ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

Н А Ц И О Н А Л Ь Н Ы Й
С Т А Н Д А Р Т
Р О С С И Й С К О Й
Ф Е Д Е Р А Ц И И

ГОСТ Р ИСО/МЭК 42001 —

(Проект, первая редакция)

Информационные технологии

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Система управления

(ISO/IEC 42001:2022, IDT)

Настоящий проект стандарта не подлежит применению до его утверждения

Москва

Российский институт стандартизации

202_

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Институт развития информационного общества» (ИРИО) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 164 «Искусственный интеллект»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 202_ г. №- ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 42001:2022 «Информационные технологии. Искусственный интеллект. Система управления» (ISO/IEC 42001:2022 «Information technology — Artificial intelligence — Management system», IDT).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок – в ежемесячном информационном указателе

«Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомления и тексты размещаются также в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.rst.gov.ru)

Содержание

Введение

Искусственный интеллект (ИИ) все чаще применяется во всех секторах, использующих информационные технологии, и, как ожидается, станет одним из основных экономических факторов. Вследствие этой тенденции, некоторые приложения могут привести к возникновению социальных проблем в ближайшие годы.

Цель настоящего стандарта — помочь организациям ответственно выполнять свою роль в отношении ИИ-систем (например, использовать, разрабатывать, осуществлять мониторинг работы или предоставлять продукты или услуги, использующие ИИ). ИИ потенциально поднимает конкретные вопросы, такие как:

- Автоматическое принятие решений с использованием ИИ, иногда непрозрачным и необъяснимым способом, может потребовать специального управления, выходящего за рамки управления классическими ИТ-системами.
- Использование анализа данных, озарения и машинного обучения, а не предписанной человеком логикой проектирования систем, как расширяет возможности применения ИИ-систем, так и изменяет способ разработки, обоснования и развертывания таких систем.
- Во время использования, ИИ-системы, осуществляющие непрерывное обучение, меняют свое поведение. Для обеспечения ответственного использования ИИ-систем даже при таком постоянно меняющемся поведении требуется особое внимание.

Настоящий стандарт содержит требования к созданию, внедрению, поддержанию в рабочем состоянии и постоянному улучшению системы менеджмента ИИ в среде организации. Организациям следует сосредоточить применение требований на характеристиках, уникальных для ИИ. Ввиду определенных особенностей ИИ, таких как

способность к постоянному обучению и улучшению или отсутствие прозрачности или объяснимости, может потребоваться использование различных мер предосторожности, в случае если при выполнении задачи с помощью ИИ возникают дополнительные опасения по сравнению с тем, если бы задача выполнялась традиционным способом. Внедрение системы менеджмента ИИ для расширения существующих структур управления является стратегическим решением для организации.

На создание и внедрение системы менеджмента ИИ оказывают влияние следующие факторы: потребности и цели организации, процессы, размер и структура и ожидания различных заинтересованных сторон. Другим набором факторов, влияющих на создание и внедрение системы менеджмента ИИ, являются многочисленные варианты использования ИИ и необходимость соблюдения надлежащего баланса между механизмами стратегического управления и инновациями. Организации могут предпочесть применять эти требования только в отношении конкретных вариантов использования ИИ высокого риска, вместо широкомасштабного применения системы менеджмента ИИ ко всем вариантам использования, поскольку такое широкое применение может помешать достижению других деловых целей, не давая при этом взамен сколько-нибудь заметной отдачи и лишь создавая дополнительные проблемы. Ожидается, что все эти факторы влияния со временем будут меняться, поэтому следует время от времени проводить их повторный анализ.

Важно обеспечить интеграцию системы менеджмента ИИ с процессами организации и общей структурой управления. При проектировании процессов, информационных систем и разработке мер управления необходимо учитывать конкретные факторы, связанные с

ИИ. Критически важными примерами таких процессов управления являются:

- определение организационных целей, вовлечение заинтересованных сторон и организационная политика;
- управление рисками и возможностями;
- процессы управления факторами, связанными с надежностью ИИ-систем, такими как защита, безопасность, справедливость, прозрачность, качество данных и качество ИИ-систем на протяжении всего их жизненного цикла.

В настоящем стандарте содержатся рекомендации по развертыванию применимых мер управления для поддержки таких процессов и отсутствуют конкретные указания по процессам управления. Для внедрения важнейших процессов, таких как управление рисками, жизненным циклом и качеством данных организация может сочетать общепринятые концепции и свой собственный опыт.

Организация, соответствующая требованиям настоящего стандарта, может создать свидетельство своей ответственности и подотчетности касательно своей роли в отношении ИИ-систем. Настоящий стандарт может использоваться, при желании, для проведения самооценки, оценки заинтересованной стороной или независимой верификации (например, сертификации) на основании этих свидетельств/доказательств.

Порядок, в котором представлены требования в настоящем стандарте, не отражает их важности и не подразумевает порядок, в котором они должны быть реализованы. Нумерация элементов списка носит исключительно справочный характер.

Совместимость с другими стандартами систем менеджмента.

В настоящем стандарте применяется высокоуровневая структура, идентичные названия подразделов, идентичный текст, общие термины

и основные определения, представленные приложении JG к Директивам ИСО/МЭК, часть 1 Сводного приложения JTC 1, дополнение 2021, и, следовательно, он совместим с аналогичными стандартами системы менеджмента.

Система менеджмента ИИ предъявляет специфические требования к управлению проблемами и рисками, возникающими в результате использования ИИ в организации. Важно отметить, что настоящий стандарт не запрещает организации внедрять другие системы менеджмента и не требует внедрения других систем менеджмента в качестве предварительного условия. Система менеджмента ИИ также не преследует цели заменить или вытеснить существующие системы менеджмента качеством, безопасностью, защитой, неприкосновенностью частной жизни или другие системы менеджмента. Этот общий подход, определенный в Приложении JG, полезен для организации при эксплуатации единой интегрированной системы менеджмента, отвечающей требованиям ряда стандартов систем менеджмента. Описание использования системы менеджмента ИИ в доменах или секторах можно найти в приложении D.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Система управления

Information technology. Artificial intelligence. Management system

Дата введения – 202_— —

1 Область применения

Настоящий стандарт определяет требования и рекомендации по созданию, внедрению, поддержанию в рабочем состоянии и постоянному улучшению системы менеджмента искусственного интеллекта (ИИ) в среде организации.

Настоящий стандарт предназначен для использования организациями, предоставляющими или использующими продукты или услуги, применяющие ИИ-системы. Настоящий стандарт призван помочь организациям ответственно разрабатывать или использовать ИИ-системы для достижения своих целей и соответствовать применимым нормативным требованиям, обязательствам, связанным с заинтересованными сторонами, и ожиданиями от них.

Настоящий стандарт применим к любой организации независимо от размера, типа и рода деятельности, которая предоставляет или использует продукты или услуги, применяющие ИИ-системы.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт [для датированных ссылок применяют только

указанное издание ссылочного стандарта, для недатированных – последнее издание (включая все изменения)]:

ISO/IEC 22989:2022, Information technology — Artificial intelligence — Artificial intelligence concepts and terminology (Информационные технологии. Искусственный интеллект. Термины и определения, связанные с искусственным интеллектом)

3 Термины и определения

В настоящем стандарте применены термины и определения по ИСО/МЭК 22989:2022, а также следующие термины с соответствующими определениями.

ИСО и МЭК поддерживают терминологические базы данных для применения в сфере стандартизации по следующим адресам:

- онлайн-платформа ИСО: доступна по ссылке: http://www.iso.org/obp;
- Электропедия МЭК: доступна по ссылке: http://www.electropedia.org/.

3.1 **организация** (organization): Лицо или группа лиц, связанные определенными отношениями, имеющие ответственность, полномочия и выполняющие свои функции для достижения их целей (3.6).

Примечание 1 – Понятие организации включает в себя, но не ограничивается следующими примерами: индивидуальный предприниматель, компания, корпорация, фирма, предприятие, орган власти, товарищество, ассоциация, благотворительные учреждения, а также их часть, или их объединение, являющиеся юридическим лицом или нет, государственные или частные.

Примечание 2 – Если организация является частью более крупного предприятия, термин «организация» относится только к той части более крупного

предприятия, которая входит в область применения системы менеджмента ИИ (3.4).

3.2 **заинтересованная сторона** (interested party/stakeholder): Лицо или организация (3.1), которые могут воздействовать на осуществление деятельности или принятие решения, быть подверженными их воздействию или воспринимать себя в качестве последних.

3.3 **высшее руководство** (top management): Лицо или группа людей, осуществляющих руководство и управление организацией (3.1) на высшем уровне.

Примечание 1 – Высшее руководство имеет право делегировать полномочия и предоставлять ресурсы в рамках организации.

Примечание 2 – Если область применения системы менеджмента (3.4) охватывает только часть организации, под высшим руководством подразумевают тех, кто осуществляет руководство и управляет этой частью организации.

3.4 **система менеджмента** (management system): Совокупность взаимосвязанных или взаимодействующих элементов организации (3.1) для разработки политик (3.5), целей (3.6) и процессов (3.8) для достижения этих целей.

Примечание 1 – Система менеджмента может относиться к одному или нескольким аспектам деятельности.

Примечание 2 – Элементы системы менеджмента определяют структуру организации, роли и ответственность, планирование и функционирование.

3.5 **политика** (policy): Намерения и направление организации (3.1), официально сформулированные ее высшим руководством (3.3).

3.6 **цель** (objective): Результат, который должен быть достигнут.

Примечание 1 – Цель может быть стратегической, тактической или оперативной.

Примечание 2 – Цели могут относиться к разным аспектам (такие, как финансовые цели, цели в области здоровья и безопасности, экологии), а также применяться на разных уровнях, например, организации в целом, проекта, продукции или процесса (3.8).

Примечание 3 – Цель может быть выражена разными способами, например, в виде намеченного результата, намерения, критерия работы, цели в области ИИ или другими словами со схожими значениями (например, целевая установка, заданная величина или задача).

Примечание 4 – В контексте системы менеджмента ИИ (3.4) цели в области ИИ, устанавливаемые организацией (3.1), согласуют с политикой в области ИИ (3.5) для достижения определенных результатов.

3.7 **риск** (risk): Влияние неопределенности на достижение целей.

Примечание 1 – Влияние выражается в отклонении от ожидаемого результата – позитивном или негативном.

Примечание 2 – Неопределенность является состоянием, связанным с недостатком, даже частично, информации, понимания или знания о событии, его последствиях или вероятности.

Примечание 3 – Риск часто определяют по отношениям к потенциальным событиям (как определено в Руководстве ИСО 73) и их последствиям (как определено в Руководстве ИСО 73) или к их комбинации.

Примечание 4 – Риск часто выражается в терминах комбинации последствий события (включая изменения в обстоятельствах) и связанных с ними вероятностей (как определено в Руководстве ИСО 73) возникновения.

3.8 **процесс** (process): Совокупность взаимосвязанных и(или) взаимодействующих видов деятельности, использующих или преобразующих входы для получения намеченного результата.

Примечание — В зависимости от контекста «намеченный результат» называется выходом, продукцией или услугой.

3.9 **компетентность** (competence): Способность применять знания и навыки для достижения намеченных результатов.

3.10 **документированная информация (документ)** (documented information): Информация, которая должна управляться и поддерживаться организацией (3.1), и носитель, который ее содержит.

Примечание 1 – Документированная информация может быть любого формата и на любом носителе и может быть получена из любого источника.

Примечание 2 – Документированная информация может относиться:

- к системе менеджмента (3.4), включая соответствующие процессы (3.8);
- информации, созданной для функционирования организации (документация);
- свидетельствам достигнутых результатов (записи).

3.11 **результаты деятельности** (performance): Измеримый результат.

Примечание 1 – Результаты деятельности могут относиться к количественным и качественным полученным данным.

Примечание 2 – Результаты деятельности могут относиться к менеджменту действий, процессам (3.8), продукции, услугам, системам или организациям (3.1).

Примечание 3 – В контексте настоящего стандарта термин результаты деятельности относится как к результатам, достигнутым с помощью ИИ-систем, так и к результатам, связанным с системой менеджмента ИИ. Правильное толкование этого термина становится понятным из контекста его употребления.

3.12 **постоянное улучшение** (continual improvement): Повторяющаяся деятельность по улучшению результатов деятельности (3.11).

3.13 **результативность** (effectiveness): Степень реализации запланированной деятельности и достижения запланированных результатов.

3.14 **требование** (requirement): Потребность или ожидание, которое установлено, обычно предполагается или является обязательным.

Примечание 1 – Слова «обычно предполагается» означают, что это общепринятая практика организации (3.1) и заинтересованных сторон (3.2), что рассматриваемые потребности или ожидания предполагаются.

Примечание 2 – Установленным является такое требование, которое определено, например, в документированной информации (3.10).

3.15 **соответствие** (conformity): Выполнение требования (3.14).

3.16 **несоответствие** (nonconformity): Невыполнение требования (3.14).

3.17 **корректирующее действие** (corrective action): Действие, предпринятое для устранения причины несоответствия (3.16) и предупреждения его повторного возникновения.

3.18 **аудит** (audit): Систематический и независимый процесс (3.8) получения свидетельств и их объективного оценивания для установления степени соответствия критериям аудита.

Примечание 1 – Аудит может быть внутренним (аудит, проводимый первой стороной) или внешним (аудит, проводимый второй или третьей стороной), а также аудит может быть совместным (аудит, проводимый для двух или более систем менеждмента одновременно).

Примечание 2 – Внутренний аудит проводится самой организацией (3.1) или от ее имени внешней стороной.

Примечание 3 – «Свидетельства аудита» и «критерии аудита» определены в ИСО 19011.

3.19 **измерение** (measurement): Процесс (3.8) определения значения.

3.20 **мониторинг** (monitoring): Определение статуса системы, процесса (3.8) или действия.

Примечание — Для определения статуса может возникнуть необходимость проверить, проконтролировать или отследить.

3.21 **персональные данные**; ПДн (personally identifiable information; PII): Любая информация: (a) которая может использоваться для идентификации субъекта ПДн, которому такая информация принадлежит; (b), которая прямо или косвенно уже связана или может быть связана с субъектом ПДн.

Примечание — Для того чтобы определить, является ли субъект ПДн идентифицируемым, следует учесть все средства, которые могут быть корректно использованы лицом, заинтересованным в обеспечении приватности, владеющим данными, или любой другой стороной для идентификации этого физического лица.

[ИСО/МЭК 29100:2011, 2.9]

3.22 **управление (риском)** (control): Меры, направленные на сохранение и изменение риска (3.7).

Примечание 1 – Управление риском охватывает, но не ограничивается этим: процессы, политику, устройства, методы и другие средства, используемые для сохранения и модификации риска.

Примечание 2 – Управление риском не всегда может привести к желаемым или ожидаемым результатам.

Примечание 3 – Предлагаемое в настоящем стандарте определение отличается от представленного в стандарте ИСО/МЭК 22989.

[ИСО 31000:2018, 3.8, добавлено примечание 3 к записи и тегу домена <риск>]

3.23 **руководящий орган** (governing body): Лицо или группа людей, которые отвечают за работу организации и ее соответствие требованиям.

Примечание 1 – Некоторые организации, особенно небольшие, могут и не иметь управляющего органа отдельного от высшего руководства.

Примечание 2 – В состав руководящего органа могут входить, но не ограничиваются нижеследующим: совет директоров, комитеты правления, наблюдательный совет, совет попечителей или надзирателей (но не ограничивается).

[ИСО/МЭК 38500:2015, 2.9, добавлены примечания к записи]

3.24 **информационная безопасность** (information security): Сохранение конфиденциальности, целостности и доступности информации.

Примечание — также сюда могут быть включены другие свойства, такие как подлинность, подотчетность, безотказность и достоверность.

[ИСО/МЭК 27000:2018, 3.28]

3.25 **оценка воздействия ИИ-системы** (AI system impact assessment): Официальный, документированный процесс, посредством которого организация, разрабатывающая, предоставляющая или использующая продукты или услуги, использующие ИИ, выявляет, оценивает и преобразует воздействие для отдельных лиц (и групп лиц) и общества.

