

Министерство науки и высшего образования Республики Казахстан
Павлодарский педагогический университет имени Әлкей Марғұлан



Утверждаю
Председатель Правления - Ректор
Е. Әмірбекұлы
24.04. 2026 г.

**СТАНДАРТ
«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОБРАЗОВАНИИ.
ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ОБУЧЕНИЯ.
ОБЩИЕ ТРЕБОВАНИЯ»**

Рассмотрено и утверждено
на заседании
Ученого совета
23.04. 2026 протокол № 8

Павлодар, 2026

Стандарт «Искусственный интеллект в образовании. Интеллектуальные системы обучения. Общие требования»» разработано в рамках программы ИРН BR28712263 «Создание комплексной научно-инновационной системы подготовки педагогических кадров по развитию одаренных детей Казахстана»

РАБОЧАЯ ГРУППА:

Руководитель рабочей группы – к.п.н., профессор А.Ж. Асаинова

Члены рабочей группы:

PhD, профессор Д.Б. Абыкенова

к.п.н., ассоциированный профессор Г.М.Абильдинова

магистр информатики, Р.А. Ельтинова

М.М. Рахимбаев

Ж.Т. Аубакирова

Содержание

1 Область применения	4
2 Актуальность разработки стандарта	4
3 Цель разработки стандарта	6
4 Объект и предмет стандартизации	6
5 Нормативная основа разработки	6
6 Термины и определения	7
7 Задачи стандарта	10
8 Потенциальные пользователи стандарта	10
9 Основные требования, которые устанавливает стандарт	11
10 Ожидаемые результаты стандарта	12
11 Практическая значимость стандарта	12
12 Классификация интеллектуальных систем обучения	12
13 Общие требования к интеллектуальным системам обучения	15
14 Требования к жизненному циклу интеллектуальной системы обучения	19
15 Требования к техническому заданию на разработку интеллектуальной системы обучения	24
16 Требования к данным обучающихся	27
17 Требования к информированию и согласию	30
18 Требования к ИИ-модулям	33
19 Требования к генеративному ИИ	35
20 Требования к человеческому контролю	38
21 Требования к прозрачности и объяснимости	41
22 Требования к недопущению дискриминации и стигматизации	43
23 Требования к безопасности	46
24 Требования к обезличиванию и псевдонимизации	50
25 Требования к журналированию и аудиту	52
26 Требования к качеству образовательного контента	55
27 Требования к интерфейсам пользователей	59
28 Требования к тестированию	62
29 Требования к апробации	66
30 Требования к мониторингу	68
31 Требования к управлению рисками	71
32 Требования к документации интеллектуальной системы обучения	73
33 Требования к оценке качества интеллектуальной системы обучения	75
34 Порядок пересмотра стандарта	77
35 Заключительные положения	78

1 Область применения

Настоящий стандарт устанавливает общие требования к разработке, внедрению, применению, оценке, мониторингу и сопровождению интеллектуальных систем обучения, используемых в организациях образования Республики Казахстан.

Объект стандартизации: интеллектуальные системы обучения (далее ИСО), применяемые в организациях образования Республики Казахстан.

Предмет стандартизации: требования к разработке, внедрению, применению, мониторингу, безопасности, этической экспертизе и оценке качества ИСО.

Цель стандарта: установить единые требования к интеллектуальным системам обучения, чтобы они были педагогически обоснованными, безопасными, прозрачными, проверяемыми, недискриминационными и применялись с человеческим контролем.

Настоящий стандарт распространяется на ИСО, применяющие технологии искусственного интеллекта, машинного обучения, генеративного искусственного интеллекта, образовательной аналитики, адаптивного обучения, автоматизированной оценки, интеллектуальной диагностики и формирования индивидуальных образовательных траекторий.

Настоящий стандарт предназначен для применения:

1. организациями образования;
2. разработчиками образовательных цифровых платформ;
3. поставщиками ИИ-решений для образования;
4. научными и исследовательскими организациями;
5. экспертными организациями;
6. уполномоченными органами в сфере образования, науки, цифрового развития и защиты данных;
7. организациями, проводящими апробацию, внедрение или оценку образовательных ИИ-систем.

Настоящий стандарт не заменяет требования законодательства Республики Казахстан в сфере образования, персональных данных, информатизации, искусственного интеллекта, цифровых данных и защиты прав несовершеннолетних, а конкретизирует их применительно к интеллектуальным системам обучения.

2 Актуальность разработки стандарта

В условиях цифровой трансформации образования и активного внедрения технологий искусственного интеллекта в учебный процесс возрастает необходимость формирования единых требований к интеллектуальным системам обучения. Такие системы могут использоваться для диагностики образовательных достижений, построения индивидуальных образовательных траекторий, генерации учебного контента,

автоматизированной обратной связи, образовательной аналитики, поддержки педагогических решений и сопровождения обучающихся.

Вместе с тем ИСО обрабатывают значительный объем данных обучающихся, включая образовательные, диагностические, поведенческие, психолого-педагогические и прогностические данные. Неправильное использование таких данных может привести к нарушению конфиденциальности, ошибочным рекомендациям, алгоритмической дискриминации, стигматизации обучающихся и снижению доверия к цифровым образовательным технологиям.

В Республике Казахстан действуют нормативные правовые акты и стандарты в сфере образования, персональных данных, информатизации, цифровой трансформации и искусственного интеллекта. Однако в настоящее время отсутствует отдельный национальный стандарт, устанавливающий специальные требования к ИСО как к образовательным ИИ-системам. В связи с этим возникает необходимость разработки национального стандарта СТ РК «Искусственный интеллект в образовании. Интеллектуальные системы обучения. Общие требования».

На сегодняшний день в образовательной сфере отсутствует единый документ, который системно определяет:

1. что считается ИСО;
2. какие виды ИСО могут применяться в образовании;
3. какие требования предъявляются к разработке ИСО;
4. какие данные обучающихся могут обрабатываться;
5. как должны защищаться персональные и чувствительные данные;
6. как должны проверяться ИИ-рекомендации;
7. какие решения нельзя принимать полностью автоматически;
8. как предотвращать дискриминацию и стигматизацию обучающихся;
9. как тестировать, апробировать и оценивать ИСО;
10. как проводить мониторинг и аудит образовательных ИИ-систем.

Отсутствие таких требований может привести к следующим рискам:

- неправомерная обработка данных обучающихся;
- использование ИИ без информирования родителей и обучающихся;
- принятие решений без участия педагога или специалиста;
- ошибочные рекомендации;
- снижение доверия к образовательным ИИ-системам;
- дискриминация отдельных групп обучающихся;
- публикация или утечка чувствительных данных;
- внедрение некачественного или педагогически необоснованного ИИ-контента.

Данный стандарт направлен на устранение указанных пробелов.

3 Цель разработки стандарта

Целью разработки стандарта является установление единых национальных требований к разработке, внедрению, применению, оценке, мониторингу и сопровождению интеллектуальных систем обучения в организациях образования Республики Казахстан.

Стандарт должен обеспечить:

1. педагогическую обоснованность ИСО;
2. защиту персональных данных обучающихся;
3. прозрачность и объяснимость ИИ-рекомендаций;
4. обязательный человеческий контроль значимых решений;
5. недопущение алгоритмической дискриминации;
6. безопасность цифровой образовательной среды;
7. качество образовательного контента, создаваемого или рекомендуемого ИИ;
8. единые подходы к апробации и мониторингу образовательных ИИ-систем.

4 Объект и предмет стандартизации

Объектом стандартизации являются ИСО, применяемые в организациях дошкольного, среднего, технического и профессионального, послесреднего, высшего и дополнительного образования Республики Казахстан.

Предметом стандартизации являются требования к:

1. жизненному циклу ИСО;
2. техническому заданию и проектной документации;
3. обработке данных обучающихся;
4. ИИ-модулям и генеративному ИИ;
5. человеческому контролю ИИ-рекомендаций;
6. прозрачности, объяснимости и проверяемости;
7. безопасности и защите данных;
8. обезличиванию и псевдонимизации;
9. недопущению дискриминации и стигматизации;
10. качеству образовательного контента;
11. тестированию, апробации, мониторингу и оценке качества.

5 Нормативная основа разработки

При разработке стандарта целесообразно учитывать:

1. Закон Республики Казахстан от 27 июля 2007 года № 319-III «Об образовании». – Текст: электронный // Информационно-правовая система «Әділет». – URL: <https://adilet.zan.kz/rus/docs/Z070000319>

2. Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите». – Текст: электронный // Информационно-правовая система «Әділет». – URL: <https://adilet.zan.kz/rus/docs/Z1300000094>
3. Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII ЗРК «Об искусственном интеллекте». – Текст: электронный // Информационно-правовая система «Әділет». – URL: <https://adilet.zan.kz/rus/docs/Z2500000230>
4. Кодекс Республики Казахстан от 9 января 2026 года № 255-VIII ЗРК «Цифровой кодекс Республики Казахстан». – Текст: электронный // Информационно-правовая система «Әділет». – URL: <https://adilet.zan.kz/rus/docs/K2600000255>
5. Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации». – Текст: электронный // Информационно-правовая система «Әділет». – URL: <https://adilet.zan.kz/rus/docs/Z1500000418>
6. Закон Республики Казахстан от 5 октября 2018 года № 183-VI ЗРК «О стандартизации». – Текст: электронный // Информационно-правовая система «Әділет». – URL: <https://adilet.zan.kz/rus/docs/Z1800000183>
7. СТ РК 1.2-2021 «Национальная система стандартизации Республики Казахстан. Порядок разработки документов по стандартизации». – Текст: официальный стандарт Республики Казахстан.
8. СТ РК ISO/IEC 42001 «Информационные технологии. Искусственный интеллект. Система менеджмента». – Текст: национальный стандарт Республики Казахстан.
9. СТ РК ISO/IEC 5338 «Информационные технологии. Искусственный интеллект. Процессы жизненного цикла систем искусственного интеллекта». – Текст: национальный стандарт Республики Казахстан.
10. СТ РК ISO/IEC 5339 «Информационные технологии. Искусственный интеллект. Руководство для приложений искусственного интеллекта». – Текст: национальный стандарт Республики Казахстан.
11. СТ РК ISO/IEC 23894 «Информационные технологии. Искусственный интеллект. Руководство по управлению рисками». – Текст: национальный стандарт Республики Казахстан.
12. СТ РК ISO/IEC 19796-1 «Информационные технологии. Обучение, образование и подготовка. Менеджмент качества, обеспечение качества и метрика». – Текст: национальный стандарт Республики Казахстан.
13. СТ РК ISO/IEC 25040 «Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения». – Текст: национальный стандарт Республики Казахстан.
14. Recommendation on the Ethics of Artificial Intelligence. – Paris: UNESCO, 2021. – URL: <https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence>
15. OECD Principles on Artificial Intelligence. – Paris: OECD, 2019. – URL: <https://oecd.ai/en/ai-principles>

6 Термины и определения

В настоящем стандарте применяются следующие термины и определения.

Искусственный интеллект - совокупность технологий, методов и программных решений, позволяющих информационной системе выполнять задачи, требующие анализа данных, распознавания закономерностей, генерации содержания, прогнозирования, классификации, принятия рекомендаций или имитации отдельных интеллектуальных функций человека.

Интеллектуальная система обучения - цифровая образовательная система, использующая методы искусственного интеллекта, машинного обучения, генеративного искусственного интеллекта, образовательной аналитики или автоматизированной обработки данных для поддержки обучения, диагностики, адаптации содержания, оценки, прогнозирования, генерации учебного контента и формирования рекомендаций.

Образовательная аналитика - сбор, обработка, анализ и интерпретация образовательных данных обучающихся с целью поддержки образовательного процесса, повышения качества обучения, выявления затруднений, построения индивидуальных траекторий и принятия педагогических решений.

Генеративный искусственный интеллект в образовании - технология искусственного интеллекта, способная создавать образовательный контент, включая тексты, задания, тесты, объяснения, обратную связь, рекомендации, изображения, сценарии, симуляции и иные учебные материалы.

ИИ-модуль - функциональный компонент интеллектуальной системы обучения, использующий методы искусственного интеллекта для анализа данных, генерации контента, прогнозирования, классификации, оценки, адаптации обучения или формирования рекомендаций.

ИИ-рекомендация - вывод, прогноз, предложение, оценка или рекомендация, сформированные интеллектуальной системой обучения на основе анализа данных обучающегося, группы обучающихся, образовательного контента или образовательного процесса.

Значимая ИИ-рекомендация - ИИ-рекомендация, которая может повлиять на образовательную траекторию, оценивание, диагностику, психолого-педагогическое сопровождение, профориентацию, доступ к образовательным возможностям, самооценку или образовательное благополучие обучающегося.

Человеческий контроль - обязательная проверка, интерпретация, подтверждение, корректировка или отклонение значимых ИИ-рекомендаций педагогом, психологом, экспертом, исследователем или иным уполномоченным специалистом.

Обучающийся как субъект данных - физическое лицо, обучающееся в организации образования, данные которого собираются, обрабатываются, анализируются или используются интеллектуальной системой обучения.

Персональные данные обучающегося - сведения, относящиеся к определенному или определяемому обучающемуся, включая идентификационные, образовательные, диагностические, поведенческие, психолого-педагогические, технические и иные данные.

Чувствительные образовательные данные - данные обучающегося, неправильная обработка или интерпретация которых может привести к нарушению конфиденциальности, стигматизации, дискриминации, психологическому вреду или ограничению образовательных возможностей. К таким данным относятся диагностические, психолого-педагогические, когнитивные, прогностические данные, сведения об особых образовательных потребностях и данные, связанные с ИИ-рекомендациями высокого уровня влияния.

Обезличивание данных - действия, в результате которых невозможно без использования дополнительной информации определить принадлежность данных конкретному обучающемуся.

Псевдонимизация данных - замена прямых идентификаторов обучающегося кодом или условным обозначением при сохранении отдельного ключа соответствия, позволяющего при необходимости восстановить связь между кодом и конкретным субъектом данных.

Алгоритмическая дискриминация - ситуация, при которой интеллектуальная система обучения создает, усиливает или воспроизводит необоснованное неравенство между обучающимися по языковому, социальному, территориальному, гендерному, культурному, физическому, психологическому, цифровому или иному признаку.

Стигматизация обучающегося - формирование, закрепление или распространение негативного ярлыка, вывода или характеристики обучающегося, способных снизить его самооценку, ограничить образовательные возможности или повлиять на отношение к нему со стороны педагогов, родителей или сверстников.

Жизненный цикл интеллектуальной системы обучения - совокупность этапов создания и использования интеллектуальной системы обучения, включая анализ потребностей, формирование требований, проектирование, разработку, тестирование, этическую экспертизу, пилотную апробацию, внедрение, мониторинг, сопровождение, обновление и вывод из эксплуатации.

Этическая экспертиза ИСО - оценка интеллектуальной системы обучения с точки зрения соблюдения прав обучающихся, защиты данных, прозрачности, человеческого контроля, недопущения дискриминации, безопасности и педагогической обоснованности.

Мониторинг ИСО - регулярное наблюдение, проверка и анализ работы интеллектуальной системы обучения, качества ее рекомендаций, безопасности данных, обращений пользователей, инцидентов и рисков.

Инцидент - событие, которое привело или могло привести к нарушению конфиденциальности, целостности, доступности, законности, этичности или

безопасности обработки данных обучающихся либо к формированию ошибочной, дискриминационной или вредной ИИ-рекомендации.

Педагогическая обоснованность ИСО - соответствие функций, данных, рекомендаций, контента и сценариев использования интеллектуальной системы обучения образовательным целям, возрастным особенностям обучающихся, методическим требованиям и задачам образовательного процесса.

7 Задачи стандарта

Для достижения цели стандарт должен решить следующие задачи:

1. определить понятие ИСО;
2. установить классификацию ИСО по функциональному назначению и уровню риска;
3. определить требования к жизненному циклу ИСО;
4. установить требования к техническому заданию на разработку ИСО;
5. определить требования к ИИ-модулям и генеративному ИИ;
6. установить требования к обработке данных обучающихся;
7. определить требования к информированию и согласию;
8. установить требования к безопасности и защите данных;
9. закрепить требования к человеческому контролю ИИ-рекомендаций;
10. определить требования к прозрачности и объяснимости;
11. установить требования к недопущению дискриминации;
12. определить требования к качеству образовательного контента;
13. установить требования к интерфейсам пользователей;
14. определить требования к тестированию, апробации и мониторингу;
15. установить требования к документации ИСО;
16. определить показатели оценки качества интеллектуальной системы обучения.

