. [40-41]

29.2. TEVV как доказательственная функция

NIST использует понятие testing, evaluation, verification and validation (TEVV) для совокупности проверочных процессов. В рамках одной программы могут быть нужны инженерные испытания, мониторинг реального использования и оценка управленческих процедур. Никакой один процент accuracy не покрывает весь набор задач. [41]

Американская практика даёт удобный пример функционального подхода: начать с оценки риска и целей системы, определить адекватные виды испытаний, документировать результат и условия его применимости. Но официальный материал NIST нельзя приравнивать к обязательному разрешению на определённое коммерческое применение в конкретном штате или секторе.

29.3. Отраслевые и договорные ограничения

В США регулирование может зависеть от отрасли, назначения и юрисдикции. Поэтому невозможен короткий правовой вывод «сертификат ISO действует во всех США». Для банковской, кадровой, медицинской и государственной сфер требуется специальное изучение применимых норм и практики контролирующих органов.

В трансграничных проектах разумно использовать общую техническую матрицу рисков и отдельно проводить юридическую квалификацию для каждой страны. Так сохраняется возможность повторно использовать проверенные тестовые доказательства без ложного утверждения, что единая оценка заменила все региональные юридические процедуры.

Практический контрольный список

1. Называть NIST AI RMF добровольной рамкой, а не сертификатом.

2. Разделять универсальную методику TEVV и обязательства конкретного сектора.

3. Проверять актуальность редакции NIST перед официальным использованием.

Американская оценка риска: граница добровольной методики

NIST AI RMF 1.0 предлагает добровольный подход к управлению рисками ИИ, а профиль генеративного ИИ дополняет его предметными рисками. Сам по себе факт использования терминов NIST не является выдачей NIST сертификата. Для действительного правового анализа следует отдельно проверять федеральные, штатные и отраслевые обязанности применительно к конкретной системе. В США нет одного универсального федерального сертификата соответствия ИИ, который заменяет все виды испытаний, надзора и договорных проверок. [39,40,41]

Практическая карта RMF может связывать управление, описание контекста, измерение и обработку риска с управленческими записями и экспериментальными тестами. Например, контроль ложных совпадений в финансовом мониторинге потребует не только уровня риска, но и порога срабатывания, обзора ложных тревог, качества списков, процесса человеческого

решения и анализа последствий отказа в обслуживании. Работа только с документами о политике без проверки реальных записей неполна.

Для международных исследований важно избегать «импорта норм»: методическая рекомендация федерального американского института не создаёт без специального основания обязательства для европейского или сингапурского поставщика. Она может быть полезным общим языком оценки, но юридический статус должен быть назван точно. Договорное включение NIST в требования закупки также следует отделять от законодательства.

Практический разбор 17.29

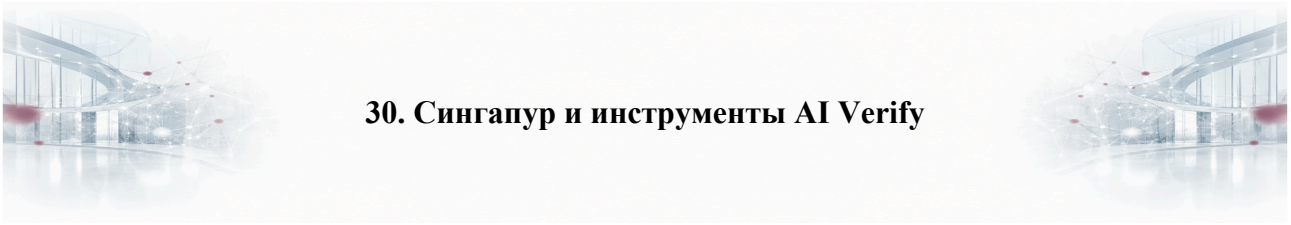
Рекомендация: Не превращать рамку NIST в сертификат

Условный пример: В презентации написано, что продукт сертифицирован NIST, но представлен внутренний профиль риска.

Разбор: Методическая рамка и выданный уполномоченным органом документ имеют разный статус.

Практические действия: Редактор проверяет основание и заменяет заявление точным описанием использованной методики.

Критерий результата: Публичный текст подтверждается реально существующим документом.



30. Сингапур и инструменты AI Verify

30.1. Тестовая инфраструктура без универсальной «лицензии»

IMDA разработала AI Verify как рамку тестирования управления ИИ и набор программных инструментов. Официальная информация описывает ориентацию на принципы прозрачности, воспроизводимости, безопасности, справедливости и других свойств, а также адаптацию для генеративного ИИ. Это полезный практический ориентир для испытаний, но его использование само по себе не создаёт юридического сертификата допуска ко всем рынкам. [42]

Технический инструмент должен оцениваться по доступному набору тестов, объёму входных данных и квалификации лица, интерпретирующего результат. Использование платформы известных разработчиков не отменяет обязанность объяснить, почему измерение отвечает юридическому вопросу конкретного заказчика.

30.2. Агентные системы в политике 2026 года

В январе 2026 года IMDA опубликовала материалы о новом подходе к управлению агентным ИИ, расширяющие внимание к системам, способным самостоятельно вызывать инструменты и совершать действия. Для assurance это означает необходимость оценивать не только качество текста, но и границы полномочий, авторизацию, остановку выполнения, журнал действий и ответственность человека. [43]

В международном сравнении подобная повестка показывает, что схемы оценки необходимо обновлять вместе с архитектурой продуктов. Однократное тестирование генеративного ответа не покрывает последствия автоматического перевода средств, изменения записи или отправки юридически значимого сообщения.

30.3. Переносимость испытаний

При сопоставлении результатов AI Verify с европейским комплаенс-досье следует анализировать конкретные методы и метрики, а не совпадение терминов. Например, тест на прозрачность интерфейса может не отвечать всем требованиям технической документации Annex IV. Хорошая инженерная методика становится релевантным доказательством только после сопоставления с обязательным предметом проверки.

В проектах ARGA можно применять логику структурированного испытания как методический образец, сохраняя разграничение между частным экспертным отчётом, признанным лабораторным результатом и законным решением по европейскому регламенту.

Практический контрольный список

1. Оценивать AI Verify как инструмент проверки, а не автоматический международный сертификат.

2. Для агентных моделей проверять реальные действия и пределы полномочий.

3. Переносить за рубеж только доказательство в допустимом объёме, не правовой статус.

Сингапур: испытательный инструмент и пределы официального признания

AI Verify представляет собой практическое направление разработки тестовой инфраструктуры и методической оценки ответственного ИИ. Использование такого инструмента может обогатить независимый протокол, но само прохождение теста не должно без дополнительного основания подаваться как государственная сертификация или разрешение на рынок. Нужно установить версию инструмента, выбранные принципы, реально выполненные проверки и статус выдавшей отчёт организации. [42]

Для агентных систем рамка IMDA, представленная в январе 2026 года и дополненная практическими случаями в мае того же года, предлагает ориентиры для ограничений полномочий, контроля жизненного цикла и ответственности человека. В заказах на агентные юридические приложения эти темы переводятся в конкретные вопросы: может ли агент получить доступ к клиентскому досье другого дела, отправить внешнее письмо, создать перевод денег, изменить исходный документ или отключить журнал. Каждая возможность требует самостоятельной проверки и правила подтверждения. [43,56]

Международное сопоставление должно разграничивать рекомендательную структуру управления, частный эксперимент и обязательный нормативный порядок. Подобная дисциплина полезна при подготовке ARGA консультационных предложений: можно ссылаться на практическую модель Сингапура как источник организационного опыта, не приписывая ей юридические последствия, которых она не создаёт.

Практический разбор 17.30

Рекомендация: Показывать границы инструментального теста

Условный пример: Набор AI Verify выполнили на подготовленных данных и объявили полную законность продукта.

Разбор: Техническая проверка не заменяет правовую квалификацию и оценку новых условий.

Практические действия: Оценщик указывает данные, функции и непроверенные свойства; юрист оценивает правовой вопрос отдельно.

Критерий результата: Публикация различает технический результат и правовой вывод.

31. ОЭСР, должная осмотрительность и негосударственные стандарты

31.1. OECD Guidance 2026 как источник процедур

В феврале 2026 года ОЭСР опубликовала Due Diligence Guidance for Responsible AI. Материал предлагает практическую структуру выявления и устранения неблагоприятных последствий при разработке и применении ИИ. Такой ориентир позволяет объединить техническое испытание с проверкой организационной ответственности и последствий для людей. [44]

Однако рекомендации ОЭСР не являются автоматически национальным обязательным порядком сертификации. Их нормативная сила возникает при специальной правовой

отсылке, договорном включении или ином установленном основании; в остальных случаях они используются как методический ориентир и источник общепризнанной практики.

31.2. Риск декларативного соответствия принципам

Организации часто объявляют приверженность прозрачности, равенству или устойчивости, но не показывают, какие процедуры из этих принципов следуют. Хорошая программа due diligence требует связи между заявленным риском, ответственной ролью, доказательством управленческого действия и механизмом пересмотра.

Например, наличие принципа «human in the loop» не доказывает, что специалист действительно может оспорить оценку машины. Необходимо видеть права доступа, время на пересмотр, возможность прекратить автоматическое действие и документы о фактическом вмешательстве.

31.3. Комплементарность разных источников

Международные руководства, стандарты и законы могут дополнять друг друга: OECD помогает выявлять неблагоприятные последствия, ISO/IEC 42001 оформляет организационные процессы, ISO/IEC 17025 поддерживает испытательную компетентность, а право ЕС задаёт особые юридические обязанности. Но они не соединяются в один «суперстандарт» и не устраняют процессуальные гарантии применимого права. [1,21,27,44]

В экспертном заключении нужно отдельно указывать, какой источник предъявляет требование, а какой лишь предлагает способ его соблюдения. Такой язык повышает пригодность материала для внешней консультации и предотвращает необоснованное расширение юридических выводов.

Практический контрольный список

1. Различать юридическое требование и добровольное руководство ОЭСР.

2. Документировать фактическое применение принципов, а не только их принятие.

3. Привязывать методический инструмент к законному объекту подтверждения.

Due diligence после заверения и механизмы исправления вреда

Руководство ОЭСР по ответственному ИИ от февраля 2026 года помещает оценку в более широкий цикл должной осмотрительности: закрепление политики, идентификация реального и потенциального воздействия, предотвращение и смягчение, отслеживание, сообщение результатов и участие в исправлении причинённого вреда. Такая логика дополняет, но не подменяет сертификацию и применимое право. Должная осмотрительность фокусируется также на людях, которые несут последствия работы системы, а не только на внутренней готовности корпорации к аудиту. [44]

Для чувствительных алгоритмов стоит заранее проектировать доступный способ оспорить вывод. Даже идеально оформленный технический сертификат не отвечает на вопрос, узнает ли пострадавший об ошибочном совпадении, получит ли возможность представить корректирующие документы и кто несёт ответственность за обновление исходного реестра. Поэтому заверение о надёжности должно содержать описание механизма исправления ошибок и предел его фактической проверки.

Внутри исследования ARGA целесообразно вести реестр затронутых сторон: клиенты, работники, контрагенты, лица из внешних баз, государственные получатели аналитики. Для каждой группы определяются риск, доступное доказательство, процедура обращения и независимая точка эскалации. Этот подход повышает практическую ценность AI Assurance для правовых и финансовых процессов по сравнению с общей декларацией «ответственного ИИ».

Практический разбор 17.31

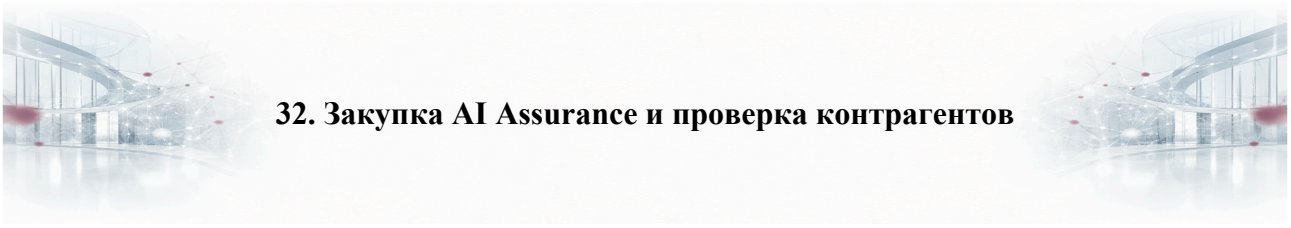
Рекомендация: Связывать должную осмотрительность с устранением вреда

Условный пример: Компания ведёт реестр рисков, но жалобы клиентов не передаются владельцам мер.

Разбор: Регистрация риска без исполнения не меняет последствия для людей.

Практические действия: Координатор связывает риск, обращение, ответственное действие и подтверждение исправления.

Критерий результата: Закрытая запись содержит проверяемый результат для затронутого лица.



