ALTYNSARIN AKADEMIASY

ЭТИЧЕСКИЕ СТАНДАРТЫ

ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ, В ТОМ ЧИСЛЕ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОРГАНИЗАЦИЯХ СРЕДНЕГО, ТЕХНИЧЕСКОГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ РК

Этические стандарты применения информационных систем, в том числе систем искусственного интеллекта в организациях среднего, технического и профессионального образования РК

Введение

Этика педагогического взаимодействия педагога и обучающегося является необходимым условием качества образования в цифровой среде. Настоящий Стандарт устанавливает принципы и обязательные требования к ответственному применению информационных технологий и искусственного интеллекта в организациях среднего, технического и профессионального образования Республики Казахстан, обеспечивая уважение достоинства личности, справедливость, инклюзию, академическую честность, безопасность и законность. Применение ИИ не подменяет профессиональное суждение педагога: **решение принимает человек**. Стандарт закрепляет требования прозрачности и подотчетности, недопущения дискриминации, минимизации данных и защиты персональных данных, а также атрибуции использования ИИ, направляя цифровую практику на поддержку учебных достижений и благополучия обучающихся.

Раздел 1. Общие положения

1.1. Назначение и статус

1.1.1. Настоящий Стандарт устанавливает обязательные требования к ответственному применению информационных систем и систем искусственного интеллекта в организациях среднего образования Республики Казахстан.

1.1.2. Стандарт учитывает необходимость стимулирования инноваций в образовательных технологиях, обеспечивая баланс между защитой прав и возможностями для развития новых решений.

1.1.3. Стандарт обязателен для организаций, подведомственных Министерству просвещения Республики Казахстан. Рекомендуется к применению в дополнительном образовании и проектах с участием обучающихся.

1.1.4. Стандарт применяется совместно с Типовыми правилами использования ИИ, Положением об управлении этикой ИИ и Положением о школьном Этическом совете по ИИ. При коллизии норм приоритет имеет законодательство Республики Казахстан.

1.2. Правовая основа

1.2.1. Конституция Республики Казахстан.

1.2.2. Международные договоры, ратифицированные Республикой Казахстан, имеющие приоритет перед законами и применяемые непосредственно, если не требуется издание закона.

1.2.3. Конституционные законы Республики Казахстан.

1.2.4. Кодексы Республики Казахстан (в т.ч. Гражданский кодекс; Трудовой кодекс; Кодекс об административных процедурах и административных процессах; Кодекс об административных правонарушениях).

1.2.5. Законы Республики Казахстан, регулирующие соответствующие отношения, включая: «Об образовании»; «О персональных данных и их защите»; «Об информатизации»; «Об авторском праве и смежных правах»; «О правах ребенка в Республике Казахстан»; а также иные законы.

1.2.6. Подзаконные нормативные правовые акты: указы Президента, постановления Правительства, приказы уполномоченных органов и иные акты, принятые во исполнение законодательных актов.

1.3. Цели

1.3.1. Защита прав и законных интересов обучающихся и педагогов.

1.3.2. Повышение качества образования при управлении рисками применения ИИ.

1.3.3. Сохранение и развитие автономных человеческих умений.

1.3.4. Обеспечение академической добросовестности и формирование индивидуального стиля обучающегося.

1.3.5. Обеспечение справедливости, недискриминации и доступности.

1.4. Область применения

1.4.1. Учебные занятия, оценивание, внеурочная деятельность, администрирование, проектная и исследовательская работа обучающихся, повышение квалификации педагогов.

1.4.2. Все классы и уровни ТиПО. Допуски ИИ дифференцируются по возрасту, предмету и виду задания.

1.5. Базовые установки

1.5.1. Многие этические вопросы применения ИИ не имеют единственно правильного решения. В сфере образования обязательны: анализ рисков, принцип предосторожности и пропорциональности, приоритет интересов ребенка, справедливость, прозрачность и подотчетность, участие заинтересованных сторон, право на пересмотр решений.

1.5.2. Признается межпоколенческий разрыв навыков. Применяется принцип «сначала порог автономных умений, затем поддержка ИИ». Ключевые формы оценивания предусматривают задания без использования ИИ. Любое использование ИИ подлежит маркировке и рефлексии.