8 Потенциальные пользователи стандарта

Пользователями стандарта могут быть:

1. Министерство просвещения Республики Казахстан;
2. Министерство науки и высшего образования Республики Казахстан;
3. Министерство искусственного интеллекта и цифрового развития Республики Казахстан;
4. уполномоченный орган в сфере цифрового развития и искусственного интеллекта;
5. Национальный орган по стандартизации;
6. организации образования;
7. разработчики цифровых образовательных платформ;
8. поставщики ИИ-решений;
9. научные и исследовательские организации;

10. педагогические университеты;
11. школы, колледжи и вузы;
12. эксперты по цифровому образованию;
13. специалисты по защите данных;
14. аккредитационные и экспертные организации;
15. педагогические работники;
16. психологи и методисты.

9 Основные требования, которые устанавливает стандарт

Стандарт устанавливает минимальные обязательные требования к ИСО.

9.1 Требования к педагогической обоснованности

ИСО должна разрабатываться для решения конкретной образовательной задачи. Каждая функция системы должна иметь педагогическое, методическое или исследовательское обоснование.

9.2 Требования к данным

ИСО должна собирать только те данные обучающихся, которые необходимы для заявленной цели. Для каждой категории данных должны быть определены цель обработки, уровень чувствительности, доступ, срок хранения и порядок удаления.

9.3 Требования к ИИ-рекомендациям

ИИ-рекомендации должны иметь вспомогательный характер. Значимые рекомендации, влияющие на образовательную траекторию, диагностику, оценивание или сопровождение обучающегося, должны проверяться человеком.

9.4 Требования к генеративному ИИ

Контент, созданный генеративным ИИ, должен проходить проверку педагогом или экспертом перед использованием. Генеративный ИИ не должен применяться для автоматического вынесения психологических, диагностических или ограничительных решений.

9.5 Требования к безопасности

ИСО должна обеспечивать аутентификацию пользователей, разграничение доступа, журналирование действий, защиту данных, контроль экспорта и реагирование на инциденты.

9.6 Требования к прозрачности

Пользователи должны быть информированы о том, что в системе используется ИИ, какие данные обрабатываются, какие рекомендации формируются и кто несет ответственность за их применение.

9.7 Требования к недискриминации

ИСО не должна создавать или усиливать неравенство между обучающимися. Результаты системы не должны использоваться для стигматизации, публичного ранжирования или ограничения образовательных возможностей.

9.8 Требования к мониторингу

Работа ИСО должна регулярно проверяться по показателям безопасности, качества рекомендаций, соблюдения доступа, жалоб, инцидентов и рисков дискриминации.

10 Ожидаемые результаты стандарта

Разработка и последующее внедрение стандарта позволяет:

1. сформировать единые требования к ИСО в Республике Казахстан;
2. повысить безопасность использования ИИ в образовании;
3. обеспечить защиту данных обучающихся;
4. повысить качество образовательных ИИ-систем;
5. снизить риски алгоритмической дискриминации;
6. обеспечить человеческий контроль значимых решений;
7. создать основу для экспертизы, сертификации и мониторинга ИСО;
8. повысить доверие педагогов, родителей и обучающихся к образовательному ИИ;
9. поддержать разработчиков при создании ИИ-решений для образования;
10. усилить национальную систему цифрового образования.

11 Практическая значимость стандарта

Практическая значимость стандарта заключается в использовании:

1. при разработке технических заданий на образовательные ИИ-системы;
2. при закупке и внедрении цифровых образовательных платформ;
3. при экспертизе ИИ-решений для школ, колледжей и вузов;
4. при разработке локальных актов организаций образования;
5. при подготовке педагогов к работе с ИИ;
6. при проведении научных исследований;
7. при оценке безопасности и качества ИСО;
8. при формировании национальной политики по ИИ в образовании.

12 Классификация ИСО

12.1 Общие положения классификации

12.1.1 ИСО классифицируются по функциональному назначению, уровню влияния на обучающегося, типу используемых технологий искусственного интеллекта и уровню риска.

12.1.2 Классификация применяется для определения требований к разработке, тестированию, апробации, человеческому контролю, защите данных и мониторингу ИСО.

12.2 Классификация по функциональному назначению

Тип ИСО	Назначение	Примеры функций
Диагностические ИСО	выявление уровня знаний, навыков, способностей, образовательных затруднений	тестирование, диагностика, анализ ошибок
Адаптивные ИСО	подбор содержания, темпа, сложности и последовательности обучения	индивидуальные задания, адаптивный маршрут
Рекомендательные ИСО	формирование образовательных, методических или профорientационных рекомендаций	рекомендации тем, курсов, заданий, траекторий
Генеративные ИСО	создание учебного контента с помощью генеративного ИИ	задания, объяснения, тесты, подсказки
Аналитические ИСО	анализ образовательных данных и построение отчетов	дашборды, прогнозы, визуализация прогресса
Оценочные ИСО	автоматизированная или полуавтоматизированная проверка заданий	проверка тестов, эссе, проектов, практических работ
Коммуникационные ИСО	поддержка взаимодействия с обучающимся через интеллектуального ассистента	чат-бот, тьютор, виртуальный помощник
Комбинированные ИСО	объединение нескольких функций	адаптивная платформа с диагностикой, аналитикой и генерацией контента

12.3 Классификация по уровню влияния на обучающегося

Уровень влияния	Характеристика	Примеры
Низкий	система предоставляет вспомогательный контент без влияния на оценивание, траекторию или решения	учебная подсказка, объяснение темы

Средний	система рекомендует задания, темы, уровень сложности или дополнительные материалы	подбор заданий, рекомендации по повторению темы
Высокий	система влияет на образовательную траекторию, диагностику, оценивание, участие в программах или сопровождение	рекомендация индивидуального маршрута, вывод о затруднениях
Критический	система затрагивает чувствительные данные, психолого-педагогические выводы, ограничения возможностей или значимые решения	вывод об одаренности, психологический риск, рекомендация ограничения участия

12.4 Классификация по типу используемой технологии

Тип технологии	Описание
Системы машинного обучения	используют модели, обученные на данных, для прогнозирования, классификации или рекомендаций
Системы генеративного ИИ	создают текст, задания, объяснения, обратную связь или иные материалы
Системы образовательной аналитики	анализируют образовательные данные и формируют отчеты
Системы обработки естественного языка	анализируют или генерируют текстовые ответы, диалоги, объяснения
Экспертно-рекомендательные системы	используют правила, модели или экспертные знания для формирования рекомендаций
Гибридные системы	объединяют несколько технологий

12.5 Классификация по уровню риска

Уровень риска	Описание	Требования
Низкий	система не обрабатывает чувствительные данные и не влияет на значимые решения	базовая проверка качества и безопасности
Средний	система использует образовательные данные и формирует рекомендации по обучению	тестирование, журналирование, педагогическая проверка

Высокий	система формирует рекомендации, влияющие на траекторию, оценивание или сопровождение	этическая экспертиза, человеческий контроль, мониторинг
Критический	система работает с чувствительными данными или может повлиять на права, самооценку, доступ к возможностям	обязательная экспертиза, ограниченная апробация, усиленная защита данных, комиссия проверка

12.5.1 ИСО высокого и критического уровня риска подлежат обязательной этической экспертизе до внедрения.

12.5.2 Для ИСО высокого и критического уровня риска обязательны:

1. документированное описание ИИ-модулей;
2. оценка рисков;
3. проверка качества данных;
4. информирование пользователей;
5. человеческий контроль значимых рекомендаций;
6. журналирование действий;
7. порядок рассмотрения жалоб и инцидентов;
8. регулярный мониторинг.

13 Общие требования к ИСО

13.1 Общие положения

13.1.1 ИСО должна разрабатываться, внедряться и применяться с учетом образовательных целей, прав обучающихся, требований безопасности, защиты данных, педагогической обоснованности и недопущения дискриминации.

13.1.2 ИСО должна использоваться как инструмент поддержки обучающегося, педагога, психолога, родителя, исследователя или организации образования, но не как механизм автоматического замещения педагогического решения.

13.1.3 ИСО не должна применяться для автоматического ограничения образовательных возможностей обучающегося, публичного ранжирования, стигматизации или принятия окончательных решений без участия человека.

13.2 Требование педагогической обоснованности

13.2.1 Каждая функция ИСО должна иметь педагогическое, методическое, диагностическое или исследовательское обоснование.

13.2.2 ИСО должна соответствовать:

1. возрастным особенностям обучающихся;
2. уровню образования;
3. языку обучения;

4. образовательным целям;
5. содержанию образовательной программы;
6. методическим требованиям;
7. принципам инклюзивности;
8. требованиям психологической безопасности.

13.2.3 Использование ИСО без ясной образовательной цели не допускается.

13.3 Требование законности и целевого использования данных

13.3.1 Обработка данных обучающихся в ИСО должна осуществляться на законном основании.

13.3.2 Данные обучающихся должны использоваться только для заранее определенных, правомерных и педагогически обоснованных целей.

13.3.3 Сбор данных «на всякий случай» или для неопределенных будущих целей не допускается.

13.3.4 Использование данных обучающихся для коммерческого профилирования, дискриминационного отбора или скрытого ранжирования не допускается.

13.4 Требование минимизации данных

13.4.1 ИСО должна собирать и обрабатывать только те данные, которые необходимы для выполнения заявленных функций.

13.4.2 Для каждой категории данных должны быть определены:

1. цель сбора;
2. источник данных;
3. уровень чувствительности;
4. срок хранения;
5. порядок доступа;
6. порядок обезличивания;
7. порядок удаления.

13.4.3 Чувствительные данные должны обрабатываться только при наличии обоснованной необходимости и усиленных мер защиты.

13.5 Требование безопасности

13.5.1 ИСО должна обеспечивать защиту данных обучающихся от несанкционированного доступа, утечки, потери, искажения, неправомерной передачи и использования не по назначению.

13.5.2 В ИСО должны быть предусмотрены:

1. аутентификация пользователей;
2. разграничение прав доступа;
3. журналирование действий;

4. защита учетных записей;
5. контроль экспорта данных;
6. резервное копирование;
7. ограничение доступа к чувствительным данным;
8. порядок реагирования на инциденты.

13.6 Требование прозрачности

13.6.1 Пользователи ИСО должны быть проинформированы о назначении системы, ее функциях, используемых данных, применении ИИ и роли человека в проверке рекомендаций.

13.6.2 Обучающийся и/или его законный представитель должны получать понятную информацию о том:

1. какие данные обрабатываются;
2. для чего используются данные;
3. какие рекомендации может формировать система;
4. кто имеет доступ к данным;
5. кто проверяет значимые рекомендации;
6. как можно задать вопрос, подать обращение или оспорить рекомендацию.

13.7 Требование объяснимости

13.7.1 Значимые ИИ-рекомендации должны быть объяснимы для педагога, обучающегося, родителя или законного представителя в доступной форме.

13.7.2 Объяснение должно включать:

1. какую рекомендацию сформировала система;
2. на каких типах данных она основана;
3. является ли рекомендация обязательной;
4. кто ее проверил;
5. какие альтернативы возможны;
6. как можно пересмотреть рекомендацию.

13.7.3 Не допускается представление ИИ-рекомендации как окончательного и безальтернативного решения.

13.8 Требование человеческого контроля

13.8.1 Значимые ИИ-рекомендации должны проходить проверку человеком.

13.8.2 К значимым рекомендациям относятся рекомендации, влияющие на:

1. образовательную траекторию;
2. оценивание;

3. диагностику способностей;
4. психолого-педагогическое сопровождение;
5. профориентацию;
6. участие в конкурсах, олимпиадах, специальных программах;
7. доступ к образовательным возможностям;
8. самооценку и психологическое благополучие обучающегося.

13.8.3 Окончательное решение по значимой рекомендации принимает уполномоченный специалист, а не ИИ-система.

13.9 Требование недопущения дискриминации

13.9.1 ИСО не должна создавать, усиливать или воспроизводить дискриминацию обучающихся.

13.9.2 При разработке и применении ИСО должны учитываться возможные различия обучающихся по:

1. языку обучения;
2. месту проживания;
3. типу организации образования;
4. социальному положению;
5. доступу к цифровой инфраструктуре;
6. полу;
7. национальности;
8. состоянию здоровья;
9. особым образовательным потребностям;
10. уровню предварительной подготовки.

13.9.3 Результаты ИСО не должны использоваться для навешивания ярлыков, публичного ранжирования, стигматизации или ограничения образовательных возможностей.

13.10 Требование качества образовательного контента

13.10.1 Образовательный контент, используемый или создаваемый ИСО, должен быть достоверным, педагогически корректным, соответствующим возрасту и образовательным целям.

13.10.2 Контент, созданный генеративным ИИ, должен проходить проверку человеком перед официальным использованием.

13.10.3 Не допускается использование контента, который содержит:

1. фактические ошибки;
2. дискриминационные формулировки;
3. психологически вредные сообщения;
4. непроверенные сведения;
5. материалы, не соответствующие возрасту обучающихся;
6. нарушения академической или исследовательской добросовестности.

13.11 Требование проверяемости

13.11.1 ИСО должна обеспечивать возможность проверки действий пользователей, обработки данных, формирования ИИ-рекомендаций и результатов человеческой проверки.

13.11.2 Для этого в системе должны быть предусмотрены:

1. журналы действий;
2. фиксация изменений данных;
3. фиксация экспорта данных;
4. фиксация проверки ИИ-рекомендаций;
5. журнал инцидентов;
6. отчеты мониторинга.

13.12 Требование управления рисками

13.12.1 На всех этапах жизненного цикла ИСО должны выявляться, оцениваться и снижаться риски.

13.12.2 К основным рискам относятся:

1. утечка данных;
2. ошибочные рекомендации;
3. дискриминация;
4. стигматизация;
5. непрозрачность решений;
6. избыточный сбор данных;
7. низкое качество образовательного контента;
8. несанкционированный доступ;
9. отсутствие человеческого контроля;
10. психологический вред обучающемуся.

13.12.3 Для ИСО высокого и критического уровня риска управление рисками является обязательным условием внедрения.

14 Требования к жизненному циклу интеллектуальной системы обучения

14.1 Общие положения

14.1.1 Разработка, внедрение и применение ИСО должны осуществляться в рамках управляемого жизненного цикла.

14.1.2 Жизненный цикл ИСО должен включать последовательные этапы: анализ потребностей, формирование требований, проектирование, разработку, тестирование, этическую экспертизу, пилотную апробацию, внедрение, мониторинг, сопровождение, обновление и вывод из эксплуатации.

14.1.3 На каждом этапе жизненного цикла должны быть определены:

1. цели этапа;
2. ответственные лица;
3. используемые данные;
4. потенциальные риски;
5. меры защиты данных;
6. критерии завершения этапа;
7. документы, подтверждающие выполнение этапа.

14.1.4 Для ИСО высокого и критического уровня риска жизненный цикл должен быть документирован в обязательном порядке.

14.2 Этап 1. Анализ потребностей

14.2.1 На этапе анализа потребностей определяется образовательная, педагогическая, диагностическая или исследовательская проблема, для решения которой предполагается разработка ИСО.

14.2.2 Анализ потребностей должен включать:

1. описание образовательной проблемы;
2. характеристику целевой группы обучающихся;
3. описание пользователей системы;
4. анализ существующих образовательных решений;
5. обоснование необходимости применения искусственного интеллекта;
6. предварительную оценку рисков;
7. определение ожидаемых результатов.

14.2.3 Разработка ИСО не допускается, если ее функции не имеют педагогического, методического или исследовательского обоснования.

14.3 Этап 2. Формирование требований

14.3.1 На этапе формирования требований разрабатывается техническое задание на ИСО.

14.3.2 Требования должны определять:

1. функциональные возможности системы;
2. категории пользователей;
3. категории обрабатываемых данных;
4. требования к ИИ-модулям;
5. требования к безопасности;
6. требования к интерфейсам;
7. требования к человеческому контролю;
8. требования к прозрачности и объяснимости;
9. требования к тестированию;
10. требования к мониторингу и сопровождению.