32. Закупка AI Assurance и проверка контрагентов

32.1. Разумный запрос документов

Заказчику рекомендуется начинать с карты целей: зачем нужен внешний результат - для закупки, регуляторного досье, защиты клиента, контроля совета директоров или публичного доверия. От цели зависит, нужна ли система менеджмента, техническое испытание, конкретный сертификат или юридическое заключение. Встречная сторона должна представить перечень возможных документов с точной областью каждого.

Минимальный пакет обычно содержит юридическое наименование оценщика, область аккредитации или нотификации при наличии, схему, версию стандарта, пример обезличенного отчёта, правила конфликта интересов, режим конфиденциальности, стоимость дополнительных испытаний и план обработки изменений.

32.2. Управление договорным предметом

Предмет договора нельзя обозначать единственной строкой «получение AI certification». Нужно определить объект, систему критериев, независимость, источники данных, конкретные виды работ, формат результата, ограничения и возможность отказа в положительном заключении. Предоплата за проведение процедуры не должна подразумевать обещание выдачи сертификата.

В случае привлечения субподрядчика следует установить обязанности по передаче сведений и ответственности за составленное заключение. Заказчик должен иметь право знать, какие существенные виды испытаний переданы третьим лицам, в том числе за пределы юрисдикции хранения чувствительных данных.

32.3. Коммерческие и правовые красные флаги

Повышенного внимания заслуживают слова «гарантированная сертификация за 48 часов», отсутствие условий отказа, ссылка на ISO без года редакции, отказ назвать аккредитующий орган, невозможность показать область аккредитации и предложение заказать «сертификат GDPR» без определения схемы и правового статуса. Это не доказывает недобросовестность автоматически, но требует запроса дополнительных доказательств.

Для ARGA целесообразно использовать двухступенчатую процедуру: первичная проверка статуса и области документов, затем содержательная проверка методов и пригодности результата для клиента. Только после этих этапов возможно профессиональное мнение о достаточности пакета.

Практический контрольный список

1. Запрашивать наименование и статус схемы до подписания договора.

2. Предусматривать отрицательное заключение как допустимый результат работы.

3. Разделять цену проведения процедуры и обещание результата.

Матрица D. Скрининг типичных ложных утверждений

Фраза	Проблема	Корректная проверка
ISO аккредитовал нашу модель	ISO публикует стандарт, а не обычно выдаёт такой статус	Кто реально выдал сертификат и какова схема?
42001 даёт CE-маркировку	Сертификат менеджмента не заменяет режим EU AI Act	Применяется ли специальная процедура?
Модель сертифицирована во всём мире	Нет универсальной схемы на любую юрисдикцию и функцию	По какому предмету и при каком признании?
Британский CAB является notified body ЕС	Аккредитация UKAS и нотификация ЕС различны	Документ уполномоченного государства и область
На 300 тестах ноль ошибок = риск ноль	Ограниченный объём испытаний	Верхняя граница и предел репрезентативности

Закупочная процедура: проверка сертификатора и стоимости уверенности

При закупке оценочных услуг цена должна соотноситься с предметом, компетенцией исполнителя и доступностью материалов, а не с обещанным статусом «сертификат всего ИИ». Техническое задание следует разделить на обязательный результат, исследовательские гипотезы, объём и исключения, квалификацию экспертов, форму выводов, допустимые основания приостановления и процедуру независимой рецензии. Для нормативно требуемых процедур необходимо предварительно установить статус компетентного органа. [19,22,23]

Запрос предложений может включать два уровня стоимости: базовую проверку публичного и документального пакета и расширенное испытание в контролируемой среде. Так устраняется стимул продавать дорогую универсальную «оценку соответствия» без понимания категорий риска. В сравнительной таблице предложений рекомендуется оценивать доступность методики, статус аккредитации, способность доказать независимость, качество отчёта об ограничениях и договорное право заказчика передавать результат своему юристу или надзорному органу.

Следует предусмотреть случаи негативного результата. Исполнитель не должен терять право на вознаграждение при обнаружении несоответствия; иначе экономическая конструкция сама угрожает беспристрастности. Заказчику необходимо владеть или иметь законный доступ к достаточным рабочим материалам, чтобы другая команда могла повторить критические выводы. Коммерческая тайна исполнителя не должна превращаться в запрет независимой проверки существенного правового утверждения.

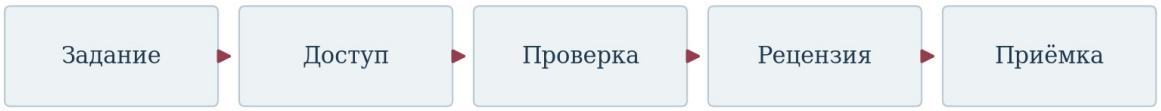


Рисунок 17.4. Приёмка услуги AI Assurance. Процедура закупки и приёмки из раздела 32: оплачивается проверяемая работа, а не обещание положительного результата.

Практический разбор 17.32

Рекомендация: Закупать проверяемый результат

Условный пример: Предложение обещает сертификат за фиксированный срок без описания тестов.

Разбор: Заказчик не знает, какие сведения получит и сможет ли использовать вывод.

Практические действия: В договор включают предмет, выборку, доступ, независимость, рецензирование и критерии приёмки.

Критерий результата: Приёмка проводится по комплекту свидетельств, а не по наличию обложки.

33. Конфиденциальность, персональные данные и доступ к модели

33.1. Правовая цель и минимально необходимый объём

Технический аудит может требовать доступа к журналам, тестовым записям, изображениям или фрагментам данных обучения. Однако требование компетентности и полноты доказательств не отменяет принципов применимого права защиты данных. Для конкретного проекта отдельно выясняются юридическое основание обработки, распределение ролей между сторонами, допустимая передача и необходимость сохранения сведений.

Если исходный корпус содержит конфиденциальные юридические досье, предпочтителен подход с искусственными кейсами и контролируемыми примерами, когда он позволяет проверить нужное свойство. Использование реальных данных может быть обосновано только отдельным анализом необходимости, мер защиты и полномочий сторон.

33.2. Техническая альтернатива полному раскрытию

Проверяющему можно предоставить удалённую контролируемую среду, согласованный API, набор тестовых функций или обезличенный журнал, если эти меры обеспечивают достаточное доказательство. Но ограничения такого доступа следует подробно описать. Нельзя объявлять проверенную систему «полностью прозрачной», когда исходные модели и части данных не исследовались.

Доказательственный стандарт должен учитывать риск утечки. Выгрузка всего массива чувствительных данных только для удобства стороннего аудитора может создать самостоятельный правовой риск, несопоставимый с целью проверки. Поэтому договор должен закреплять доступ по ролям, журнал операций и безопасное уничтожение избыточных копий.

33.3. Коммерческая тайна и процедурная защита

Участники могут ссылаться на коммерческую тайну, чтобы ограничить раскрытие определённых сведений. В специальном режиме Annex VII AI Act предусмотрены механизмы доступа к необходимой информации с учётом охраны интеллектуальной собственности и коммерческой тайны. Это показывает, что охрана тайны и внешняя проверка должны быть сбалансированы, а не противопоставлены. [6]

В экспертной работе можно применять независимую защищённую комнату данных, протокол фиксации действий, предварительное определение допустимых выборок и отдельное приложение о конфиденциальности. Если критическое свидетельство недоступно, итог должен честно показывать эту границу.

Практический контрольный список

1. Определить правовые основания доступа и передачи данных.

2. По возможности использовать искусственные и обезличенные тестовые досье.

3. Фиксировать, какое ограничение доступа влияет на силу заключения.

Правомерный доступ к данным как условие качества аудита

Часто встречается ложная альтернатива: либо раскрыть аудитору весь массив персональных данных, либо отказаться от независимой проверки. Между этими крайностями существуют контролируемый просмотр, выборка под надзором, отделение метаданных, псевдонимизация, синтетические тестовые случаи и создание доказуемых контрольных сумм. Конкретная мера зависит от цели, допустимого правового основания, технического риска и возможности повторения испытания. Никакая общая ссылка на статус аудитора не заменяет необходимости определить разрешённый объём обработки и передачи. [18,39,44]

Для юридических дел следует отдельно оценивать профессиональную тайну, ограничения клиента, режим хранения и возможность передачи за пределы разрешённой инфраструктуры. В соглашении нужны цели обработки, круг лиц, условия удаления рабочих копий, способ уведомления об инциденте и процедура подтверждения уничтожения временных данных. Для независимого эксперта полезно сохранить реестр полученных материалов и доказательство удаления, но не создавать дополнительную копию чувствительного архива ради удобства.

Если заказчик не может раскрыть критические данные даже в контролируемой среде, эксперт должен ограничить предмет заключения. Обоснованный вывод «не представилось возможным проверить частоту ошибок на реальных записях» профессионально предпочтительнее необоснованной фразы о доказанной безопасности. В таких ситуациях иногда допустимо выдавать заключение о методологии или организационном процессе без вывода о фактической работе системы.

Практический разбор 17.33

Рекомендация: Разделять конфиденциальный доступ и публичный вывод

Условный пример: Аудитору нужен журнал с персональными сведениями, заказчик готов передать его всем участникам.

Разбор: Избыточное раскрытие не требуется для проверки большинства выводов.

Практические действия: Ответственный предоставляет минимальные роли доступа и обезличенный пакет для рецензента.

Критерий результата: Журнал доступа и состав публичного пакета подтверждают минимизацию.

34. Отраслевые сценарии: банки, санкции, международное сотрудничество

34.1. Автоматизированная проверка санкционных совпадений

Система санкционного скрининга обычно сопоставляет имена, транслитерации, даты рождения, документы и корпоративные связи с внешними источниками. Юридический риск зависит не от самого обнаружения сходства, а от следующего действия организации: ручного расследования, ограничения операции или передачи информации компетентному органу. Проверка должна охватывать происхождение источников, качество нормализации и правила исключения ошибочной идентичности.

В сертификационной схеме следует отдельно проверять полноту выявления релевантных записей и частоту необоснованных совпадений. В противном случае высокий показатель общей точности может скрывать ситуацию, когда система регулярно затрагивает невиновных клиентов и не предусматривает эффективной коррекции.

34.2. AML/KYC и автоматическая оценка клиентского риска

Модели AML/KYC часто соединяют структуру транзакций с риском страны, отрасли и поведения клиента. Документ о сертификации корпоративного AIMS не является доказательством законности конкретной блокировки либо отказа в обслуживании. Для спорного эпизода нужны правила модели, источники исходных данных, журнал операций, роль сотрудника и правовое основание принятого решения.

Для ARGA полезна модель ограниченной независимой проверки: исследование источников данных, сопоставление показателей ошибок и анализ возможности клиента оспорить вывод. При этом заключение не должно подменять полномочия финансового регулятора и не

должно содержать непроверенные утверждения о фактическом поведении какого-либо банка.

34.3. Международный розыск и правоохранительная аналитика

Алгоритмическая система поиска похожих персон, если она применяется в международном полицейском сотрудничестве, требует повышенного внимания к источнику записи, законности доступа, статусу ордера, идентификации личности и исправлению неверных сведений. Рассматривать совпадение по имени как достоверную идентичность недопустимо. Даже технически точная система не подтверждает сама по себе наличие правового основания задержания.

Настоящий пример является условным исследовательским сценарием и не утверждает, что конкретная международная организация использует описанный алгоритм. Для каждого реального дела применимость стандартов AI Assurance зависит от доказательств существования системы, вида данных и доступных процессуальных процедур.

Практический контрольный список

1. Фиксировать, в какой момент алгоритмический флаг приводит к правовому действию.

2. Проверять идентичность по независимым признакам, а не только совпадение имени.

3. Отделять техническую ошибку от юридической квалификации и компетенции властей.

Профильные сценарии: санкции, финансовые расследования и полицейские данные

Для санкционного совпадения целевое свойство включает не только техническое обнаружение похожей записи, но и раздельную работу с идентификаторами, датами, источниками, транслитерациями и обновлениями списков. Ошибка может приводить к необоснованной блокировке обслуживания или к пропуску значимого совпадения. Поэтому в протоколе следует сопоставлять метрики обнаружения и ложных тревог с процедурой ручного разрешения неопределённых случаев. Итоговая ответственность за применяемое решение определяется соответствующим правом и внутренним распределением полномочий, а не фактом использования сертифицированной модели. [39,44]

В международном полицейском сотрудничестве предъявляются дополнительные требования к происхождению и корректировке исходных данных. Независимая оценка инструмента распознавания не подтверждает законность помещения лица в конкретную базу; обратная сторона также верна: законное ведение базы не доказывает правильность автоматического установления личности. Эти две цепочки требуется исследовать отдельно. Для аналитического подразделения ARGA важны прозрачные ссылки на материалы, обработка однофамильцев и запрет приписывать личности статус только по модельному скорингу.