1.6. Педагогическая целесообразность и индивидуальный стиль

1.6.1. Организации образования обеспечивают формирование индивидуального стиля мышления и письма обучающихся посредством регулярной самостоятельной практики.

1.6.2. Нерациональное использование ИИ, приводящее к утрате или несформированности индивидуального стиля, не допускается.

1.6.3. Запрещается делегировать ИИ или третьим лицам выполнение работ,

направленных на проверку собственных рассуждений, аргументации и стиля обучающегося, если иное не предусмотрено заданием.

1.6.4. Требования к выполнению письменных и устных работ:

а) Черновой этап выполняется автономно без ИИ. Разрешается последующая редакторская поддержка ИИ с обязательной рефлексией о внесенных изменениях.

б) В заданиях с допуском ИИ педагог устанавливает минимальный автономный вклад обучающегося и критерии его подтверждения.

в) Любой текст, созданный или существенно отредактированный с применением ИИ, подлежит маркировке с указанием инструмента, версии при наличии, режима использования и характера правок.

г) При сомнениях в авторстве обязательны устная защита, сравнительный анализ работ и дополнительные задания без ИИ.

д) В проектных и исследовательских работах допускается «редакторский» режим ИИ (язык, структура, форматирование, визуализация). «Авторский» режим, при котором ИИ генерирует основные идеи, аргументацию или результаты при целях задания на собственное рассуждение, запрещается.

1.7. Навигация в информационном изобилии

1.7.1. Педагоги и обучающиеся обязаны осваивать и применять навыки ориентации в избыточной информации, включая материалы, сгенерированные ИИ.

1.7.2. Обязательные результаты обучения:

а) Компиляция и конвертирование материалов под цель и аудиторию.

б) Выделение главного и сжатие содержания без потери смысла.

в) Выявление логических ошибок, манипуляций и фейковой информации, базовая проверка фактов и трассировка источников.

г) Контекстуальная адаптация знаний между предметами и задачами.

1.7.3. Организации образования обеспечивают повышение квалификации педагогов по указанным навыкам, включая:

а) Модульные программы по применению ИИ как редактора, ассистента поиска, агрегатора и проверяющего.

б) Тренажеры по критическому чтению и проверке аргументации.

в) Методические кейсы с матрицами допусков ИИ, примерами рефлексии и типовыми ошибками.

г) Введение микрооценивания заданий по компиляции, фактчекингу и выявлению логических ошибок.

д) Супервизию и обмен практиками на уровне школы и региона.

1.8. Принципы ответственного применения ИИ

1.8.1. Человекоцентричность и приоритет интересов ребенка.

1.8.2. Предосторожность и пропорциональность рискам.

1.8.3. Справедливость и недискриминация.

1.8.4. Прозрачность, объяснимость, подотчетность, право на пересмотр.

1.8.5. Академическая добросовестность и сохранение автономных умений.

1.8.6. Конфиденциальность, минимизация и безопасность данных.

1.8.7. Педагогическая целесообразность и доказательная эффективность.

1.8.8. Инклюзивность и доступность. Языковая и культурная чувствительность.

1.8.9. Совместимость, интероперабельность и кибербезопасность.

1.9. Роли и ответственность

1.9.1. Министерство просвещения Республики Казахстан: формирование нормативной базы, финансирование мероприятий, контроль исполнения.

1.9.2. Национальная академия образования имени Ы. Алтынсарина: методическая политика, разработка типовых материалов, оценка практик.

1.9.3. Организация образования: принятие локальных актов, ведение матриц допусков ИИ по предметам и классам, защита данных, функционирование школьного Этического совета по ИИ, подготовка кадров.

1.9.4. Педагог: проектирование заданий с указанием целей, допусков ИИ и минимального автономного вклада, организация маркировки использования ИИ, оценивание и обратная связь.

1.9.5. Обучающийся: соблюдение требований Стандарта, маркировка использования ИИ, рефлексия и защита работ.

1.9.6. Родители или законные представители: предоставление информированного согласия в предусмотренных случаях, поддержка правил академической добросовестности.

1.9.7. Поставщики ИИ-сервисов: соблюдение законодательства Республики Казахстан, обеспечение безопасности, прозрачности и сопровождаемости решений.

1.10. Допуски ИИ в учебном процессе

1.10.1. Устанавливаются уровни допуска: запрещено, ограниченно разрешено, разрешено. Уровень допуска фиксируется в задании и в матрице допусков по предмету.