4 Среда организации

4.1 Понимание организации и ее среды

Организация должна определить внешние и внутренние факторы, относящиеся к ее намерениям и влияющие на ее способность достигать намеченного(ых) результата(ов) ее системы менеджмента ИИ.

Следует учитывать общее назначение ИИ-систем, которые разрабатываются, предоставляются или используются организацией. Организация должна определить свои роли в отношении ИИ-систем. Эти роли могут включать, но не ограничиваются нижеследующими:

- поставщики решений по ИИ, включая поставщиков платформ ИИ, поставщиков продуктов или услуг ИИ;
- производители ИИ, включая разработчиков ИИ;
- потребители ИИ, включая пользователей ИИ;
- партнеры по ИИ, включая системного интегратора ИИ и поставщика данных;
- субъекты ИИ, включая субъекты данных, и другие субъекты;
- соответствующие органы власти, включая директивные и регулирующие органы.

Подробное описание этих ролей и их взаимосвязи с жизненным циклом ИИ-системы приведено в стандарте ИСО/МЭК 22989:2022. Роли организации определяют применимость и степень применимости требований и мер управления, изложенных в настоящем стандарте.

Внешние и внутренние факторы, подлежащие рассмотрению в соответствии с настоящим пунктом, могут варьироваться в зависимости от ролей и юрисдикции организации и их влияния на ее способность достигать предполагаемых результатов при помощи системы

менеджмента ИИ. Они могут включать в себя, но не ограничиваются нижеследующими:

a) рассмотрением вопросов, связанных с внешней средой, таких как:

1) применимые юридические обязательства, включая запрещенное использование ИИ;

2) политики, руководящие принципы и решения регулирующих органов, оказывающие влияние на толкование или обеспечение соблюдения юридических обязательств;

3) стимулы или последствия, связанные с предполагаемой целью и использованием ИИ-систем;

4) культура, традиции, ценности, нормы и этика;

5) конкурентная среда и тенденции для новых продуктов и услуг, использующих ИИ-системы.

b) рассмотрением вопросов, связанных с внутренней средой, таких как:

1) организационная среда, управление, цели (см. приложение C), политики и процедуры;

2) договорные обязательства;

3) определение технических требований для удовлетворения потребностей, указанных в пунктах a) и b).

Роль организации может быть определена обязательствами, связанными с категориями данных, которые обрабатывает организация (например, обработчик ПДн или оператор ПДн при обработке ПДн). Для получения информации о ПДн и о ролях в обработке ПДн обратитесь к [6]. Роли также могут определяться юридическими обязательствами, характерными для ИИ-систем.

4.2 Понимание потребностей и ожиданий заинтересованных сторон

Организация должна определить:

- заинтересованные стороны, имеющие отношение к системе менеджмента ИИ;
- соответствующие требования этих заинтересованных сторон;
- какие из этих требований будут выполнены с помощью системы менеджмента ИИ.

Заинтересованной стороной может быть любое лицо, заинтересованное в ИИ. В стандарте ИСО/МЭК 22989:2022 (5.19) представлен обзор ролей заинтересованных сторон в области ИИ.

4.3 Определение области применения системы менеджмента ИИ

Организация должна определить границы системы менеджмента ИИ и охватываемую ею деятельность, чтобы установить область ее применения.

При определении области применения организация должна рассматривать:

- внешние и внутренние факторы (см. 4.1);
- требования (см. 4.1);

Область применения должна быть задокументирована.

Область применения системы менеджмента ИИ должна определять деятельность организации в отношении требований настоящего стандарта к системе менеджмента ИИ, руководству,

планированию, поддержке, эксплуатации, производительности, оценке, улучшению, мерам управления и целям.

4.4 Система менеджмента ИИ

Организация должна разработать, внедрить, поддерживать в рабочем состоянии и постоянно улучшать систему менеджмента ИИ, включая необходимые процессы и их взаимодействия, в соответствии с требованиями настоящего стандарта.

5 Лидерство

5.1 Лидерство и приверженность

Высшее руководство должно демонстрировать свое лидерство и приверженность в отношении системы менеджмента ИИ посредством:

- обеспечения разработки политики (см. 5.2) и целей (см. 6.2) в области ИИ, которые согласуются со стратегическим направлением организации;
- обеспечения интеграции требований системы менеджмента ИИ в деловые процессы организации;
- обеспечения доступности ресурсов, необходимых для системы менеджмента ИИ;
- распространения в организации понимания важности результативного управления ИИ и соответствия требованиям системы менеджмента ИИ;
- обеспечения достижения системой менеджмента ИИ намеченных результатов;

- вовлечения, руководства и оказания поддержки участия работников в обеспечении результативности системы менеджмента ИИ;
- поддержки постоянного улучшения;
- поддержки других соответствующих руководителей в демонстрации ими лидерства в сфере их ответственности.

5.2 Политика в области ИИ

Высшее руководство должно разработать политику в области ИИ, которая:

a) соответствует намерениям организации;

b) создает основу для установления целей в области ИИ;

c) включает в себя обязательство соответствовать применимым требованиям;

d) включает в себя обязательство постоянно улучшать систему менеджмента ИИ.

Политика в области ИИ должна:

- быть доступной и быть документированной;
- ссылаться на другие политики организации, где это применимо;
- доводиться до сведения работников организации;
- быть доступной для заинтересованных сторон, где это уместно.

Примечание – Рекомендации для организаций при разработке политик в области ИИ приведены в [2].

5.3 Функции, ответственность и полномочия

Высшее руководство должно обеспечить в организации распределение соответствующих обязанностей, ответственности и полномочий.

Высшее руководство должно распределить обязанности, ответственность и полномочия для:

a) обеспечения соответствия системы менеджмента ИИ требованиям настоящего стандарта;

b) отчетности высшему руководству о результатах функционирования системы менеджмента ИИ.

6 Планирование

6.1 Действия в отношении рисков и возможностей

6.1.1 Общие положения

При планировании в системе менеджмента ИИ организация должна учесть факторы (см. 4.1) и требования (см. 4.2) и определить риски и возможности, подлежащие рассмотрению для:

- обеспечения уверенности в том, что система менеджмента ИИ может достичь своих намеченных результатов;
- предотвращения или уменьшения их нежелательного влияния;
- достижения постоянного улучшения.

Организация должна установить и поддерживать в актуальном состоянии критерии риска ИИ, позволяющие:

- отличать приемлемые риски от неприемлемых;
- проведение оценки рисков ИИ;
- проведение обработки рисков ИИ;

- проведение оценки воздействия рисков ИИ.

Рекомендации по определению степени и типа риска, который организация готова принять или сохранять, приведены в [2] и [3].

Организация должна определять возможности в соответствии со следующими факторами:

- предметная область и среда применения ИИ-системы;
- бизнес-требования и предполагаемое использование;
- внешняя и внутренняя среда (см. 4.1)

Организация должна планировать:

a) действия по рассмотрению этих рисков и возможностей;

b) то, каким образом:

1) интегрировать и внедрить эти действия в процессы своей системы менеджмента ИИ;

2) оценивать результативность этих действий.

Организация должна сохранять документированную информацию о действиях, предпринятых для выявления и рассмотрения рисков и возможностей ИИ.

Рекомендации по организации управления рисками для организаций, предоставляющих или использующих продукты, системы и услуги ИИ, приведены в [3].

Примечание 1 – Среда организации и ее деятельность могут оказывать влияние на деятельность организации по управлению рисками.

Примечание 2 – Способ определения риска и, следовательно, представления об управлении рисками может варьироваться в зависимости от секторов и отраслей промышленности. Нормативное определение риска, изложенное в 3.7, как поясняется в примечаниях к определению, позволяет получить широкое представление о риске, применимое к любому сектору, например, к секторам, упомянутым в D.1. Роль организации в рамках оценки рисков заключается в том, чтобы сначала принять видение риска, адаптированное к ее среде. Это может включать подход к риску с помощью определений, используемых

в секторах, для которых разрабатывается и используется ИИ-система, таких как определение из [27] (ссылка на [18], [34], [19]).

6.1.2 Оценка рисков ИИ

Организация должна определить и внедрить процесс оценки рисков ИИ, который должен:

a) основываться на политике в области ИИ (см. 5.2) и целях ИИ (см. 6.2) и согласоваться с ними;

b) обеспечивать уверенность в том, что повторные оценки рисков ИИ дают непротиворечивые, достоверные и сопоставимые результаты;

c) определять риски, которые помогают или препятствуют достижению целей ИИ;

d) проводить анализ рисков ИИ:

1) оценивать потенциальные последствия для организации, отдельных лиц и общества, которые могут произойти в результате наступления выявленных рисков;

2) оценивать реальную вероятность наступления выявленных рисков;

3) определять уровни рисков.

Примечание – При оценке последствий в рамках 6.1.2 d) 1), организация может использовать оценку воздействия ИИ-системы, как указано в 6.1.4.

e) оценивать риски ИИ, т.е.:

1) сравнивать результаты анализа рисков ИИ с критериями рисков, установленными в соответствии с 6.1.1;

2) определять приоритетность обработки проанализированных рисков ИИ.

Организация должна хранить документированную информацию о процессе оценки рисков ИИ.

6.1.3 Обработка рисков ИИ

Опираясь на результаты оценки рисков, организация должна определить и применить процесс обработки рисков ИИ для:

a) выбора подходящих вариантов обработки рисков ИИ;

b) определения всех мер управления, необходимых для реализации выбранного(ых) варианта(ов) обработки рисков ИИ; сравнения мер управления, определенных в соответствии с указанными в приложении А для проверки того, что никакие необходимые меры управления не были упущены. В приложении А приведены базовый перечень мер управления для достижения организационных целей и рассмотрения рисков, связанных с проектированием и использованием ИИ-систем. Организация должна рассмотреть меры управления, приведенные в приложении А, относящиеся к внедрению вариантов обработки рисков ИИ. Организация должна определить, необходимы ли дополнительные меры управления помимо указанных в приложении А для реализации всех вариантов обработки рисков;

Примечание – Цели управления неявным образом включены в выбранные меры управления. Организация может выбрать необходимые ей меры и цели управления, перечисленные в приложении А. Приведенные в приложении А меры и цели управления, не являются исчерпывающими, и организация может рассмотреть необходимость дополнительных мер управления и целей их применения. При необходимости организация может разрабатывать меры управления или взять их из существующих источников. Управление рисками ИИ может быть интегрировано в другие системы менеджмента, если это применимо.

c) подготовки ведомости применимости мер управления, которая содержит: необходимые меры управления (см. b)); обоснования их применения; информацию о том, реализованы или нет необходимые меры управления; обоснования неприменения мер управления,

представленных в приложении А. Обоснование для неприменения мер управления может включать случаи, когда меры управления не считаются необходимыми в результате оценки риска и когда они не требуются применимыми внешними требованиями (или подпадают под исключения в соответствии с ними).

Примечание – Организация может предоставить документированные обоснования для исключения любых целей управления в целом или для конкретных ИИ-систем, будь то перечисленные в приложении А или установленные самой организацией.

d) разработка плана обработки рисков ИИ и обращение к приложению В для получения рекомендаций по внедрению мер управления, определенных в пункте b);

e) согласование и (или) утверждения плана обработки рисков ИИ и принятие остаточных рисков ИИ владельцами рисков.

Меры управления должны быть:

- согласованы с целями, указанными в 6.2;
- доступны в виде документированной информации;
- доведены до сведения внутри организации;
- доступны заинтересованным сторонам, по мере необходимости.

Организация должна хранить документированную информацию о процессе обработки рисков ИИ.

6.1.4 Оценка воздействия ИИ-системы

Организация должна провести оценку потенциальных последствий для отдельных лиц и обществ, которые могут возникнуть в результате разработки или использования ИИ-систем. Оценка воздействия ИИ-системы должна определять потенциальные последствия

развертывания и предполагаемого использования ИИ-системы для отдельных лиц и обществ. Результат оценки воздействия на систему должен быть задокументирован и, в случае необходимости, предоставлен соответствующим заинтересованным сторонам.

Организации следует рассмотреть вопрос о влиянии ИИ-системы на следующие вопросы:

- правовое положение или жизненные возможности отдельных лиц;
- физическое или психологическое благополучие отдельных лиц;
- универсальные права человека;
- общество.

Организация может интегрировать оценку воздействия ИИ-системы в свою оценку рисков (6.1.2). Пункт B.5 предусматривает меры управления для оценки воздействия ИИ-систем.

Примечание – В некоторых средах (таких как ИИ-системы, критически важных для безопасности или конфиденциальности) организация может потребовать проведение оценки воздействия ИИ-системы на конкретную дисциплину (например, на безопасность, конфиденциальность или защиту) как часть общей деятельности организации по управлению рисками.

6.2 Цели ИИ и планирование их достижения

В организации должны быть установлены цели ИИ применительно к соответствующим функциям и уровням управления организацией.

Цели ИИ должны:

a) быть согласованными с политикой в области ИИ (5.2);

b) быть измеримыми (если это практически осуществимо);

c) учитывать применимые требования ИИ;

d) подлежать мониторингу с точки зрения их достижения;

e) быть доведены до сведения всех заинтересованных сторон;

f) при необходимости актуализироваться;

g) быть доступной и применяться как документированная информация;

h) демонстрировать способность организации выполнять юридические обязательства.

При планировании способов достижения целей в области ИИ организация должна определить:

- что должно быть сделано;
- какие для этого требуются ресурсы;
- кто будет нести ответственность;
- сроки достижения целей;
- каким образом будут оцениваться полученные результаты.

Неисключительный перечень целей ИИ, связанных с управлением рисками, приведен в приложении С.

6.3 Планирование изменений

В тех случаях, когда организация выявляет необходимость в изменениях системы менеджмента ИИ, эти изменения должны осуществляться на плановой основе системным образом.

7 Средства обеспечения

7.1 Ресурсы

Организация должна определить и обеспечить наличие ресурсов, необходимых для создания, внедрения, поддержки и постоянного улучшения системы менеджмента ИИ.

7.2 Компетентность

Организация должна:

- определить необходимую компетентность лиц(а), выполняющих(его) работу под ее управлением, которая оказывает влияние на результаты деятельности и результативность ИИ-системы
- обеспечивать компетентность этих лиц на основе соответствующего образования, подготовки и(или) опыта;
- там, где это применимо, предпринимать действия, направленные на получение требуемой компетентности, и оценивать результативность предпринятых действий.

Сохранять соответствующую документированную информацию как свидетельство компетентности.

Примечание – Применимые действия могут включать, например проведение обучения, наставничество или перераспределение обязанностей среди имеющихся работников; или же наем лиц, обладающих требуемым уровнем компетентности.

7.3 Осведомленность

Лица, выполняющие работу под управлением организации, должны быть осведомлены о:

- политике в области ИИ (5.2);
- своем вкладе в обеспечение результативности системы менеджмента ИИ, включая пользу от улучшения результатов деятельности ИИ;
- последствиях несоответствия требованиям системы менеджмента ИИ.

7.4 Обмен информацией

Организация должна определить порядок внутреннего и внешнего обмена информацией, относящейся к системе менеджмента ИИ, включая:

- какая информация будет передаваться;
- когда будет передаваться информация;
- кому будет передаваться информация;
- каким образом она будет передаваться.

7.5 Документированная информация

7.5.1 Общие положения

Система менеджмента ИИ организации должна включать:

а) документированную информацию, требуемую в соответствии с настоящим стандартом;

b) документированную информацию, определенную организацией как необходимую для обеспечения результативности системы менеджмента ИИ.

Примечание – Объем документированной информации системы менеджмента ИИ одной организации может отличаться от другой в зависимости от:

- от размера организации и вида ее деятельности, процессов, продукции и услуг;
- сложности процессов и их взаимодействия;
- компетентности работников.