14.3.3 Требования должны быть согласованы с педагогическими, техническими, правовыми и этическими аспектами применения ИСО.

14.4 Этап 3. Проектирование

14.4.1 На этапе проектирования формируется архитектура ИСО.

14.4.2 Проектирование должно предусматривать:

1. структуру модулей системы;
2. модель данных;
3. роли пользователей;
4. уровни доступа;
5. сценарии использования;
6. алгоритмы обработки данных;
7. описание ИИ-модулей;
8. механизм человеческой проверки ИИ-рекомендаций;
9. механизм журналирования;
10. механизм обезличивания и псевдонимизации данных;
11. порядок реагирования на инциденты.

14.4.3 При проектировании должен применяться принцип безопасности и защиты данных по умолчанию.

14.4.4 Архитектура ИСО должна позволять отключать или ограничивать отдельные ИИ-модули при выявлении рисков.

14.5 Этап 4. Разработка

14.5.1 На этапе разработки осуществляется программная реализация ИСО.

14.5.2 Разработка должна выполняться в соответствии с утвержденным техническим заданием и проектной документацией.

14.5.3 В процессе разработки должны быть реализованы:

1. пользовательские интерфейсы;
2. база данных;
3. модули обработки образовательных данных;
4. ИИ-модули;
5. механизмы безопасности;
6. разграничение доступа;
7. журналирование действий;
8. механизмы экспорта и обезличивания данных;
9. функции человеческой проверки ИИ-рекомендаций;
10. административные инструменты.

14.5.4 Для разработки и отладки преимущественно должны использоваться тестовые, синтетические, обезличенные или псевдонимизированные данные.

14.5.5 Использование реальных персональных данных обучающихся на этапе разработки допускается только при наличии правового основания, ограниченного доступа и обоснованной необходимости.

14.6 Этап 5. Внутреннее тестирование

14.6.1 До апробации ИСО должна пройти внутреннее тестирование.

14.6.2 Внутреннее тестирование должно включать:

1. функциональное тестирование;
2. тестирование безопасности;
3. тестирование ролей доступа;
4. тестирование обработки данных;
5. тестирование журналирования;
6. тестирование обезличивания;
7. тестирование ИИ-рекомендаций;
8. тестирование генеративного контента;
9. тестирование пользовательских интерфейсов;
10. тестирование сценариев отказа, удаления данных и инцидентов.

14.6.3 По итогам тестирования составляется отчет.

14.6.4 ИСО не допускается к апробации при наличии критических ошибок, связанных с безопасностью, доступом, обработкой персональных данных, корректностью ИИ-рекомендаций или возможным вредом обучающемуся.

14.7 Этап 6. Этическая экспертиза

14.7.1 До начала пилотной апробации ИСО высокого или критического уровня риска должна пройти этическую экспертизу.

14.7.2 Этическая экспертиза должна оценивать:

1. цели применения ИСО;
2. категории данных обучающихся;
3. наличие информирования и согласия;
4. минимизацию данных;
5. доступ к данным;
6. защиту чувствительных данных;
7. прозрачность ИИ-рекомендаций;
8. механизм человеческого контроля;
9. риск дискриминации;
10. риск стигматизации;
11. риск психологического вреда;
12. порядок реагирования на инциденты.

14.7.3 По итогам этической экспертизы может быть принято одно из решений:

1. допустить ИСО к апробации;
2. допустить ИСО к апробации с ограничениями;
3. направить ИСО на доработку;
4. запретить апробацию до устранения рисков.

14.8 Этап 7. Пилотная апробация

14.8.1 Пилотная апробация проводится в ограниченном масштабе с участием определенной группы пользователей.

14.8.2 До начала пилотной апробации должны быть выполнены следующие условия:

1. утверждено техническое задание;
2. проведено внутреннее тестирование;
3. проведена этическая экспертиза;
4. определены ответственные лица;
5. настроена матрица доступа;
6. получены необходимые согласия;
7. пользователи проинформированы о назначении системы;
8. подготовлен план мониторинга.

6.8.3. В ходе апробации фиксируются:

1. количество участников;
2. используемые функции ИСО;
3. категории обрабатываемых данных;
4. ИИ-рекомендации;
5. случаи человеческой проверки;
6. обращения пользователей;
7. ошибки и инциденты;
8. корректирующие меры.

14.8.4 По итогам пилотной апробации составляется отчет.

14.9 Этап 8. Оценка качества

14.9.1 После пилотной апробации проводится оценка качества ИСО.

14.9.2 Оценка качества должна включать:

1. педагогическую полезность;
2. точность и корректность ИИ-рекомендаций;
3. качество образовательного контента;
4. удобство интерфейса;
5. безопасность данных;
6. соблюдение человеческого контроля;
7. отсутствие признаков дискриминации;
8. уровень удовлетворенности пользователей;
9. количество ошибок и инцидентов;
10. соответствие техническому заданию.

14.9.3 По итогам оценки принимается решение о доработке, повторной апробации или внедрении ИСО.

14.10 Этап 9. Внедрение

14.10.1 Внедрение ИСО допускается после успешного завершения тестирования, этической экспертизы, пилотной апробации и оценки качества.

14.10.2 Перед внедрением организация образования должна обеспечить:

1. инструктаж пользователей;
2. назначение ответственных лиц;
3. настройку доступа;
4. наличие порядка работы с обращениями;
5. наличие порядка реагирования на инциденты;
6. план мониторинга;
7. документацию для пользователей.

14.10.3 Внедрение ИСО должно быть поэтапным и контролируемым.

14.11 Этап 10. Мониторинг

14.11.1 В период применения ИСО должен проводиться регулярный мониторинг.

14.11.2 Мониторинг должен включать:

1. качество ИИ-рекомендаций;
2. корректность работы ИИ-модулей;
3. соблюдение доступа к данным;
4. безопасность обработки данных;
5. жалобы и обращения пользователей;
6. инциденты;
7. признаки дискриминации;
8. случаи отклонения ИИ-рекомендаций специалистами;
9. качество образовательного контента;
10. соблюдение требований настоящего стандарта.

14.11.3 По итогам мониторинга составляется отчет.

14.11.4 При выявлении высокого риска использование отдельного модуля или всей ИСО должно быть ограничено до устранения нарушений.

14.12 Этап 11. Сопровождение и обновление

14.12.1 Сопровождение ИСО включает техническую поддержку, устранение ошибок, обновление модулей, доработку интерфейсов, корректировку ИИ-моделей и обновление документации.

14.12.2 Любое значимое обновление ИСО должно проходить оценку влияния на:

1. данные обучающихся;
2. качество ИИ-рекомендаций;
3. безопасность;
4. человеческий контроль;

5. риск дискриминации;
6. пользовательский опыт;
7. соответствие настоящему стандарту.

14.12.3 При изменении ИИ-модуля высокого или критического уровня риска проводится повторная этическая экспертиза.

14.13 Этап 12. Вывод из эксплуатации

14.13.1 При прекращении использования ИСО должен быть обеспечен безопасный вывод системы из эксплуатации.

14.13.2 Вывод из эксплуатации должен включать:

1. уведомление ответственных лиц и пользователей;
2. прекращение доступа;
3. архивирование необходимых данных;
4. удаление данных, срок хранения которых истек;
5. обезличивание исследовательских данных;
6. сохранение отчетной документации;
7. фиксацию факта вывода системы из эксплуатации.

14.13.3 Вывод ИСО из эксплуатации не должен приводить к утрате прав обучающихся на доступ к информации о своих данных, если такие права предусмотрены законодательством.

15 Требования к техническому заданию на разработку ИСО

15.1 Общие положения

15.1.1 Разработка ИСО должна осуществляться на основании технического задания.

15.1.2 Техническое задание является основным документом, определяющим цель, функции, пользователей, данные, ИИ-модули, требования к безопасности, прозрачности, человеческому контролю, тестированию и оценке качества ИСО.

15.1.3 Техническое задание должно быть согласовано с заинтересованными сторонами, включая педагогических, технических, правовых и этических экспертов.

15.2 Структура технического задания

Техническое задание на разработку ИСО должно включать следующие разделы:

1. основание для разработки;
2. цель и назначение ИСО;
3. область применения;
4. категории пользователей;

5. функциональные требования;
6. требования к данным;
7. требования к ИИ-модулям;
8. требования к генеративному ИИ;
9. требования к человеческому контролю;
10. требования к прозрачности и объяснимости;
11. требования к безопасности;
12. требования к обезличиванию и псевдонимизации;
13. требования к журналированию;
14. требования к интерфейсам;
15. требования к образовательному контенту;
16. требования к тестированию;
17. требования к апробации;
18. требования к мониторингу;
19. требования к документации;
20. критерии приемки.

15.3 Требования к описанию цели и назначения

15.3.1 В техническом задании должна быть четко определена образовательная, диагностическая, методическая, исследовательская или управленческая цель разработки ИСО.

15.3.2 Описание цели должно отвечать на следующие вопросы:

1. какую образовательную проблему решает ИСО;
2. для какой категории обучающихся она предназначена;
3. какие функции выполняет ИИ;
4. какие решения поддерживает система;
5. какие результаты ожидаются;
6. какие риски могут возникнуть.

15.3.3 Не допускается разработка ИСО с неопределенной или слишком общей целью.

15.4 Требования к описанию пользователей

15.4.1 В техническом задании должны быть определены категории пользователей ИСО.

15.4.2 К пользователям могут относиться:

1. обучающиеся;
2. родители или законные представители;
3. педагоги;
4. психологи;
5. методисты;
6. исследователи;
7. администраторы организации образования;

8. системные администраторы;
 9. разработчики;
 10. эксперты;
 11. представители уполномоченных организаций;
 12. другие.
- 15.4.3 Для каждой категории пользователей должны быть определены:
1. цели использования системы;
 2. доступные функции;
 3. доступные категории данных;
 4. ограничения доступа;
 5. ответственность пользователя.

15.5 Требования к функциональному описанию

15.5.1 В техническом задании должны быть описаны все основные функции ИСО.

15.5.2 Для каждой функции указывается:

1. назначение функции;
2. пользователь функции;
3. входные данные;
4. выходные результаты;
5. связь с ИИ-модулями;
6. уровень риска;
7. необходимость человеческой проверки;
8. требования к журналированию;
9. ограничения применения.

15.6 Требования к описанию данных

15.6.1 Техническое задание должно содержать карту данных ИСО.

15.6.2 Карта данных должна включать:

Категория данных	Источник	Цель обработки	Уровень чувствительности	Кто имеет доступ	Срок хранения	Способ защиты

15.6.3 Для каждой категории данных должны быть указаны правовое основание обработки, необходимость получения согласия и порядок удаления.

15.7 Требования к описанию ИИ-модулей

15.7.1 Каждый ИИ-модуль должен быть описан в техническом задании.

15.7.2 Описание ИИ-модуля должно включать:

1. название модуля;
2. назначение;
3. используемые данные;

4. выходной результат;
5. алгоритмический подход;
6. уровень влияния на обучающегося;
7. уровень риска;
8. ограничения;
9. требования к человеческой проверке;
10. порядок отключения модуля;
11. требования к мониторингу.

15.8 Требования к критериям приемки

15.8.1 Техническое задание должно содержать критерии приемки ИСО.

15.8.2 Критерии приемки должны включать:

1. выполнение заявленных функций;
2. корректность обработки данных;
3. отсутствие критических ошибок;
4. соблюдение прав доступа;
5. работоспособность механизмов журналирования;
6. возможность обезличивания данных;
7. корректность формирования ИИ-рекомендаций;
8. наличие человеческой проверки значимых рекомендаций;
9. безопасность пользовательских данных;
10. соответствие образовательным целям.

16 Требования к данным обучающихся

16.1 Общие положения

16.1.1 Обработка данных обучающихся в ИСО должна осуществляться в соответствии с законодательством Республики Казахстан, настоящим стандартом и утвержденными внутренними документами организации.

16.1.2 Данные обучающихся должны использоваться только для заранее определенных, правомерных и педагогически обоснованных целей.

16.1.3 ИСО не должна собирать данные, не связанные с назначением системы.

16.1.4 Для несовершеннолетних обучающихся должны быть предусмотрены специальные меры защиты, информирования и согласия.

16.2 Категории данных обучающихся

16.2.1 В ИСО могут обрабатываться следующие категории данных:

Код	Категория данных	Примеры
D1	Идентификационные данные	ФИО, ИИН, возраст, класс, организация образования

D2	Контактные данные	контакты обучающегося или законного представителя
D3	Образовательные данные	оценки, результаты заданий, тестов, проектов
D4	Диагностические данные	результаты диагностики знаний, способностей, когнитивных показателей
D5	Поведенческие данные в системе	время выполнения заданий, активность, частота ошибок
D6	Психолого-педагогические данные	мотивация, эмоциональное состояние, стресс, сопровождение
D7	Данные ИИ-рекомендаций	прогнозы, индивидуальные траектории, рекомендации
D8	Технические данные	IP-адрес, устройство, дата и время входа
D9	Обезличенные исследовательские данные	массивы без прямой идентификации
D10	Сгенерированный образовательный контент	задания, объяснения, обратная связь, созданные ИИ

16.3 Требования к минимизации данных

16.3.1 В ИСО должны собираться только минимально необходимые данные.

16.3.2 Перед началом обработки данных должно быть определено:

1. зачем собирается каждая категория данных;
2. является ли категория данных обязательной;
3. можно ли достичь цели без данной категории данных;
4. какие риски связаны с ее обработкой;
5. кто будет иметь доступ;
6. как долго данные будут храниться.

16.3.3 Сбор избыточных данных не допускается.

16.4 Требования к чувствительным данным

16.4.1 К чувствительным данным в контексте ИСО относятся:

1. психолого-педагогические данные;
2. диагностические данные;
3. когнитивные показатели;
4. данные о мотивации и эмоциональном состоянии;
5. данные об особых образовательных потребностях;
6. прогнозы образовательного развития;
7. ИИ-рекомендации высокого или критического уровня влияния.

16.4.2 Чувствительные данные должны обрабатываться только при наличии обоснованной необходимости.

16.4.3 Доступ к чувствительным данным должен быть ограничен.

16.4.4 Чувствительные данные не должны использоваться для публичного ранжирования, стигматизации или ограничения образовательных возможностей обучающегося.

16.5 Требования к качеству данных

16.5.1 Данные, используемые в ИСО, должны быть:

1. точными;
2. актуальными;
3. релевантными;
4. достаточными;
5. проверяемыми;
6. не избыточными;
7. полученными правомерным способом.

16.5.2 ИСО должна предусматривать возможность исправления ошибочных или устаревших данных.

16.5.3 ИИ-рекомендации не должны формироваться на основе заведомо неполных, ошибочных или устаревших данных.

16.6 Требования к доступу к данным

16.6.1 Доступ к данным обучающихся должен предоставляться по ролям.

16.6.2 Доступ должен соответствовать принципу минимально необходимого доступа.

16.6.3 Для каждой роли должны быть определены:

1. доступные категории данных;
2. разрешенные действия;
3. ограничения;
4. срок доступа;
5. ответственность пользователя.

16.6.4 Неактуальные доступы должны своевременно блокироваться.

16.7 Требования к срокам хранения

16.7.1 Сроки хранения данных должны определяться целями обработки, требованиями законодательства и внутренними документами организации.

16.7.2 Данные не должны храниться дольше, чем это необходимо для достижения заявленной цели.

16.7.3 По истечении срока хранения данные подлежат удалению, обезличиванию или архивированию в установленном порядке.

16.8 Требования к удалению данных

16.8.1 ИСО должна предусматривать возможность удаления данных в случаях, предусмотренных законодательством и внутренними документами организации.

16.8.2 Удаление данных должно фиксироваться.

16.8.3 При отзыве согласия законным представителем несовершеннолетнего обучающегося дальнейшая обработка данных должна быть прекращена, если иное не предусмотрено законодательством.

16.8.4 Если данные уже необратимо обезличены и не позволяют идентифицировать обучающегося, они могут использоваться в агрегированном виде в соответствии с установленными целями.

17 Требования к информированию и согласию

17.1 Общие положения

17.1.1 До начала использования ИСО обучающиеся и/или их законные представители должны быть проинформированы о назначении системы, целях обработки данных, применении искусственного интеллекта, возможных ИИ-рекомендациях, правах пользователей и мерах защиты данных.