1.10.2. В итоговых и иных высокозначимых оцениваниях применение ИИ запрещается, за исключением технологий доступности для обучающихся с особыми образовательными потребностями.

1.10.3. В текущей учебной практике допускается применение ИИ преимущественно в редакторских и организационных функциях. Содержательные функции разрешаются по решению педагога при соблюдении минимального автономного вклада обучающегося.

1.10.4. Любое применение ИИ подлежит обязательной маркировке и краткой рефлексии обучающегося.

Настоящие Стандарты имеют обязательные Приложения A-D.

В документе использованы следующие термины и сокращения:

AI Impact Assessment (далее – AIA)	Этико-правовая оценка воздействия. Формализованная процедура до внедрения и при

	существенных изменениях информационных систем и/или систем искусственного интеллекта, которая выявляет и документирует правовые, этические, социальные и педагогические риски, определяет меры их снижения, условия допуска и порядок последующего мониторинга.
Атрибуция (Attribution)	Указание и раскрытие информации о факте, объеме и способе использования генеративного искусственного интеллекта при создании учебной или иной работы.
Биометрические данные	Персональные данные, характеризующие физиологические и биологические особенности человека (изображение лица, голос, походка), которые позволяют установить его личность.
Вендор	Поставщик. Сторонняя организация, являющаяся разработчиком или поставщиком ИС и/или СИИ, используемой в организации образования.
Генеративный искусственный интеллект (далее – GenAI)	Класс систем искусственного интеллекта, способных создавать новый оригинальный контент (текст, изображения, код, аудио) на основе полученных от пользователя запросов (промптов).
Dark patterns	Намеренные приёмы в интерфейсе и текстах, вводящие пользователя в заблуждение или принуждающие к действиям, выгодным платформе, а не пользователю.
Data Protection Impact Assessment (далее – DPIA)	Оценка воздействия на защиту данных. Процедура анализа и снижения рисков для прав и свобод людей, связанных с обработкой их персональных данных. Проводится Уполномоченным органом для систем высокого риска.
Дипфейк (Deepfake)	Реалистичные, сгенерированные искусственным интеллектом медиаматериалы (видео, аудио), в которых внешность или голос человека изменены или подделаны. Создание дипфейков о реальных лицах без их согласия и маркировки запрещено.
Информационная безопасность в сфере информатизации (далее	Состояние защищенности электронных информационных ресурсов, информационных

– информационная безопасность, ИБ)	систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз.
Инцидент	Событие (или совокупность событий) при использовании ИС и/или СИИ в организации образования, которое привело либо могло привести к нарушению прав обучающихся или работников, к ущербу организации, либо к нарушению конфиденциальности, целостности или доступности данных и сервисов; в частности, утечка или несанкционированный доступ к персональным данным, генерация вредного или дискриминационного контента/выводов модели, технический сбой или отказ
Искусственный интеллект (Artificial Intelligence, далее – ИИ)	Информационно-коммуникационная технология, позволяющая имитировать или превосходить когнитивные функции человека, с целью выполнения интеллектуальных задач и поиска решений.
Информационная система (далее – ИС)	Организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач.
Human-in-the-Loop (Человек в контуре, далее – HITL)	Метод, используемый в ИИ и машинного обучения (МО), который подразумевает вовлечение человеческого суждения и знаний в процесс создания и эксплуатации систем ИИ.
Минимизация данных	Принцип, согласно которому для конкретной цели должен собираться и обрабатываться только минимально необходимый объем персональных данных.
Минимальные метрики качества и предвзятости	Набор показателей и порогов для типовых сценариев ИИ согласно Приложению D.
НАО	Национальная академия образования им. Ы.Алтынсарина.