7.5.2 Создание и актуализация документированной информации

При создании и актуализации документированной информации организация должна соответствующим образом обеспечить:

- идентификацию и описание (например, наименование, дата, автор или ссылочный номер);
- формат (например, язык, версия программного обеспечения, графические средства) и носитель информации (например, бумажный или электронный);
- анализ, пересмотр и одобрение с точки зрения пригодности и адекватности.

7.5.3 Управление документированной информацией

Документированная информация, требуемая системой менеджмента ИИ и настоящим стандартом, должна находиться под управлением в целях обеспечения:

a) ее доступности и пригодности для использования, где и когда это необходимо;

b) надлежащей защиты (например, от несоблюдения конфиденциальности, от ненадлежащего использования или потери целостности).

Для управления документированной информацией организация должна предусматривать следующие действия в той степени, насколько это применимо:

- распространение, обеспечение доступа, поиска и использование;
- хранение и сохранность документов, включая их читаемость;
- управление изменениями (например, управление версиями/редакциями);
- соблюдение сроков хранения и порядка уничтожения.

Документированная информация внешнего происхождения, определенная организацией как необходимая для планирования и системы менеджмента ИИ, должна быть соответствующим образом идентифицирована и находиться под управлением.

Примечание – Доступ к документированной информации подразумевает разрешение только просмотра документированной информации или разрешение просмотра с полномочиями по внесению изменений в документированную информацию.

8 Деятельность

8.1 Планирование и управление

Организация должна планировать, внедрять процессы, необходимые для выполнения требований и для выполнения действий, определенных в разделе 6, и осуществлять управление этими процессами посредством:

- установления критериев для процессов;
- осуществления управления процессами на основе установленных критериев.

Организация должна хранить документированную информацию в объеме, необходимом для обеспечения уверенности в том, что процессы выполнялись так, как это было запланировано.

Организация должна управлять запланированными изменениями и анализировать последствия непредусмотренных изменений, предпринимая, при необходимости, меры по смягчению любых негативных воздействий.

Организация должна обеспечивать, чтобы процессы, продукция или услуги организации, осуществляемые с использованием аутсорсинга и имеющих отношение к системе менеджмента ИИ, находились под управлением.

8.2 Оценка рисков ИИ

Организация должна проводить оценку рисков ИИ в соответствии с 6.1.2 через запланированные интервалы или в случае предполагаемых или произошедших значительных изменений.

Организация должна хранить документированную информацию о результатах проведенных оценок рисков ИИ.

8.3 Обработка рисков ИИ

Организация должна реализовать план обработки рисков ИИ в соответствии с 6.1.3 и осуществить проверку его эффективности.

Для новых рисков, выявленных в процессе проведения оценки рисков и требующих обработки, должен быть выполнен процесс обработки рисков.

В случае выявления неэффективности способов обработки рисков, определенных планом обработки рисков, они должны быть пересмотрены в соответствии с 6.1.3, и план обработки рисков должен быть актуализирован. Организация должна хранить документированную информацию о результатах проведенных мероприятий по устранению рисков ИИ.

8.4 Оценка воздействия ИИ-системы

Организация должна проводить оценку воздействия ИИ-системы в соответствии с 6.1.4 через запланированные промежутки времени или в случае предполагаемых значительных изменений.

Организация должна хранить документированную информацию о результатах проведенных оценок воздействия ИИ-системы.

9 Оценка результатов деятельности

9.1 Мониторинг, измерение, анализ и оценка

Организация должна определить:

- объекты мониторинга и измерение;
- методы проведения мониторинга, измерения, анализа и оценки, необходимые для обеспечения достоверных результатов;
- когда должны проводиться мониторинг и измерения;

- когда результаты мониторинга и измерений должны быть проанализированы и оценены.

Следует обеспечить наличие документированной информации, свидетельствующей о полученных результатах.

Организация должна оценить результаты деятельности и результативность системы менеджмента ИИ.

9.2 Внутренний аудит

9.2.1 Общие положения

Организация должна проводить внутренние аудиты через запланированные интервалы времени для получения информации, что система менеджмента ИИ:

a) соответствует:

1) собственным требованиям организации к ее системе менеджмента ИИ;

2) требованиям настоящего стандарта;

b) эффективно внедрена и функционирует.

9.2.2 Программа внутреннего аудита

Организация должна планировать, разрабатывать, реализовывать и поддерживать в актуальном состоянии программу(мы) аудитов, включая периодичность и методы проведения аудитов, а также ответственность, планируемые для проверки требования и предоставление отчетности.

Программа(мы) аудитов должна(ы) разрабатываться с учетом важности проверяемых процессов и результатов предыдущих аудитов.

Организация должна:

a) определить цели, критерии и область проверки для каждого аудита;

b) отбирать аудиторов и проводить аудит таким образом, чтобы обеспечить объективность и беспристрастность процесса аудита;

c) обеспечивать передачу информации о результатах аудитов соответствующим руководителям.

Организация должна сохранять соответствующую документированную информацию как свидетельство реализации программы аудита и полученных результатов аудита.

9.3 Анализ со стороны руководства

9.3.1 Общие положения

Высшее руководство должно анализировать через за планированные интервалы времени систему менеджмента ИИ в целях обеспечения ее постоянной пригодности, адекватности и результативности.

9.3.2 Входные данные анализа со стороны руководства

Анализ со стороны руководства должен включать в себя рассмотрение:

a) степени реализации решений, осуществляемых по результатам предыдущих анализов со стороны руководства;

b) изменений во внешних и внутренних факторах, касающихся системы менеджмента ИИ;

c) изменений в потребностях и ожиданиях заинтересованных сторон, касающихся системы менеджмента ИИ;

d) информации о результатах деятельности в области ИИ, включая тенденции, относящиеся к:

1) выявлению несоответствий и применению корректирующих действий;

2) результатам мониторинга и измерений;

3) результатам аудитов;

e) потенциальных возможностей для постоянного улучшения системы.

9.3.3 Выходные данные анализа со стороны руководства

Выходные данные анализа со стороны руководства должны включать в себя решения, относящиеся к возможностям постоянного улучшения и анализ необходимости внесения любых изменений в систему менеджмента ИИ.

Организация должна хранить документированную информацию как свидетельство результатов анализов со стороны руководства.

10 Улучшения

10.1 Постоянное улучшение

Организация должна постоянно улучшать пригодность, адекватность и результативность системы менеджмента ИИ.

10.2 Несоответствия и корректирующие действия

При выявлении несоответствий организация должна:

a) реагировать на данное несоответствие и насколько применимо:

1) предпринимать действия по управлению и коррекции выявленного несоответствия;

2) предпринимать действия в отношении последствий данного несоответствия;

b) оценивать необходимость действий по устранению причин данного несоответствия с тем, чтобы избежать его повторного появления или появления в другом месте посредством:

1) анализа несоответствия;

2) определения причин, вызвавших появление несоответствия;

3) определения наличия аналогичного несоответствия или возможности его возникновения где-либо еще;

c) осуществлять необходимые корректирующие действия;

d) проанализировать результативность каждого предпринятого корректирующего действия;

e) вносить при необходимости изменения в систему менеджмента ИИ.

Корректирующие действия должны соответствовать последствиям выявленных несоответствий.

Следует обеспечить наличие документированной информации, свидетельствующей о:

- характере несоответствий и любых последующих предпринятых действий;
- результатах всех корректирующих действий.

Приложение А
(обязательное)

Меры и цели управления

А.1 Общие положения

Перечисленные в таблице А.1 цели, а также меры управления служат организации ориентиром для достижения организационных целей и устранения рисков, связанных с проектированием и эксплуатацией ИИ-систем. Перечень мер управления, содержащийся в данной таблице, не является исчерпывающим, и организация может разработать и внедрить собственные меры управления (см. 6.1.3).

В приложении В приведены рекомендации по внедрению мер управления, перечисленных в таблице А.1. В первой колонке таблицы А.1 приведена перекрестная ссылка на конкретный раздел приложения В.

Таблица А.1 — Меры управления и цели их применения

В.2 Политики в области ИИ		
Цель: Обеспечить получение от руководства руководящих указаний и поддержки ИИ-систем в соответствии с деловыми потребностями и применимыми правовыми обязательствами, включая договорные		
В.2.2	Политика в области ИИ	Меры управления Организация должна задокументировать политику развития и использования ИИ-систем
В.2.3	Согласование с другими организационными политиками	Меры управления Организация должна определить, каким образом цели организации в отношении ИИ-систем могут повлиять на другие ее политики и каким образом другие политики могут оказаться применимыми в отношении данных целей
В.2.4	Пересмотр политики в области ИИ	Меры управления Политика в области ИИ должна пересматриваться в плановом порядке (и дополнительно по мере необходимости) для обеспечения ее постоянной уместности, адекватности и эффективности
В.3 Организация внутренней деятельности		
Цель: обеспечить в организации подотчетность, поддерживающую ее ответственный подход к внедрению, эксплуатации и управлению ИИ-системами		

Продолжение таблицы А.1

В.3.2	Роли и обязанности ИИ	Меры управления Роли и ответственность за ИИ должны быть определены и распределены в соответствии с потребностями
В.3.3	Информирование о проблемах	Меры управления Организация должна определить и внедрить процесс, позволяющий сотрудникам организации сообщать о проблемах, связанных с ролью организации в отношении ИИ-системы на протяжении всего ее жизненного цикла
В.4 Ресурсы ИИ-систем		
Цель: обеспечить учет организацией ресурсов ИИ-системы (включая ее компоненты и активы) для полного понимания и рассмотрения связанных рисков и последствий		
В.4.2	Документация ресурсов	Меры управления Организация должна выявить и задокументировать соответствующие ресурсы, необходимые для выполнения операций на конкретных стадиях жизненного цикла ИИ-системы, а также для иных связанных с ИИ видов деятельности, актуальных для организации
В.4.3	Ресурсы данных	Меры управления В рамках идентификации ресурсов организация должна документировать информацию о ресурсах данных, используемых для ИИ-системы
В.4.4	Инструментальные ресурсы	Меры управления В рамках идентификации ресурсов организация должна документировать информацию об инструментальных ресурсах, используемых для ИИ-системы
В.4.5	Системы и вычислительные ресурсы	Меры управления В рамках идентификации ресурсов организация должна документировать информацию о системе и вычислительных ресурсах, используемых для ИИ-системы
В.4.6	Человеческие ресурсы	Меры управления В рамках идентификации ресурсов организация должна документировать информацию о человеческих ресурсах, используемых для разработки, развертывания и эксплуатации ИИ-системы

Продолжение таблицы А.1

B.5 Оценка воздействия ИИ-систем		
Цель: провести оценку воздействия системы на заинтересованные стороны ИИ-системы на протяжении всего ее жизненного цикла		
B.5.2	Процесс оценки воздействия ИИ-системы	Меры управления Организация должна провести оценку: потенциальных последствий для отдельных для отдельных лиц, сообществ и организаций, которые могут возникнуть в результате разработки или использования ИИ-систем
B.5.3	Документация по оценке воздействия ИИ-системы	Меры управления Организация должна документировать результаты оценки воздействия ИИ-системы и сохранять соответствующие документы в течение установленных сроков хранения
B.5.4	Оценка воздействия ИИ-системы на отдельных лиц, организаций или сообществ	Меры управления Организация должна проводить оценку и документировать потенциальное воздействие ИИ-систем на отдельных лиц, организаций или сообществ на протяжении всего жизненного цикла системы
B.5.5	Оценка воздействия ИИ-систем на общество	Меры управления Организация должна проводить оценку и документировать потенциальное воздействие своих ИИ-систем на общество на протяжении всего их жизненного цикла
B.6 Жизненный цикл ИИ-системы		
Цель: обеспечить определение и документирование организацией целей и внедрения процессов ответственного проектирования и разработки ИИ-систем		
B.6.1 Руководство по управлению разработкой ИИ-системы		
B.6.1.2	Цели для разработки ИИ-системы	Меры управления Организация должна определить и задокументировать цели, которыми следует руководствоваться при разработке надежных и заслуживающих доверие ИИ-систем, а также учитывать эти цели и интегрировать меры по их достижению в
B.6.1.3	Процессы для надежного проектирования системы разработки ИИ-систем	Меры управления Организация должна определить и задокументировать конкретные процессы проектирования и разработки ИИ-системы

Продолжение таблицы А.1

В.6.2 Жизненный цикл разработки ИИ-системы		
В.6.2.2	Требования и спецификация к системе ИИ	Меры управления Организация должна определить и задокументировать требования к новым системам ИИ или существенным усовершенствованиям существующих систем
В.6.2.3	Документация по проектированию и разработке ИИ-системы	Меры управления Организация должна документировать проектирование и разработку ИИ-системы на основе организационных целей, задокументированных требований и установленных в спецификациях критериев
В.6.2.4	Верификация и валидация ИИ-системы	Меры управления Организация должна определить и задокументировать меры верификации и валидации для ИИ-системы и указать критерии для их использования
В.6.2.5	Развертывание ИИ-системы	Меры управления Организация должна задокументировать план развертывания и обеспечить выполнение соответствующих требований до инициирования самого развертывания
В.6.2.6	Функционирование и мониторинг ИИ-системы	Меры управления Организация должна определить и задокументировать необходимые элементы для непрерывной работы ИИ-системы. Как минимум, это должно включать мониторинг системы и производительности, ремонт, обновления и поддержку
В.6.2.7	Техническая документация системы ИИ	Меры управления Организация должна определить, какая техническая документация по ИИ-системе необходима для каждой соответствующей категории заинтересованных сторон, таких как пользователи, партнеры, контролирующие органы, и предоставить им техническую документацию в соответствующей форме
В.6.2.8	Ведение журналов событий ИИ-системой	Меры управления Во время работы ИИ-системы при необходимости должно быть включено автоматическое ведение журналов событий

Продолжение таблицы А.1

В.7 Данные для ИИ-систем		
Цель: обеспечить понимание организацией роли и воздействия данных в ИИ-системах при применении и разработке, предоставлении или использовании ИИ-систем на протяжении их жизненного цикла		
В.7.2	Данные для разработки и усовершенствования ИИ-системы	Меры управления Организация должна определять, документировать и внедрять процессы управления данными, связанные с разработкой ИИ-систем
В.7.3	Сбор данных	Меры управления Организация должна определить и задокументировать подробную информацию о сборе и отборе данных, используемых в ИИ-системах
В.7.4	Качество данных для ИИ-систем	Меры управления Организация должна определить и задокументировать требования к качеству данных и обеспечить соответствие данных, используемых для разработки и эксплуатации ИИ-системы этим
В.7.5	Происхождение данных	Меры управления Организация должна определить и задокументировать процесс проверки и документирования сведений о происхождении данных, используемых в ее ИИ-системах на протяжении жизненного цикла данных и ИИ-системы
В.7.6	Подготовка данных	Меры управления Организация должна определить и задокументировать свои потребности и подходы к подготовке данных
В.8 Информация для заинтересованных сторон ИИ-систем		
Цель: обеспечить предоставление соответствующим заинтересованным сторонам необходимой информации для понимания и оценки рисков и их последствий (как положительных, так и отрицательных)		
В.8.2	Системная документация и информация для пользователей	Меры управления Организация должна определить и предоставить необходимую информацию пользователям системы
В.8.3	Понятность предоставленной информации	Меры управления Информация, предоставляемая заинтересованным сторонам, должна быть прозрачной, понятной и подходящей для них

Продолжение таблицы А.1

B.8.4	Внешняя отчетность	Меры управления Организация должна предоставить возможности для отчетности о неблагоприятных воздействиях системы
B.8.5	Информирование об инцидентах	Меры управления Организация должна определить и задокументировать план информирования об инцидентах пользователей системы
B.8.6	Информация для заинтересованных сторон	Меры управления Организация должна определить и задокументировать свои обязательства по предоставлению информации о ИИ-системе заинтересованным сторонам
B.9 Использование ИИ-систем		
Цель: обеспечить ответственное использование ИИ организацией, в соответствии с политиками организации		
B.9.2	Процессы ответственного использования ИИ	Меры управления Организация должна определить и задокументировать процессы ответственного использования ИИ-систем
B.9.3	Цели ответственного использования ИИ-системы	Меры управления Организация должна определить и задокументировать цели, которыми следует руководствоваться при ответственном использовании ИИ-систем
B.9.4	Предполагаемое использование ИИ-системы	Меры управления Организация должна обеспечить, что ИИ-система используется в соответствии с предполагаемым использованием ИИ-системы и сопровождающей ее документацией
B.10 Взаимоотношения с третьими сторонами		
Цель: Обеспечить, чтобы, в случаях, когда третьи стороны задействованы на какой-либо стадии жизненного цикла ИИ-системы, организация понимала свои обязанности и оставалась подотчетной за них, будучи при этом способной оценивать и снижать риск зависимости от третьих сторон в выполнении возложенных на них обязанностей и позволяя третьим сторонам оценивать и рассматривать проблемы и риски, связанные с зависимостью от продуктов и услуг ИИ, разработанных организацией		

Окончание таблицы А.1

B.10.2	Распределение обязанностей	Меры управления Организация должна обеспечить распределение обязанностей в рамках жизненного цикла своей ИИ-системы между организацией, ее партнерами, поставщиками, заказчиками и третьими сторонами
B.10.3	Поставщики	Меры управления Организация должна обеспечить соблюдение ее поставщиками ответственного подхода к разработке ИИ-систем
B.10.4	Заказчики	Меры управления Организация должна обеспечить, чтобы ее ответственный подход к разработке ИИ-систем учитывал ожидания и потребности их клиентов

Приложение В
(обязательное)

Руководство по внедрению мер управления по обработке рисков ИИ

В.1 Общие положения

Руководство по внедрению, приведенное в настоящем приложении, относится к мерам управления, перечисленным в приложении А. В настоящем приложении содержится более подробная информация в поддержку внедрения мер управления, перечисленных в приложении А, и достижения цели управления.