В финансовом расследовании полезно тестировать не только качество выявления связи, но и воспроизводимость графа связей и объяснимость выбранного источника. Автоматическое обнаружение необычной операции является поводом для профессиональной проверки, а не доказательством неправомерного происхождения актива. Отчёт AI Assurance должен запрещать расширительное прочтение вероятностной оценки как установленного юридического факта.

Практический разбор 17.34

Рекомендация: Разделять сигнал совпадения и решение о клиенте

Условный пример: Продукт помечает однофамильца как санкционное совпадение.

Разбор: Показатель сходства не устанавливает идентичность и не определяет правовое последствие.

Практические действия: Специалист сверяет дополнительные идентификаторы и документирует основание ручного решения.

Критерий результата: В итоговом досье различены машинный сигнал и мотивированное решение.

35. Кейс-стади: юридический помощник и пределы сертификации

35.1. Состав условной системы

Условный юридический помощник извлекает документы, формирует обобщение и предлагает проект ответа. Досье assurance включает сертификат AIMS поставщика, отчёт о тестировании ссылок, журнал изменения поискового индекса и описание человеческой проверки. Исследователь рассматривает эти материалы раздельно: у них разные объекты, даты и проверяемые свойства. Затем устанавливает, какие материалы относятся к реально применяемой сборке, а какие характеризуют только одного участника цепочки.

При тестировании система должна получать искусственные досье с неоднозначными датами, противоречащими документами, отсутствующими приложениями, разноязычными именами и фальшивыми указаниями внутри файлов. Цель - выяснить, отличает ли она проверенное фактическое основание от догадки и умеет ли отказаться от результата при недостатке данных.

35.2. Программа измерения

В программе измерения выделяются три самостоятельных исхода: досье без неверной существенной ссылки; полнота обязательных фактов; сохранение доказательственного статуса сведений. Дополнительно регистрируются отказы и случаи, когда специалисту невозможно установить правильный ответ. Общий балл не объединяет эти исходы без обоснования: снижение числа ложных ссылок может сопровождаться потерей существенного документа. Решение должно учитывать каждый критический критерий.

Для доступа к чувствительным делам разумно использовать искусственные корпуса и синтетические вариации. Результаты на таком корпусе полезны для ограниченной демонстрации качества, но не дают статистической гарантии поведения на всех реальных делах; в заключении эта граница указывается отдельно.

35.3. Правомерный язык заключения

При положительном ограниченном результате заключение указывает проверенную конфигурацию, набор задач, определение успешного досье, исходные количества, правило

решения и выполненные ограничения. Если правило не выполнено из-за неопределённости, сообщается, каких доказательств не хватает. Квалификация сертификата приводится отдельным выводом. Она не повышает автоматически статистическую уверенность в результате испытания.

Недопустимо сообщать «юридический помощник сертифицирован для международного правосудия», если не установлены схема, предмет, уполномоченный орган и критерии. Наличие подписи внешнего эксперта само по себе этого статуса не создаёт.

Практический контрольный список

1. Использовать искусственный корпус с проверяемыми эталонами.

2. Включать тестирование происхождения ссылок и сопротивления недоверенным инструкциям.

3. Формулировать вывод без обещания юридической безошибочности.

Полный цикл проверки юридического помощника

Испытание юридического помощника организуется как проверка обещания в установленной области. Сначала эксперты определяют существенные положения по каждому досье и допустимые варианты вывода. Затем фиксируются материалы, доступные системе, и выполняется тест без корректировки эталона под ответы. Независимые оценщики проверяют ссылки и существенные пропуски, сохраняя первоначальные разногласия. На завершающей стадии другой специалист восстанавливает расчёт по исходным меткам и проверяет соответствие языка заключения данным.

Контроль включает сопоставление первичного документа и интерпретации его содержания. Существующий URL не подтверждает применимость процитированного правила. Проверяются редакция, юрисдикция, дата действия и фактические предпосылки. При расхождении между комментарием и первичным актом фиксируется причина выбора основания. Если вопрос остаётся спорным, критерий успешности допускает мотивированное указание неопределённости; уверенная формулировка без основания не считается преимуществом.

Для последующей эксплуатации рекомендуется распределить операции на уровни. Помощник вправе подготовить черновую хронологию, но юридическая квалификация и направление адресату требуют одобрения ответственного специалиста. При невозможности установить источник ключевого факта система должна показывать пробел, а не дополнять его наиболее вероятной догадкой. Независимое заверение охватывает такую архитектуру контроля лишь в пределах действительно испытанной конфигурации.

Проверка достаточности условного досье юридического помощника

Поставщик заявляет, что юридический помощник «подтверждён для подготовки документов без обязательной проверки специалистом». Представлены сертификат системы менеджмента, испытание на 100 досье с 94 успешными исходами и внутреннее описание проверки цитат. Условная задача исследователя — определить, какую часть заявления подтверждают эти материалы и какое дополнительное исследование требуется.

Свидетельство	Что может подтверждать	Что требует отдельной проверки
Сертификат AIMS	Процессы в указанной области и периоде	Качество ответов конкретной сборки
94 успеха из 100 досье	Наблюдаемую долю при заданной разметке	Отбор, интервалы, пропуски и порог решения
Описание проверки цитат	Наличие документированной процедуры	Её фактическое исполнение и пропущенные дефекты
Совокупность материалов	Отдельные элементы обоснования	Допустимость отказа от проверки специалистом

Сначала уточняется, что считается успехом: в этом примере все существенные ссылки досье должны иметь надлежащее первичное основание. Затем восстанавливаются исходные метки и проверяются шесть неуспешных случаев. По условному правилу раздела 23 нижняя граница интервала должна составлять не менее 90%; при данном объёме она около 87,5%. Оснований для предусмотренного положительного решения недостаточно. Сертификат менеджмента не меняет этот расчёт.

Даже выполнение критерия по ссылкам не подтвердило бы всё исходное заявление. Полнота правового анализа, сохранение фактических оговорок и последствия самостоятельного направления документа остаются отдельными вопросами. Обоснованный итог — сузить заверение до исследованного свойства, запросить недостающие данные и определить условия дополнительной оценки. Человеческая проверка отменяется только при самостоятельном правовом и техническом обосновании такого решения.

Практический разбор 17.35

Рекомендация: Проверять утверждение о работе без юриста

Условный пример: На 100 условных досье помощник успешно обработал 94, поставщик предлагает отменить ручную проверку.

Разбор: Шесть неуспехов требуют квалификации; средняя доля не подтверждает безопасность самостоятельного использования.

Практические действия: Эксперт разбирает все шесть случаев, проверяет критические ошибки и назначает ограниченный режим с контролем.

Критерий результата: Решение о режиме связано с тяжестью ошибок, а не только процентом.



36. Предлагаемая институциональная программа Observatoire ARGA

36.1. Роль независимого аналитического центра

Наиболее реалистичное направление для ARGA - правовая и доказательственная экспертиза заявлений об AI-системах, выбор регуляторного маршрута и подготовка аналитических заключений для институциональных консультаций. Такая работа не требует объявлять себя

аккредитационным органом либо нотифицированным органом ЕС. Границы полномочий должны указываться прямо и в договоре, и в самом отчёте.

Рекомендуется вести единый реестр международных стандартов и нормативных изменений, отдельно регистрируя, что является действующим законом, официально опубликованным стандартом, проектом и экспертным предложением. В октябре 2026 года такой реестр особенно важен из-за изменения дат AI Act и перехода мировой инфраструктуры аккредитации.

36.2. Три возможных продукта при существующих ресурсах

Первый продукт - Regulatory Route Memorandum: краткая квалификация сферы, субъекта, категорий риска, применимого законодательства и необходимых документов. Второй - Evidence Sufficiency Review: анализ документов и источников с явно ограниченным заключением о достаточности доказательств. Третий - Third-Party Assurance Due Diligence: проверка подлинности и области сертификата, аккредитации и применимости результата к деятельности клиента.

Каждый продукт должен содержать перечень исключений. Например, исследование юридических документов без независимого доступа к программной среде не подтверждает техническую устойчивость модели. Такая честность ограничивает коммерческий риск и повышает пригодность материалов для профессионального использования.

36.3. Международные консультации и условия подачи

Для внешнего обсуждения ARGA может предложить узкие рекомендации: стандартный машиночитаемый паспорт области сертификата, обязательное сообщение о смене модели, документальное различение лабораторного теста и системы менеджмента, а также проверяемую процедуру жалоб. Инициативы следует соотносить с официальной повесткой соответствующего адресата. Нельзя объявлять позицию направленной или принятой, пока это не подтверждено документально.

Внутреннее согласование осуществляется согласно действующему порядку ARGA. Аналитическая публикация может стать приложением к позиции, но самостоятельный доклад не подтверждает ни аккредитацию, ни назначение в систему AI Act. Результат институциональной работы следует оценивать по проверяемым исходящим документам и официальным ответам.

Практический контрольный список

1. Внедрить единый паспорт заявления и стандартизированный перечень ограничений.

2. Проверять статус сторонних сертификатов без присвоения ARGA чужих полномочий.

3. Связывать международные консультационные позиции с подтверждённой компетенцией и актуальными источниками.

Модель исследовательской программы ARGA без ложной аккредитации

Исследовательская программа ARGA может оценивать качество квалификации assurance-досье без присвоения полномочий аккредитованного органа. Основной вопрос пилота:

способны ли разные эксперты по единой инструкции выявлять подмену предмета и получать сопоставимые выводы о достаточности свидетельств? Для проверки используются обезличенные или специально подготовленные комплекты с известными ограничениями. Результат измеряется по пропущенным существенным несоответствиям и причинам экспертных разногласий, а не по объёму выпущенных заключений.

Перед пилотом утверждаются паспорт утверждения, словарь статусов, перечень критических ошибок квалификации и порядок независимой проверки. Один комплект может содержать одновременно корректный сертификат менеджмента и неподтверждённое обещание технической безошибочности. Процедура должна сохранить оба вывода. После первого этапа инструкция уточняется, а её новая редакция проверяется на другом наборе: согласование ответов на уже разобранных примерах не подтверждает переносимость навыка.

Международные консультации стоит связывать с подтверждаемыми наблюдениями, а не общими заявлениями о «мировой сертификации». Потенциальные предложения касаются паспортов области оценки, стандартов хранения доказательств, защиты от ошибочных идентификаций и взаимной понятности маркировок аккредитации. Для каждого внешнего участия требуется установить открытый канал, предмет консультации, срок, результат отправки и документальное подтверждение. Внутреннее исследование не должно изображаться как позиция международной организации.

Практический разбор 17.36

Рекомендация: Пилотировать процедуру экспертной квалификации

Условный пример: Два эксперта одинаково читают сертификат, но по-разному оценивают его достаточность.

Разбор: Методике нужны операционные правила и проверка воспроизводимости.

Практические действия: Куратор утверждает паспорт утверждения, независимую оценку и разбор расхождений на новом наборе.

Критерий результата: Результат пилота показывает причины расхождений и пригодность инструкции.

37. Заключение и пределы международного взаимного признания

37.1. Многоуровневое, но не автоматическое доверие

Мировая архитектура assurance развивается как совокупность стандартов менеджмента, компетентности оценщиков, специальных продуктовых схем, национального регулирования и соглашений об аккредитации. Эти механизмы усиливают друг друга, но не образуют универсальный документ, который позволяет использовать ИИ в любой сфере без новой правовой оценки. Международное признание результата действует в пределах соответствующей области и не устраняет обязанностей принимающей юрисдикции. [19,21-28,37-38]

Методологический вывод заключается в необходимости раздельно оценивать предмет свидетельства, качество метода и юридическую область результата. Перенос заверения допустим только при подтверждённой сопоставимости этих условий. Внешний статус документа может обосновывать доверие к процедуре в её области, но не расширяет набор исследованных свойств. Эта граница должна сохраняться и в полном заключении, и в его кратком публичном изложении.

37.2. Предложения по прозрачности

Для международного обмена результатами оценки целесообразен обязательный для каждой выбранной схемы паспорт: кто проверен, что проверено, какая версия, какая область аккредитации, по какому критерию, когда, какими методами и какие свойства исключены. Также желательно стандартизировать уведомление о приостановлении и значительном изменении системы.

Отдельного обсуждения требуют правила раскрытия статистической неопределённости, критерии оценки уязвимых групп и защита конфиденциальных данных при внешних испытаниях. Без этих элементов трансграничное признание может превратиться в формальное соглашение о логотипах при непроверяемом содержании документов.

37.3. Итоговое правило для ARGA

Перед использованием результата ARGA проверяет четыре основания: точность заявленного свойства; соответствие свидетельств этому свойству; выполнение критерия по установленному правилу; допустимость использования заключения в конкретной юрисдикции и процедуре. Неразрешённый пробел обозначается адресно. Итогом может быть рекомендация использовать документ в узкой области, запросить недостающие материалы, провести отдельное испытание или отклонить чрезмерное заявление.