17.1.2 Информирование должно быть понятным, доступным и соответствующим возрасту обучающегося.

17.1.3 В отношении несовершеннолетних обучающихся информирование законного представителя является обязательным, если обработка данных требует согласия в соответствии с законодательством Республики Казахстан.

17.1.4 Обучающемуся должна быть предоставлена информация простым языком, без сложных юридических и технических формулировок.

17.2 Содержание информирования

17.2.1 Информация для обучающегося и/или законного представителя должна включать:

1. наименование организации, использующей ИСО;
2. назначение интеллектуальной системы обучения;
3. цели обработки данных;
4. категории обрабатываемых данных;
5. сведения о применении искусственного интеллекта;
6. виды ИИ-рекомендаций, которые может формировать система;
7. указание на то, что значимые ИИ-рекомендации проверяются человеком;
8. круг лиц, имеющих доступ к данным;
9. сроки хранения данных;

10. порядок обезличивания данных;
11. права обучающегося и/или законного представителя;
12. порядок отзыва согласия;
13. порядок подачи обращения или жалобы;
14. контактные данные ответственного лица.

17.2.2 Информирование не должно создавать у обучающегося или родителя ложного впечатления, что искусственный интеллект принимает окончательные решения без участия человека.

17.3 Требования к согласию

17.3.1 Если обработка данных обучающегося требует согласия, такое согласие должно быть получено до начала обработки данных.

17.3.2 Согласие должно быть добровольным, информированным, конкретным и документально зафиксированным.

17.3.3 Согласие должно содержать:

1. сведения об обучающемся;
2. сведения о законном представителе, если применимо;
3. цель обработки данных;
4. перечень категорий данных;
5. описание использования ИСО и ИИ-модулей;
6. срок действия согласия;
7. порядок отзыва согласия;
8. сведения о возможном обезличенном использовании данных;
9. подпись лица, дающего согласие, или электронное подтверждение, если применяется электронная форма.

17.3.4 Согласие не должно быть сформулировано слишком широко или неопределенно.

17.3.5 Не допускается получение согласия путем скрытого согласия, принуждения или включения условий, которые ограничивают право обучающегося на обязательное образование.

17.4 Особенности согласия для несовершеннолетних обучающихся

17.4.1 Для несовершеннолетних обучающихся согласие на обработку данных предоставляется родителем или иным законным представителем в порядке, установленном законодательством Республики Казахстан.

17.4.2 Помимо согласия законного представителя, несовершеннолетнему обучающемуся должно быть разъяснено:

1. что такое ИСО;
2. зачем используются его данные;
3. кто сможет видеть результаты;
4. как помогает ИИ;
5. что ИИ может ошибаться;

6. что важные решения проверяет человек;
7. что обучающийся может задавать вопросы;
8. что обучающийся может сообщить взрослому о дискомфорте.

17.4.3 Отказ законного представителя от участия обучающегося в ИСО не должен приводить к ухудшению оценок, отношения педагогов или ограничениям доступа к обязательному образованию.

17.5 Частичное согласие

17.5.1 В ИСО должна быть предусмотрена возможность частичного согласия, если система обрабатывает разные категории данных или использует разные функции.

17.5.2 Например, законный представитель может отдельно выразить согласие или отказ на:

1. участие обучающегося в диагностике;
2. обработку психолого-педагогических данных;
3. использование обезличенных данных в научных целях;
4. получение ИИ-рекомендаций;
5. использование сгенерированного ИИ-контента;
6. участие в пилотной апробации.

17.5.3 ИСО должна учитывать ограничения частичного согласия при обработке данных.

17.6 Отзыв согласия

17.6.1 Обучающийся и/или его законный представитель должны иметь возможность отозвать согласие в установленном порядке.

17.6.2 При отзыве согласия организация должна:

1. зафиксировать дату и основание отзыва;
2. прекратить дальнейшую обработку данных, если отсутствует иное правовое основание;
3. исключить данные из активной обработки;
4. удалить, обезличить или архивировать данные в установленном порядке;
5. уведомить заявителя о принятых мерах.

17.6.3 Отзыв согласия не должен иметь негативных последствий для обучающегося.

17.7 Документирование информирования и согласия

17.7.1 Организация, использующая ИСО, должна вести учет информированных согласий.

17.7.2 Реестр согласий должен содержать:

№	ФИО обучающегося	Класс / группа	ФИО законного представителя	Дата согласия	Вид согласия	Статус
---	------------------	----------------	-----------------------------	---------------	--------------	--------

1					☐ полное ☐ частичное	☐ действует ☐ отозвано
2					☐ полное ☐ частичное	☐ действует ☐ отозвано

17.7.3 Данные обучающегося не должны передаваться в обработку ИСО, если необходимое согласие отсутствует или отозвано.

18 Требования к ИИ-модулям

18.1 Общие положения

18.1.1 Каждый ИИ-модуль ИСО должен иметь определенное назначение, описание входных данных, выходных результатов, ограничений, рисков и требований к человеческой проверке.

18.1.2 ИИ-модуль должен использоваться только в рамках заявленной функции и не должен выполнять скрытые или неописанные действия с данными обучающихся.

18.1.3 ИИ-модули, влияющие на образовательную траекторию, оценивание, диагностику, психолого-педагогическое сопровождение или доступ к образовательным возможностям, относятся к модулям повышенного риска.

18.2 Документация ИИ-модуля

18.2.1 Для каждого ИИ-модуля должна быть подготовлена документация.

18.2.2 Документация ИИ-модуля должна включать:

Раздел документации	Содержание
Наименование модуля	название ИИ-модуля
Назначение	какую задачу выполняет модуль
Пользователи	кто использует результаты модуля
Входные данные	какие данные используются
Выходные результаты	какие рекомендации, прогнозы или материалы формируются
Алгоритмический подход	описание метода на понятном уровне
Уровень риска	низкий, средний, высокий, критический
Уровень влияния	влияет / не влияет на значимые решения
Ограничения	случаи, когда модуль нельзя применять
Человеческая проверка	кто и как проверяет результат
Мониторинг	какие показатели контролируются

Отключение	порядок ограничения или отключения модуля
------------	---

18.3 Требования к входным данным ИИ-модуля

18.3.1 Входные данные ИИ-модуля должны быть релевантными заявленной функции.

18.3.2 Не допускается использование данных, которые:

1. не связаны с образовательной задачей;
2. собраны без правового основания;
3. являются избыточными;
4. являются ошибочными или устаревшими;
5. могут привести к дискриминации без соответствующей оценки риска;
6. не прошли необходимую проверку качества.

18.3.3 Для модулей высокого и критического уровня риска должна проводиться оценка качества входных данных.

18.4 Требования к выходным результатам ИИ-модуля

18.4.1 Результаты работы ИИ-модуля должны быть представлены в форме, понятной соответствующему пользователю.

18.4.2 Выходные результаты должны содержать указание на их рекомендательный, предварительный или вспомогательный характер, если они могут повлиять на решение человека.

18.4.3 Не допускается формирование результатов в виде стигматизирующих или окончательных утверждений.

Недопустимые формулировки:

1. «обучающийся не способен»;
2. «обучающийся неодаренный»;
3. «участие в олимпиаде не рекомендуется окончательно»;
4. «система решила, что обучающийся слабый»;
5. «перспективы развития отсутствуют».

Допустимые формулировки:

1. «рекомендуется дополнительная поддержка по теме»;
2. «система выявила возможное затруднение, требуется проверка педагога»;
3. «предварительно рекомендуется задание повышенного уровня»;
4. «результат требует экспертной интерпретации»;
5. «рекомендация является вспомогательной».

18.5 Требования к точности и корректности

18.5.1 Для ИИ-модулей должны быть определены показатели качества и корректности.

18.5.2 В зависимости от назначения модуля могут применяться следующие показатели:

1. точность рекомендаций;
2. доля ошибочных рекомендаций;
3. доля отклоненных рекомендаций специалистами;
4. стабильность результатов;
5. полнота анализа;
6. соответствие педагогической логике;
7. отсутствие грубых ошибок;
8. отсутствие признаков дискриминации;
9. качество сгенерированного контента;
10. удовлетворенность пользователей.

18.5.3 Если ИИ-модуль регулярно формирует ошибочные, вредные, дискриминационные или необъяснимые рекомендации, его использование должно быть приостановлено до доработки.

18.6 Требования к ИИ-модулям высокого и критического риска

18.6.1 ИИ-модули высокого и критического риска должны проходить предварительную экспертизу до внедрения.

18.6.2 Для таких модулей обязательны:

1. описание используемых данных;
2. оценка качества данных;
3. оценка риска дискриминации;
4. описание ограничений;
5. человеческая проверка результатов;
6. журналирование рекомендаций;
7. порядок рассмотрения спорных случаев;
8. регулярный мониторинг;
9. порядок отключения модуля.

18.6.3 ИИ-модуль критического риска не должен применяться в массовом режиме без пилотной апробации и экспертного заключения.

18.7 Порядок отключения ИИ-модуля

18.7.1 Организация должна предусмотреть возможность временного ограничения или отключения ИИ-модуля.

18.7.2 Основаниями для отключения являются:

1. выявление дискриминационных результатов;
2. грубые ошибки рекомендаций;

3. утечка или неправомерная обработка данных;
4. жалобы пользователей высокого уровня риска;
5. отсутствие возможности объяснить значимые рекомендации;
6. нарушение требований настоящего стандарта;
7. технический сбой, влияющий на безопасность или корректность работы.

18.7.3 После устранения нарушений модуль может быть повторно введен в эксплуатацию только после проверки.

19 Требования к генеративному ИИ

19.1 Общие положения

19.1.1 Генеративный искусственный интеллект в составе ИСО может использоваться для создания, адаптации, пояснения, преобразования или анализа образовательного контента.

19.1.2 Использование генеративного ИИ должно быть педагогически обоснованным, безопасным, проверяемым и прозрачным для пользователей.

19.1.3 Генеративный ИИ не должен заменять профессиональное педагогическое, психологическое, методическое или экспертное решение.

19.2 Допустимые функции генеративного ИИ

19.2.1 Генеративный ИИ может использоваться для:

1. создания учебных заданий;
2. подготовки вариантов тестов;
3. создания объяснений по теме;
4. генерации подсказок;
5. подготовки тренировочных упражнений;
6. адаптации текста под возраст обучающегося;
7. создания примеров и кейсов;
8. подготовки вариантов обратной связи;
9. помощи педагогу в разработке урока;
10. подготовки черновиков методических материалов;
11. генерации учебных сценариев;
12. поддержки диалогового взаимодействия с обучающимся.

19.2.2 Сгенерированный контент должен проходить проверку человеком перед официальным использованием в образовательном процессе.

19.3 Запрещенные функции генеративного ИИ

19.3.1 Генеративный ИИ не должен использоваться для:

1. окончательной диагностики способностей обучающегося;
2. автоматического психологического заключения;

3. присвоения статуса «одаренный», «неодаренный», «слабый», «неперспективный»;
4. принятия решений об отборе, исключении, ограничении или переводе обучающегося;
5. генерации унижающих, дискриминационных или стигматизирующих характеристик;
6. создания недостоверных отчетов;
7. фальсификации образовательных или научных результатов;
8. обработки персональных данных в открытых внешних ИИ-сервисах без правового основания;
9. замены педагогической оценки без проверки специалистом;
10. создания контента, не соответствующего возрасту обучающихся.

19.4 Требования к промптам и запросам

19.4.1 Запросы к генеративному ИИ не должны содержать персональные данные обучающихся, если сервис не предназначен и не разрешен для такой обработки.

19.4.2 В промптах запрещается указывать:

1. ФИО обучающегося;
2. ИИН или иные идентификаторы;
3. контактные данные;
4. индивидуальные диагностические результаты;
5. психологические сведения;
6. данные о здоровье;
7. сведения об особых образовательных потребностях в идентифицируемом виде;
8. фотографии, аудио- и видеоматериалы;
9. данные, позволяющие прямо или косвенно идентифицировать обучающегося.

19.4.3 При необходимости использования образовательного примера данные должны быть обезличены или заменены условными данными.

19.5 Требования к проверке сгенерированного контента

19.5.1 Контент, созданный генеративным ИИ, должен быть проверен педагогом, методистом, исследователем или иным уполномоченным специалистом перед использованием.

19.5.2 Проверка должна включать:

1. фактическую достоверность;
2. соответствие учебной программе;
3. соответствие возрасту обучающихся;
4. языковую корректность;
5. отсутствие дискриминационных формулировок;

6. отсутствие психологически вредного содержания;
7. соответствие педагогической цели;
8. оригинальность и академическую добросовестность;
9. отсутствие персональных данных;
10. качество объяснений и заданий.

19.5.3 Контент, не прошедший проверку, не допускается к официальному использованию.

19.6 Маркировка ИИ-контента

19.6.1 В случаях официального использования контента, созданного или существенно измененного генеративным ИИ, должна применяться маркировка.

19.6.2 Возможные формулировки маркировки:

1. «Материал подготовлен с использованием инструментов искусственного интеллекта и проверен педагогом».
2. «Задание создано с применением генеративного ИИ и прошло методическую проверку».
3. «Обратная связь сформирована ИИ-системой и проверена специалистом».

19.6.3 Маркировка не требуется для внутренних черновиков, если они не передаются обучающимся, родителям или внешним пользователям.

19.7 Ответственность за использование генеративного ИИ

19.7.1 Ответственность за использование сгенерированного контента несет лицо или организация, применяющие его в образовательном процессе.

19.7.2 Недопустимо ссылаться на генеративный ИИ как на самостоятельного автора окончательного педагогического, диагностического или методического решения.

19.7.3 При выявлении ошибки в сгенерированном контенте организация должна принять меры по исправлению, уведомлению пользователей при необходимости и предотвращению повторения ошибки.

20. Требования к человеческому контролю

20.1 Общие положения

20.1.1 ИСО должна применяться как инструмент поддержки педагогических, методических, диагностических, психологических и управленческих решений, но не как самостоятельный субъект принятия окончательных решений.

20.1.2 Значимые ИИ-рекомендации, способные повлиять на образовательную траекторию, оценивание, диагностику, психолого-

педагогическое сопровождение, профориентацию, доступ к образовательным возможностям или самооценку обучающегося, подлежат обязательной человеческой проверке.

20.1.3 Человеческий контроль должен быть организован таким образом, чтобы уполномоченный специалист мог понять, оценить, принять, изменить или отклонить ИИ-рекомендацию.

20.1.4 Окончательная ответственность за применение ИИ-рекомендации возлагается на человека или организацию, использующую ИСО, а не на алгоритм или программную систему.

20.2 Виды рекомендаций, требующих обязательной проверки

20.2.1 Обязательной человеческой проверке подлежат следующие ИИ-рекомендации:

1. рекомендации по индивидуальной образовательной траектории;
2. рекомендации по уровню сложности обучения;
3. рекомендации по переводу обучающегося на индивидуальную программу;
4. выводы о признаках одаренности или образовательных затруднений;
5. рекомендации по участию в олимпиадах, конкурсах, проектах, специальных программах;
6. рекомендации по психолого-педагогическому сопровождению;
7. профориентационные рекомендации;
8. рекомендации, связанные с мотивацией, стрессом, перегрузкой или эмоциональным состоянием;
9. рекомендации, способные повлиять на оценивание;
10. рекомендации, способные ограничить или расширить доступ к образовательным возможностям.

20.2.2 Рекомендации низкого риска, такие как учебные подсказки, объяснения терминов, тренировочные задания или дополнительные материалы, могут проверяться выборочно, если они не влияют на значимые решения.