Руководство по внедрению не всегда является подходящим и достаточным во всех ситуациях, и не всегда соответствует специфическим требованиям организации к управлению. Организация может расширить или изменить данное руководство или сформировать свое собственное руководство по внедрению мер управления в соответствии со своими конкретными требованиями и потребностями в обработке рисков.

Приложение В следует использовать в качестве руководства для определения и внедрения мер управления по обработке рисков ИИ в системе менеджмента ИИ, определенной в настоящем стандарте. Меры управления и рекомендации по их применению, описанные в настоящем приложении, относятся к мерам управления, перечисленным в приложении А. Дополнительные организационные и технические меры управления, отличные от тех, которые включены в настоящее приложение, при необходимости могут быть определены путем оценки рисков.

Настоящее приложение можно рассматривать как отправную точку для разработки руководящих принципов для конкретной организации. Не все описанные в настоящем стандарте меры управления и рекомендации применимы во всех организациях и для всех ИИ-систем. Для удовлетворения конкретных потребностей организации и для устранения выявленных рисков могут потребоваться дополнительные меры управления и рекомендации по их применению, не включенные в данное приложение.

B.2 Политики в области ИИ

B.2.1 Общие положения

Цель

Обеспечить получение от руководства руководящих указаний и поддержки ИИ-систем в соответствии с деловыми потребностями и применимыми правовыми обязательствами, включая договорные.

B.2.2 Политика в области ИИ

Меры управления

Организация должна задокументировать политику разработки и использования ИИ-систем.

Руководство по внедрению

Политика в области ИИ должна основываться на:

- бизнес-стратегии;
- ценностях и культуре организации, а также на степени риска, который организация готова принять или сохранить;
- уровне риска, создаваемого ИИ-системами;
- юридических обязательствах, в том числе в соответствии с договором;
- совокупности рисков организации;
- воздействии на соответствующие заинтересованные стороны.

Политика в области ИИ должна включать (в дополнение к требованиям 5.2):

- принципы, которыми руководствуется вся деятельность организации, связанная с ИИ;
- процессы обработки отклонений и исключений из политики.

Политика в области ИИ должна, где это уместно, принимать во внимание специфические аспекты, предоставляя дополнительные рекомендации и/или ссылаясь на другие политики, в которых эти аспекты рассматриваются. Примерами таких аспектов являются:

- ресурсы и активы ИИ;
- необходимость проведения оценки воздействия ИИ-системы (см. 6.1.4);
- разработка ИИ-системы.

Разработка, закупка, эксплуатация и использование ИИ-систем должны регулироваться соответствующими политиками.

B.2.3 Согласование с другими политиками организации

Меры управления

Организация должна определить, какие другие политики могут быть затронуты целями организации в отношении ИИ-систем или применяться к ним.

Руководство по внедрению

Деятельность в области ИИ пересекается с деятельностью в ряде других областей, таких как качество, безопасность, защита персональных данных. Организации следует провести тщательный анализ, чтобы определить, пересекаются ли текущие политики и где именно, и либо актуализировать эти политики, если требуются обновления, либо включить положения в политику в области ИИ.

Дополнительная информация

Политики, установленные руководящим органом от имени организации, должны лежать в основе политики в области ИИ. Стандарт [2] содержит рекомендации для членов руководящего органа организации по внедрению ИИ-системы и управлению ею на протяжении всего ее жизненного цикла.

B.2.4 Пересмотр политики в области ИИ

Меры управления

Политики в области ИИ должны пересматриваться через запланированные интервалы времени или в случае происходящих существенных изменений для обеспечения уверенности в сохранении их приемлемости, адекватности и результативности.

Руководство по внедрению

Исполнитель указанной руководством роли должен нести ответственность за разработку, анализ, пересмотр и оценку политики в области ИИ или ее составных частей. Процесс анализа и пересмотра должен включать оценку возможностей для совершенствования политик организации и ее подхода к управлению ИИ-системами, реагируя на изменения в среде организации, в деловых обстоятельствах, в правовых условиях и в техническом окружении.

При проведении анализа политики в области ИИ следует учитывать результаты проверок со стороны руководства.

B.3 Организация внутренней деятельности

B.3.1 Общие положения

Цель

Установить подотчетность внутри организации для поддержания ее ответственного подхода к внедрению, эксплуатации и управлению ИИ-системами.

B.3.2 Роли и обязанности ИИ

Меры управления

Роли и обязанности для ИИ должны быть определены и распределены в соответствии с потребностями организации

Руководство по внедрению

Определение ролей и обязанностей имеет решающее значение для обеспечения подотчетности всей организации за ее роль в отношении ИИ-системы на протяжении всего ее жизненного цикла. Для обеспечения охвата всех соответствующих областей организация должна учитывать политики в области ИИ, цели ИИ и выявленные риски при распределении ролей и обязанностей. Организация может расставлять приоритеты в распределении ролей и обязанностей. Примерами областей, которые могут потребовать определенных ролей и обязанностей, могут быть следующие:

- управление рисками;
- оценка воздействия ИИ-системы;
- управление активами и ресурсами;
- защита;
- безопасность;
- конфиденциальность;
- развитие;
- результаты деятельности;
- человеческий надзор;
- взаимоотношения с поставщиками;
- демонстрация способности последовательно выполнять юридические обязательства;
- управление качеством данных (на протяжении всего жизненного цикла).

Ответственность различных ролей должна быть определена на уровне, подходящем для лица (лиц) для выполнения своих обязанностей.

B.3.3 Информирование о проблемах

Меры управления

Организация должна определить и внедрить процесс, позволяющий сотрудникам организации сообщать о проблемах, связанных с ролью организации в отношении ИИ-системы на протяжении всего ее жизненного цикла.

Руководство по внедрению

Механизм отчетности должен выполнять следующие функции:

a) подбор вариантов обеспечения конфиденциальности, анонимности или и того, и другого;

b) быть доступным лицам, работающим по найму и по контракту;

c) быть укомплектованным квалифицированными специалистами;

d) устанавливать соответствующие полномочия по расследованию и разрешению споров для лиц, указанных в подпункте b);

e) предусматривать механизмы для своевременного представления отчетности и доведения ее до сведения руководства;

f) обеспечивать эффективную защиту от ответных действий как для лиц, связанных с отчетностью, так и с расследованием (например, позволяя выполнять отчетность анонимно и конфиденциально);

g) предоставлять отчеты в соответствии с пунктом 4.4 и, при необходимости, e); сохраняя конфиденциальность и анонимность a)) и соблюдая общие рекомендации деловой конфиденциальности

h) в соответствующие сроки обеспечивать механизмы реагирования.

Примечание — В рамках данного процесса организация может использовать существующие механизмы отчетности.

В дополнение к руководству по внедрению, приведенному в этом пункте, организации следует дополнительно рассмотреть [5].

B.4 Ресурсы ИИ-систем

B.4.1 Общие положения

Цель

Обеспечить учет организацией ресурсов (включая компоненты и активы ИИ-системы) ИИ-системы для полного понимания рисков и воздействий и устранения их последствий.

B.4.2 Документация ресурсов

Меры управления

Организация должна определить и задокументировать соответствующие ресурсы, необходимые для деятельности на данных стадиях жизненного цикла ИИ-системы, и другие связанные с ИИ виды деятельности, имеющие значение для организации.

Руководство по внедрению

Документирование ресурсов ИИ-системы имеет решающее значение для понимания рисков, а также потенциальных воздействий ИИ-системы (как положительных, так и отрицательных) на отдельных лиц и общества в целом. Документация таких ресурсов (которые используют, например, диаграммы потоков данных или схемы архитектуры системы) может служить основой для оценки воздействия ИИ-системы (см. B.5).

Ресурсы могут включать в себя, но не ограничиваются нижеследующим:

- компоненты ИИ-системы;
- информационные ресурсы, т.е. данные, используемые на любой стадии жизненного цикла ИИ-системы;
- инструментальные средства (например, алгоритмы, модели или инструменты ИИ);
- системные и вычислительные ресурсы (например, аппаратное обеспечение для разработки и запуска моделей ИИ, хранилище данных и инструментальные средства);
- человеческие ресурсы, то есть лица, обладающие необходимым опытом (например, для разработки, продаж, обучения, эксплуатации и технического обслуживания ИИ-системы) в соответствии с ролью организации на протяжении всего жизненного цикла ИИ-системы.

Ресурсы могут предоставляться самой организацией, ее клиентами или третьими лицами.

Дополнительная информация

Документация о ресурсах также может помочь определить наличие ресурсов, и, в случае их отсутствия рассмотреть возможность пересмотра спецификации проектирования ИИ-системы или требований к ее развертыванию.

B.4.3 Ресурсы данных

Меры управления

В рамках идентификации ресурсов организация должна документировать информацию о ресурсах данных, используемых для ИИ-системы.

Руководство по внедрению

Документация по данным включает в себя, но не ограничивается следующими темами:

- происхождение данных;
- дата последнего обновления или модификации данных (например, тег даты в метаданных);
- категории данных - для машинного обучения (например, обучающие, валидационные, тестовые и производственные данные);
- категории данных (см. [9]);
- процесс маркировки данных;
- предполагаемое использование данных;
- качество данных, описанное в [11];
- подготовка данных.

B.4.4 Инструментальные ресурсы

Меры управления

В рамках идентификации ресурсов организация должна задокументировать информацию об инструментальных средствах, используемых для ИИ-системы.

Руководство по внедрению

Инструментальные средства для ИИ-системы и, в частности, для машинного обучения, могут включать в себя, но не ограничиваются следующими:

- типы алгоритмов и модели машинного обучения;
- инструменты или процессы обработки данных;
- методы оптимизации;

- методы оценивания;
- инструменты предоставления ресурсов;
- инструменты, способствующие разработке моделей;
- программное обеспечение для проектирования, разработки и развертывания ИИ-систем;
- рекомендации по поводу различной семантики чисел с плавающей запятой в аппаратном обеспечении разработки и развертывания.

Дополнительная информация

Стандарт [10] содержит подробное руководство по типам, методам и подходам к различным инструментальным средствам для машинного обучения.

B.4.5 Система и вычислительные ресурсы

Меры управления

В рамках идентификации ресурсов организация должна документировать информацию о системе и вычислительных ресурсах, используемых для ИИ-системы.

Руководство по внедрению

Информация о системе и вычислительных ресурсах для ИИ-системы может содержать, но не ограничивается следующим:

- требования к ресурсам ИИ-системы (для обеспечения возможности работы системы на устройствах с ограниченными ресурсами);
- данные о расположении системы и вычислительных ресурсов (например, локальные, облачные вычисления или периферийные вычисления);
- ресурсы обработки (включая сеть и хранилище);
- данные о влиянии аппаратного обеспечения, используемого для выполнения рабочих нагрузок ИИ-системы (например, воздействие на окружающую среду в результате использования или производства аппаратного обеспечения или стоимость использования аппаратного обеспечения).

Необходимо учитывать, что для обеспечения постоянного улучшения ИИ-систем могут потребоваться различные ресурсы. Разработка, развертывание и эксплуатация системы могут иметь различные системные потребности и требования. В стандарте ИСО/МЭК 22989:2022 описываются различные аспекты использования системных ресурсов.

B.4.6 Человеческие ресурсы

Меры управления

В рамках идентификации ресурсов организация должна документировать информацию о человеческих ресурсах, используемых для разработки, развертывания и эксплуатации ИИ-системы.

Руководство по внедрению

Организация должна учитывать потребность в различных экспертных знаниях и определять типы ролей, необходимых для функционирования системы. Например, организация может включать определенные демографические группы, связанные с наборами данных, используемыми для подготовки моделей машинного обучения, если это является необходимым компонентом проектирования системы. К необходимым человеческим ресурсам относятся, но не ограничиваются:

- специалисты по обработке данных;
- роли, связанные с человеческим надзором за ИИ-системами;
- исследователи и специалисты в области ИИ, а также эксперты в предметной области, имеющие отношение к системам ИИ.

На разных стадиях жизненного цикла ИИ-системы могут потребоваться различные ресурсы.

B.5 Оценка воздействия ИИ-систем

B.5.1 Общие положения

Цель

Оценить воздействие ИИ-системы на отдельные лица и общества, затронутые ИИ-системой на протяжении всего ее жизненного цикла.

B.5.2 Процесс оценки воздействия ИИ-системы

Меры управления

Организация должна оценить потенциальные последствия для отдельных лиц и обществ, которые могут возникнуть в результате разработки или использования ИИ-систем.

Руководство по внедрению

Поскольку ИИ-системы потенциально оказывают значительное влияние на отдельные лица, группы лиц и общества, организация, предоставляющая и

использующая такие системы, должна учитывать предполагаемое назначение и использование этих систем, а также воздействие этих систем на эти группы.

Организации следует рассмотреть следующие вопросы (но не ограничиваться ими):

a) обстоятельства, при которых следует проводить оценку воздействия ИИ-системы, могут включать в себя, но не ограничиваться нижеследующим:

1) критичность предполагаемой цели и среды, в которой используется ИИ-система, или любые существенные изменения в них;

2) сложность технологии ИИ и уровень автоматизации ИИ-систем или какие-либо существенные изменения в этом;

3) чувствительность типов данных и источников, обрабатываемых ИИ-системой, или любые существенные изменения в них.

b) элементы, являющиеся частью процесса оценки воздействия ИИ-системы, который может включать:

1) идентификацию (например, источников, событий и результатов);

2) анализ (например, последствий и вероятности);

3) оценку (например, принятие решений и расстановка приоритетов);

4) обработку (например, меры по смягчению последствий);

5) документацию, отчетность и информирование (см. 7.4, 7.5 и B.3.3);

c) кем будет проводиться оценка воздействия ИИ-системы;

d) каким образом можно использовать оценку воздействия ИИ-системы (например, какое воздействие она может оказывать на проектирование или использование системы (см. B.6 и B.8), может ли она инициировать проверки и предоставлять разрешения);

e) отдельные лица и общества, которые рассматриваются на основе предполагаемого назначения, использования и характеристик системы (например, оценка отдельных лиц, групп лиц или обществ).