Следующий исследовательский этап — пилотная проверка воспроизводимости квалификации и разбор существенных расхождений между экспертами. На её основе можно уточнить паспорт области заверения и предложить требования к раскрытию неопределённости для международного обсуждения. Правовые положения актуализируются на дату конкретного использования. Сам факт подготовки настоящего доклада не означает проведения пилота или подтверждения свойств реального продукта.

Практический контрольный список

1. Не приравнивать взаимное признание аккредитации к признанию каждого AI-продукта.

2. Требовать паспорт области и условий действия любого важного заверения.

3. Сохранять различие между экспертным мнением, сертификатом и юридической декларацией.

ПРАКТИЧЕСКИЕ ПРИЛОЖЕНИЯ

Границы трансграничной переносимости и окончательный тест вывода

Главный юридический результат исследования заключается в различении доверия к компетентности оценщика, оценки конкретного объекта и признания результата в определённой правовой процедуре. Международная договорённость органов аккредитации способствует сопоставимости результатов, но не создаёт самостоятельного разрешения на выход любого ИИ на рынок или на использование его в уголовном судопроизводстве. Для каждого применения нужно найти конкретную норму, договор либо подтверждённую практику признания. [19,35-38]

Поэтому итоговое заключение о сертификате целесообразно строить в форме шести последовательных ответов: кем он выдан; какова действующая область полномочий; какой объект и версия проверены; по каким критериям; какие свойства действительно установлены; для какой юрисдикции и процедуры результат имеет значение. При отрицательном ответе хотя бы на один существенный вопрос не следует автоматически объявлять документ недействительным. Следует сформулировать точный пробел и требуемое дополнительное подтверждение.

Для ARGA перспективным результатом станет унифицированный набор проверочных форм, в котором каждая внешняя рекомендация может быть проверена другим специалистом. Программа должна допускать изменение выводов после появления новых материалов, отзыв устаревших свидетельств и доступность исправления ошибочных данных о людях. Тем самым AI Assurance становится не декоративным сертификатом, а процедурой ответственного обращения с неопределённостью и с последствиями решений.

Практический разбор 17.37

Рекомендация: Ограничивать итоговое признание подтверждённой областью

Условный пример: Набор свидетельств достаточен для внутренней подготовки текста, но его предлагают для автономной подачи.

Разбор: Новая область включает последствия, которые испытания не проверяли.

Практические действия: Утверждающий сохраняет ограниченный режим; для расширения задаёт дополнительные испытания и правовую проверку.

Критерий результата: Итог перечисляет допустимое использование, исключения и условия пересмотра.

Приложение 1. Паспорт утверждения и результата AI Assurance

Паспорт нужен для того, чтобы последующий получатель отчёта не воспринимал сертификат шире предусмотренной области. В каждом проекте используется одна карточка на самостоятельное утверждение. Если по одному продукту подтверждаются защита данных, функциональное качество и управление рисками, следует завести как минимум три записи с разными критериями.

Код	Поле	Что необходимо указать
A01	Точное утверждение	Одно проверяемое предложение без абсолютных обещаний
A02	Тип результата	Экспертный обзор / технический тест / сертификация / аккредитация / правовая декларация
A03	Юридическое лицо	Регистрационное и коммерческое название, при необходимости филиал
A04	Объект	Модель, компонент, готовая система либо система менеджмента
A05	Идентификатор версии	Модель/код/API/дата выпуска/контрольная сумма
A06	Назначение	Допустимые виды использования и группа пользователей
A07	Границы	Включённые и исключённые функции, внешние сервисы
A08	Нормативный источник	Акт, статья, стандарт с годом или частная схема
A09	Критерий	Порог, метод, допустимая ошибка, способ измерения
A10	Метод	Аудит, наблюдение, тест, анализ документов
A11	Данные	Происхождение, объём, принципы выборки и разметки
A12	Компетенции	Команда, независимость, отраслевые эксперты
A13	Оценщик	Полное наименование CAB или исследователя
A14	Аккредитация	Наименование AB, номер, область, дата и статус; «нет» при отсутствии
A15	Нотификация	Страна, номер и область по специальному праву; «не применяется» при отсутствии

Код	Поле	Что необходимо указать
A16	Доказательства	Реестр приложенных материалов и ограничений доступа
A17	Непроверенное	Вопросы вне задания; недостаточные данные; внешние компоненты
A18	Результат	Подтверждено / частично / не подтверждено / не оценивалось
A19	Временная граница	Дата, актуальная версия, критерии переоценки
A20	Публичная формулировка	Краткий точный текст, допускаемый для публикации

Рекомендуемая процедура принятия паспорта: ведущий аналитик заполняет поля A01-A11, технический специалист проверяет A05-A11, юридический рецензент анализирует A08 и A15, ответственный за независимость подтверждает A12-A14, редактор согласовывает A20. Любое существенное изменение поля A05, A06 или A08 запускает решение о повторной оценке.

> **Примечание** Поле A14 не должно заполняться словом «ISO» в графе аккредитационного органа. Следует назвать учреждение, которое действительно вынесло решение об аккредитации. [21,24]

Дополнительное методическое уточнение

При заполнении паспорта нельзя оставлять графу «нормативное основание» в виде общего слова «ISO». Нужно обозначать конкретную редакцию, характер стандарта и связь с заявленным результатом. Для юридической применимости также требуется дата: существующий сертификат может быть получен до изменения действующих требований. Каждый параметр, на который невозможно получить подтверждение, фиксируется как «не установлен», а не как «не применимо». Именно эти две категории обычно смешивают в коммерческих анкетах.

Приложение 2. Протокол проверки подлинности и области сертификата

Протокол служит для внешнего подтверждения сведений, которые организация представила в своём рекламном материале. Он не проверяет техническую правильность всего заключения: это отдельный этап. Рекомендуется сохранить датированную копию

реестрового результата либо запись поиска, исключив персональные данные, не необходимые для цели.

Порядок проверки

1. Получить документ от стороны и отметить идентификатор, наименование, версию стандарта и заявленный предмет.

2. Установить полное юридическое наименование органа, который выдал документ, и сопоставить подпись или электронный идентификатор.

3. Определить статус: добровольная сертификация, аккредитованная оценка, нотификация, испытание либо консультационный отчёт.

4. Если заявлена аккредитация, открыть официальный реестр AB и проверить совпадение наименования, номера, статуса, площадок и области.

5. Проверить относящуюся к данной области систему взаимного признания. В 2026 году учитывать Global Accreditation Cooperation Incorporated и действующие правила региональных соглашений.

6. Если заявлена нотификация по AI Act, запросить подтверждение компетентной власти и соответствующей области процедур.

7. Сопоставить объект сертификата с конкретной системой или организационной функцией, о которой делает заявление поставщик.

8. Сохранить документированное решение: подтверждено, обнаружено расхождение, требуется уточнение, статус не проверен.

Контроль	Да / Нет / Не установлено	Документ и комментарий
Совпадение юридического лица	_____	_____
Действующий статус	_____	_____
Версия стандарта указана	_____	_____
Область включает требуемую услугу	_____	_____
Подписант компетентен	_____	_____
Аккредитация подтверждена	_____	_____
Нотификация подтверждена при необходимости	_____	_____
Результат относится к нужной версии	_____	_____

Контроль	Да / Нет / Не установлено	Документ и комментарий
Указан срок действия/надзора	_____	_____
Есть процедура жалобы/изменения	_____	_____

Существенное несоответствие не следует закрывать одной устной фразой поставщика. Если в реестре отображается другой статус, требуется официальное разъяснение выдавшей стороны или органа аккредитации. При отсутствии проверки можно использовать нейтральную формулировку «копия предоставлена поставщиком; независимое подтверждение действующего статуса не получено».

Дополнительное методическое уточнение

Проверка реестра документируется как отдельное доказательственное действие. Предпочтительно сохранять URL официальной базы, дату обращения, строку поискового запроса и обнаруженную карточку. Если официальный реестр предоставляет только ограниченные сведения, требуется указать именно эти пределы, а не утверждать, что статус отсутствует. Если реестр и копия расходятся, до официального разъяснения результат помечается как спорный.

Приложение 3. Карта регуляторного маршрута по AI Act (редакция 2026)

Ниже приведена последовательность исследовательских вопросов. Это схема предварительного отбора, а не замена официальной юридической квалификации конкретного продукта. Ссылки сделаны на изменённый консолидированный текст AI Act по состоянию на 27 июля 2026 года. [1-8]

Маршрут анализа

1. Установить, входит ли система и её участник в территориальную и предметную сферу EU AI Act.

2. Проверить специальные запреты и обязанности, которые могут применяться независимо от high-risk классификации.

3. Описать реальное назначение системы, а не маркетинговое название технологии.

4. Проверить основание high-risk: статья 6(1) и Annex I либо статья 6(2) и Annex III; зафиксировать особые исключения.

5. Проверить действующую дату обязанности: 2 декабря 2027 года для установленного случая Annex III или 2 августа 2028 года для установленного случая Annex I; не игнорировать иные даты.

6. Для Annex III пунктов 2-8 определить предусмотренный Annex VI; для пункта 1 проверить выбор Annex VI/Annex VII и условия стандартизации.

7. Для Annex I применить отраслевую процедуру оценки и специальные условия интеграции норм AI Act.

8. Отдельно определить статус нотифицированного органа, если он юридически необходим, и требуемый объём технической документации.

9. Сформировать перечень необходимых деклараций, обозначений, регистраций и обязательств после выпуска.

10. Назначить точку переоценки после изменения системы, стандарта либо законодательного срока.

Факт	**Что должен доказать участник**	**Основание**
Категория по Annex III	Конкретный пункт и назначение системы	Ст. 6, приложение III [1]
Категория по Annex I	Отраслевой акт и класс продукта	Ст. 6(1), приложение I [1]
Маршрут оценки	Почему Annex VI, VII либо секторная процедура	Ст. 43 [4]
Дата применения	Ссылка на изменённую статью 113	Ст. 113 [3]
Гармонизация	Публикация ссылки и охват требований	Ст. 40 [7]
Свидетельство третьей стороны	Нотификация и область органа	Ст. 28-31 [9-12]
Декларация и маркировка	Ответственность и идентификатор системы	Ст. 47-48 [15-16]

Дополнительное методическое уточнение

Условный пример: кадровая система может подпадать под Annex III, при этом её добровольный сертификат AIMS не заменяет установленных законом обязанностей провайдера. Другой пример: медицинское изделие, включающее ИИ как компонент безопасности, может потребовать анализа отраслевой процедуры и пункта Annex I. В обоих случаях дата исполнения конкретной обязанности и статус участника указываются отдельно; сходство алгоритма не делает маршруты одинаковыми. [1,4]

Приложение 4. Функциональная карта стандартов ISO/IEC и источников ЕС

В таблице разграничены объекты стандартов по их официальным открытым описаниям. Это синтез автора, а не дословная матрица обязанностей из платных текстов. При реальном заказе следует проверить доступность полной нормативной редакции и её включение в конкретную схему оценки. [21-31]

Инструмент	Основной объект	Типовой вопрос применения
ISO/IEC 42001:2023	Менеджмент ИИ	Организация системно управляет рисками ИИ?
ISO/IEC 42006:2025	Орган сертификации AIMS	Способен ли он компетентно и последовательно сертифицировать AIMS?
ISO/IEC 17021-1:2015	Орган сертификации систем менеджмента	Есть ли компетентность и беспристрастность процесса?
ISO/IEC 17065:2012	Орган сертификации продукта/процесса/услуги	Есть ли применимая продуктовая схема?
ISO/IEC 17025:2017	Испытательная лаборатория	Надёжен ли конкретный метод измерения в признанной области?
ISO/IEC 17029:2019	Орган валидации/верификации	Правдиво или пригодно определённое утверждение по схеме?
ISO/IEC 17011:2017	Орган аккредитации	Компетентен ли аккредитующий субъект?
ISO/IEC 42005:2025	Оценка воздействия системы	Какие последствия возможны для людей и общества?
ISO/IEC 25059:2023	Модель качества AI-систем	Какие свойства качества описать и оценить?
AI Act: Annex VI	Самооценка поставщика по законному маршруту	Как выполнены обязательные проверки внутри организации?
AI Act: Annex VII	Нотифицированный орган и техническое досье	Как проведена специальная правовая оценка и надзор?

Не следует выводить правовую презумпцию соответствия AI Act из любого столбца выше. Действие презумпции требует условий статей 40-42 и самостоятельной проверки ссылки на гармонизированный стандарт в Официальном журнале ЕС. [7-8,47]

Дополнительное методическое уточнение

В реестре нормативных критериев следует использовать отдельную отметку «опубликованная действующая редакция» / «финальный проект» / «не проверено». В октябре 2026 года обозначения ISO/IEC FDIS 17065 и ISO/IEC FDIS 25059 не означают опубликованный стандарт; их значение ограничено прогнозом развития схем. Закупка не должна подменять действующий критерий проектным документом без ясного согласия и объяснения. [25,26,30,31]

Приложение 5. Модельный протокол испытания санкционных совпадений

Пример полностью условный, не относится к конкретной финансовой организации и не содержит реальных персональных данных. Цель - показать структуру испытания в рамках узкого AI Assurance: отделить математическое качество сравнения от юридически значимого решения оператора.