20.3 Уровни человеческой проверки

Уровень проверки	Когда применяется	Кто проверяет
Базовая проверка	учебные подсказки, объяснения, дополнительные задания	педагог или методист выборочно
Педагогическая проверка	рекомендации по заданиям, темам, уровню сложности	педагог
Психолого-педагогическая проверка	рекомендации, связанные с мотивацией, стрессом, эмоциональным состоянием	психолог, педагог

Экспертная проверка	диагностика одаренности, траектории развития, участие в программах	экспертная группа
Комиссионная проверка	спорные, высокорисковые или потенциально дискриминационные рекомендации	этическая комиссия / рабочая группа

20.4 Требования к процедуре проверки

20.4.1 При проверке ИИ-рекомендации специалист должен оценить:

1. на каких данных основана рекомендация;
2. достаточно ли данных для такого вывода;
3. актуальны ли использованные данные;
4. не содержит ли рекомендация фактических ошибок;
5. не противоречит ли она педагогическому наблюдению;
6. не содержит ли она дискриминационных или стигматизирующих формулировок;
7. не ограничивает ли она образовательные возможности обучающегося;
8. можно ли объяснить рекомендацию обучающемуся и/или законному представителю;
9. требуется ли дополнительная диагностика или консультация специалиста;
10. может ли рекомендация быть применена без вреда для обучающегося.

20.4.2 Проверяющий специалист должен учитывать возраст, язык обучения, образовательный контекст, индивидуальные особенности, социальные условия, доступ к цифровым ресурсам и особые образовательные потребности обучающегося.

20.4.3 Рекомендация не должна применяться, если специалист не может оценить ее обоснованность или выявляет риск вреда.

20.5 Возможные решения по результатам проверки

По итогам проверки ИИ-рекомендации специалист принимает одно из следующих решений:

Решение	Содержание
Принять рекомендацию	рекомендация признана обоснованной и безопасной
Принять с уточнением	рекомендация может применяться после педагогического или экспертного комментария

Направить дополнительную проверку	на	данных недостаточно или есть сомнения в корректности рекомендации
Отклонить рекомендацию		рекомендация признана ошибочной, вредной, дискриминационной или необоснованной
Передать комиссионное рассмотрение	на	рекомендация имеет высокий риск или вызывает спор

20.6 Фиксация человеческой проверки

20.6.1 ИСО должна обеспечивать фиксацию факта человеческой проверки значимых ИИ-рекомендаций.

20.6.2 Должны фиксироваться:

1. дата формирования ИИ-рекомендации;
2. тип рекомендации;
3. уровень риска;
4. специалист, проводивший проверку;
5. принятое решение;
6. комментарий специалиста;
7. дата проверки;
8. факт изменения, отклонения или подтверждения рекомендации.

20.6.3 Фиксация проверки используется для аудита, мониторинга, рассмотрения обращений и оценки качества ИСО.

20.7 Запрещенные действия

При использовании ИИ-рекомендаций запрещается:

1. применять значимые рекомендации без проверки человеком;
2. принимать окончательные решения только на основании ИИ-вывода;
3. скрывать от пользователя факт использования ИИ;
4. представлять ИИ-рекомендацию как безошибочную;
5. использовать ИИ-рекомендации для стигматизации обучающегося;
6. ограничивать образовательные возможности без экспертной проверки;
7. игнорировать жалобы обучающегося или законного представителя;
8. использовать непонятные, необъяснимые или противоречивые рекомендации;
9. применять рекомендации, основанные на неполных, ошибочных или устаревших данных;
10. использовать ИИ для автоматического присвоения обучающемуся статуса “одаренный”, “неодаренный”, “слабый” или “неперспективный”.

21 Требования к прозрачности и объяснимости

21.1 Общие положения

21.1.1 ИСО должна быть прозрачной для пользователей в части назначения, используемых данных, функций искусственного интеллекта, характера ИИ-рекомендаций, ограничений системы и роли человека.

21.1.2 Прозрачность означает, что обучающийся, законный представитель, педагог, психолог, администратор или иной пользователь должны понимать, как и для чего применяется ИСО.

21.1.3 Объяснимость означает возможность предоставить понятное разъяснение значимой ИИ-рекомендации, ее основания, ограничений и порядка пересмотра.

21.2 Информация, предоставляемая пользователям

21.2.1 Пользователям ИСО должна быть доступна информация о:

1. назначении системы;
2. организации, применяющей систему;
3. категориях пользователей;
4. функциях ИСО;
5. наличии ИИ-модулей;
6. применении генеративного ИИ;
7. категориях обрабатываемых данных;
8. целях обработки данных;
9. видах ИИ-рекомендаций;
10. роли человека в принятии решений;
11. ограничениях системы;
12. порядке подачи обращения или жалобы;
13. порядке исправления или удаления данных, если применимо.

21.2.2 Для несовершеннолетних обучающихся информация должна быть представлена простым и доступным языком.

21.3 Требования к объяснению ИИ-рекомендаций

21.3.1 Значимая ИИ-рекомендация должна сопровождаться возможностью объяснения.

21.3.2 Объяснение должно включать:

1. краткое содержание рекомендации;
2. цель рекомендации;
3. типы данных, на которых основана рекомендация;
4. указание на предварительный или вспомогательный характер рекомендации;
5. сведения о специалисте, проверившем рекомендацию;

6. возможные альтернативы;
 7. порядок уточнения, пересмотра или оспаривания.
- 21.3.3 Объяснение должно быть адаптировано к типу пользователя:

Пользователь	Характер объяснения
Обучающийся	простое, поддерживающее, без стигматизирующих формулировок
Родитель / законный представитель	понятное описание данных, рекомендации и роли человека
Педагог	педагогическое основание, ограничения, рекомендации к применению
Психолог	контекст, риски, необходимость профессиональной интерпретации
Исследователь	методическое и аналитическое основание
Администратор	организационные последствия и ограничения

21.4 Запрещенные формулировки

21.4.1 В интерфейсе ИСО, отчетах, рекомендациях и сообщениях пользователям не допускаются формулировки, создающие впечатление окончательного, дискриминационного или стигматизирующего решения.

21.4.2 Запрещенные формулировки:

1. «ИИ окончательно определил уровень обучающегося»;
2. «система доказала, что обучающийся неодаренный»;
3. «обучающийся не способен к данному направлению»;
4. «алгоритм решил, что участие невозможно»;
5. «прогноз отрицательный, развитие нецелесообразно»;
6. «решение системы не подлежит пересмотру»;
7. «обучающийся слабый»;
8. «перспективы отсутствуют».

21.4.3 Рекомендуемые формулировки:

1. «система выявила возможное затруднение, требуется педагогическая проверка»;
2. «рекомендация является предварительной»;
3. «результат следует рассматривать как один из источников информации»;
4. «предлагается дополнительная поддержка по теме»;
5. «рекомендация проверена специалистом»;
6. «возможны альтернативные образовательные маршруты»;
7. «окончательное решение принимает педагог/специалист».

21.5 Требования к интерфейсу прозрачности

21.5.1 В ИСО должны быть предусмотрены элементы интерфейса, позволяющие пользователю понять:

1. когда используется ИИ;
2. какие функции выполняет ИИ;
3. какие данные применяются;
4. является ли рекомендация автоматической;
5. проверена ли рекомендация человеком;
6. как задать вопрос или запросить объяснение.

21.5.2 Если контент создан генеративным ИИ, это должно быть обозначено в случаях, предусмотренных настоящим стандартом.

21.5.3 Система должна позволять пользователю отличать:

1. данные, введенные человеком;
2. данные, полученные из образовательного процесса;
3. автоматически сформированные рекомендации;
4. рекомендации, проверенные человеком;
5. контент, созданный генеративным ИИ.

21.6 Ограничения объяснимости

21.6.1 Если техническая природа ИИ-модуля не позволяет полностью объяснить алгоритмическую логику, пользователю должно быть предоставлено минимально необходимое объяснение на уровне:

1. цели рекомендации;
2. типов использованных данных;
3. ограничений системы;
4. уровня уверенности или необходимости проверки;
5. роли человека в принятии решения.

21.6.2 Невозможность полного технического объяснения не освобождает организацию от обязанности обеспечить человеческий контроль и возможность пересмотра значимой рекомендации.

22 Требования к недопущению дискриминации и стигматизации

22.1 Общие положения

22.1.1 ИСО должна разрабатываться, тестироваться, внедряться и применяться таким образом, чтобы не создавать, не усиливать и не воспроизводить дискриминацию обучающихся.

22.1.2 ИСО не должна использоваться для стигматизации, публичного ранжирования, ограничения образовательных возможностей или формирования негативных ярлыков в отношении обучающихся.

22.1.3 Недопущение дискриминации должно обеспечиваться на всех этапах жизненного цикла ИСО: от проектирования и сбора данных до мониторинга и сопровождения.

22.2 Потенциальные основания дискриминации

22.2.1 При разработке и применении ИСО должны учитываться риски необоснованного различия в отношении обучающихся по следующим признакам:

1. язык обучения;
2. место проживания;
3. городской или сельский статус организации образования;
4. тип организации образования;
5. социально-экономическое положение семьи;
6. уровень цифровой доступности;
7. пол;
8. национальность;
9. состояние здоровья;
10. инвалидность;
11. особые образовательные потребности;
12. уровень предварительной подготовки;
13. участие или неучастие в дополнительных образовательных программах;
14. семейные обстоятельства;
15. иные обстоятельства, которые могут повлиять на результаты анализа.

22.3 Требования к данным для предотвращения дискриминации

22.3.1 Данные, используемые ИСО, должны оцениваться на предмет полноты, репрезентативности, качества и потенциальной предвзятости.

22.3.2 Не допускается использование наборов данных, которые систематически исключают отдельные группы обучающихся или приводят к искаженным результатам.

22.3.3 При использовании данных из разных организаций образования необходимо учитывать различия в:

1. учебных программах;
2. языке обучения;
3. цифровой инфраструктуре;
4. доступе к дополнительному образованию;
5. социальном и территориальном контексте;
6. уровне подготовки обучающихся.

22.3.4 Для ИСО высокого и критического уровня риска должна проводиться оценка риска алгоритмической предвзятости.

22.4 Требования к результатам ИСО

22.4.1 Результаты работы ИСО не должны использоваться как единственное основание для выводов о способностях, перспективах, потенциале или ограничениях обучающегося.

22.4.2 Запрещается автоматическое присвоение обучающемуся негативных или ограничивающих категорий.

22.4.3 Результаты ИСО должны рассматриваться как один из источников информации наряду с:

1. педагогическим наблюдением;
2. результатами учебной деятельности;
3. мнением психолога при необходимости;
4. индивидуальным контекстом обучающегося;
5. динамикой развития;
6. мнением обучающегося и/или законного представителя в значимых случаях.

22.5 Требования к формулировкам

22.5.1 Формулировки ИСО должны быть поддерживающими, нейтральными и ориентированными на развитие.

22.5.2 Не допускаются формулировки:

1. «неодаренный»;
2. «слабый»;
3. «неперспективный»;
4. «не способен»;
5. «не подходит»;
6. «низкий потенциал» без контекста и профессиональной интерпретации;
7. «развитие нецелесообразно»;
8. «исключить из программы» как автоматическая рекомендация.

22.5.3 Рекомендуются формулировки:

1. «требуется дополнительная поддержка»;
2. «выявлена зона развития»;
3. «рекомендуется дополнительная диагностика»;
4. «предлагается индивидуальный темп обучения»;
5. «результат требует интерпретации специалистом»;
6. «возможны разные образовательные траектории».

22.6 Мониторинг дискриминационных рисков

22.6.1 Организация, применяющая ИСО, должна проводить мониторинг возможных дискриминационных эффектов.

22.6.2 Мониторинг должен включать:

1. анализ распределения рекомендаций по группам обучающихся;
2. анализ жалоб и обращений;
3. проверку случаев отклонения рекомендаций специалистами;
4. оценку частоты ошибочных рекомендаций;
5. проверку различий в результатах по языку обучения, типу школы, месту проживания и иным значимым признакам;
6. экспертное рассмотрение спорных случаев.

22.6.3 При выявлении признаков дискриминации использование соответствующего ИИ-модуля должно быть ограничено или приостановлено до устранения причин.

22.7 Реагирование на стигматизирующие или дискриминационные результаты

22.7.1 Если ИСО сформировала стигматизирующий, дискриминационный или потенциально вредный результат, организация должна:

1. не применять такой результат;
2. зафиксировать случай как инцидент;
3. провести проверку исходных данных;
4. провести человеческую экспертизу рекомендации;
5. уведомить ответственных лиц;
6. при необходимости уведомить законного представителя;
7. принять меры по корректировке ИИ-модуля;
8. провести повторную проверку после доработки.

22.7.2 Повторяющиеся случаи дискриминационных или стигматизирующих результатов являются основанием для приостановления использования ИИ-модуля.

23 Требования к безопасности

23.1 Общие положения

23.1.1 ИСО должна обеспечивать защиту данных обучающихся, пользователей, образовательной организации и иных участников образовательного процесса от несанкционированного доступа, утечки, искажения, потери, неправомерной передачи и использования не по назначению.

23.1.2 Требования безопасности должны учитываться на всех этапах жизненного цикла ИСО: при проектировании, разработке, тестировании, апробации, внедрении, эксплуатации, сопровождении, обновлении и выводе из эксплуатации.

23.1.3 Безопасность ИСО должна обеспечиваться совокупностью организационных, технических, программных и процедурных мер.

23.1.4 Для ИСО, обрабатывающих персональные, чувствительные, диагностические или психолого-педагогические данные обучающихся, должны применяться усиленные меры защиты.

23.2 Требования к управлению доступом

23.2.1 Доступ к ИСО должен предоставляться только идентифицированным и авторизованным пользователям.

23.2.2 В ИСО должны быть реализованы:

1. учетные записи пользователей;
2. идентификация пользователя;
3. аутентификация пользователя;
4. разграничение прав доступа по ролям;
5. ограничение доступа к чувствительным данным;
6. блокировка или удаление неактуальных учетных записей;
7. контроль действий пользователей;
8. фиксация изменений прав доступа.

23.2.3 Доступ пользователя должен соответствовать его роли и функциональным обязанностям.

23.2.4 Пользователь не должен иметь доступ к данным, которые не требуются для выполнения его функций.

23.2.5 Передача учетной записи, логина, пароля или иного средства доступа другим лицам не допускается.

23.3 Требования к ролям пользователей

23.3.1 В ИСО должны быть определены роли пользователей.

23.3.2 Минимальный перечень ролей может включать:

1. обучающийся;
2. родитель или законный представитель;
3. педагог;
4. психолог;
5. методист;
6. исследователь;
7. администратор организации образования;
8. системный администратор;
9. разработчик;
10. эксперт;
11. ответственный за защиту данных;
12. представитель уполномоченной организации.

23.3.3 Для каждой роли должны быть определены:

1. доступные функции;
2. доступные категории данных;
3. разрешенные действия;

4. запрещенные действия;
5. уровень доступа;
6. срок доступа;
7. ответственность пользователя.

23.4 Требования к защите чувствительных данных

23.4.1 Чувствительные данные обучающихся должны храниться и обрабатываться с усиленными мерами защиты.

23.4.2 К чувствительным данным относятся:

1. психолого-педагогические данные;
2. диагностические данные;
3. когнитивные показатели;
4. сведения об эмоциональном состоянии;
5. сведения о мотивации;
6. данные об особых образовательных потребностях;
7. прогностические данные;
8. ИИ-рекомендации высокого или критического уровня влияния.

23.4.3 Доступ к чувствительным данным должен предоставляться только уполномоченным специалистам.

23.4.4 Разработчики и технические специалисты не должны иметь доступ к чувствительным данным в идентифицируемом виде, если такой доступ не является технически необходимым и специально разрешенным.

23.4.5 Для технической отладки рекомендуется использовать тестовые, синтетические, обезличенные или псевдонимизированные данные.

23.5 Требования к хранению данных

23.5.1 Данные, обрабатываемые ИСО, должны храниться в защищенной информационной среде.

23.5.2 Не допускается хранение персональных и чувствительных данных:

1. в открытых облачных папках;
2. в публичных репозиториях;
3. в общедоступных электронных таблицах;
4. на личных устройствах без разрешения;
5. в незащищенных мессенджерах;
6. в файлах без ограничения доступа;
7. в системах, не предназначенных для хранения таких данных.

23.5.3 Идентификационные данные должны по возможности храниться отдельно от исследовательских, диагностических и аналитических массивов.

23.5.4 Сроки хранения данных должны быть определены до начала обработки.

23.6 Требования к передаче данных

23.6.1 Передача данных из ИСО допускается только при наличии правового основания, служебной необходимости и соблюдении требований безопасности.

23.6.2 Передача данных должна осуществляться через защищенные каналы или утвержденные организацией способы обмена.