При оценке воздействия следует учитывать элементы ИИ-системы, включая используемые данные, подходы к ИИ и саму конечную систему.

Процессы могут варьироваться в зависимости от роли организации (независимо от того, применяются они для использования, подготовки или разработки ИИ-системы) и области применения ИИ, а также в зависимости от конкретных дисциплин, для которых учитывается воздействие (например, защита, конфиденциальность и безопасность).

Дополнительная информация

Для некоторых дисциплин или организаций детальное рассмотрение воздействия на отдельных лиц и общества является частью управления рисками, особенно в таких дисциплинах, как информационная безопасность, охрана труда и экологический менеджмент. Организация должна определить, в достаточной ли степени оценки воздействия конкретной дисциплины, выполняемые в рамках такого процесса управления рисками, учитывают соображения ИИ, и в этом случае отдельная оценка воздействия ИИ-системы не требуется.

Примечания

1 Значение термина «оценка воздействия» зависит от контекста или дисциплины. Например, в дисциплине «окружающая среда» оценка воздействия сосредоточена только на выявлении и анализе воздействия, в то время как в дисциплине «конфиденциальность» она охватывает оценку рисков и их обработку.

2 В стандарте [3] описывается, как организация может проводить анализ воздействия для самой организации, а также для отдельных лиц и обществ в рамках общего процесса управления рисками.

B.5.3 Документация по оценке воздействия ИИ-системы

Меры управления

Организация должна документировать результаты проведения оценок воздействия ИИ-системы и сохранять результаты в течение определенного периода.

Руководство по внедрению

Сохранение документации имеет большое значение при определении информации, которая должна быть доведена до сведения пользователей и других заинтересованных сторон.

Результаты проведения оценок воздействия ИИ-системы должны сохраняться и актуализироваться по мере необходимости в соответствии с элементами оценки воздействия ИИ-системы, задокументированными в B.5.2. Сроки хранения документации могут определяться графиками хранения организации или регламентироваться юридическими обязательствами или другими требованиями.

Тем не менее, существует ряд требований, соответствие которым в рамках системы управлении ИИ организация может демонстрировать посредством

разработки ряда документов. Среди них следует выделить описания процессов, которые могут включать, но не ограничиваются нижеследующим:

- положительное и отрицательное воздействие ИИ-системы на соответствующих лиц и общества;
- предсказуемые сбои, их потенциальные последствия и меры, принимаемые для их смягчения;
- соответствующие демографические группы, к которым применима система;
- сложность системы;
- роль людей во взаимоотношениях с системой, включая возможности человеческого надзора, процессы и инструменты, доступные для предотвращения негативных воздействий;
- трудоустройство и повышение компетентности персонала.

B.5.4 Оценка воздействия ИИ-системы на отдельных лиц и группы лиц

Меры управления

Организация должна оценивать и документировать потенциальное воздействие ИИ-систем на отдельных лиц или группы лиц на протяжении всего жизненного цикла системы.

Руководство по внедрению

При проведении оценки воздействия на отдельных лиц организация должна учитывать принципы управления, политики и цели в области ИИ, присущие ей. Лица, использующие систему ИИ или лица, чьи персональные данные обрабатываются ИИ-системой, могут предъявлять требования к надежности ИИ-системы. Следует принимать во внимание особую потребность в защите таких групп, как дети, инвалиды, пожилые люди и рабочие. Организация должна провести оценку ожиданий и рассмотреть средства их реализации в рамках оценки воздействия на систему.

В зависимости от области назначения и применения ИИ-системы, в рамках оценки следует учитывать следующие области воздействия (но не ограничиваться ими):

- справедливость;
- прозрачность и объяснимость;
- защита и конфиденциальность;

- безопасность и гигиена труда;
- финансовые последствия;
- доступность;
- права человека.

Дополнительная информация

При необходимости организация должна консультироваться с экспертами (например, с исследователями, экспертами в предметной области или пользователями), чтобы, насколько это возможно, получить полное представление о потенциальном воздействии системы на лиц.

B.5.5 Оценка воздействия ИИ-систем на общество

Меры управления

Организация должна оценивать и документировать потенциальное воздействие ИИ-систем на общество на протяжении всего их жизненного цикла.

Руководство по внедрению

Воздействие на общество может сильно варьироваться в зависимости от среды организации и типов ИИ-систем. Воздействие ИИ-систем на общество может быть как позитивным, так и негативным. Примерами таких потенциальных социальных воздействий могут служить:

- экологическая устойчивость (включая воздействие на природные ресурсы и выбросы парниковых газов);
- экономика (включая доступ к финансовым услугам, возможности трудоустройства, налоги, торговлю и коммерцию);
- правительство (включая законодательные процессы, дезинформацию в политических целях, системы национальной безопасности и уголовного правосудия);
- здоровье и безопасность (включая доступ к медицинскому обслуживанию, медицинскую диагностику и лечение, а также потенциальный физический вред);
- нормы, традиции, культура и ценности (включая дезинформацию, которая приводит к предубеждениям или причиняет вред отдельным лицам).

Дополнительная информация

Разработка и использование ИИ-систем может потребовать значительных вычислительных ресурсов, что может оказать соответствующее воздействие на

экологическую устойчивость (например, выбросы парниковых газов из-за увеличения энергопотребления, воздействие на воду, землю, флору и фауну). Аналогичным образом, ИИ-системы могут использоваться для повышения экологической устойчивости других систем (например, сокращения выбросов парниковых газов, связанных со строительством и транспортировкой). Организация должна учитывать воздействие ИИ-систем в контексте своих общих целей и стратегий в области экологической устойчивости.

Организации следует рассмотреть вопрос о способах использования ИИ-системы не по назначению для причинения вреда обществу и о возможности ее применения для устранения исторического ущерба. Например, могут ли ИИ-системы препятствовать доступу к финансовым услугам, таким как кредиты, гранты, страхование и инвестиции и могут ли ИИ-системы улучшить доступ к этим инструментам?

ИИ-системы использовались для оказания влияния на результаты выборов и создания дезинформации (например, дипфейки цифровых медиа), которые могут привести к политическим и социальным волнениям. При применении правительством ИИ-систем в целях уголовного правосудия был выявлен риск алгоритмической предвзятости по отношению к отдельным лицам или группе лиц, обусловленный использованием ИИ. Следует также рассмотреть вопрос о том, каким образом злоумышленники могут злоупотреблять ИИ-системами и усиливают ли ИИ-системы исторически сложившиеся социальные предубеждения.

ИИ-системы могут использоваться для диагностики и лечения заболеваний, а также для оценки критериев определения тех граждан, которые имеют право на медицинские льготы. ИИ-системы также развертываются в сценариях, где сбои в работе (машин) могут привести к летальному исходу или травмам людей (например, в случае с беспилотными автомобилями, взаимодействия человека и машины). Организация должна учитывать как положительные, так и отрицательные результаты при использовании ИИ-систем в сценариях, связанных со здоровьем и безопасностью людей.

Примечание — В стандарте [28] содержится высокоуровневый обзор этических и социальных проблем, связанных с системами и ИИ-приложениями. В нем содержится неполный перечень рекомендаций по созданию и использованию этичного и социально приемлемого ИИ.

B.6 Жизненный цикл ИИ-системы

B.6.1 Руководство по разработке ИИ-системы

B.6.1.1 Общие положения

Цель

Обеспечить определение и документирование целей, а также внедрение процессов ответственного проектирования и разработки надежных ИИ-систем.

B.6.1.2 Цели ответственного развития ИИ-системы

Меры управления

Организация должна определить и задокументировать цели, которыми следует руководствоваться при ответственной разработке ИИ-систем, а также учитывать эти цели и интегрировать меры по их достижению в жизненный цикл разработки.

Руководство по внедрению

Организация должна определить цели (см. 6.2), оказывающие влияние на процессы проектирования и разработки ИИ-системы и учитывать их. Например, если организация определяет «справедливость» как одну из целей, это следует учитывать при определении требований, сборе данных, их обработке, обучении модели, верификации, валидации и т.д. Организация должна предоставить требования и руководящие принципы, необходимые для обеспечения интеграции мер на различных этапах (например, требование об использовании конкретного инструмента или метода тестирования для устранения несправедливости или нежелательной предвзятости) для достижения таких целей.

Дополнительная информация

Методы ИИ используются для усиления мер безопасности, таких как обнаружение прогнозирования угроз и предотвращение атак на систему безопасности. Имеется в виду применение методов ИИ, которые можно использовать для усиления мер безопасности для защиты как ИИ-систем, так и обычных программных систем, не основанных на ИИ. В приложении С приведены примеры организационных целей по управлению рисками, которые могут быть полезны при определении целей разработки ИИ-системы.

B.6.1.3 Процессы ответственного проектирования и разработки ИИ-систем

Меры управления

Организация должна определить и задокументировать конкретные процессы проектирования и разработки ИИ-системы.

Руководство по внедрению

Ответственная разработка системных процессов ИИ включает в себя рассмотрение, помимо прочего, следующих вопросов:

- стадии жизненного цикла (общая модель жизненного цикла ИИ-системы представлена в стандарте ИСО/МЭК 22989:2022, однако организация может указать свои собственные стадии жизненного цикла);
- требования к тестированию и предполагаемые ресурсы тестирования;
- требования человеческого надзора, включая процессы и инструменты, особенно в случае, если ИИ-система может воздействовать на физические лица;
- на каких этапах следует проводить оценку воздействия ИИ-системы;
- требования и правила к данным для обучения (например, какие данные можно использовать, утвержденные поставщики данных и маркировка);
- требуемый опыт (в предметной или другой области) или обучение для разработчиков ИИ-систем или и то, и другое;
- критерии выпуска;
- согласования и подписи, необходимые на различных этапах;
- управление изменениями;
- удобство использования и управляемость;
- вовлечение заинтересованных сторон.

Конкретные процессы проектирования и разработки зависят от функциональности и технологий ИИ, которые предполагается использовать в системе ИИ.

B.6.2 Жизненный цикл разработки ИИ-системы

B.6.2.1 Общие положения

Цель

Определить критерии и требования для каждой стадии жизненного цикла ИИ-системы.

B.6.2.2 Требования и спецификация к системе ИИ

Меры управления

Организация должна определить и задокументировать требования к новым системам ИИ или существенным усовершенствованиям существующих систем.

Руководство по внедрению

Организация должна задокументировать обоснование разработки ИИ-системы и ее цели. Некоторые из факторов, которые следует учитывать, документировать и понимать, могут включать:

a) чем обусловлена разработка ИИ-системы (например, экономическое обоснование, запрос клиента или политика правительства);

b) метрики показателей успеха (каким образом определяется соответствие ИИ-системы целям и спецификациям ее производительности).

Требования к ИИ-системе должны быть определены и охватывать весь ее жизненный цикл. Такие требования следует пересматривать в случаях, когда разработанная ИИ-система не функционирует должным образом или появляется новая информация, которая может быть использована для изменения и улучшения требований. Например, разработка ИИ-системы может стать невыполнимой с финансовой точки зрения.

Дополнительная информация

Процессы для описания жизненного цикла ИИ-системы предусмотрены стандартом [22]. Для получения дополнительной информации об ориентированном на человека проектировании интерактивных систем см. [29].

B.6.2.3 Документация по проектированию и разработке ИИ-системы

Меры управления

Организация должна документировать проектирование и разработку ИИ-системы на основе целей организации, документированных требований и критериев спецификации.

Руководство по внедрению

Существует множество вариантов проектирования, необходимых для функционирования ИИ-системы, включая, но не ограничиваясь следующими:

- подход к машинному обучению (например, контролируемый или неконтролируемый);
- алгоритм обучения и тип используемой модели машинного обучения;
- методы обучения модели и качество данных (см. B.7);

- проведение оценки и улучшение моделей;
- аппаратные и программные компоненты;
- угрозы безопасности, зафиксированные на протяжении всего жизненного цикла ИИ-системы; угрозы безопасности, характерные для ИИ-систем, включают отравление данными, кражу моделей или атаки с инверсией моделей;
- интерфейс и представление выходных данных;
- способы взаимодействия людей и системы;
- вопросы функциональной совместимости и переносимости.

Между проектированием и разработкой может быть несколько итераций, при этом на данном этапе документация должна поддерживаться в актуальном состоянии, и должна быть доступна конечная документация по архитектуре системы.

Дополнительная информация

Для получения дополнительной информации об ориентированном на пользователя проектировании интерактивных систем, см. [29].

B.6.2.4 Верификация и валидация ИИ-системы

Меры управления

Организация должна определить и задокументировать методы верификации и валидации для ИИ-системы и указать критерии для их использования.

Руководство по внедрению

Методы верификациии и валидации могут включать, но не ограничиваться следующими:

- методологии и инструменты тестирования;
- выбор тестовых данных и их репрезентативность в отношении предполагаемой области использования;
- требования к критериям выпуска.

Организация должна определить и задокументировать следующие критерии оценки, но не ограничиваясь ими:

- этапы проведения оценки компонентов ИИ-системы и всей ИИ-системы в целом на предмет рисков, связанных с воздействием на отдельных лиц и общества;
- этапы оценки могут включать следующие критерии:

  1) требования к надежности и безопасности ИИ-системы, включая допустимую частоту ошибок для показателей деятельности / производительности ИИ-системы;

2) ответственные цели разработки и использования ИИ-систем, подобные тем, которые указаны в В.6.1.2 и В.9.3;

3) эксплуатационные факторы, такие как качество данных, предполагаемое использование, включая допустимые диапазоны каждого эксплуатационного фактора;

4) любые предполагаемые виды применения, которые могут потребовать определения более строгих эксплуатационных факторов, включая различные допустимые диапазоны эксплуатационных факторов или более низкую частоту ошибок;

- методы, рекомендации или показатели, используемые для оценки того, могут ли соответствующие заинтересованные стороны, которые принимают решения или подпадают под действие решений, основанных на результатах работы ИИ-системы, адекватно интерпретировать результаты работы ИИ-системы. Периодичность проведения оценки должна быть определена и может зависеть от результатов оценки воздействия ИИ-системы;
- любые приемлемые факторы, которые могут объяснить неспособность достичь целевого минимального уровня производительности, особенно когда ИИ-система оценивается на предмет воздействия на отдельных людей и общества (например, низкое разрешение изображения для систем компьютерного зрения или фоновый шум, влияющий на системы распознавания речи). Мероприятия по борьбе с низкой производительностью ИИ-системы, обусловленной вышеперечисленными факторами также следует задокументировать.

Систему ИИ следует оценивать в соответствии с задокументированными критериями оценки.

В случаях, когда ИИ-система не может соответствовать задокументированным критериям оценки, особенно в отношении целей ответственной разработки и использования ИИ-системы (см. В .6.1.2, В.9.3), организация должна пересмотреть или устранить недостатки предполагаемого использования ИИ-системы, свои требования к производительности и то, как организация может эффективно реагировать на воздействие на отдельных лиц и общества.

Дополнительная информация о том, как обеспечить надежность нейронных сетей представлена в [16].

B.6.2.5 Развертывание ИИ-системы

Меры управления

Организация должна задокументировать план развертывания и обеспечить выполнение соответствующих требований до инициирования процесса развертывания.

Руководство по внедрению

ИИ-системы могут разрабатываться в одних средах и развертываться в других (например, разрабатываться локально и развертываться в облачных вычислениях), и организация должна учитывать эти различия при разработке плана развертывания. Также следует рассмотреть вопрос о том, развертываются ли компоненты отдельно (например, программное обеспечение и модель могут быть разработаны независимо друг от друга). Кроме того, организация должна установить набор требований, которые должны быть выполнены до выпуска и развертывания (иногда называемых «критериями выпуска»). Критерии выпуска могут включать в себя: принятые методы верификации и валидации, выполненные показатели производительности, пройденное пользовательское тестирование, а также полученные согласование руководства и подписи. План развертывания должен учитывать перспективы соответствующих заинтересованных сторон и их воздействие на них.