Поле протокола	Условное заполнение	Ограничение
Назначение	Первичный поиск возможных совпадений	Не решение о блокировке
Система	Matcher X, версия 2.4, настройки 2026-10	Новая версия требует оценки
Эталон	200 размеченных искусственных записей	Не реальная статистика банка
Положительные случаи	80 подтверждённых совпадений	Базовая частота искусственно высока
TP	60 верно выявленных совпадений	В условном корпусе
FP	20 ошибочно отмеченных несовпадений	Может вредить клиенту
FN	20 пропущенных совпадений	Может вести к неполному контролю
TN	100 верно отклонённых несовпадений	В условном корпусе
Precision	60/(60+20) = 75%	Зависит от распространённости класса
Recall	60/(60+20) = 75%	Не отражает цену ошибки

Поле протокола	Условное заполнение	Ограничение
FPR	20/(20+100) = 16,7%	Относится к отрицательным случаям
Контроль человека	Обязательная проверка флага оператором	Требует отдельного аудита
Юридическое решение	Не оценивалось	Требуется анализ полномочий и основания

Различие между precision и recall сохраняется, хотя в данном учебном наборе они случайно равны. Для реального проекта необходимо определить схему отбора, разметчиков, языковые группы, пороги и механизм восстановления ошибочной идентичности. Иначе даже верно посчитанные дроби не дают надёжного заключения о пригодности инструмента.

Дополнительное методическое уточнение

Для каждого среза оценщик должен проверить, не повторяются ли одни и те же исходные личности в тренировочной и тестовой части. При наличии таких повторов высокая метрика может отражать запоминание, а не способность обнаруживать новые случаи. Тест на редких совпадениях нужно дополнять качественной ревизией каждого пропуска и документированным решением о необходимости человеческого пересмотра.

Приложение 6. Статистическая неопределённость: воспроизводимые учебные расчёты

Числа приведены только для демонстрации принципов статистической оценки. Они не являются результатами испытаний какой-либо организации. Допущения каждой модели указаны отдельно, поскольку изменение схемы отбора может сделать её недопустимой.

Учебный вопрос	Расчёт	Вывод и граница
94 успеха из 100	94/100 = 94%; 95% Wilson = 87.5% - 97.2%	Не доказывает качество >94% в генеральной совокупности
0 сбоев из 300	1 - 0,05^(1/300) = 0.99%	Односторонняя верхняя граница 95% при биномиальных предпосылках
0 сбоев из 1000	1 - 0,05^(1/1000) = 0.30%	Редкий риск не становится нулевым
FPR в примере Annex 5	20/(20+100) = 16,7%	Частота ошибки на истинно отрицательных случаях
Разрыв точности между группами	(90/100) - (60/80) = 15 п.п.	Нужно изучить состав групп и доверительные интервалы

Интервал Уилсона не исправляет нерепрезентативность выборки и не учитывает зависимые серии запросов. В случае кластерных данных, проверки одного и того же клиента с вариациями имени и послеобученных моделей необходимо выбрать другую статистическую модель либо отчётливо ограничить силу вывода. Ни один рассчитанный показатель сам по себе не является юридическим доказательством отсутствия дискриминации или безусловной безопасности.

Дополнительное методическое уточнение

Все величины в приложении иллюстративные, не получены в ходе испытания реальных систем. При демонстрации результата необходимо явно назвать предположение о независимости наблюдений, критерии отнесения к истинной категории и использованную формулу. Если эти предпосылки нарушены, обычный численный интервал не обладает заявленным покрытием. Это особенно существенно для групп связанных проверок и повторяющихся имён.

Приложение 7. Реестр доказательств для ограниченного независимого анализа

Данный образец пригоден как приложение к техническому заданию на экспертную работу. Он отделяет полученный документ от интерпретации. Колонка «необходимо дополнительно» предотвращает ложное впечатление завершённости проверки при неполном пакете.

ID	Предполагаемое доказательство	Проверка	Открытый вопрос
E01	Документ о назначении системы	Сопоставление с фактическими функциями	Есть ли скрытые сценарии?
E02	Схема компонентов и поставщиков	Проверка внешних зависимостей	Кто обновляет API?
E03	Регламент изменения версий	История фактических выпусков	Изменяется ли модель без уведомления?
E04	Техническое досье	Сверка с Annex IV при применимости	Все ли разделы актуальны?
E05	План проверки качества данных	Происхождение и разметка	Возможна ли утечка обучающих примеров?
E06	Отчёт испытаний	Метрика, выборка, контрольные данные	Независим ли эталон?

ID	Предполагаемое доказательство	Проверка	Открытый вопрос
E07	Документы об обжаловании	Анализ процедуры и реальных кейсов	Возможен ли пересмотр человеком?
E08	Сертификат AIMS	Область сертификации	Включён ли конкретный процесс?
E09	Реестр аккредитации CAB	Номер, статус, область	Соответствует ли проверенной услуге?
E10	Нотификация AI Act	Область полномочий	Не относится ли к другой процедуре?
E11	Журнал инцидентов	Проверка полноты и действий	Были ли неучтённые жалобы?
E12	Договор с внешней моделью	Права доступа и уведомление об изменениях	Обновляет ли провайдер модель без согласия?
E13	Протокол конфликта интересов	Оценка независимости команды	Были ли консультативные отношения?
E14	Журнал применений	Выборка реальных решений	Человек проверяет флаги?
E15	Решение о достаточности	Подписи, замечания, ограничения	Кто утверждает публичный вывод?

Оригиналы чувствительных материалов желательно хранить в закрытом хранилище с разграничением доступа, а в приложении к отчёту отражать только код, тип и дату. Выгрузка реального клиентского досье в публичную версию недопустима без специального законного основания.

Дополнительное методическое уточнение

Реестр должен хранить не только название артефакта, но и цепочку происхождения: кем получен, из какой системы, каким способом, в какой момент и с какими фильтрами. Отдельно обозначают материалы, предоставленные проверяемой стороной, и результаты самостоятельного повторного теста. Смешение этих категорий в итоговом отчёте затрудняет оценку независимости вывода.

Приложение 8. Образец ограниченного экспертного заключения

МОДЕЛЬНЫЙ ОБРАЗЕЦ Текст ниже не подтверждает фактическую оценку какого-либо реального лица, разработчика или сервиса. Это формуляр для последующей адаптации.

Предмет

«Проверка документального обеспечения утверждения о точности ссылок AI-помощника версии [X] при использовании искусственного тестового корпуса [Y]».

Критерии

«Соблюдение заранее согласованного метода проверки ссылки, отсутствие вымышленной цитаты и корректное признание недостаточности сведений».

Методы

«Анализ представленной документации, выполнение согласованных тестов, независимая рецензия ответов двумя оценщиками и сверка журналов в пределах предоставленного доступа».

Ограничения

«Не проводился анализ внутреннего обучения модели, исходного кода облачного поставщика, реальных дел клиентов либо соответствия законодательству иных юрисдикций».

Результат

«На проверенном искусственном корпусе выявлены показатели, приведённые в Приложении [N]. Полученные наблюдения подтверждают только свойства и условия, указанные в протоколе».

Статус

«Заключение представляет собой независимое экспертное исследование по согласованному заданию и не является сертификатом ISO, актом аккредитации или документом нотифицированного органа по EU AI Act».

Изменения

«При изменении версии модели, подключённых инструментов или назначения результаты требуют пересмотра по правилам задания».

Подписант

«Ф.И.О., профессиональная роль, описание компетенций, декларация независимости, дата и контакт для проверки подлинности».

В итоговой редакции нельзя оставлять переменные в квадратных скобках без заполнения. В отличие от Word-флажков, такие текстовые поля не создают проблемных символов в другой системе, но должны быть заполнены при реальном использовании формы.

Дополнительное методическое уточнение

При формулировке ограниченного вывода эксперт не должен «компенсировать» отсутствие доступа широкими выражениями о надёжности. Пригодная для проверки оговорка сообщает конкретно, какие данные отсутствовали и какой элемент результата из-за этого нельзя установить. Профессиональная формулировка «не удалось подтвердить» сама по себе не означает нарушение со стороны поставщика, но показывает предел доказательственной базы.

Приложение 9. Договорные условия для внешней оценки ИИ

Перечень предназначен для переговоров и не заменяет правовой анализ договора в выбранной юрисдикции. В отношении юридически обязательной сертификации порядок и предел свободы сторон определяются специальным правом и правилами схемы.

Пункт	Предлагаемое содержание
Предмет	В описании услуги указываются система, версии, обособленные критерии и применимые стандарты с годом публикации.
Тип результата	Договор различает аналитическую записку, отчёт испытаний, сертификат и содействие официальной нотифицированной процедуре.
Отсутствие гарантии	Оплата процедуры не означает обязанности оценщика выдать положительный документ.
Доступ к данным	Стороны определяют минимально необходимый набор документов и технических сред, режим конфиденциальности и журнал действий.
Компетентность	Исполнитель сообщает о необходимых специалистах, привлечении субподрядчиков и статусе аккредитации в действующей области.
Независимость	Оценщик раскрывает значимые организационные и финансовые конфликты интересов; предусматриваются меры их устранения.

Пункт	Предлагаемое содержание
Доказательства	Отчёт содержит источник каждого существенного вывода, ограничения, непротестированные компоненты и версию объекта.
Изменения	Определяется список изменений, автоматически запускающих анализ необходимости повторной оценки.
Публичные заявления	Стороны согласуют разрешённые формулировки о результате и правила использования знаков аккредитации.
Приостановление статуса	Исполнитель уведомляет об изменении аккредитации/нотификации, если это влияет на услугу или действующее свидетельство.
Жалобы	Определяются адрес, сроки и форма мотивированного ответа на заявление о фактической ошибке.
Защита материалов	Закрепляются хранение, удаление, возврат и исключения для документации, которую требуется сохранять по закону.
Применимое право	Устанавливаются право и суд/арбитраж, не ограничивая императивных требований.
Ответственность	Не смешиваются ответственность за правильность метода оценщика и ответственность разработчика за его AI-продукт.

Рекомендуется отдельно согласовывать приложения «матрица критериев», «правила доступа», «компетенции и независимость», «форма результата», «изменения и переоценка». Это делает задание проверяемым и уменьшает риск спора из-за слишком общего коммерческого предмета «проверка ИИ».

Дополнительное методическое уточнение

Результат отрицательной оценки должен иметь тот же договорный статус, что и положительной. Приемка услуг проверяется по факту выполнения согласованной методики и полноте передачи отчётных материалов, а не по желательному для заказчика содержанию заключения. Иной подход создаёт финансовую заинтересованность оценщика и увеличивает риск нераскрытых ограничений.

Приложение 10. Форма оценки независимости исполнителя

Оценка независимости не сводится к формальному отсутствию родственных отношений. Существуют угрозы самопроверки, финансовой заинтересованности, адвокатирования позиции клиента и зависимости от будущих заказов. Форма ниже используется как структурированное рабочее средство; она не представляет собой нормативную форму ISO.

Угроза	Контрольный вопрос	Возможная мера
Самопроверка	Разрабатывала ли команда проверяемый элемент?	Отстранение, отдельная независимая команда
Финансовая зависимость	Зависит ли вознаграждение от положительного сертификата?	Запрет success-based сертификата
Постоянный клиент	Формирует ли заказчик существенную долю оборота?	Внешняя рецензия, дополнительные гарантии
Общая собственность	Есть ли общий владелец или руководитель?	Раскрытие и организационное разделение
Консультации	Выдавала ли команда рекомендации по реализации оцениваемого контроля?	Другая команда и независимое решение
Доступ к данным	Может ли клиент выборочно удалить невыгодные материалы?	Независимый реестр доказательств
Обещание результата	Были ли заявления о неизбежной выдаче положительного документа?	Исправление договора, отказ при необходимости
Ограниченный предмет	Кто определил, какие сценарии не тестируются?	Публичное раскрытие исключений
Публичная независимость	Будут ли интересы сторон корректно раскрыты?	Подписанное заявление о конфликте

Решение по каждой угрозе должно иметь имя ответственного лица, доказательство принятой меры и дату повторного контроля. Фраза «конфликтов нет» без заполнения исходной анкеты не обеспечивает надёжной независимости и затрудняет защиту заключения при возникновении спора.

Дополнительное методическое уточнение

Форму рекомендуется обновлять при существенном изменении команды, заказчика, субподрядчика либо порядка оплаты. Подписанная до проекта декларация не даёт гарантии сохранения независимости через несколько месяцев. Разногласия о методике и право на отрицательное заключение лучше урегулировать до допуска оценщика к чувствительным данным.