23.6.3 Передача персональных или чувствительных данных через личные мессенджеры, незащищенную электронную почту, открытые ссылки или общедоступные папки не допускается.

23.6.4 Передача данных внешним экспертам, исследователям или организациям должна осуществляться преимущественно в обезличенном или агрегированном виде.

23.6.5 Факт передачи данных должен быть зафиксирован.

23.7 Требования к экспорту данных

23.7.1 ИСО должна ограничивать экспорт данных в соответствии с ролью пользователя.

23.7.2 Экспорт персональных и чувствительных данных должен быть доступен только уполномоченным лицам.

23.7.3 При экспорте данных система должна предупреждать пользователя о наличии прямых идентификаторов или чувствительных данных, если такая функция технически предусмотрена.

23.7.4 Для исследовательских, отчетных и экспертных целей экспорт должен осуществляться в обезличенном или агрегированном виде.

23.7.5 Все операции экспорта должны фиксироваться в журнале действий.

23.8 Требования к резервному копированию

23.8.1 Для ИСО должны быть предусмотрены процедуры резервного копирования данных.

23.8.2 Резервные копии должны храниться в защищенной среде.

23.8.3 Доступ к резервным копиям должен быть ограничен.

23.8.4 Порядок создания, хранения, восстановления и удаления резервных копий должен быть документирован.

23.8.5 Резервные копии не должны использоваться для целей, не связанных с обеспечением работоспособности и восстановления ИСО.

23.9 Требования к реагированию на инциденты безопасности

23.9.1 В организации, использующей ИСО, должен быть установлен порядок реагирования на инциденты безопасности.

23.9.2 К инцидентам безопасности относятся:

1. несанкционированный доступ;
2. утечка данных;
3. потеря данных;
4. искажение данных;
5. неправомерный экспорт;
6. передача данных третьим лицам без основания;
7. нарушение матрицы доступа;
8. загрузка персональных данных в открытые ИИ-сервисы;
9. сбой, повлиявший на корректность ИИ-рекомендаций;
10. вредная, дискриминационная или стигматизирующая рекомендация.

23.9.3 При выявлении инцидента организация должна:

1. зафиксировать инцидент;
2. ограничить доступ к затронутым данным или модулю;
3. уведомить ответственное лицо;
4. оценить уровень риска;
5. принять меры по устранению последствий;
6. при необходимости уведомить обучающегося и/или законного представителя;
7. провести анализ причин;
8. принять меры по предотвращению повторения.

24 Требования к обезличиванию и псевдонимизации

24.1 Общие положения

24.1.1 Для научного анализа, отчетности, публикаций, внешней экспертизы, тестирования и разработки ИСО должны преимущественно использоваться обезличенные, псевдонимизированные или агрегированные данные.

24.1.2 Обезличивание и псевдонимизация применяются для снижения риска идентификации обучающегося и защиты его прав.

24.1.3 Обезличивание не должно ухудшать качество научного или педагогического анализа в большей степени, чем это необходимо для защиты данных.

24.1.4 Порядок обезличивания и псевдонимизации должен быть документирован.

24.2 Данные, подлежащие удалению или маскированию

24.2.1 При подготовке обезличенного массива должны быть удалены или замаскированы прямые идентификаторы:

1. ФИО обучающегося;
2. ИИН при наличии;

3. точный адрес;
4. номер телефона;
5. электронная почта;
6. логин пользователя;
7. фотография;
8. аудио- и видеозаписи;
9. сведения о родителях или законных представителях;
10. иные сведения, позволяющие прямо идентифицировать обучающегося.

24.2.2 Косвенные идентификаторы должны быть обобщены или маскированы, если в совокупности они позволяют определить обучающегося.

К косвенным идентификаторам относятся:

1. точная школа;
2. точный класс;
3. малый населенный пункт;
4. редкое достижение;
5. уникальная образовательная траектория;
6. редкая особая образовательная потребность;
7. сочетание возраста, класса, школы и результата.

24.3 Псевдонимизация данных

24.3.1 При псевдонимизации прямые идентификаторы обучающегося заменяются кодом.

24.3.2 Рекомендуемый формат кода:

EDU-AI-S-0001

где:

- EDU-AI - обозначение образовательной ИИ-системы;
- S - обучающийся;
- 0001 - порядковый номер участника.

24.3.3 Таблица соответствия “код - ФИО” должна храниться отдельно от исследовательского массива данных.

24.3.4 Доступ к ключу соответствия должен быть ограничен.

24.3.5 Передача ключа соответствия внешним экспертам, разработчикам и лицам, не имеющим правового основания, не допускается.

24.4 Обезличивание исследовательских массивов

24.4.1 Исследовательский массив должен содержать только те данные, которые необходимы для конкретной исследовательской, аналитической или экспертной цели.

24.4.2 Перед использованием исследовательского массива должны быть выполнены следующие действия:

1. удаление прямых идентификаторов;

2. замена ФИО кодами;
3. исключение контактных данных;
4. обобщение редких признаков;
5. проверка малых групп;
6. удаление узнаваемых текстовых фрагментов;
7. проверка риска повторной идентификации;
8. фиксация ответственного лица.

24.4.3 Если риск повторной идентификации сохраняется, данные должны быть дополнительно агрегированы или исключены из массива.

24.5 Обезличивание текстовых данных

24.5.1 Текстовые ответы обучающихся, комментарии, эссе, проектные работы и переписка с ИСО должны проверяться на наличие идентифицирующих сведений.

24.5.2 Перед использованием текстовых данных в научных, отчетных или экспертных целях необходимо удалить или заменить:

1. имена обучающихся;
2. имена родителей;
3. имена педагогов;
4. название школы;
5. населенный пункт;
6. контактные данные;
7. уникальные обстоятельства, позволяющие идентифицировать обучающегося.

24.5.3 При невозможности надежного обезличивания текстовый фрагмент не должен использоваться в публикации или внешней экспертизе.

24.6 Обезличивание визуальных и аудиоматериалов

24.6.1 Фото-, видео- и аудиоматериалы относятся к данным повышенного риска.

24.6.2 Использование таких материалов допускается только при наличии отдельного правового основания и специальных мер защиты.

24.6.3 Для публикаций и внешних материалов должны использоваться материалы, не позволяющие идентифицировать обучающегося, либо материалы с отдельным согласием.

24.6.4 При отсутствии отдельного согласия фото-, видео- и аудиоматериалы не должны включаться в публичные отчеты, презентации или публикации.

24.7 Проверка риска повторной идентификации

24.7.1 Перед публикацией, передачей или внешним использованием обезличенных данных должна проводиться проверка риска повторной идентификации.

24.7.2 Проверка должна учитывать:

1. размер группы;
2. уникальность признаков;
3. наличие редких достижений;
4. сочетание возраста, школы, класса и результата;
5. наличие текстовых фрагментов;
6. наличие визуальных материалов;
7. доступность внешней информации, с которой можно сопоставить данные.

24.7.3 При наличии риска повторной идентификации данные должны быть дополнительно обезличены, агрегированы или исключены.

25 Требования к журналированию и аудиту

25.1 Общие положения

25.1.1 ИСО должна обеспечивать журналирование значимых действий пользователей, операций с данными, формирования ИИ-рекомендаций, человеческой проверки, экспорта данных, изменений доступа и инцидентов.

25.1.2 Журналирование необходимо для обеспечения прозрачности, проверяемости, безопасности, расследования инцидентов, мониторинга и аудита.

25.1.3 Журналы должны быть защищены от несанкционированного изменения, удаления или подмены.

25.2 Действия, подлежащие журналированию

25.2.1 В ИСО должны фиксироваться следующие действия:

1. вход пользователя в систему;
2. выход из системы;
3. неуспешные попытки входа;
4. просмотр персональных данных;
5. просмотр чувствительных данных;
6. создание или изменение данных;
7. удаление данных;
8. экспорт данных;
9. изменение роли пользователя;
10. предоставление или прекращение доступа;
11. формирование ИИ-рекомендации;

12. проверка ИИ-рекомендации человеком;
13. отклонение или изменение рекомендации;
14. формирование отчета;
15. загрузка или выгрузка файлов;
16. регистрация инцидента;
17. изменение настроек ИИ-модуля;
18. отключение или включение ИИ-модуля.

25.3 Состав записи журнала

25.3.1 Запись журнала должна содержать:

1. дату и время действия;
2. идентификатор пользователя;
3. роль пользователя;
4. тип действия;
5. объект действия;
6. категорию данных;
7. результат действия;
8. технический идентификатор устройства или IP-адрес, если применимо;
9. сведения об ошибке, если действие не выполнено;
10. отметку о критичности действия, если применимо.

25.3.2 Для операций с чувствительными данными запись журнала должна содержать дополнительную отметку о повышенном уровне контроля.

25.4 Журналирование ИИ-рекомендаций

25.4.1 Для значимых ИИ-рекомендаций должны фиксироваться:

1. дата и время формирования рекомендации;
2. тип рекомендации;
3. код обучающегося или иной идентификатор;
4. уровень риска;
5. данные или категории данных, использованные для формирования рекомендации;
6. статус проверки человеком;
7. итоговое решение специалиста;
8. комментарий специалиста;
9. факт принятия, изменения или отклонения рекомендации.

25.4.2 Журналирование ИИ-рекомендаций должно обеспечивать возможность последующего аудита и анализа качества рекомендаций.

25.5 Аудит ИСО

25.5.1 Аудит ИСО проводится для проверки соблюдения требований настоящего стандарта, безопасности данных, корректности доступа, человеческого контроля и качества ИИ-рекомендаций.

25.5.2 Аудит может быть:

1. внутренним;
2. внешним;
3. плановым;
4. внеплановым;
5. тематическим;
6. послеинцидентным.

25.5.3 Аудит должен включать проверку:

1. технической документации;
2. матрицы доступа;
3. журналов действий;
4. журналов инцидентов;
5. ИИ-рекомендаций;
6. фактов человеческой проверки;
7. обезличенных массивов;
8. обращений пользователей;
9. мер по устранению нарушений.

25.6 Периодичность аудита

25.6.1 Для ИСО высокого и критического уровня риска аудит должен проводиться регулярно.

25.6.2 Рекомендуемая периодичность:

Вид ИСО	Минимальная периодичность аудита
Низкий риск	по решению организации
Средний риск	не реже одного раза в год
Высокий риск	не реже одного раза в полугодие
Критический риск	не реже одного раза в квартал и после каждого значимого инцидента

25.7 Отчет по результатам аудита

25.7.1 По итогам аудита составляется отчет.

25.7.2 Отчет должен содержать:

1. дату аудита;
2. состав проверяющих;
3. объект аудита;
4. проверенные документы;
5. выявленные нарушения;

6. уровень риска;
7. рекомендации по устранению;
8. сроки устранения;
9. ответственных лиц;
10. итоговое заключение.

25.7.3 При выявлении нарушений высокого уровня риска эксплуатация отдельного модуля или всей ИСО может быть ограничена до устранения нарушений.

26 Требования к качеству образовательного контента

26.1 Общие положения

26.1.1 Образовательный контент, используемый, создаваемый, адаптируемый или рекомендуемый интеллектуальной системой обучения, должен соответствовать образовательным целям, возрастным особенностям обучающихся, требованиям учебных программ, педагогическим принципам и нормам академической добросовестности.

26.1.2 К образовательному контенту в ИСО относятся:

1. учебные тексты;
2. задания;
3. тесты;
4. объяснения;
5. подсказки;
6. примеры;
7. кейсы;
8. симуляции;
9. обратная связь;
10. рекомендации по обучению;
11. визуальные материалы;
12. интерактивные упражнения;
13. материалы, созданные генеративным ИИ.

26.1.3 Контент, созданный или существенно измененный с использованием искусственного интеллекта, должен проходить проверку человеком перед официальным применением в образовательном процессе.

26.2 Требования к достоверности

26.2.1 Образовательный контент должен быть достоверным, проверяемым и соответствующим современному уровню научных, учебных и методических знаний.

26.2.2 Не допускается использование контента, содержащего:

1. фактические ошибки;
2. недостоверные сведения;

3. вымышленные источники;
4. искаженные определения;
5. некорректные формулы;
6. логические ошибки;
7. противоречия учебной программе;
8. неподтвержденные утверждения, представленные как факт.

26.2.3 Для контента высокого образовательного значения должна быть предусмотрена педагогическая или методическая проверка.

26.3 Требования к соответствию образовательной программе

26.3.1 Контент ИСО должен соответствовать:

1. уровню образования;
2. классу или курсу обучения;
3. учебной программе;
4. образовательным целям;
5. языку обучения;
6. уровню сложности;
7. ожидаемым результатам обучения;
8. методике преподавания соответствующего предмета.

26.3.2 Если контент выходит за рамки учебной программы, это должно быть явно обозначено как дополнительный, расширенный или углубленный материал.

26.3.3 Контент не должен подменять обязательные требования образовательной программы неутвержденными или случайно сгенерированными материалами.

26.4 Требования к возрастной уместности

26.4.1 Контент должен соответствовать возрасту, уровню развития, учебному опыту и психологическим особенностям обучающихся.

26.4.2 Не допускается использование материалов, которые:

1. содержат чрезмерно сложные объяснения без адаптации;
2. вызывают психологический дискомфорт;
3. содержат пугающие, унижающие или травмирующие примеры;
4. используют недопустимые сравнения между обучающимися;
5. содержат содержание, не соответствующее возрасту;
6. формируют чувство неуспешности или неполноценности.

26.4.3 Для несовершеннолетних обучающихся контент должен быть изложен понятным, поддерживающим и педагогически корректным языком.

26.5 Требования к языковой корректности

26.5.1 Контент ИСО должен быть грамматически, стилистически и терминологически корректным.

26.5.2 При использовании нескольких языков обучения контент должен быть проверен на:

1. правильность терминов;
2. отсутствие смысловых искажений при переводе;
3. соответствие языку обучения;
4. понятность для обучающихся;
5. отсутствие дискриминационных или уничижительных выражений.

26.5.3 Автоматический перевод образовательного контента должен проходить проверку специалистом перед использованием.

26.6 Требования к недискриминационному содержанию

26.6.1 Образовательный контент не должен содержать дискриминационных, стереотипных, унижающих или стигматизирующих формулировок.

26.6.2 Не допускается контент, который прямо или косвенно унижает обучающихся по признакам:

1. языка;
2. пола;
3. национальности;
4. места проживания;
5. социального положения;
6. состояния здоровья;
7. инвалидности;
8. особых образовательных потребностей;
9. религии;
10. культурной принадлежности;
11. уровня подготовки;
12. цифрового доступа.

26.6.3 Примеры, задания и кейсы должны быть инклюзивными и уважительными.

26.7 Требования к обратной связи

26.7.1 Обратная связь, формируемая ИСО, должна быть поддерживающей, понятной и ориентированной на развитие обучающегося.

26.7.2 Обратная связь должна:

1. указывать на конкретную ошибку или затруднение;
2. предлагать способ улучшения;
3. не унижать обучающегося;
4. не использовать ярлыки;
5. не создавать ощущение окончательной неуспешности;
6. быть адаптированной к возрасту;
7. при необходимости направлять к педагогу.

26.7.3 Недопустимые формулировки обратной связи:

1. “ты не способен решить это задание”;
2. “у тебя слабый уровень”;
3. “ты не подходишь для этой темы”;
4. “перспективы низкие”;
5. “система определила, что ты не справишься”.

26.7.4 Рекомендуемые формулировки:

1. “попробуй еще раз, обрати внимание на этот шаг”;
2. “эта тема требует дополнительной практики”;
3. “рекомендуется повторить материал”;
4. “можно выбрать задание немного проще и затем вернуться к этому уровню”;
5. “обратись к педагогу за пояснением”.

26.8 Требования к контенту, созданному генеративным ИИ

26.8.1 Контент, созданный генеративным ИИ, должен проходить проверку перед использованием.

26.8.2 Проверка должна включать:

1. достоверность;
2. соответствие учебной программе;
3. отсутствие фактических ошибок;
4. соответствие возрасту;
5. корректность языка;
6. отсутствие дискриминационных формулировок;
7. отсутствие персональных данных;
8. отсутствие вредного или неподходящего содержания;
9. соответствие педагогической цели;
10. академическую добросовестность.

26.8.3 Генеративный ИИ не должен использоваться как единственный источник учебного контента без педагогической проверки.