B.6.2.6 Эксплуатация и мониторинг ИИ-системы

Меры управления

Организация должна определить и задокументировать необходимые элементы для непрерывной работы ИИ-системы. Как минимум, это должно включать мониторинг системы и производительности, ремонт, обновления и поддержку.

Руководство по внедрению

Любое действие для эксплуатации и мониторинга может иметь различные аспекты. Например:

- Мониторинг системы и производительности может включать мониторинг общих ошибок и сбоев, а также проверку того, работает ли система с производственными данными должным образом. Технические критерии эффективности могут включать показатели успешности в решении проблем и в выполнении задач, а также уровни доверия. Другие критерии могут быть связаны с выполнением обязательств или ожиданий и потребностей заинтересованных

сторон, включая, например, постоянный мониторинг для обеспечения соответствия требованиям заказчика или применимым законодательным требованиям;

- Некоторые развернутые ИИ-системы повышают свою эффективность в результате МО, при применении которого производственные и выходные данные используются для дальнейшего обучения модели МО. При применении непрерывного обучения, организации следует осуществлять контроль производительности ИИ-системы для обеспечения гарантии, что она продолжает соответствовать целям проектирования и оперирует производственными данными по назначению; / для обеспечения соответствия организацией;

- Производительность некоторых ИИ-систем может измениться, даже если такие системы не используют непрерывное обучение. Как правило это происходит из-за концепции или смещения данных в производственных данных. В таких случаях мониторинг может выявить необходимость в переобучении, для обеспечения гарантии, что ИИ-система продолжает соответствовать целям проектирования и оперирует производственными данными по назначению. Более подробную информацию можно найти в [10].

- Ремонт может включать в себя устранение ошибок и сбоев в системе. Организации следует внедрить процессы реагирования на эти факторы и их устранения. Кроме того, обновления могут быть необходимы по мере развития системы, выявления меньшего количества критических факторов или в результате внешних выявленных факторов (например, несоответствие ожиданиям клиентов или юридическим обязательствам). Необходимо внедрить процессы обновления системы, включая затронутые обновлением компоненты, график обновления, информацию для пользователей о том, что подлежит обновлению;

- Системные обновления также могут включать изменения в работе системы, новые или модифицированные виды использования по назначению или другие изменения в функциональности системы. В организации должны быть внедрены процедуры для реагирования на операционные изменения, включая информирование пользователей;

- Поддержка системы может быть внутренней, внешней или и той, и другой, в зависимости от потребностей организации и способа приобретения системы. Процессы поддержки должны учитывать то, каким образом осуществляется обращение пользователей за соответствующей помощью,

сообщается о проблемах и инцидентах, а также поддерживаются соглашения об уровне обслуживания и показателях;

- Если ИИ-системы используются для целей, отличных от тех, для которых они были разработаны, или способами, которые не предполагались, следует рассмотреть целесообразность такого использования;
- Организация, применяющая или разрабатывающая ИИ-системы, должна выявить характерные для них угрозы информационной безопасности. Угрозы информационной безопасности, характерные для ИИ, включают, но не ограничиваются следующими: отравление данных, кражу моделей и атаки с инверсией моделей.

Дополнительная информация

Организации следует учитывать эксплуатационные характеристики, которые могут повлиять на заинтересованные стороны, и учитывать это при разработке и определении критериев эффективности.

Критерии эффективности для действующих ИИ-систем должны определяться рассматриваемой задачей, такой как классификация, регрессия, ранжирование, кластеризация или уменьшение размерности.

Критерии эффективности могут включать статистические аспекты, такие как частота ошибок и продолжительность обработки. Для каждого критерия организация должна определить все соответствующие показатели, а также взаимозависимости между показателями. Для каждого показателя организация должна рассмотреть приемлемые значения, основанные, например, на рекомендациях эксперта в предметной области и анализе ожиданий заинтересованных сторон относительно существующих практик, не связанных с ИИ.

Например, организация может определить, что оценка F1 является подходящим показателем эффективности, основываясь на ее оценке влияния ложноположительных и ложноотрицательных результатов, как описано в [15]. Затем организация может установить значение F1, которому, как ожидается, будет соответствовать ИИ-система. Следует оценить возможность решения этих проблем с помощью существующих мер. В противном случае, следует рассмотреть возможность внесения изменений в существующие меры или определить дополнительные меры для выявления этих проблем и их устранения.

Организация должна учитывать эффективность действующих систем или процессов, не связанных с ИИ, и использовать их в качестве потенциально релевантного контекста при установлении критериев эффективности.

Организация должна дополнительно обеспечить, чтобы средства и процесс, используемые для оценки ИИ-системы, включая, где применимо, отбор оценочных данных и управление ими, повышали полноту и надежность оценки ее эффективности в соответствии с определенными критериями.

Разработка методологий оценки эффективности может основываться на критериях, показателях и ценностях/значениях. Описанные критерии должны отражать объем данных и типы процессов, используемых при оценке, а также роли и опыт персонала, проводящего оценку.

Методологии оценки эффективности должны максимально точно отражать атрибуты и характеристики функционирования и использования для обеспечения полезности и актуальности результатов оценки. Некоторые аспекты оценки эффективности могут потребовать контролируемого введения ошибочных или ложных данных или процессов для оценки влияния на эффективность.

Модель качества в [13] может быть использована для определения критериев эффективности.

B.6.2.7 Техническая документация по системе ИИ

Меры управления

Во время работы ИИ-системы при необходимости должно быть включено автоматическое ведение журналов событий.

Руководство по внедрению

Техническая документация ИИ-системы может включать, но не ограничивается следующими элементами:

- общее описание ИИ-системы, включая ее предполагаемое назначение;
- инструкции по эксплуатации;
- технические допущения о развертывании и эксплуатации ИИ-системы (среда выполнения, соответствующие программные и аппаратные возможности, предположения, сделанные на основе данных, и т.д.);
- технические ограничения (например, допустимая частота ошибок, точность, надежность, робастность);
- возможности мониторинга и функции, позволяющие пользователям или операторам влиять на работу системы.

Элементы документации, относящиеся ко всем стадиям жизненного цикла ИИ-системы (как определено в стандарте ИСО/МЭК 22989:2022), могут включать, но не ограничиваться:

- спецификацию проектирования и архитектуры системы;
- проектирование и меры по обеспечению качества, принятые в процессе разработки системы;
- информацию о данных, используемых при разработке системы;
- сделанные допущения и принятые меры по обеспечению качества данных (например, предполагаемые статистические распределения);
- управленческие действия (например, управление рисками), осуществляемые в ходе разработки или эксплуатации ИИ-системы;
- записи о верификации и валидации;
- записи о изменениях, вносимых в систему ИИ во время ее эксплуатации;
- документация по оценке воздействия, в соответствии с пунктом B.5.

Организация должна документировать техническую информацию, связанную с ответственной эксплуатацией ИИ-системы. Это может включать, но не ограничивается:

- документирование плана по устранению неизвестных сбоев. Это может включать, например, необходимость описания плана отката для ИИ-системы, отключения функций ИИ-системы, процесса обновления или плана уведомления клиентов, пользователей и т.д. об изменениях в системе ИИ, актуализированной информации о системных сбоях и способах их устранения;
- документирование процессов мониторинга работоспособности ИИ-системы (т.е. использование ИИ-системы по назначению и в пределах ее нормальных эксплуатационных возможностей, также называемое наблюдаемостью) и процессов устранения сбоев ИИ-системы;
- документирование стандартных операционных процедур для ИИ-системы, включая то, какие события следует отслеживать и каким образом журналы событий расставляются по приоритетам и просматриваются. Это также может включать в себя способы анализа и предотвращения сбоев;
- документирование ролей персонала, ответственного за работу ИИ-системы, а также ролей лиц, ответственных за подотчетность использования системы, особенно в отношении устранения последствий сбоев ИИ-системы или управления обновлениями ИИ-системы;

- обновления системы документов также могут включать изменения в работе системы, новые или измененные виды использования по назначению или другие изменения в функциональности системы. В организации должны быть внедрены процедуры для реагирования на операционные изменения, включая информирование пользователей и проведение внутренней оценки типа изменений. Некоторые серьезные изменения могут потребовать проведение переоценки рисков.

Документация должна быть актуальной и точной. Документация должна быть одобрена соответствующим руководством организации.

При предоставлении пользовательской документации следует принимать во внимание меры управления, приведенные в таблице А.1.

В.6.2.8 Ведение журналов событий ИИ-системой

Меры управления

Организации следует определить, на каких стадиях жизненного цикла ИИ-системы следует включить ведение журналов событий. Как минимум, ведение журналов необходимо при непосредственном использовании ИИ-системы.

Руководство по внедрению

Организация должна обеспечить ведение журналов для ИИ-систем, которые она развертывает, для автоматического сбора и записи журналов событий, связанных с определенными событиями, происходящими во время работы. Ведение журнала для ИИ-систем может включать, но не ограничивается следующим:

- отслеживание функциональности ИИ-системы для обеспечения надлежащей/правильной работы ИИ-системы;
- обнаружение функционирования ИИ-системы за пределами ее предполагаемых условий эксплуатации, что может привести к нежелательному функционированию на производственных данных или воздействиям на соответствующие заинтересованные стороны посредством мониторинга работы ИИ-системы.

Журналы событий ИИ-системы могут включать в себя информацию, такую как время и дата каждого использования ИИ-системы, производственные данные, с которыми она работает; выходные данные, которые выходят за рамки предполагаемой работы ИИ-системы, и т.д.

Журналы событий должны храниться до тех пор, пока это требуется для предполагаемого использования ИИ-системы и в соответствии с политиками хранения данных организации и ее юридическими обязательствами, связанными с хранением данных.

Примечание — В зависимости от законодательства, некоторые системы искусственного интеллекта, такие как системы биометрической идентификации, могут предъявлять дополнительные требования к ведению журнала и организации должны быть осведомлены об этих требованиях.

B.7 Данные для ИИ-систем

B.7.1 Общие положения

Цель

Обеспечить понимание организацией роли и влияния данных в ИИ-системах при применении и разработке, предоставлении или использовании ИИ-систем на протяжении их жизненного цикла.

B.7.2 Данные для разработки и усовершенствования ИИ-системы

Меры управления

Организация должна определять, документировать и внедрять процессы управления данными, связанные с разработкой ИИ-систем.

Руководство по внедрению

Управление данными может включать различные темы, которые организации следует рассмотреть, включая:

- последствия для конфиденциальности и защиты в связи с использованием данных, некоторые из которых могут носить конфиденциальный характер;
- угрозы безопасности, которые могут возникнуть в результате разработки ИИ-систем, зависящей от данных;
- аспекты прозрачности и объяснимости, включая происхождение данных и возможность предоставить объяснение того, как данные используются для определения выходных данных ИИ-системы, если система требует прозрачности и объяснимости;

- репрезентативность обучающих данных по сравнению с рабочей областью использования;
- точность и целостность данных.

Подробная информация о жизненном цикле ИИ-системы и концепциях управления данными приведена в стандарте ИСО/МЭК 22989:2022.

B.7.3 Сбор данных

Меры управления

Организация должна определить и задокументировать подробную информацию о сборе и отборе данных, используемых в ИИ-системах.

Руководство по внедрению

Организации могут потребоваться различные категории данных из разных источников в зависимости от области применения их ИИ-систем.

Детали сбора данных могут включать:

- категории данных, необходимых для функционирования ИИ-системы;
- количество необходимых данных;
- источники данных (например, внутренние, приобретенные, совместно используемые, открытые данные, синтетические);
- характеристики источника данных (например, статические, потоковые, собранные, сгенерированные автоматически);
- демографические данные и характеристики субъекта данных;
- предварительная обработка данных (например, информация о предыдущем использовании, соответствие требованиям конфиденциальности и безопасности);
- происхождение данных.

Категории данных и структура использования данных, представленные в [9] могут быть использованы для документирования подробных сведений о сборе и использовании данных.

B.7.4 Качество данных для ИИ-систем

Меры управления

Организация должна определить и задокументировать требования к качеству данных и обеспечить соответствие данных, используемых для разработки и эксплуатации ИИ-системы этим требованиям.

Руководство по внедрению

Качество данных, используемых для разработки и эксплуатации ИИ-систем, потенциально оказывает значительное влияние на достоверность результатов работы системы. В стандарте [4] качество данных определяется как степень, в которой характеристики данных удовлетворяют заявленным и подразумеваемым потребностям при использовании в определенных условиях. Для ИИ-систем, в которых используется контролируемое или полуконтролируемое машинное обучение, важно, чтобы качество обучающих, валидационных, тестовых и производственных данных было определено, измерено и улучшено, насколько это возможно, и организация должна гарантировать, что данные соответствуют своему прямому назначению. Организации следует учитывать влияние предвзятости на производительность и справедливость системы и вносить необходимые коррективы в модель и данные, используемые для повышения производительности и справедливости до приемлемых уровней для каждого конкретного варианта использования.

Дополнительная информация

Дополнительная информация о качестве данных представлена в [11], посвященных качеству данных для аналитики и МО. Информация о различных формах искажения данных, используемых в ИИ-системах представлена в [14].

B.7.5 Происхождение данных

Меры управления

Организация должна определить и задокументировать процесс верификации и записи происхождения данных, используемых в ее ИИ-системах, на протяжении жизненного цикла данных и ИИ-системы.

Руководство по внедрению

Согласно стандарту [12], запись о происхождения данных может включать информацию о создании, обновлении, транскрипции, абстрагировании, валидации и передаче управления данными. Кроме того, обмен данными (без передачи управления) и преобразования данных могут рассматриваться как происхождение данных.

B.7.6 Подготовка данных

Меры управления

Организация должна определить и задокументировать свои потребности в подготовке данных и подходы к этому.

Руководство по внедрению

Данные, используемые в системе ИИ, обычно требуют подготовки для применения в конкретной задаче ИИ. Например, алгоритмы машинного обучения иногда проявляют нетерпимость к отсутствующим или неправильным записям, ненормальному распределению и широко варьирующимся масштабам. Для повышения качества данных можно использовать методы подготовки и преобразования. Неспособность должным образом подготовить данные потенциально может привести к ошибкам ИИ-системы. Распространенные методы подготовки и преобразования данных, используемые в ИИ-системах, включают:

- статистическое исследование данных (например, распределение, среднее значение, медиана, стандартное отклонение, диапазон, стратификация, выборка) и спецификация статистических метаданных (например, инициатива по документированию данных [25]);
- очистка данных (т.е. исправление записей, устранение отсутствующих записей);
- вменение/условное исчисление (т.е. методы заполнения недостающих записей);
- нормализация;
- масштабирование;
- обозначение целевых переменных;
- кодирование (например, преобразование категориальных переменных в числа).

Для выполнения данной задачи ИИ, организация должна задокументировать свои критерии выбора конкретных методов подготовки данных и преобразований, а также конкретные методы и преобразования, используемые в задаче ИИ.

Примечание — Дополнительную информацию о подготовке данных, специфичных для машинного обучения, см. в [11] и [10].

B.8 Информация для заинтересованных сторон

B.8.1 Общие положения

Цель

Обеспечить предоставление соответствующим заинтересованным сторонам необходимой информации для понимания и оценки рисков и их последствий (как положительных, так и отрицательных).

B.8.2 Системная документация и информация для пользователей

Меры управления

Организация должна определить и предоставить необходимую информацию пользователям системы.

Руководство по внедрению

В зависимости от контекста, информация о ИИ-системе может включать в себя как технические детали и инструкции, так и общие уведомления пользователей о том, что они взаимодействуют с ИИ-системой. К этому можно отнести саму систему, а также потенциальные результаты работы системы (например, уведомление пользователей о том, что изображение создано с помощью ИИ).