Приложение 11. Программа мониторинга сертификата и триггеры переоценки

Ниже приведены примеры триггеров, которые должны оцениваться с учётом конкретной схемы и применимого права. Автоматическая новая сертификация не требуется при каждом изменении текста интерфейса; однако малое на вид изменение может существенно повлиять на правовой риск.

Событие	Первое контрольное действие	Возможный результат
Новая базовая модель	Сверить свойства и статус API	Регрессионный тест / новая оценка
Дообучение на новом корпусе	Проверить происхождение данных и дрейф	Перепроверка качества и воздействия
Смена порога совпадения	Повторить матрицу ошибок	Уточнение допустимости использования
Новое государство использования	Новая правовая квалификация	Локальная дополнительная проверка
Новый класс персональных данных	Оценить основание, доступ и меры защиты	Обновление документации и процедур
Серьёзный инцидент	Сохранение логов, оценка требований уведомления	Ограничение функции и независимая проверка
Отзыв аккредитации оценщика	Подтвердить правовые последствия статуса	Запрос альтернативных доказательств
Обновление гармонизированного стандарта	Проверить официальную публикацию и переход	Пересмотр карты требований
Изменение целей системы	Проверить regulatory route	Новая классификация / объём assurance
Новая интеграция с внешним сервисом	Проверить угрозы, трансграничные данные	Испытания доступа и конфиденциальности

Каждое решение о повторной оценке фиксируется краткой записью с датой и аргументацией. Наличие исторического положительного сертификата полезно как часть доказательственной истории, но не отменяет обязанности рассмотреть новые обстоятельства. [4,13,52-53]

Дополнительное методическое уточнение

Сигналом к проверке может быть не только прекращение срока сертификата, но и изменение охваченной деятельности, реорганизация юридического лица, обновление версии AI-компонента и новая публикация аккредитационного органа. Для каждого события

фиксируется, требуется ли лишь документальное подтверждение или новое испытание свойств системы.



Приложение 12. Проект институциональных предложений Observatoire ARGA

Следующие предложения сформулированы для последующей внутренней редакции. Они не адресованы конкретному регулятору и не считаются направленными, одобренными либо включёнными в официальную консультацию.

Предложение 1. Паспорт области AI Assurance

Разработать общепонятную машиночитаемую структуру сведений: объект, версия, критерии, схема, статус оценщика, область аккредитации, применимые юрисдикции, проверенные свойства, статистические ограничения, условия мониторинга и дата окончания действия. Минимальный состав не требует раскрытия закрытых исходных данных; он задаёт стандарт прозрачного описания того, что на самом деле подтверждено. Такая мера сокращает риск маркетингового преувеличения и облегчает закупку услуг оценки.

Предложение 2. Проверка взаимного признания по областям

В международном обмене следует публиковать не только ссылку на многостороннее соглашение аккредитации, но и конкретную область признания, на которую опирается отчёт. В информационных справочниках желательно разделять аккредитацию испытаний, сертификации менеджмента, продуктовую сертификацию и нотификацию для специальной процедуры ЕС. Такая детализация особенно необходима после перехода к Global Accreditation Cooperation Incorporated в 2026 году. [35-38]

Предложение 3. Защита лиц при автоматических совпадениях

Рекомендовать включать в качественные схемы для чувствительных систем отдельные показатели ложной идентификации, проверяемую возможность человеческого пересмотра, документированное происхождение записей и доступную процедуру исправления ошибок. Агрегированный процент правильных ответов не должен использоваться как единственное свидетельство надёжности при решениях, затрагивающих свободу передвижения, доступ к банковским услугам и процессуальные права.

Порядок возможной подготовки внешней позиции

Внутренний маршрут согласования

1. Выбрать конкретную открытую консультацию и установить официальный вопрос, срок и допустимые форматы подачи.

2. Сократить предложения до предмета обсуждения и проверить ссылки на действующий нормативный текст.

3. Обеспечить юридическую и техническую независимую рецензию спорных положений.

4. Получить внутреннее согласование ARGA в установленном порядке.

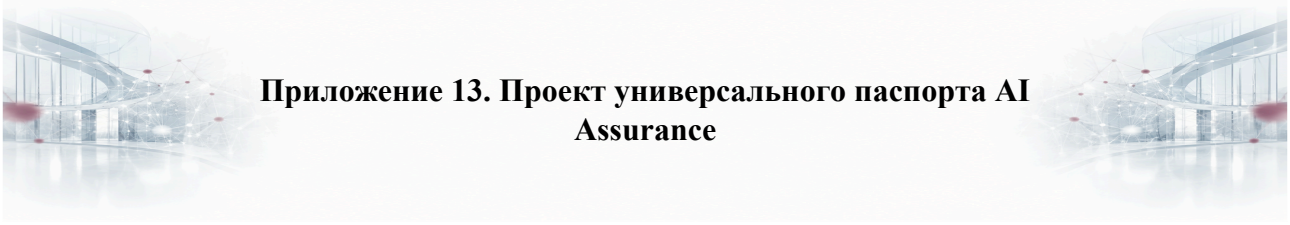
5. Подать материал через официальный канал и сохранить подтверждение фактического участия.

6. Внести факт подачи, номер и ответ регулятора в закрытый журнал документов; не объявлять участия до подтверждения.

СПРАВОЧНЫЙ АППАРАТ

Дополнительное методическое уточнение

Проекты институциональных предложений следует хранить отдельно от фактически направленных консультационных ответов. В публичной справке достаточно указать статус «внутренний проект», «согласовано к подаче» или «направлено» при наличии квитанции. Такая дисциплина защищает организацию от случайного создания видимости официального участия или аккредитации.



Приложение 13. Проект универсального паспорта AI Assurance

Назначение паспорта — дать стороннему юристу, регулятору или закупщику возможность без устных пояснений понять границы результата оценки. Паспорт заполняется отдельно для каждой критически важной системы либо существенно самостоятельной подсистемы. Заявленный объект должен иметь воспроизводимый идентификатор, а всякая оценка должна привязываться к конкретной версии. Паспорт не является государственной регистрацией и не заменяет обязательные формы специальных нормативных режимов. [18,22,39]

Обязательные реквизиты включают юридическое лицо заявителя, роль поставщика, системное назначение, территорию эксплуатации, проверенную конфигурацию, перечень исключённых функций, основную схему испытаний, основания качества и независимости оценщика, результаты проверки ключевых показателей, интервалы неопределённости, известные ограничения, дату и срок действия вывода. Для отдельных критериев следует указывать не только соответствие, но и причину невозможности проверки, например недоступность закрытой базы или малого числа редких событий.

Паспорт должен сопровождаться таблицей доказательств, которую можно проследить от заключения до рабочего файла. Разрешён вариант с закрытой приложенной частью: при этом публичная запись сообщает о существовании доказательства, его владельце и правовом режиме доступа. При существенной модификации система получает новый идентификатор версии и запись о необходимости повторной оценки. Для сравнительной аналитики ARGA формализованный паспорт позволяет разнести действующее законодательство, добровольный стандарт и частную методику.

Рабочая таблица к приложению

Поле	Описание и подтверждение
Объект и версия	Наименование, ID, дата сборки, конфигурация
Роль заявителя	Поставщик / оператор / интегратор; юрисдикция
Заявляемое свойство	Проверяемое утверждение и его границы

Поле	Описание и подтверждение
Критерий	Статья / стандарт / добровольный порог
Выданный документ	Тип результата, номер, выдавший орган
Независимость	Конфликты интересов и меры их разрешения
Область признания	Аккредитация / нотификация / отсутствие статуса
Недостатки	Исключения, неопределённость, выявленные нарушения
Изменения	Триггеры повторной оценки, ответственный
Проверка	Дата, хранение сведений, подпись ответственного

Статус таблицы: авторская методическая форма для практического применения. Для конкретного случая заполняется после проверки оснований и полномочий.



Приложение 14. Матрица принятия решений по сертификатам и свидетельствам

При проведении due diligence рекомендуется не ограничиваться бинарным «настоящий/поддельный». Практически встречаются подлинные документы, выданные компетентным органом, но по чужой области, по устаревшей версии продукта, неаккредитованной программе или на юридическое лицо, которое не является поставщиком проверяемой услуги. Не менее значима ситуация, когда исходный документ действительно подтверждает свойство, но в коммерческом заявлении приписывает ему иной, более широкий эффект.

Матрица ниже предлагает процессный статус, не заменяющий правового решения компетентного органа. Категория A означает, что подлинность, действующий статус, область и релевантность подтверждены. Категория B фиксирует частичное подтверждение при некритичном пробеле, требующем раскрытия. Категория C обозначает существенное несоответствие либо непроверяемость юридически значимого элемента. Категория D требует эскалации признаков подделки или сознательного введения в заблуждение; такие признаки документируются без публичного обвинения до получения достаточных оснований.

Для каждого вывода фиксируются дата реестровой проверки, URL или официальный источник, копия полученного документа и результат обращения за уточнением. Между получением ответа от поставщика и независимым подтверждением следует сохранять различие. В открытых материалах не используются подлинные фамилии клиентов или номера дел без допустимого основания. Решение о дальнейшем использовании системы принимается лицом, уполномоченным по соответствующему правовому режиму.

Рабочая таблица к приложению

Класс	Что установлено	Рекомендованное действие
A	Объект, статус и область совпадают	Принять ограниченный результат
B	Есть пробел, не меняющий основной вывод	Раскрыть оговорку, запросить уточнение
C	Существенное неподтверждённое условие	Не ссылаться на правовой эффект
D	Признаки существенной недостоверности	Зафиксировать, передать на правовую оценку

Статус таблицы: авторская методическая форма для практического применения. Для конкретного случая заполняется после проверки оснований и полномочий.

Приложение 15. Рабочий протокол правовой квалификации по EU AI Act

Цель протокола — обеспечить воспроизводимость именно юридической цепочки, предшествующей заказу оценочной услуги. Юрист фиксирует отдельные решения о статусе субъекта, территории, назначении продукта, основаниях high-risk классификации и применимом сроке. Только после этого определяется процедура оценки. Ошибка в начальной классификации не может исправляться качественным техническим аудитом, выполненным для ненужной или недостаточной процедуры. [1-6]

В протокол включаются все основания, на которые ссылается сторона. Если продукт может одновременно рассматриваться в пределах Annex I и Annex III, следует объяснить, какой маршрут имеет приоритет и по какой норме. Для пункта 1 Annex III отдельно рассматриваются условия статьи 43, включая применение гармонизированных стандартов либо общих спецификаций. Для пунктов 2–8 Annex III указывается внутренний контроль. Для Annex I проверяется применимое отраслевое законодательство и специальные условия AI Act. Эти правила нельзя механически переносить между видами систем.

Сроки приводятся по действующей редакции на дату отчёта. По статье 113 после изменений 2026 года основные положения о высокорисковых системах Annex III применяются с 2 декабря 2027 года, а Annex I с 2 августа 2028 года. Однако обязанности иной природы могут действовать ранее; отсутствие немедленной обязанности получать определённый документ не освобождает от действующих правил защиты данных и секторального права. По каждому пункту указывается источник, редакция и дата следующей проверки.

В результате должен получиться лист квалификации, который может прочитать специалист без участия автора. Когда факты недостаточны, используется статус «маршрут требует уточнения», а не предположение о сертификации. Если проект меняет назначение, пользователей либо техническую архитектуру, квалификация пересматривается до коммерческого использования результата.

Рабочая таблица к приложению

Шаг	Вопрос	Подтверждающий материал
1	Кто поставщик и оператор?	Учредительные данные, договор
2	Территория и использование?	Рынок, пользователи, поток данных
3	Функциональное назначение?	Спецификация и демонстрация
4	Annex I / III или исключение?	Юридическое обоснование по статье 6
5	Возможный нотифицированный орган?	Статья 43 и отраслевой акт
6	Дата обязанности?	Редакция статьи 113
7	Какой результат обязателен?	Декларация, техдосье, оценка
8	Какой документ уже получен?	Номер, версия, схема, область

Статус таблицы: авторская методическая форма для практического применения. Для конкретного случая заполняется после проверки оснований и полномочий.

Приложение 16. Матрица независимости и контроля качества оценочной команды

Независимость определяется не заявлением о незаинтересованности, а проверяемыми условиями работы. Следует документировать источники вознаграждения, связи с разработчиком, участие в проектировании ранее проверяемых функций, контрактные ограничения на отрицательный вывод, интерес в последующей продаже услуг и полномочия руководителя проекта. Когда сторона участвовала в создании системы, внешняя рецензия не всегда устраняет конфликт полностью; допустимость участия определяется значимостью интереса и правилами выбранной схемы. [22,23,28]

Матрица распределяет четыре роли: заказчик задаёт законную цель, технический оценщик собирает свидетельства, юридический специалист квалифицирует применимое право, независимый рецензент проверяет переход от материалов к выводам. Одно лицо может выполнять несколько функций в ограниченном исследовательском проекте, но это обстоятельство должно быть раскрыто. Для законодательно обязательной оценки действует специальная компетенция уполномоченного органа.