26.8.4 Если сгенерированный контент используется официально, он должен быть маркирован в соответствии с требованиями настоящего стандарта.

26.9 Требования к обновлению контента

26.9.1 Контент ИСО должен регулярно пересматриваться и обновляться.

26.9.2 Обновление контента проводится при:

1. изменении учебной программы;
2. выявлении ошибок;
3. поступлении жалоб пользователей;
4. изменении методических требований;
5. выявлении дискриминационных или вредных формулировок;

- 6. обновлении ИИ-модулей;
 - 7. изменении возрастной группы обучающихся.
- 26.9.3 Изменения контента должны фиксироваться в журнале изменений.

26.10 Оценка качества контента

26.10.1 Качество образовательного контента должно оцениваться до внедрения и в процессе использования ИСО.

26.10.2 Оценка качества может включать следующие показатели:

Показатель	Описание
Достоверность	отсутствие фактических ошибок
Соответствие программе	связь с учебными целями и результатами
Возрастная уместность	соответствие возрасту и уровню обучающихся
Языковая корректность	правильность терминов, грамматики и стиля
Методическая ценность	полезность для обучения
Инклюзивность	отсутствие дискриминационных формулировок
Безопасность	отсутствие психологически вредного содержания
Проверяемость	возможность проверить источник или основание
Адаптивность	возможность подбора под уровень обучающегося
Удобство восприятия	понятность и логичность подачи

27 Требования к интерфейсам пользователей

27.1 Общие положения

27.1.1 Интерфейсы ИСО должны быть понятными, доступными, безопасными и соответствующими возрасту, роли и задачам пользователей.

27.1.2 Интерфейс должен поддерживать прозрачность использования ИИ, информирование пользователя, защиту данных, человеческий контроль и возможность обращения за помощью.

27.1.3 Интерфейс не должен создавать психологическое давление, формировать негативные ярлыки, публично сравнивать обучающихся или представлять ИИ-рекомендации как окончательные решения.

27.2 Требования к интерфейсу обучающегося

27.2.1 Интерфейс обучающегося должен быть простым, понятным и поддерживающим.

27.2.2 Интерфейс обучающегося должен обеспечивать:

1. доступ к заданиям;
2. получение обратной связи;

3. просмотр собственного прогресса в понятной форме;
4. получение подсказок;
5. возможность задать вопрос или обратиться за помощью;
6. указание на использование ИИ, если это применимо;
7. понятное объяснение рекомендаций;
8. отсутствие доступа к данным других обучающихся.

27.2.3 Интерфейс обучающегося не должен:

1. публично сравнивать его с другими обучающимися;
2. отображать унижающие рейтинги;
3. использовать ярлыки «слабый», «неодаренный», «неперспективный»;
4. показывать негативные прогнозы без педагогического сопровождения;
5. создавать ощущение наказания за ошибку;
6. скрывать факт автоматической рекомендации.

27.3 Требования к интерфейсу педагога

27.3.1 Интерфейс педагога должен обеспечивать возможность педагогической интерпретации данных и проверки ИИ-рекомендаций.

27.3.2 Интерфейс педагога должен позволять:

1. просматривать учебный прогресс обучающихся;
2. видеть рекомендации ИСО;
3. получать сведения о том, какие данные использованы для рекомендации;
4. принимать, изменять или отклонять ИИ-рекомендацию;
5. оставлять педагогический комментарий;
6. фиксировать итоговое решение;
7. видеть предупреждения о высоком уровне риска рекомендации;
8. передавать спорный случай на дополнительную проверку;
9. видеть только те данные, к которым педагог имеет право доступа.

27.3.3 Интерфейс педагога должен напоминать, что ИИ-рекомендации являются вспомогательными и не заменяют профессиональное педагогическое решение.

27.4 Требования к интерфейсу родителя или законного представителя

27.4.1 Если в ИСО предусмотрен интерфейс родителя или законного представителя, он должен быть понятным, безопасным и ограниченным данными конкретного обучающегося.

27.4.2 Интерфейс должен обеспечивать:

1. просмотр общей информации о назначении ИСО;
2. информацию о целях обработки данных;

3. доступ к данным своего ребенка в установленном объеме;
4. возможность получить объяснение значимой ИИ-рекомендации;
5. возможность направить обращение;
6. возможность ознакомиться со статусом согласия;
7. информацию о порядке отзыва согласия.

27.4.3 Родитель или законный представитель не должен иметь доступ к данным других обучающихся.

27.5 Требования к интерфейсу психолога

27.5.1 Интерфейс психолога должен обеспечивать доступ только к тем данным, которые необходимы для психолого-педагогического сопровождения.

27.5.2 Интерфейс психолога должен позволять:

1. просматривать релевантные диагностические и психолого-педагогические данные;
2. интерпретировать результаты;
3. проверять рекомендации, связанные с мотивацией, эмоциональным состоянием, стрессом или сопровождением;
4. оставлять профессиональный комментарий;
5. ограничивать передачу чувствительных данных другим пользователям;
6. передавать спорные случаи на экспертное рассмотрение.

27.5.3 Интерфейс психолога должен исключать автоматическое формирование окончательного психологического заключения без участия специалиста.

27.6 Требования к интерфейсу исследователя

27.6.1 Интерфейс исследователя должен быть ориентирован преимущественно на работу с обезличенными, псевдонимизированными или агрегированными данными.

27.6.2 Интерфейс исследователя должен обеспечивать:

1. доступ к исследовательским массивам без прямых идентификаторов;
2. формирование статистических отчетов;
3. выгрузку обезличенных данных;
4. анализ образовательных результатов;
5. проверку качества данных;
6. исключение прямого доступа к ФИО, контактам и иным идентификаторам, если это не требуется и специально не разрешено.

27.7 Требования к интерфейсу администратора

27.7.1 Интерфейс администратора должен обеспечивать техническое управление системой без избыточного раскрытия содержательных данных обучающихся.

27.7.2 Интерфейс администратора должен позволять:

1. создавать и блокировать учетные записи;
2. назначать роли;
3. управлять правами доступа;
4. просматривать технические журналы;
5. контролировать работоспособность системы;
6. фиксировать инциденты;
7. ограничивать доступ при нарушениях.

27.7.3 Администратор не должен по умолчанию иметь доступ к чувствительным диагностическим и психолого-педагогическим данным обучающихся.

27.8 Требования к доступности интерфейсов

27.8.1 Интерфейсы ИСО должны учитывать потребности пользователей с разным уровнем цифровой грамотности.

27.8.2 При проектировании интерфейсов рекомендуется учитывать:

1. простоту навигации;
2. понятность терминов;
3. адаптацию под возраст;
4. доступность для пользователей с особыми образовательными потребностями;
5. возможность использования на разных устройствах;
6. ясность сообщений об ошибках;
7. возможность получить помощь;
8. поддержку государственного, русского и при необходимости иных языков обучения.

28 Требования к тестированию

28.1 Общие положения

28.1.1 До апробации и внедрения интеллектуальная система обучения должна пройти комплексное тестирование.

28.1.2 Тестирование должно подтвердить, что ИСО соответствует функциональным, педагогическим, техническим, этическим и безопасностным требованиям.

28.1.3 Результаты тестирования должны быть документально зафиксированы.

28.1.4 ИСО не допускается к апробации или внедрению при наличии критических ошибок, влияющих на безопасность данных, корректность ИИ-рекомендаций, права обучающихся или возможность причинения вреда.

28.2 Виды тестирования

28.2.1 ИСО должна пройти следующие виды тестирования:

1. функциональное тестирование;
2. тестирование безопасности;
3. тестирование ролей и доступа;
4. тестирование обработки данных;
5. тестирование обезличивания и псевдонимизации;
6. тестирование ИИ-модулей;
7. тестирование генеративного контента;
8. тестирование человеческой проверки рекомендаций;
9. тестирование журналирования;
10. тестирование пользовательских интерфейсов;
11. тестирование производительности;
12. тестирование сценариев отказа, удаления данных и отзыва согласия;
13. тестирование реагирования на инциденты.

28.3 Функциональное тестирование

28.3.1 Функциональное тестирование должно проверить соответствие функций ИСО техническому заданию.

28.3.2 Проверяются:

1. регистрация и авторизация пользователей;
2. работа пользовательских ролей;
3. ввод и сохранение данных;
4. выполнение заданий;
5. формирование рекомендаций;
6. генерация контента;
7. просмотр результатов;
8. работа аналитических отчетов;
9. экспорт данных;
10. обработка ошибок.

28.4 Тестирование безопасности

28.4.1 Тестирование безопасности должно проверить защищенность данных и доступов.

28.4.2 Проверяются:

1. корректность аутентификации;
2. разграничение доступа;

3. защита чувствительных данных;
4. блокировка неактуальных учетных записей;
5. невозможность доступа к чужим данным;
6. фиксация попыток несанкционированного доступа;
7. ограничения экспорта данных;
8. защита административных функций;
9. сохранность журналов;
10. реагирование на инциденты.

28.5 Тестирование ИИ-модулей

28.5.1 Тестирование ИИ-модулей должно проверить корректность, безопасность, объяснимость и педагогическую уместность результатов.

28.5.2 Проверяются:

1. корректность входных данных;
2. стабильность результатов;
3. соответствие рекомендаций образовательной цели;
4. отсутствие очевидных ошибок;
5. отсутствие дискриминационных результатов;
6. отсутствие стигматизирующих формулировок;
7. возможность человеческой проверки;
8. возможность отклонения рекомендации;
9. фиксация рекомендации в журнале;
10. возможность отключения модуля.

28.6 Тестирование генеративного ИИ

28.6.1 При наличии генеративного ИИ проводится отдельное тестирование создаваемого контента.

28.6.2 Проверяются:

1. фактическая достоверность;
2. соответствие учебной программе;
3. возрастная уместность;
4. отсутствие вредного содержания;
5. отсутствие персональных данных в запросах и ответах;
6. отсутствие дискриминационных формулировок;
7. качество объяснений;
8. корректность заданий;
9. маркировка ИИ-контента;
10. возможность педагогической проверки.

28.7 Тестирование человеческого контроля

28.7.1 Тестирование должно подтвердить, что значимые ИИ-рекомендации могут быть проверены человеком.

28.7.2 Проверяются:

1. отображение рекомендации специалисту;
2. возможность принять рекомендацию;
3. возможность изменить рекомендацию;
4. возможность отклонить рекомендацию;
5. возможность добавить комментарий;
6. фиксация проверяющего специалиста;
7. фиксация даты проверки;
8. передача спорной рекомендации на экспертное рассмотрение.

28.8 Тестирование отзыва согласия и удаления данных

28.8.1 ИСО должна пройти тестирование сценариев отзыва согласия и удаления данных.

28.8.2 Проверяются:

1. фиксация отзыва согласия;
2. прекращение дальнейшей обработки данных;
3. исключение обучающегося из активных процедур;
4. удаление или обезличивание данных;
5. фиксация удаления;
6. сохранение данных только при наличии правового основания;
7. корректное уведомление ответственных лиц.

28.9 Документирование результатов тестирования

28.9.1 По итогам тестирования составляется отчет.

28.9.2 Отчет должен содержать:

Раздел	Содержание
Наименование ИСО	
Дата тестирования	
Версия системы	
Вид тестирования	
Ответственные лица	
Выявленные ошибки	
Уровень риска	
Принятые меры	
Остаточные риски	

Итоговое заключение	
---------------------	--

28.9.3. Ошибки классифицируются по уровню риска:

Уровень ошибки	Описание
Низкий	не влияет на безопасность и права пользователей
Средний	влияет на удобство или отдельные функции
Высокий	может повлиять на данные, рекомендации или доступ
Критический	создает риск утечки, дискриминации, вреда или неправомерной обработки

28.9.4 Критические ошибки должны быть устранены до начала апробации или внедрения.

29 Требования к апробации

29.1 Общие положения

29.1.1 Апробация интеллектуальной системы обучения проводится до ее широкого внедрения в образовательный процесс.

29.1.2 Цель апробации - проверить работоспособность, педагогическую полезность, безопасность, качество ИИ-рекомендаций, корректность обработки данных, удобство интерфейса и соответствие ИСО требованиям настоящего стандарта.

29.1.3 Апробация должна проводиться в контролируемых условиях, с ограниченным кругом участников, при наличии ответственных лиц, плана апробации, механизмов мониторинга и порядка реагирования на инциденты.

29.1.4 ИСО высокого и критического уровня риска не допускается к апробации без предварительного тестирования, оценки рисков и этической экспертизы.

29.2 Условия допуска к апробации

29.2.1 До начала апробации должны быть выполнены следующие условия:

1. разработано техническое задание;
2. подготовлена проектная и техническая документация;
3. определены категории пользователей;
4. определены категории обрабатываемых данных;
5. проведено внутреннее тестирование;
6. проведена проверка безопасности;

7. проведена этическая экспертиза, если система относится к высокому или критическому уровню риска;
8. определены ответственные лица;
9. настроены роли и уровни доступа;
10. подготовлены формы информирования и согласия;
11. получены необходимые согласия;
12. подготовлен план апробации;
13. определен порядок человеческой проверки ИИ-рекомендаций;
14. подготовлен журнал инцидентов;
15. подготовлен план мониторинга.

29.3 План апробации

29.3.1 План апробации должен содержать:

Раздел плана	Содержание
Наименование ИСО	название системы
Цель апробации	что проверяется
Место проведения	организация образования
Сроки проведения	начало и окончание
Участники	обучающиеся, педагоги, психологи, родители, исследователи
Функции системы	какие модули апробируются
Категории данных	какие данные обрабатываются
Ответственные лица	координатор, технический специалист, педагог, психолог
Порядок информирования	как информируются участники
Порядок согласия	как собираются согласия
Порядок мониторинга	как фиксируются результаты
Порядок реагирования на инциденты	что делать при ошибке или жалобе
Критерии завершения	условия окончания апробации

29.4 Ограниченная пилотная апробация

29.4.1 Первичная апробация ИСО должна проводиться в ограниченном масштабе.

29.4.2 Ограниченная апробация применяется для:

1. проверки базовой работоспособности;
2. выявления технических ошибок;
3. проверки интерфейсов;
4. оценки корректности обработки данных;
5. проверки ИИ-рекомендаций;
6. оценки человеческого контроля;
7. выявления рисков дискриминации или стигматизации;

8. оценки реакции пользователей.

29.4.3 Расширение апробации допускается только после анализа результатов ограниченного пилота и устранения выявленных рисков.

29.5 Сбор данных в ходе апробации

29.5.1 В ходе апробации должны собираться только те данные, которые необходимы для заявленных целей.

29.5.2 В ходе апробации фиксируются:

1. число участников;
2. категории пользователей;
3. используемые функции ИСО;
4. категории обработанных данных;
5. сформированные ИИ-рекомендации;
6. случаи человеческой проверки;
7. принятые, измененные и отклоненные рекомендации;
8. обращения пользователей;
9. жалобы;
10. технические ошибки;
11. инциденты;
12. корректирующие меры.

29.5.3 Результаты апробации для внешних отчетов и публикаций должны использоваться в обезличенном или агрегированном виде.

29.6 Критерии успешности апробации

29.6.1 Апробация считается успешной, если:

1. система выполняет заявленные функции;
2. критические ошибки не выявлены;
3. персональные данные защищены;
4. доступы работают корректно;
5. журналирование функционирует;
6. значимые ИИ-рекомендации проходят человеческую проверку;
7. не выявлены признаки систематической дискриминации;
8. не выявлены стигматизирующие формулировки;
9. пользователи получают понятные объяснения;
10. образовательный контент соответствует требованиям качества;
11. инциденты фиксируются и устраняются;
12. пользователи могут обратиться за разъяснением или помощью.

29.7 Отчет по итогам апробации

29.7.1 По итогам апробации составляется отчет.

29.7.2 Отчет должен включать:

1. сведения об ИСО;
2. период апробации;
3. место проведения;
4. состав участников;
5. использованные функции;
6. категории обработанных данных;
7. результаты тестирования в реальных условиях;
8. количество и типы ИИ-рекомендаций;
9. результаты человеческой проверки;
10. выявленные ошибки;
11. обращения и жалобы;
12. инциденты;
13. оценку рисков;
14. оценку педагогической полезности;
15. рекомендации по доработке;
16. итоговое заключение.