Рекомендации относительно того, какую информацию следует предоставлять пользователям, включают в себя, помимо прочего:

- назначение системы;
- информация о том, что пользователь взаимодействует с ИИ;
- каким образом осуществляется взаимодействие с системой;
- каким образом и в какие сроки необходимо переопределять систему;
- технические требования к работе системы и ограничения системы;
- информация о точности и производительности;
- соответствующая информация, полученная в результате проведения оценки воздействия, включая потенциальные преимущества, вред и риски, особенно если они применимы в конкретных средах или определенных демографических группах (см. B.5.2);
- пересмотр утверждений о преимуществах системы;
- обновления и изменения в методах работы системы;
- контактная информация;
- учебные материалы для эксплуатации системы.

Информация может предоставляться пользователям различными способами, включая документированные инструкции по эксплуатации, оповещения и другие уведомления, встроенные в саму систему, информацию на веб-странице и т.д. В зависимости от того, какие методы использует организация для предоставления информации, она должна подтвердить, что пользователи имеют доступ к этой информации и что предоставленная информация является полной, актуальной и точной.

B.8.3 Понятность и доступность предоставляемой информации

Меры управления

Информация, предоставляемая заинтересованным сторонам, должна быть прозрачной, понятной и подходящей для них.

Руководство по внедрению

Хотя системы искусственного интеллекта могут быть сложными, крайне важно, чтобы пользователи могли понимать, что они взаимодействуют не только с искусственным интеллектом, но и с тем, как работает система, а также относительные преимущества, вред и риски взаимодействия с системой. Некоторая системная документация обязательно может быть предназначена для более технических целей (например, для системных администраторов), и организация должна понимать потребности различных заинтересованных сторон и то, что для них может означать понятность. Информация также должна быть доступной, как с точки зрения простоты ее поиска, так и для пользователей, которым могут потребоваться дополнительные меры по обеспечению доступности.

B.8.4 Внешняя отчетность

Меры управления

Организация должна предоставить возможности для информирования о неблагоприятных воздействиях системы.

Руководство по внедрению

Организации следует отслеживать работу системы на предмет сообщений о выявленных проблемах и сбоях, а также предоставлять пользователям или другим внешним сторонам возможность сообщать о неблагоприятных воздействиях (например, о несправедливости).

B.8.5 Информирование об инцидентах

Меры управления

Организация должна определить и задокументировать план информирования пользователей системы об инцидентах.

Руководство по внедрению

Инциденты, связанные с ИИ-системой, могут быть специфичными для самой ИИ-системы или связаны с информационной безопасностью или конфиденциальностью (например, утечка данных). Организация должна понимать свои обязательства по уведомлению пользователей и других заинтересованных сторон об инцидентах, в зависимости от среды, в которой работает система. Например, к инциденту с компонентом ИИ, который является частью продукта и влияет на безопасность, могут предъявляться иные требования к уведомлению, чем к системам других типов. Организация должна быть осведомлена о юридических обязательствах (таких как контракты) и регулирующей деятельности, которая может устанавливать требования в отношении:

- типов инцидентов, о которых необходимо сообщать;
- сроков уведомления;
- должны ли быть уведомлены соответствующие органы и какие именно;
- деталей, которые необходимо сообщить.

Организация может интегрировать мероприятия по реагированию на инциденты и отчетности для ИИ в свою более широкую организационную деятельность по управлению инцидентами. При этом, организации следует учитывать уникальные требования, связанные с ИИ-системами или отдельными компонентами ИИ-систем (например, утечка персональных данных в обучающих данных для системы может иметь различные требования к отчетности, связанные с конфиденциальностью). В стандартах [17] и [8] представлены дополнительные сведения об управлении инцидентами в целях обеспечения безопасности и конфиденциальности соответственно.

B.8.6 Информация для заинтересованных сторон

Меры управления

Организация должна определить и задокументировать свои обязательства по предоставлению информации о ИИ-системе заинтересованным сторонам.

Руководство по внедрению

В некоторых случаях юрисдикция может потребовать предоставления информации о системе регулирующим органам. Информация может быть доведена до сведения заинтересованных сторон, таких как клиенты или регулирующие органы, в соответствующие сроки. Сюда может относиться, например:

- техническая документация по системе, включая, но не ограничиваясь этим, наборы данных для обучения, валидации и тестирования, а также обоснования выбора алгоритмов и записи о верификации и валидации;
- риски, связанные с использованием ИИ-системы;
- результаты оценок воздействия ИИ-системы;
- журналы событий и другие системные записи.

Организация должна понимать свои обязательства в этом отношении и обеспечить передачу соответствующей информации соответствующим органам власти. Кроме того, организация должна понимать требования юрисдикции в отношении информации, передаваемой правоохранительным органам.

B.9 Использование ИИ-систем

B.9.1 Общие положения

Цель

Обеспечение организацией ответственного использования ИИ и в соответствии с политиками организации.

B.9.2 Процессы ответственного использования ИИ

Меры управления

Организация должна определить и задокументировать процессы ответственного использования ИИ-систем.

Руководство по внедрению

В зависимости от среды организации может быть множество рекомендаций для определения того, какую систему ИИ лучше использовать. Независимо от того, кто является разработчиком ИИ-системы - организация или третья сторона, в задачи организации входит проанализировать эти рекомендации и разработать политики для их учета. Вот некоторые примеры:

- требуемые утверждения;
- затраты (включая расходы на текущий мониторинг и техническое обслуживание);

- утвержденные требования к поставщикам;
- юридические обязательства, применимые к организации.

Если организация приняла политики использования других систем, активов и т.д., при желании эти политики могут быть использованы.

B.9.3 Цели ответственного использования ИИ-системы

Меры управления

Организация должна определить и задокументировать цели, которыми следует руководствоваться при ответственном использовании ИИ-систем.

Руководство по внедрению

Организация, действующая в разных средах, может иметь разные ожидания и цели в отношении того, что представляет собой ответственное развитие ИИ-систем. В соответствии со средой, организации следует определить свои цели в отношении надежного использования. Некоторые цели включают в себя:

- справедливость;
- подотчетность;
- прозрачность;
- объяснимость
- надежность;
- безопасность;
- робастность и избыточность;
- конфиденциальность и защита;
- доступность.

После определения своих целей, организация должна внедрить механизмы для их достижения внутри организации. Это может включать определение того, соответствует ли стороннее решение / решение сторонних разработчиков/производителей целям организации или применимо ли решение, разработанное внутри организации для предполагаемого использования. Организация должна определить, на каких стадиях жизненного цикла ИИ-системы следует внедрять значимые цели человеческого надзора. К этому можно отнести:

- привлечение рецензентов для проверки выходных данных ИИ-системы, в том числе наделение полномочиями отменять решения, принимаемые ИИ-системами;

- обеспечение внедрения человеческого надзора, если это требуется для осуществления допустимого использования ИИ-системы в соответствии с инструкциями или другой документацией, связанной с предполагаемым развертыванием ИИ-системы;
- мониторинг производительности ИИ-системы, включая точность выходных данных ИИ-системы;
- оповещение соответствующих заинтересованных сторон о проблемах, связанных с выходными данными ИИ-системы, и их воздействии;
- оповещение о проблемах, связанных с изменениями в производительности или способности ИИ-системы выдавать правильные выходные данные на основе производственных данных;
- рассмотрение вопроса о том, подходит ли автоматизированное принятие решений для ответственного подхода к использованию ИИ-систем и предполагаемого использования ИИ-системы.

Необходимость внедрения человеческого надзора может быть обоснована оценками воздействия, описанными в А.5. Персонал, участвующий в деятельности по человеческому надзору за ИИ-системой, должен быть проинформирован и понимать инструкции и другую документацию, связанную с ИИ-системой, а также обязанности, которые они выполняют для достижения целей человеческого надзора. При сообщении о проблемах с производительностью человеческий надзор может дополнить автоматизированный мониторинг.

Дополнительная информация

В приложении С приведены примеры целей по управлению рисками в организации, которые могут быть полезны при определении целей использования ИИ-системы.

В.9.4 Предполагаемое использование ИИ-системы

Меры управления

Организация должна гарантировать, что ИИ-система используется в соответствии с предполагаемым использованием ИИ-системы и сопровождающей ее документацией.

Руководство по внедрению

Систему ИИ должна быть развернута в соответствии с инструкциями и другой документацией, связанной с ИИ-системой (см. В.8.2). Для развертывания могут

потребоваться конкретные ресурсы для поддержки развертывания, включая необходимость обеспечения надлежащего контроля со стороны персонала (см. B.9.3). Для приемлемого использования и обеспечения корректной работы ИИ-системы необходимо обеспечить согласованность данных, используемых в работе ИИ-системы с документацией, связанной с ИИ-системой.

Следует контролировать работу ИИ-системы (см. B.6.2.6). В тех случаях, когда правильное развертывание ИИ-системы в соответствии с надлежащими инструкциями вызывает обеспокоенность в отношении воздействия на соответствующие заинтересованные стороны или юридические обязательства, организация должна сообщить о своих опасениях соответствующему персоналу внутри организации, а также любым сторонним поставщикам ИИ-системы.

Организации следует рассмотреть возможность ведения журналов событий или другой документации, связанной с развертыванием и эксплуатацией ИИ-системы, которую можно использовать для демонстрации того, что ИИ-система используется по назначению, или для информирования о проблемах, связанных с предполагаемым использованием ИИ-системы. Журналы событий и другую документацию следует хранить в течение определенного периода времени в соответствии с предполагаемым использованием ИИ-системы, политиками хранения данных, принятыми в организации и соответствующими юридическими обязательствами по хранению данных.

B.10 Взаимоотношения с третьими сторонами

B.10.1 Общие положения

Цель

Обеспечение гарантии, что при вовлечении третьих сторон на любой стадии жизненного цикла ИИ-системы организация понимает свои обязанности и остается подотчетной за них, имея при этом возможность оценивать и снижать риск зависимости от третьих сторон в выполнении возложенных на них обязанностей и позволяя третьим сторонам оценивать и устранять риски, связанные с использованием продуктов и услуг ИИ, разработанных организацией.

B.10.2 Распределение обязанностей

Меры управления

Организации следует обеспечить распределение обязанностей в рамках жизненного цикла ИИ-системы между организацией, ее партнерами, поставщиками, клиентами и третьими сторонами.

Руководство по внедрению

В жизненном цикле ИИ-системы обязанности могут быть разделены между сторонами, предоставляющими данные, сторонами, предоставляющими алгоритмы и модели, сторонами, разрабатывающими или использующими систему ИИ и несущими ответственность перед некоторыми или всеми заинтересованными сторонами. Организации следует документально оформить все стороны, участвующие в жизненном цикле ИИ-системы, и их роли, а также определить их обязанности и при необходимости, отобразить в контрактном соглашении.

При поставке ИИ-системы третьей стороне, организация должна обеспечить соблюдение ею ответственного подхода к разработке ИИ-систем. Меры управления и рекомендации представлены в B.6. Организация должна предоставить необходимую документацию (см. B.6.2.7 и B.8.2) по ИИ-системе соответствующим заинтересованным сторонам и третьей стороне, которой организация поставляет ИИ-системы.

В случаях, если обрабатываемые данные включают ПДн, обязанности обычно распределяются между обработчиками ПДн и операторами ПДн. Дополнительная информация об обработчиках ПДн и операторах ПДн содержится в [6]. При необходимости сохранить конфиденциальность ПДн, следует рассмотреть средства контроля, подобные представленным в [8]. Исходя из деятельности организации и деятельности ИИ-системы по обработке данных ПДн и роли организации в применении и разработке ИИ-систем на протяжении всего их жизненного цикла, можно считать, что организация выполняет роль обработчика ПДн (или совместного обработчика ПДн), оператора ПДн или и того, и другого.

B.10.3 Поставщики

Меры управления

Организация должна обеспечить соблюдение ее поставщиками ответственного подхода к разработке ИИ-систем.

Руководство по внедрению

Организация может идентифицировать риски, связанные с ее поставщиками продуктов и услуг, использующими ИИ-системы, и может принять решение об устранении рисков, потребовав от своих поставщиков внедрить и поддерживать в рабочем состоянии систему менеджмента ИИ или соответствующие меры управления, представленные в приложении А и, возможно, меры управления из других источников.

Если организация считает, что ИИ-система или компоненты ИИ-системы от поставщика не работают должным образом или могут привести к негативным последствиям для отдельных лиц и обществ, что не соответствует ответственному подходу к системам ИИ, принятому организацией, организация вправе потребовать от поставщика принятия корректирующих мер. Организация может принять решение о сотрудничестве с поставщиком для достижения этой цели.

Организация должна обеспечить предоставление поставщиком ИИ-системы надлежащей и адекватной документации, относящуюся к системе ИИ. См. B.6.2.7 и B.8.2.

B.10.4 Заказчики

Меры управления

При ответственном подходе к разработке ИИ-систем должны быть учтены ожидания и потребности клиентов организации.

Руководство по внедрению

Организация может определить риски, связанные с использованием ее продуктов и услуг ИИ заказчиком, а также принять решение об устранении выявленных рисков, путем предоставления соответствующей информации заказчику для его последующей обработки соответствующих рисков.

Ограничение возможной области применения ИИ-системы необходимо довести до сведения заказчика. См. B.6.2.7 и B.8.2.

Приложение С
(справочное)

Потенциальные организационные цели и источники рисков, связанные с применением ИИ

С.1 Общие положения

В настоящем приложении излагаются потенциальные организационные цели, источники рисков и описания, которые организация может учитывать при управлении рисками. Настоящее приложение не претендует на то, чтобы считаться исчерпывающим или применимым к каждой организации. Необходимо определить цели и источники риска, релевантные/применимые для/к организации. В стандарте [3] представлена более подробная информация относительно целей и источников риска, а также их взаимосвязи с управлением рисками. Оценка ИИ-систем, первоначальная, регулярная и когда это оправдано, предоставляет доказательства для оценки ИИ-системы в соответствии с целями организации.

С.2 Цели

С.2.1 Справедливость

Ненадлежащее применение ИИ-систем для автоматизированного принятия решений может привести необъективности по отношению к конкретным лицам или группам лиц.

С.2.2 Защита

В контексте ИИ и, в частности, в отношении ИИ-систем, основанных на подходах МО, следует рассматривать новые факторы защиты, выходящие за рамки классических проблем информационной и системной безопасности.

С.2.3 Безопасность

Безопасность понимается в данном контексте, как гарантия того, что система при определенных условиях не приведет к состоянию, при котором жизнь, здоровье, имущество или окружающая среда окажутся под угрозой.

С.2.4 Конфиденциальность

Неправильное использование или разглашение личных и конфиденциальных данных (например, медицинских записей) может привести к негативным

последствиям для субъектов данных. Таким образом, защита конфиденциальности стала серьезной проблемой при анализе больших данных и ИИ [1].

С.2.5 Робастность

В ИИ свойства робастности демонстрируют способность (или неспособность) системы обеспечивать сопоставимую производительность на новых данных с данными, на которых она была обучена, или данными типичных операций.

С.2.6 Прозрачность и объяснимость

Прозрачность относится как к характеристикам организации, эксплуатирующей ИИ-системы, так и к самим этим системам. Объяснимость относится к объяснениям важных факторов, влияющих на результаты работы ИИ-системы, которые предоставляются в форме, понятной и доступной для заинтересованных сторон.

С.2.7 Подотчетность

Использование ИИ может изменить существующие системы подотчетности. Там, где раньше люди несли бы ответственность за свои действия, теперь их действия могут поддерживаться ИИ-системой или основываться на ней.

С.2.8 Доступность

При применении ИИ-систем, необходимо учитывать их потенциальную способность изменять свое поведение, а также последствия, касающиеся доступности системы и потенциальных эффектов.

С.2.9 Удобство сопровождения

Удобство сопровождения — способность ИИ-системы изменяться для исправления дефектов и адаптироваться к новым требованиям.

С.2.10 Доступность и качество обучающих данных

Системам ИИ, основанным на МО, необходимы данные для обучения, валидации и тестирования, чтобы обучать и верифицировать системы на предмет предполагаемого поведения.

С.2.11 Опыт в области ИИ

Необходима группа преданных своему делу специалистов с междисциплинарными навыками и опытом в оценке, разработке и развертывании ИИ-систем.