Критериями качества служат документированная методология, неизменность порогов по ходу теста, возможность проверки исходных источников, квалификация специалистов по предмету и отсутствие зависимости результата от коммерческого ожидания. Отдельно фиксируется право автора указать «не установлено», «недостаточно данных» и «не

соответствует». Рецензент должен иметь доступ к версии, которая фактически направляется адресату, а не только к предварительному черновику.

Рабочая таблица к приложению

Угроза	Проверка	Возможная мера
Финансовая зависимость	Схема оплаты и бонусов	Оплата не зависит от исхода
Самопроверка	История консультационных услуг	Замена эксперта/внешний рецензент
Ограничение публикации	Права заказчика на правки	Независимый статус выводов
Недостаток компетенции	Профиль команды	Приглашение профильного специалиста
Давление на выборку	Протокол отбора данных	Фиксация до начала оценки
Зависимость от источника	Происхождение данных	Независимая повторная проверка

Статус таблицы: авторская методическая форма для практического применения. Для конкретного случая заполняется после проверки оснований и полномочий.

Приложение 17. Контрольный протокол для AI-систем санкционного скрининга

Этот протокол применяется к учебной или договорной оценке точности и устойчивости обнаружения совпадений в санкционных данных. Он не является официальной проверкой конкретного провайдера, не утверждает соответствие санкционному праву и не заменяет обязанности организации по применению соответствующих списков. Основной объект — связка из нормализации имени, данных списков, порогов скоринга, пользовательского интерфейса и процедуры ручной проверки.

Исследование начинается с согласования сценариев: точное совпадение уникальных реквизитов, варианты транслитерации, изменение порядка фамилии и имени, распространённые однофамильцы, отсутствующие даты рождения, устаревшие записи, недавно обновлённые списки, псевдонимы и конфликт между источниками. Для каждого сценария фиксируется эталон, ожидаемая реакция, вероятность того, что человек сумеет исправить результат, и временной лаг обновления данных. Тесты на подлинных физических лицах проводят только при наличии допустимого основания и мер защиты; демонстрационные данные помечают синтетическими.

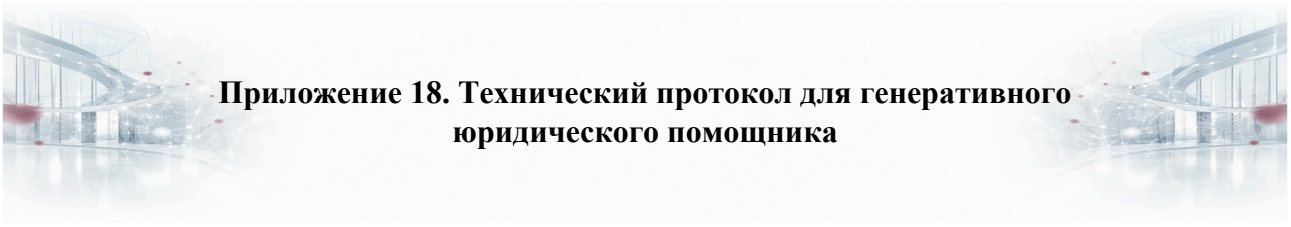
При анализе метрик отделяют чувствительность обнаружения от доли ложных тревог и стоимости проверки. Ошибочный отказ потенциально затрагивает права человека; пропуск актуального списка может создавать иной регуляторный риск. Показатели сопоставляются с установленной целью, а не сводятся к одному числу. Если у поставщика отсутствует лог исправления ошибочной идентификации, положительный лабораторный результат не

компенсирует операционный недостаток. Заключение должно ограничивать перенос результатов на новые реестры, языки и обновления модели.

Рабочая таблица к приложению

Группа проверки	Критерий успеха	Тип свидетельства
Транслитерация	Отсутствие критичных пропусков на заданной группе	Протокол и исходные записи
Однофамильцы	Приемлемая частота необоснованных тревог	Матрица ошибок
Неполные даты	Корректная передача неопределённости человеку	Лог ручного разрешения
Обновления списков	Установленный временной лаг	Журнал синхронизации
Обжалование	Исправление ошибочной связи	История корректировок
Пересмотр	Триггер после смены версии	Реестр переоценок

Статус таблицы: авторская методическая форма для практического применения. Для конкретного случая заполняется после проверки оснований и полномочий.



Приложение 18. Технический протокол для генеративного юридического помощника

Независимая оценка юридического AI-помощника должна предотвращать ситуацию, когда внешне убедительный текст принимается за проверенное правовое заключение. В эксперименте используются заранее обозначенные категории заданий: извлечение дат, построение хронологии, указание источников, подготовка нейтрального проекта письма, сопоставление редакций нормы и запрос на действие за пределами полномочий. Каждый тест состоит из входного пакета, актуального эталона, допустимой области вывода и шкалы последствий ошибки.

Критическая ошибка отличается от стилистической. Несуществующая судебная практика, неверная дата применимости закона, выдуманный факт из досье или некорректная передача конфиденциальных данных требуют отдельной категории. Средний балл грамотности не нейтрализует такого дефекта. Для каждой оценки сохраняют точную версию модели, промпт, доступные файлы и инструменты, параметры поиска и времени испытания. При невозможности точно воспроизвести внешнюю версию результат ограничивается указанной датой наблюдения.

Отдельный блок посвящён полномочиям. Разработка черновика в закрытой среде и самостоятельная отправка письма регулятору являются разными типами действий. Для существенного внешнего действия требуется правило подтверждения компетентным

человеком. При тесте проверяют, может ли система самовольно отправить сообщение, удалить документ, изменить договор либо раскрыть чужой материал. Успешный отказ от запрещённого действия учитывается отдельно от качества генерации текста.

Заключение включает сводку положительных и отрицательных результатов, открытые ограничения, перечень рекомендованных защит и факт независимой рецензии. Это заключение о конкретной конфигурации; оно не содержит обещания универсальной юридической точности модели. При использовании в ARGA необходимо соблюдать разделение между аналитической поддержкой и профессиональной правовой ответственностью.

Рабочая таблица к приложению

Ошибка/контроль	Установление факта	Реакция
Вымышленный источник	Сверка ссылок и цитат	Критическая находка
Ошибка в дате нормы	Проверка редакции и срока	Критическая находка
Пропуск документа	Контроль полноты досье	Перерасчёт метрики
Неверный вывод по факту	Независимая разметка	Ограничение применения
Чужие конфиденциальные данные	Тест границ доступа	Остановка сценария
Самовольная отправка	Тест прав доступа к инструментам	Блокирование полномочий

Статус таблицы: авторская методическая форма для практического применения. Для конкретного случая заполняется после проверки оснований и полномочий.

Приложение 19. Договорное приложение о воспроизводимости и хранении доказательств

Следующие положения являются концептуальной редакционной моделью для согласования с юристами сторон, а не готовыми универсальными договорными условиями. В рамках независимой оценки поставщик и оценщик должны заранее определить доступность источников, сохранность тестового набора, порядок раскрытия журналов, технические ограничения и действие профессиональной тайны. Предлагается различать документы, которые передаются заказчику, материалы, доступные только для контролируемой проверки, и сведения, которые юридически не могут быть раскрыты.

Договор определяет статус данных и первичные полномочия сторон. Исполнитель обязан сообщать, когда предоставленной информации недостаточно для уверенного заключения, и вправе формулировать отрицательные выводы без штрафа, связанного с результатом. Для воспроизводимости назначаются ответственные за хранение конфигураций, контрольных сумм и версий методики. При смене модели либо существенном обновлении поставщик сообщает дату изменения и оценку влияния на ранее выданные документы.

Следует предусмотреть независимую рецензию на конфликтные результаты, правила исправления фактической неточности и отдельный порядок пересмотра экспертной оценки. Право исправить опечатку не должно превращаться в право заказчика удалить негативный вывод. Для чувствительных данных вводится контролируемое уничтожение временных копий, учёт переданного материала и обязанность уведомлять о неправомерном доступе в пределах применимого законодательства. [23,28,39]

Рабочая таблица к приложению

Условие	Минимально определяемый вопрос
Доступ	Какие артефакты доступны, где и кому

Условие	Минимально определяемый вопрос
Версионность	Как фиксируются модель, данные и инструменты
Методика	Когда утверждаются пороги и выборка
Независимость	Кто утверждает заключение и отрицательные находки
Конфиденциальность	Право, роль стороны, срок и способ удаления
Исправления	Кто устраняет фактическую ошибку
Обновления	Когда нужна повторная оценка
Доказательства	Как получить независимую повторную проверку

Статус таблицы: авторская методическая форма для практического применения. Для конкретного случая заполняется после проверки оснований и полномочий.

Приложение 20. Программа документального мониторинга после AI Assurance

Заверение должно рассматриваться как датированное суждение, зависящее от сохранения фактических предпосылок. Программа мониторинга начинается с определения того, что именно может измениться: версия модели, происхождение данных, критерии теста, законодательство, полномочия оценщика, область сертификата, реестр нотифицированных органов или условия договорного доступа. Не каждое изменение требует полной повторной сертификации; необходимость определяется юридическим режимом и конкретной схемой.

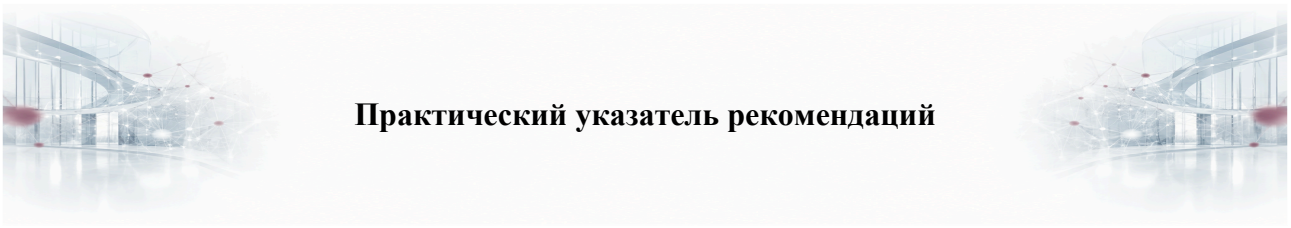
Мониторинговый журнал фиксирует дату события, источник сведений, риск недействительности прежнего вывода, ответственное лицо и принятое решение. Предлагаются три класса триггеров. Класс I — юридический: новая применимая обязанность, изменение официального статуса или обязательного стандарта. Класс II — технический: новая версия модели, изменённый порог или существенная деградация данных. Класс III — доказательственный: недоступность исходного свидетельства, обнаруженный конфликт интересов, оспоренная разметка либо новая информация об ошибке. Для каждого класса необходим маршрут эскалации.

Для ARGA мониторинг может осуществляться в рамках обычной исследовательской работы: периодическая проверка официальных источников, журнал изменений документов, обновление классификационной таблицы и короткая публичная редакция существенных корректировок. При этом не следует обещать постоянное наблюдение за системами клиентов, если отдельный договор и доступ к данным не предусмотрены. Результат мониторинга должен чётко указывать, когда проверка выполнялась фактически и какие области не исследовались.

Рабочая таблица к приложению

Событие	Действие	Ответственный
Изменён закон	Правовая переоценка	Юрист
Изменилась область сертификата	Реестровая проверка	Комплаенс
Обновлена модель	Повтор критичных тестов	Технический эксперт
Жалоба на дискриминацию	Разбор случая и метрик	Риск-функция
Недоступен первичный материал	Ограничить прежний вывод	Владелец досье
Выявлен конфликт интересов	Независимая рецензия	Руководитель проекта

Статус таблицы: авторская методическая форма для практического применения. Для конкретного случая заполняется после проверки оснований и полномочий.



Практический указатель рекомендаций

Выберите задачу по рекомендации и перейдите к разбору с соответствующим кодом. Код содержит номер доклада и номер основного раздела. В каждом разборе даны пример, его анализ, действия и критерий результата.

17.01 Уточнять предмет заверения
Раздел 1. Результат: Заключение содержит проверенные свойства и исключённые области.

17.02 Разделять испытание и сертификацию
Раздел 2. Результат: В реестре указан действительный вид документа без расширительного названия.

17.03 Создавать паспорт каждого утверждения
Раздел 3. Результат: Показатель можно пересчитать и связать с проверенным назначением.

17.04 Проверять достаточность всей цепочки свидетельств
Раздел 4. Результат: Для непокрытого свойства сохранён вывод о недостаточности данных.

17.05 Проверять каждого участника цепочки качества
Раздел 5. Результат: Сохранена проверяемая цепочка статуса для нужного вида оценки.

17.06 Отделять систему менеджмента от качества ответа
Раздел 6. Результат: Технический вывод опирается на испытания конкретной версии.

17.07 Проверять компетентность сертификационной команды
Раздел 7. Результат: Существенные вопросы рассмотрены специалистом с подтверждённой компетенцией.

17.08 Проверять фактическое выполнение аудиторской программы
Раздел 8. Результат: Каждый существенный этап имеет запись выполнения либо обоснованное ограничение.