29.7.3 По итогам апробации может быть принято одно из решений:

1. рекомендовать ИСО к внедрению;
2. рекомендовать ИСО к внедрению с ограничениями;
3. направить ИСО на доработку;
4. провести повторную апробацию;
5. приостановить использование ИСО.

30 Требования к мониторингу

30.1 Общие положения

30.1.1 После начала апробации или внедрения ИСО должен проводиться регулярный мониторинг.

30.1.2 Мониторинг направлен на проверку качества, безопасности, этичности, педагогической полезности, корректности ИИ-рекомендаций, соблюдения прав обучающихся и защиты данных.

30.1.3 Мониторинг проводится организацией, использующей ИСО, разработчиком, оператором системы, экспертной группой или иным уполномоченным субъектом.

30.2 Объекты мониторинга

30.2.1 Мониторингу подлежат:

1. корректность работы ИСО;
2. качество ИИ-рекомендаций;
3. качество образовательного контента;

4. соблюдение доступа к данным;
5. соблюдение информирования и согласия;
6. корректность обезличивания;
7. работа механизмов человеческого контроля;
8. обращения пользователей;
9. жалобы;
10. инциденты;
11. признаки дискриминации;
12. признаки стигматизации;
13. безопасность данных;
14. стабильность работы системы;
15. соответствие требованиям настоящего стандарта.

30.3 Виды мониторинга

Вид мониторинга	Когда проводится
Предварительный	до начала апробации
Плановый	регулярно в период применения ИСО
Тематический	при проверке отдельного модуля, функции или риска
Внеплановый	при жалобе, инциденте или ошибочной рекомендации
Послеинцидентный	после утечки, сбоя, дискриминационного результата
Итоговый	по завершении этапа апробации или внедрения

30.4 Показатели мониторинга

30.4.1 Минимальные показатели мониторинга:

Направление	Показатель
Согласие	доля участников с оформленным согласием
Доступ	количество нарушений прав доступа
Безопасность	количество инцидентов безопасности
ИИ-рекомендации	доля рекомендаций, проверенных человеком
Качество рекомендаций	доля отклоненных или измененных рекомендаций
Контент	количество выявленных ошибок в учебных материалах
Дискриминация	наличие различий в рекомендациях по группам обучающихся
Обращения	количество жалоб и запросов на разъяснение
Обезличивание	наличие прямых идентификаторов в исследовательских массивах
Интерфейс	число ошибок и затруднений пользователей
Надежность	количество технических сбоев
Удовлетворенность	отзывы педагогов, обучающихся, родителей

30.5 Мониторинг ИИ-рекомендаций

30.5.1 ИИ-рекомендации должны регулярно проверяться на:

1. корректность;
2. педагогическую обоснованность;
3. объяснимость;
4. отсутствие дискриминации;
5. отсутствие стигматизации;
6. соответствие исходным данным;
7. необходимость человеческой проверки;
8. влияние на обучающегося.

30.5.2 Особое внимание уделяется рекомендациям высокого и критического уровня риска.

30.5.3 Рекомендации, которые часто отклоняются специалистами, должны быть проанализированы для выявления причин ошибок.

30.6 Мониторинг обращений и жалоб

30.6.1 Организация должна учитывать обращения обучающихся, родителей, педагогов и других пользователей.

30.6.2 Анализ обращений должен включать:

1. количество обращений;
2. тип обращения;
3. срок рассмотрения;
4. принятые меры;
5. повторяемость проблемы;
6. необходимость доработки ИСО.

30.6.3 Обращения, связанные с вредом обучающемуся, дискриминацией, утечкой данных или стигматизацией, должны рассматриваться в приоритетном порядке.

30.7 Отчет мониторинга

30.7.1 По итогам мониторинга составляется отчет.

30.7.2 Отчет мониторинга должен содержать:

1. дату мониторинга;
2. объект мониторинга;
3. проверяемый период;
4. состав рабочей группы;
5. проверенные документы и журналы;
6. выявленные нарушения;
7. уровень риска;
8. обращения и жалобы;
9. инциденты;
10. качество ИИ-рекомендаций;

11. качество контента;
 12. меры по устранению нарушений;
 13. ответственных лиц;
 14. сроки повторной проверки;
 15. итоговое решение.
- 30.7.3 По итогам мониторинга может быть принято решение:
1. продолжить использование ИСО;
 2. продолжить использование с ограничениями;
 3. доработать отдельные модули;
 4. ограничить доступ к данным;
 5. провести повторную экспертизу;
 6. приостановить работу отдельного ИИ-модуля;
 7. приостановить использование ИСО.

31 Требования к управлению рисками

31.1 Общие положения

31.1.1 Разработка, внедрение и применение ИСО должны сопровождаться выявлением, оценкой, снижением и мониторингом рисков.

31.1.2 Управление рисками должно осуществляться на всех этапах жизненного цикла ИСО.

31.1.3 Для ИСО высокого и критического уровня риска управление рисками является обязательным условием апробации и внедрения.

31.2 Основные категории рисков

Категория риска	Возможное проявление
Правовой риск	обработка данных без основания или согласия
Этический риск	вред обучающемуся, стигматизация, давление
Риск безопасности	утечка, потеря, несанкционированный доступ
Педагогический риск	неверная траектория, некачественная рекомендация
Риск дискриминации	неравные рекомендации для разных групп
Технический риск	сбой, ошибка, недоступность системы
Риск качества данных	неполные, устаревшие или ошибочные данные
Риск генеративного ИИ	недостоверный, вредный или неподходящий контент
Репутационный риск	снижение доверия к организации или ИСО
Риск непрозрачности	невозможность объяснить значимую рекомендацию

31.3 Процесс управления рисками

31.3.1 Управление рисками включает:

1. выявление риска;

2. описание риска;
3. определение причины риска;
4. оценку вероятности и возможного вреда;
5. определение уровня риска;
6. разработку мер снижения;
7. назначение ответственного лица;
8. мониторинг остаточного риска;
9. пересмотр риска после изменений системы.

31.4 Оценка уровня риска

31.4.1 Уровень риска определяется по сочетанию вероятности и возможного вреда.

Уровень риска	Описание
Низкий	риск маловероятен и не оказывает существенного влияния
Средний	риск возможен, но последствия ограничены
Высокий	риск вероятен или может существенно повлиять на данные, права или обучение
Критический	риск может привести к утечке, дискриминации, вреду обучающемуся или нарушению прав

31.4.2 Критические риски должны быть устранены до внедрения ИСО.

31.4.3 Высокие риски требуют мер снижения, мониторинга и ответственного лица.

31.5 Реестр рисков

31.5.1 Для ИСО высокого и критического уровня риска должен вестись реестр рисков.

№	Риск	Причина	Последствия	Уровень риска	Меры снижения	Ответственный	Статус
1				☐ низкий ☐ средний ☐ высокий ☐ критический			
2				☐ низкий ☐ средний ☐ высокий ☐ критический			
3				☐ низкий ☐ средний ☐ высокий ☐ критический			

31.6 Минимальные меры снижения рисков

Риск	Мера снижения
Утечка данных	разграничение доступа, журналирование, защищенное хранение
Ошибочная ИИ-рекомендация	человеческая проверка, мониторинг отклонений
Дискриминация	аудит рекомендаций по группам обучающихся
Стигматизация	запрет ярлыков, педагогическая интерпретация
Избыточный сбор данных	минимизация данных, карта данных
Непрозрачность	объяснение рекомендаций, информирование пользователей
Низкое качество контента	педагогическая проверка
Технический сбой	тестирование, резервное копирование
Неправомерный экспорт	ограничения выгрузки, журнал экспорта
Нарушение согласия	реестр согласий, блокировка обработки при отзыве

32 Требования к документации ИСО

32.1 Общие положения

32.1.1 Для каждой ИСО должна быть подготовлена документация, подтверждающая соответствие системы требованиям настоящего стандарта.

32.1.2 Документация должна быть актуальной, доступной ответственным лицам и обновляться при изменении функций, данных, ИИ-модулей или условий применения системы.

32.2 Обязательный комплект документации

32.2.1 Минимальный комплект документации ИСО включает:

1. техническое задание;
2. описание архитектуры системы;
3. описание пользователей и ролей;
4. карту данных;
5. матрицу доступа;
6. описание ИИ-модулей;
7. описание генеративных функций;
8. политику обработки данных;
9. порядок информирования и согласия;
10. регламент обезличивания;
11. порядок человеческой проверки ИИ-рекомендаций;

12. порядок реагирования на инциденты;
13. отчет тестирования;
14. заключение этической экспертизы, если применимо;
15. отчет апробации;
16. отчет мониторинга;
17. журнал изменений;
18. инструкции пользователей;
19. инструкция администратора;
20. реестр рисков.

32.3 Техническая документация

32.3.1 Техническая документация должна включать:

1. описание архитектуры;
2. описание базы данных;
3. описание интеграций;
4. описание API, если применимо;
5. описание механизмов безопасности;
6. описание журналирования;
7. описание резервного копирования;
8. описание ролей доступа;
9. описание процедур обновления;
10. описание вывода из эксплуатации.

32.4 Документация ИИ-модулей

32.4.1 Документация ИИ-модулей должна включать:

1. назначение модуля;
2. входные данные;
3. выходные результаты;
4. алгоритмический подход;
5. ограничения применения;
6. уровень риска;
7. порядок человеческой проверки;
8. показатели качества;
9. порядок мониторинга;
10. порядок отключения.

32.5 Пользовательская документация

32.5.1 Пользовательская документация должна быть подготовлена для основных групп пользователей:

1. обучающихся;
2. педагогов;

3. родителей или законных представителей;
4. психологов;
5. исследователей;
6. администраторов.

32.5.2 Документация для обучающихся должна быть изложена простым и доступным языком.

32.5.3 Документация для педагогов должна включать порядок интерпретации ИИ-рекомендаций и напоминание об их вспомогательном характере.

32.6 Журнал изменений

32.6.1 Все значимые изменения ИСО должны фиксироваться в журнале изменений.

32.6.2 Журнал изменений должен содержать:

Дата	Версия	Изменение	Причина	Риск	Ответственный
				☐ низкий ☐ средний ☐ высокий ☐ критический	

32.6.3 Изменения ИИ-модулей высокого и критического риска должны проходить повторную оценку рисков и при необходимости этическую экспертизу.

33 Требования к оценке качества ИСО

33.1 Общие положения

33.1.1 Оценка качества ИСО проводится для определения соответствия системы образовательным, техническим, этическим, безопасностным и пользовательским требованиям.

33.1.2 Оценка качества проводится до внедрения, после апробации и в процессе эксплуатации.

33.2 Направления оценки качества

Направление	Что оценивается
Педагогическая полезность	помогает ли система достижению образовательных целей
Точность ИИ-рекомендаций	корректность и обоснованность рекомендаций
Качество контента	достоверность, возрастная уместность, методическая ценность

Безопасность данных	защита, доступ, журналирование
Прозрачность	понятность функций ИИ
Объяснимость	возможность объяснить значимые рекомендации
Человеческий контроль	проверка значимых рекомендаций специалистом
Недискриминация	отсутствие предвзятых результатов
Удобство использования	понятность интерфейса
Надежность	стабильность работы
Документированность	наличие необходимой документации
Соответствие стандарту	выполнение требований настоящего стандарта

33.3 Показатели оценки качества

33.3.1 Для оценки качества ИСО могут использоваться следующие показатели:

1. доля корректно выполненных функций;
2. количество технических ошибок;
3. количество критических ошибок;
4. доля ИИ-рекомендаций, проверенных человеком;
5. доля отклоненных ИИ-рекомендаций;
6. количество жалоб пользователей;
7. количество инцидентов безопасности;
8. количество выявленных дискриминационных результатов;
9. уровень удовлетворенности педагогов;
10. уровень удовлетворенности обучающихся;
11. уровень удовлетворенности родителей;
12. количество ошибок в сгенерированном контенте;
13. полнота документации;
14. соответствие техническому заданию.

33.4 Методы оценки качества

33.4.1 Оценка качества ИСО может проводиться с использованием:

1. экспертной оценки;
2. педагогической экспертизы;
3. технического тестирования;
4. анализа журналов;
5. анализа ИИ-рекомендаций;
6. анализа обращений и жалоб;
7. опросов пользователей;
8. сравнения с техническим заданием;
9. аудита безопасности;
10. анализа образовательных результатов;
11. проверки обезличенных массивов данных.

33.5 Итоговое заключение о качестве

33.5.1 По результатам оценки качества составляется заключение.

33.5.2 Заключение может содержать одно из решений:

1. ИСО соответствует требованиям стандарта;
2. ИСО соответствует требованиям стандарта с замечаниями;
3. ИСО требует доработки;
4. ИСО не допускается к внедрению;
5. отдельный ИИ-модуль подлежит ограничению или отключению.

34 Порядок пересмотра стандарта

34.1 Общие положения

34.1.1 Настоящий стандарт подлежит периодическому пересмотру с учетом развития законодательства, технологий ИИ, практики применения ИСО и международных стандартов.

34.1.2 Пересмотр стандарта может проводиться планово или внепланово.

34.2 Основания для пересмотра

Основаниями для пересмотра стандарта являются:

1. изменение законодательства Республики Казахстан;
2. принятие новых международных или национальных стандартов в области ИИ;
3. развитие генеративного ИИ;
4. появление новых рисков;
5. результаты апробации ИСО;
6. результаты мониторинга и аудита;
7. обращения организаций образования;
8. предложения разработчиков и экспертов;
9. выявление пробелов в требованиях стандарта;
10. необходимость гармонизации с международными подходами.

34.3 Периодичность пересмотра

34.3.1 Плановый пересмотр стандарта рекомендуется проводить не реже одного раза в пять лет.

34.3.2 Внеплановый пересмотр проводится при существенном изменении нормативной, технологической или образовательной среды.

34.4 Порядок внесения изменений

34.4.1 Предложения по изменению стандарта могут вноситься:

1. уполномоченными органами;
2. национальным органом по стандартизации;
3. организациями образования;
4. научными организациями;
5. разработчиками ИИ-систем;
6. экспертными организациями;
7. профессиональными объединениями;
8. иными заинтересованными сторонами.

34.4.2 Изменения должны проходить экспертное обсуждение и согласование в установленном порядке.

35 Заключительные положения

35.1 Настоящий стандарт устанавливает общие требования к ИСО, применяемым в организациях образования Республики Казахстан.

35.2 Стандарт направлен на обеспечение безопасного, прозрачного, педагогически обоснованного, проверяемого и недискриминационного использования искусственного интеллекта в образовании.

35.3 ИСО должна применяться как инструмент поддержки обучающегося, педагога, родителя, психолога, исследователя и организации образования.

35.4 ИИ не должен заменять профессиональное педагогическое, психологическое, методическое или экспертное решение в случаях, когда результат влияет на права, образовательные возможности, самооценку или благополучие обучающегося.

35.5 Значимые ИИ-рекомендации должны проходить человеческую проверку.

35.6 Данные обучающихся должны обрабатываться только на законных основаниях, в заранее определенных целях, с соблюдением принципов минимизации, безопасности, конфиденциальности и проверяемости.

35.7 ИСО не должна использоваться для дискриминации, стигматизации, скрытого ранжирования или автоматического ограничения образовательных возможностей обучающихся.

35.8 Организации, разрабатывающие, внедряющие или применяющие ИСО, должны обеспечивать:

1. документацию системы;
2. информирование пользователей;
3. защиту данных;
4. человеческий контроль;
5. мониторинг;
6. управление рисками;

7. реагирование на инциденты;
8. регулярную оценку качества.

35.9 Настоящий стандарт может применяться как основа для:

1. разработки образовательных ИИ-платформ;
2. подготовки технических заданий;
3. экспертизы ИИ-систем в образовании;
4. разработки локальных актов организаций образования;
5. проведения апробации и внедрения ИСО;
6. оценки качества и безопасности образовательных ИИ-систем;
7. подготовки педагогов и специалистов к использованию ИИ;
8. формирования национальной политики в сфере искусственного

интеллекта в образовании.

35.10 Главный принцип настоящего стандарта:

ИИ в образовании должен усиливать возможности человека, защищать права обучающегося, повышать качество обучения и не использоваться как инструмент автоматического ограничения, стигматизации или дискриминации.