С.3 Источники риска

С.3.1 Уровень автоматизации

Уровень автоматизации может оказывать влияние на различные проблемные области, такие как безопасность, справедливость или защита.

С.3.2 Отсутствие прозрачности и объяснимости

Неспособность предоставить соответствующую информацию заинтересованным сторонам может быть источником риска (например, с точки зрения надежности и подотчетности организации).

С.3.3 Сложность рабочей среды

Когда системы искусственного интеллекта работают в сложных условиях, где диапазон ситуаций широк, может возникнуть неопределенность в отношении производительности и, следовательно, источник риска (например, сложная среда автономного вождения).

С.3.4 Проблемы жизненного цикла системы

Источники риска могут появляться на протяжении всего жизненного цикла ИИ-системы (например, недостатки в проектировании, неадекватное развертывание, отсутствие технического обслуживания).

С.3.5 Проблемы с аппаратным обеспечением системы

Источники риска, связанные с аппаратным обеспечением, включают аппаратные ошибки, основанные на дефектных компонентах или переносом обученных моделей МО между разными системами.

С.3.6 Технологическая готовность

Источники риска могут быть связаны с менее зрелой технологией из-за неизвестных факторов, но также и с более зрелой технологией из-за технологической самоуспокоенности.

С.3.7 Источники риска, связанные с машинным обучением

Качество данных, используемых для МО, и процесс, используемый для сбора данных, также могут быть источником риска, поскольку это может повлиять на такие цели, как безопасность и робастность (например, из-за проблем с качеством данных или их искажения).

Приложение D
(справочное)

Использование системы менеджмента ИИ в разных доменах или секторах

D.1 Общие положения

Как указано в пункте 1, представленная система менеджмента применима к любой организации, предоставляющей или использующей продукты или услуги, применяющие ИИ-системы. Таким образом, система потенциально применима к большому разнообразию продуктов и услуг в различных секторах, на которые распространяются обязательства, передовая практика, ожидания или договорные обязательства по отношению к заинтересованным сторонам. Примерами секторов являются:

- здоровье;
- оборона;
- транспорт;
- финансы;
- трудоустройство;
- энергия.

Для ответственной разработки и использования ИИ-систем следует рассмотреть различные организационные задачи (см. возможные цели в приложении С). Настоящий стандарт содержит требования и рекомендации для рассмотрения с точки зрения конкретной технологии ИИ. Для нескольких потенциальных целей существуют общие или отраслевые стандарты системы менеджмента. Эти стандарты системы менеджмента обычно рассматривают цель с технологически нейтральной точки зрения, в то время как система менеджмента ИИ учитывает специфику технологии ИИ.

ИИ-системы состоят не только из компонентов, использующих технологию ИИ, но могут использовать самые разные технологии и компоненты. Таким образом, при ответственной разработке и использования ИИ-систем следует принимать во внимание не только специфику ИИ, но и систему в целом со всеми используемыми технологиями и компонентами. Даже в части, касающейся технологии ИИ, следует принимать во внимание другие не связанные с ИИ аспекты. Например, поскольку ИИ представляет собой технологию обработки информации, к нему применяются

общие соображения информационной безопасности, помимо факторов информационной безопасности, специфичных для ИИ. Такие цели, как безопасность, защита, конфиденциальность и воздействие на окружающую среду, должны управляться комплексно, а не отдельно для ИИ и других компонентов системы. Таким образом, для ответственной разработки и использования систем менеджмента ИИ важное значение имеет интеграция системы менеджмента ИИ с общими или отраслевыми стандартами систем управления по соответствующим темам.

D.2 Интеграция системы менеджмента ИИ с другими стандартами систем менеджмента

При предоставлении или использовании ИИ у организации могут быть цели или обязательства, связанные с аспектами, которые являются темами других стандартов системы менеджмента. К ним могут относиться, например, безопасность, конфиденциальность, качество и соответственно темы, описанные в [17], [8] и [18]. Стандарты системы менеджмента ИСО разработаны таким образом, чтобы облегчить их интегрированное использование.

При использовании или разработке ИИ потенциальными соответствующими общими стандартами системы менеджмента, но не ограничиваясь этим, являются:

- ИСО/МЭК 27001 [17]: В большинстве случаев безопасность является ключом к достижению целей организации с помощью ИИ-системы. Способы достижения цели обеспечения безопасности зависят от среды и собственных политик организации. Если организация определяет необходимость внедрения системы менеджмента ИИ и решения задач безопасности аналогичным тщательным и систематическим образом, она также может рассмотреть возможность внедрения системы менеджмента информационной безопасностью в соответствии со стандартом ИСО/МЭК 27001. Учитывая, что стандарт ИСО/МЭК 27001 и системы менеджмента ИИ имеют схожую структуру, их комплексное использование упрощается и приносит большую пользу организации. В таком случае способ внедрения мер управления, которые (частично) относятся к информационной безопасности в настоящем стандарте (см. B.6.1.2), может быть интегрирован с внедрением организацией стандарта ИСО/МЭК 27001.
- ИСО/МЭК 27701 [8]: Во многих средах и прикладных областях ПДн обрабатываются ИИ-системами. После этого организация может соблюдать

применимые обязательства в отношении конфиденциальности, а также свои собственные политики и цели. Аналогичным образом, что касается стандарта ИСО/МЭК 27001, организация может извлечь выгоду из интеграции стандарта ИСО/МЭК 27701 с системой управления ИИ. Цели и меры управления системы управления ИИ, связанные с конфиденциальностью (см. B.2.3 и B.5.4), могут быть интегрированы с внедрением организацией стандарта ИСО/МЭК 27701.

- ИСО 9001 [18]: Для многих организаций соответствие стандарту ИСО 9001 является ключевым признаком того, что они ориентированы на клиента и действительно заботятся о внутренней результативности. Независимая оценка соответствия стандарту ИСО 9001 облегчает ведение бизнеса во всех организациях и вселяет доверие клиентов к продуктам и услугам. Уровень доверия клиентов может быть значительно повышен, если система менеджмента ИИ внедряется совместно со стандартом ИСО 9001 при использовании технологий ИИ. Система менеджмента ИИ может дополнять требования стандарта ИСО 9001 (управление рисками, разработка программного обеспечения, согласованность цепочки поставок и т.д.), помогая организации достигать своих целей.

Помимо общих стандартов системы менеджмента, упомянутых выше, система менеджмента ИИ также может использоваться совместно с системой менеджмента, предназначенной для конкретного сектора. Например, и стандарт [23], и система менеджмента ИИ актуальны для ИИ-систем, которые используются для производства, подготовки и логистики продуктов питания. Другим примером является стандарт [19]. Внедрение системы менеджмента ИИ может поддерживать требования, относящиеся к программному обеспечению медицинских изделий [19] или требования других международных стандартов медицинского сектора, таких как [20]. Например, для программного обеспечения медицинских изделий может быть реализован подход к управлению рисками в соответствии со стандартом [30].

D.3 Схема сертификации

D.3.1 Оценка соответствия системы менеджмента в рамках сертификации продукции, процесса или услуги

В соответствии с [24] система менеджмента ИИ может быть предметом оценки соответствия третьими сторонами (сертификации).

Если ИИ-система, которой организация намеревается управлять с помощью системы менеджмента ИИ, является частью продукта, услуги или процесса, и эта

система должна пройти оценку соответствия третьей стороной, система менеджмента ИИ производителя, поставщика или импортера должна быть включена в процесс сертификации в соответствии с [26] и должна разработать надлежащую программу оценки соответствия согласно [21].

Для определения пригодности схем оценки соответствия (согласно [31], (4.6.3)) надлежащие программы оценки соответствия должны быть предварительно оценены органом по аккредитации. В этом случае орган по оценке соответствия, осуществляющий сертификацию продукции, процесса или услуги, может оценить систему менеджмента ИИ на основе настоящего стандарта в соответствии с [24] благодаря функциональному подходу к оценке соответствия, изложенному в [32] и в рамках области применения [26].

Необходимыми условиями для этого являются соблюдение органом по оценке соответствия сертификации продукции требований ИСО/МЭК 17065:2012 (6.2.1 и 6.2.2.1) и аккредитация в соответствии с областью применения настоящего стандарта.

На рисунке D.1 представлен функциональный подход к комплексной оценке соответствия на основе ИСО/МЭК 17065 в отношении ИИ.

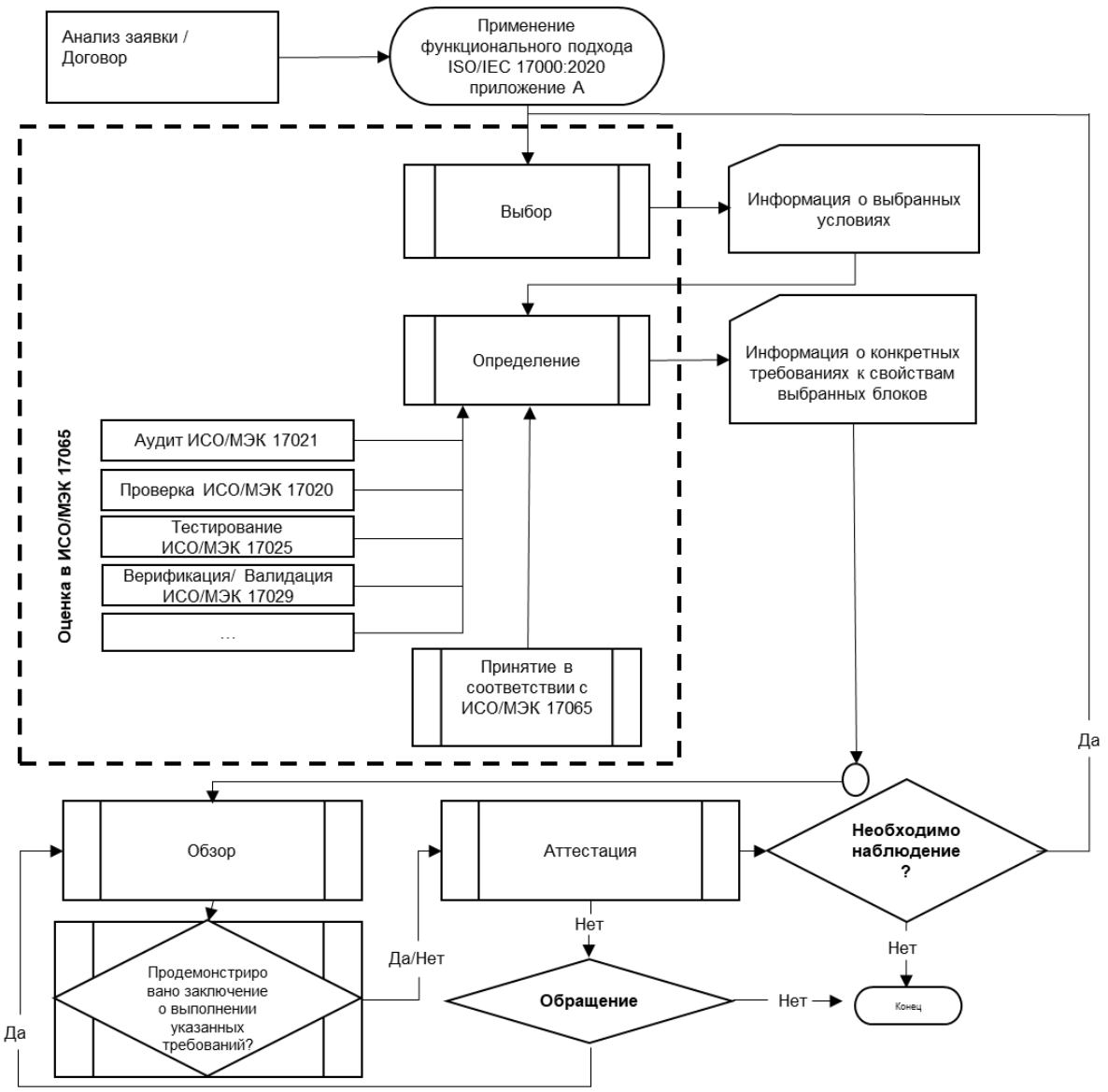

Рисунок D.1 — Функциональный подход к оценке соответствия ИИ

D.3.2 Признание существующих сертификатов систем менеджмента в процессах сертификации продукции

Организация, уже проводившая стороннюю оценку соответствия системы менеджмента в соответствии с [24], может предоставить сертификат, а также необходимые документы от органа по оценке в орган по оценке по сертификации продукции.

Орган по оценке сертификации продукции должен следовать процедуре в соответствии с [26] в отношении признания результатов оценки, связанных с завершенной сертификацией системы менеджмента, как указано в настоящем стандарте. Данная процедура позволяет избежать дублирования оценок соответствия.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 22989:2022	—	*
* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде стандартов.		

Библиография

[1]	ISO/IEC TR 24028:2020	Information techn ology — Artificial intelligence — Overview of trustworthiness in artificial intelligence
[2]	ISO/IEC 38507:2022	Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations
[3]	ISO/IEC 23894:2023	Information technology — Artificial intelligence — Guidance on risk management
[4]	ISO/IEC 25024:2015	Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaR E) — Measurement of data quality
[5]	ISO 37002:2021	Whistleblowing management systems — Guidelines
[6]	ISO/IEC 29100:2011	Information technology — Security techniques — Privacy framework
[7]	ISO 31000:2018	Risk management — Guidelines
[8]	ISO/IEC 27701:2019	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
[9]	ISO/IEC 19944-1:2020	Cloud computing and distributed platforms — Data flow, data categories and data use — Part 1: Fundamentals
[10]	ISO/IEC 23053:2022	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
[11]	ISO/IEC 5259 (all parts)	Data quality for analytics and Machine Learning (ML)

[12] ISO 8000-2:2020 Data quality — Part 2: Vocabulary

[13] ISO/IEC 25059:2023 Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality Model for AI systems

[14] ISO/IEC TR 24027:2021 Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making

[15] ISO/IEC TS 4213:2022 Information technology — Artificial Intelligence — Assessment of machine learning classification performance

[16] ISO/IEC TR 24029-1:2021 Artificial intelligence (AI) — Assessment of the robustness of neural networks — Part 1: Overview

[17] ISO/IEC 27001:2022 Information technology — Security techniques — Information security management systems — Requirements

[18] ISO 9001:2015 Quality management systems — Requirements

[19] ISO 13485:2016 Medical devices — Quality management systems — requirements for regulatory purposes

[20] IEC 62304:2006 Medical device software — Software life cycle processes

[21] ISO/IEC 17067:2013 Conformity assessment — Fundamentals for product certification and guidelines for product certification schemes

[22] ISO/IEC 5338 Information technology — Artificial intelligence — AI system life cycle process

[23] ISO 22000:2018 Food safety management systems — Requirements for any organization in the food chain

[24] ISO/IEC 17021-1:2015 Conformity assessment — Requirements for bodies providing audit and certification of management systems— Part 1: Requirements

[25] DDI Lifecycle 3.3, 2020-04-15. Data Documentation Initiative (DDI) Alliance. [viewed on 2022-02¬19]. Available at: https://ddialliance.org/Specification/DDI-Lifecycle/3.3/

[26] ISO/IEC 17065:2012 Conformity assessment — Requirements for bodies certifying products, processes and services

[27] ISO/IEC Guide 51:2014 Safety aspects — Guidelines for their inclusion in standards

[28] ISO/IEC TR 24368:2022 Information technology — Artificial intelligence — Overview of ethical and societal concerns

[29] ISO 9241-210:2019 Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems

[30] ISO 14971:2019 Medical devices — Application of risk management to medical devices

[31] ISO/IEC 17011:2017 Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies

[32] ISO/IEC 17000:2020 Conformity assessment — Vocabulary and general principles

[33] ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary

[34] IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety related systems — Part 1: General requirements

УДК 004.8:006.354 ОКС 35.020

Ключевые слова: ИИ-система, система менеджмента, цель, риск, процесс, документированная информация, требование, постоянное улучшение, соответствие, несоответствие, аудит.

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