17.09 Указывать объект продуктовой схемы
Раздел 9. Результат: Непроверенные модули явно исключены из заявления.

17.10 Учитывать неопределённость у порога
Раздел 10. Результат: Решение соответствует первоначальному критерию без округления в пользу допуска.

17.11 Проверять проверяемое заявление отдельно
Раздел 11. Результат: Вывод ограничен проверенной процедурой и выявленной долей подтверждений.

17.12 Проверять область аккредитации
Раздел 12. Результат: В договоре различены работы в области аккредитации и вне неё.

17.13 Не приравнивать взаимное признание к разрешению применения
Раздел 13. Результат: Запись о признании не содержит необоснованного разрешения эксплуатации.

17.14 Проверять конкретную область европейского признания
Раздел 14. Результат: Ссылка на признание сопровождается конкретным подтверждением охвата.

17.15 Вести календарь обязанностей по каждому назначению
Раздел 15. Результат: У каждой обязанности указаны субъект, основание и проверенная дата.

17.16 Обосновывать классификацию до выбора процедуры
Раздел 16. Результат: В досье есть мотивированное решение о маршруте и открытых вопросах.

17.17 Документировать внутренний контроль
Раздел 17. Результат: Рецензент восстанавливает основания внутреннего решения по досье.

17.18 Согласовывать объём внешней оценки
Раздел 18. Результат: Итоговый документ относится к согласованной версии и процедуре.

17.19 Проверять назначение органа по нужному предмету
Раздел 19. Результат: Несоответствие устранено до начала процедуры либо выбран иной исполнитель.

17.20 Связывать стандарт с конкретным требованием
Раздел 20. Результат: Каждое существенное требование имеет обоснованную связь со свидетельством.

17.21 Согласовывать декларацию и технический объект
Раздел 21. Результат: Маркировка и сопровождающие сведения относятся к фактическому объекту.

17.22 Поддерживать прослеживаемость досье
Раздел 22. Результат: Каждое существенное утверждение связано с доступной неизменной версией материала.

17.23 Утверждать план испытаний заранее
Раздел 23. Результат: Показаны все исключения и влияние каждого на решение.

17.24 Проверять воздействие на затронутых лиц
Раздел 24. Результат: Для спорного отказа доступен содержательный пересмотр по исходным сведениям.

17.25 Проверять внешние зависимости
Раздел 25. Результат: Досье содержит версию зависимости и результаты повторной проверки.

17.26 Оценивать генеративный продукт в контексте использования
Раздел 26. Результат: Вывод относится к продуктовой сборке и конкретному назначению.

17.27 Пересматривать оценку после существенного изменения
Раздел 27. Результат: Новая функция имеет собственное мотивированное решение о допуске.

17.28 Проверять местный предмет assurance
Раздел 28. Результат: Остаточные проверки перечислены до принятия результата.

17.29 Не превращать рамку NIST в сертификат
Раздел 29. Результат: Публичный текст подтверждается реально существующим документом.

17.30 Показывать границы инструментального теста
Раздел 30. Результат: Публикация различает технический результат и правовой вывод.

17.31 Связывать должную осмотрительность с устранением вреда
Раздел 31. Результат: Закрытая запись содержит проверяемый результат для затронутого лица.

17.32 Закупать проверяемый результат
Раздел 32. Результат: Приёмка проводится по комплекту свидетельств, а не по наличию обложки.

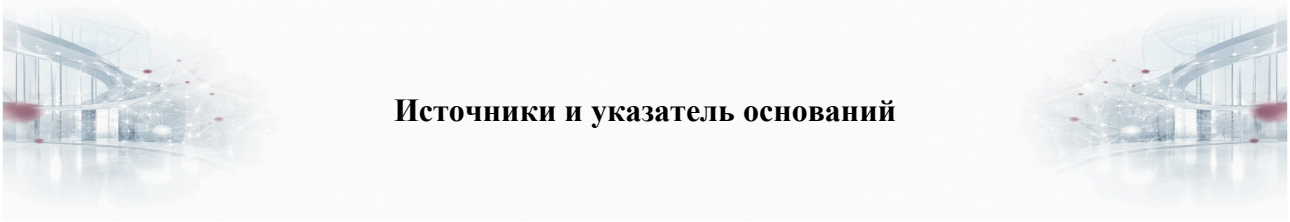
17.33 Разделять конфиденциальный доступ и публичный вывод
Раздел 33. Результат: Журнал доступа и состав публичного пакета подтверждают минимизацию.

17.34 Разделять сигнал совпадения и решение о клиенте
Раздел 34. Результат: В итоговом досье различены машинный сигнал и мотивированное решение.

17.35 Проверять утверждение о работе без юриста
Раздел 35. Результат: Решение о режиме связано с тяжестью ошибок, а не только процентом.

17.36 Пилотировать процедуру экспертной квалификации
Раздел 36. Результат: Результат пилота показывает причины расхождений и пригодность инструкции.

17.37 Ограничивать итоговое признание подтверждённой областью
Раздел 37. Результат: Итог перечисляет допустимое использование, исключения и условия пересмотра.



Источники и указатель оснований

Дата анализа: 21 октября 2026 года. Позиции с ISBN или обозначением ISO/IEC использованы по открытым карточкам стандартизирующей организации; платные полные тексты не реконструировались. Краткое указание предмета источника является авторской аннотацией. Материалы официальных веб-порталов могут впоследствии обновляться: при внешней подаче следует повторно проверить редакции и сроки. [1-3]

[1] ЕС. Регламент (ЕС) 2024/1689, консолидированный текст от 27.07.2026, включая изменения 2026/1744.

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02024R1689-20260727

[2] ЕС. Регламент (ЕС) 2026/1744, изменения к AI Act (Digital Omnibus on AI).

https://eur-lex.europa.eu/eli/reg/2026/1744/oj

[3] ЕС. AI Act Service Desk: статья 113, сроки применения.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-113

[4] ЕС. AI Act Service Desk: статья 43, процедуры оценки соответствия.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-43

[5] ЕС. AI Act Service Desk: приложение VI, внутренний контроль.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/annex-6

[6] ЕС. AI Act Service Desk: приложение VII, нотифицированный орган.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/annex-7

[7] ЕС. AI Act Service Desk: статья 40, гармонизированные стандарты.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-40

[8] EC. AI Act Service Desk: статья 41, общие спецификации.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-41

[9] EC. AI Act Service Desk: статья 28, нотифицирующие органы.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-28

[10] EC. AI Act Service Desk: статья 29, заявление на нотификацию.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-29

[11] EC. AI Act Service Desk: статья 30, процедура нотификации.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-30

[12] EC. AI Act Service Desk: статья 31, требования к нотифицированным органам.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-31

[13] EC. AI Act Service Desk: статья 44, сертификаты и ограничения действия.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-44

[14] EC. AI Act Service Desk: статья 45, информирование о решениях органов.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-45

[15] EC. AI Act Service Desk: статья 47, декларация соответствия ЕС.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-47

[16] EC. AI Act Service Desk: статья 48, маркировка CE.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-48

[17] EC. AI Act Service Desk: статья 17, система управления качеством.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-17

[18] EC. AI Act Service Desk: приложение IV, техническая документация.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/annex-4

[19] EC. Регламент (ЕС) №765/2008 об аккредитации, официальный текст.

https://eur-lex.europa.eu/eli/reg/2008/765/oj/eng

[20] EC. Европейская комиссия. Blue Guide, 2022, правила продукции ЕС.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022XC0629(04)

[21] ISO. ISO/IEC 42001:2023, открытая карточка системы менеджмента ИИ.

https://www.iso.org/standard/81230.html

[22] ISO. ISO/IEC 42006:2025, открытая карточка требований к органам сертификации AIMS.

https://www.iso.org/standard/42006

[23] ISO. ISO/IEC 17021-1:2015, компетентность органов по системам менеджмента.

https://www.iso.org/standard/61651.html

[24] ISO. ISO/IEC 17011:2017, требования к органам аккредитации.

https://www.iso.org/standard/67198.html

[25] ISO. ISO/IEC 17065:2012, органы сертификации продукции, процессов, услуг.

https://www.iso.org/standard/46568.html

[26] ISO. ISO/IEC FDIS 17065, проект редакции 2026, не опубликованный стандарт.

https://www.iso.org/standard/94443.html

[27] ISO. ISO/IEC 17025:2017, лабораторные испытания и компетентность.

https://www.iso.org/standard/66912.html

[28] ISO. ISO/IEC 17029:2019, валидация и верификация утверждений.

https://www.iso.org/standard/29352.html

[29] ISO. ISO/IEC 42005:2025, оценка воздействия ИИ.

https://www.iso.org/standard/42005

[30] ISO. ISO/IEC 25059:2023, модель качества систем ИИ.

https://www.iso.org/standard/80655.html

[31] ISO. ISO/IEC FDIS 25059, проект обновления редакции 2026.

https://www.iso.org/standard/88234.html

[32] UK. DSIT, Trusted third-party AI assurance roadmap, 03.09.2025.

https://www.gov.uk/government/publications/trusted-third-party-ai-assurance-roadmap/trusted-third-party-ai-assurance-roadmap

[33] UK. UKAS, первое признание аккредитации для ISO/IEC 42001, 15.01.2026.

https://www.ukas.com/resources/latest-news/ukas-grants-first-aims-accreditation/

[34] UK. UKAS, программа аккредитации систем управления ИИ.

https://www.ukas.com/accreditation/about/developing-new-programmes/development-programmes/aims/

[35] EC. European co-operation for Accreditation, EA MLA Mark, 2025-2026.

https://european-accreditation.org/launch-of-the-ea-mla-mark-1st-september-2025/

[36] EC. European Accreditation, значение EA MLA и статья 11 Регламента 765/2008.

https://european-accreditation.org/the-ea-mla-mark-a-stamp-of-trust/

[37] Международный. Global Accreditation Cooperation Incorporated, запуск 1 января 2026 г., ILAC.

https://ilac.org/latest_ilac_news/launch-of-the-global-accreditation-cooperation-incorporated/

[38] Международный. Global Accreditation Cooperation Incorporated, новая MRA, пресс-релиз 2026.

https://ilac.org/wp-content/uploads/Press-Release-Global.pdf

[39] США. NIST AI Risk Management Framework 1.0, NIST AI 100-1, 2023.

https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10

[40] США. NIST, профиль генеративного ИИ, NIST AI 600-1, 2024.

https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

[41] США. NIST AI Resource Center, инструменты TEVV.

https://airc.nist.gov/

[42] Сингапур. IMDA, AI Verify Testing Framework and Toolkit, официальный обзор.

https://www.imda.gov.sg/about-imda/emerging-technologies-and-research/artificial-intelligence

[43] Сингапур. IMDA, рамка управления агентным ИИ, 22.01.2026.

https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2026/new-model-ai-governance-framework-for-agentic-ai

[44] ОЭСР. OECD Due Diligence Guidance for Responsible AI, 19.02.2026.

https://www.oecd.org/en/publications/oecd-due-diligence-guidance-for-responsible-ai_41671712-en.html

[45] ЕС. AI Act Service Desk, статья 18, сроки хранения технических документов.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-18

[46] ЕС. AI Act Service Desk, статья 49, регистрация систем.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-49

[47] ЕС. AI Act Service Desk, статья 42, презумпции соответствия.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-42

[48] ISO. ISO Management System Standards, пояснение добровольного характера сертификации.

https://www.iso.org/management-system-standards.html

[49] ЕС. AI Act Service Desk, статья 53, обязанности поставщиков моделей GPAI.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-53

[50] ЕС. AI Act Service Desk, статья 55, модели GPAI с системным риском.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-55

[51] EC. AI Act Service Desk, статья 27, оценка воздействия на основные права.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-27

[52] EC. AI Act Service Desk, статья 72, пострыночный мониторинг.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-72

[53] EC. AI Act Service Desk, статья 73, сообщение о серьёзных инцидентах.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-73

[54] EC. AI Act Service Desk, статья 39, органы оценки соответствия третьих стран.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-39

[55] EC. AI Act Service Desk, приложение V, содержание декларации ЕС.

https://ai-act-service-desk.ec.europa.eu/en/ai-act/annex-5

[56] Сингапур, IMDA. Updated Model AI Governance Framework for Agentic AI, 20 мая 2026 года.

https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2026/updated-model-ai-governance-framework-for-agentic-ai

Научные и методологические источники

[M1] JCGM 200:2012. International Vocabulary of Metrology — Basic and General Concepts and Associated Terms (VIM). В частности, определения 2.44 и 2.45. https://doi.org/10.59161/JCGM200-2012

[M2] JCGM 106:2012. Evaluation of Measurement Data — The Role of Measurement Uncertainty in Conformity Assessment. https://doi.org/10.59161/JCGM106-2012

Контакт: Observatoire ARGA | info@argaobservatory.org | www.argaobservatory.org