Обезличивание персональных данных	Действия, в результате совершения которых определение принадлежности персональных данных субъекту персональных данных невозможно.
Обработка персональных данных	Действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных;
ООП	Особые образовательные потребности.
Оперативный центр информационной безопасности (далее – ОЦИБ)	Юридическое лицо или структурное подразделение юридического лица, осуществляющее деятельность по защите электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации.
Организация образования (далее – ОО)	Организация образования, реализующая общеобразовательные учебные программы дошкольного воспитания и обучения, начального, основного среднего, общего среднего образования, специализированные общеобразовательные и специальные учебные программы.
Персональные данные (далее – ПД)	Сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе.
Privacy by Design/Default (Спроектированная защита данных и конфиденциальность по умолчанию)	Концепция, согласно которой защита данных должна быть встроена в процесс разработки технологий, продуктов и услуг, а не рассматриваться как дополнительная мера.
Provenance (происхождение данных/контента)	Документированная цепочка источников и изменений объекта (данных, модели, медиа): кто и когда создал, из чего, какими средствами, какие версии и операции применялись, кем

	утверждалось. Используется для аутентичности, трассируемости, аудита и воспроизводимости; фиксируется в метаданных, журналах и «картах» модели/датасета.
Прокторинг	Процедура контроля за ходом онлайн-экзамена или тестирования с целью подтверждения личности сдающего и обеспечения академической честности. Стандарт накладывает строгие ограничения на используемые в прокторинге технологии.
Промпт (Запрос)	Инструкция или задача в виде текста, кода или изображения, подаваемая пользователем GenAI для создания контента. Стандарт запрещает включать персональные данные в промпты без законного основания.
Разрешенный сценарий использования	Конкретный способ применения СИИ, включённой в Реестр, для определённой цели и аудитории в установленном процессе, одобренный Этическим советом организации и оформленный его решением с условиями и мерами контроля.
Реестр доверенных информационных систем, в том числе систем искусственного интеллекта (далее – Реестр)	Утвержденный Уполномоченным органом перечень ИС и систем искусственного интеллекта, которые прошли комплексную экспертизу и допущены к использованию в ОО РК.
Система искусственного интеллекта (далее – СИИ)	Объект информатизации, функционирующий на основе искусственного интеллекта.
Собственная работа	Результат, созданный обучающимся без недозволенной помощи.
Социальное скорингование	Автоматизированная оценка или ранжирование людей на основе их социального поведения, характеристик или данных, которая влияет на их статус или доступ к возможностям. Данным стандартом запрещена.
Статус соответствия	«в норме», «под наблюдением», «ограничить»,

	«приостановить» - присваивается Уполномоченным органом по результатам R-1.
ТиПО	Техническое и профессиональное образование.
Трансграничная передача данных	Передача персональных данных на территорию иностранного государства. Допускается только при наличии правовых оснований и достаточных гарантий защиты.
Уполномоченный орган	Центральный государственный орган (Министерство просвещения РК) или уполномоченная им организация (НАО), ответственные за экспертизу, допуск, разработку правил и аудит ИС и/или СИИ в образовании.
Форма R-1	Одностраничный отчёт вендора по метрикам из Приложения D, размещаемый в записи Реестра и обновляемый не реже одного раза в год и при мажорных изменениях.
Эмоциональный ИИ (далее – Эмо-ИИ)	Технологии ИИ, предназначенные для распознавания, анализа или вывода эмоционального состояния человека по его лицу, голосу или другим физиологическим данным. Применение таких технологий в отношении обучающихся и работников запрещено данным стандартом.
Избыточные данные	Сведения, собранные или хранящиеся сверх необходимого для цели обработки: лишние **по объёму** (ненужные поля, дубли) и/или **по времени хранения** (держатся дольше требуемого).

Раздел 2. Принципы и обязательные требования

2.1. Законность и права ребёнка

2.1.1. Применение ИС и/или СИИ в ОО осуществляется в соответствии с законодательством РК и международными обязательствами.

2.1.2. Обработка ПД допускается только при наличии законного основания и строго в пределах заявленной цели.

2.1.3. Наилучшие интересы ребёнка имеют приоритет при планировании, внедрении и эксплуатации ИС и/или СИИ.

2.1.4. Сбор данных сверх минимально необходимого объёма не допускается.

2.2. Справедливость и недискриминация

2.2.1. Не допускается дифференциация по признакам пола, языка, состояния здоровья, социального статуса и иным защищаемым основаниям.

2.2.2. ОО обеспечивает сопоставимое качество и точность результатов на государственном и русском языках, а также для обучающихся с особыми образовательными потребностями.

2.2.3. Социальное скорингование обучающихся и работников запрещается.

2.3. Прозрачность и объяснимость

2.3.1. Пользователи подлежат предварительному уведомлению о факте и целях применения ИС и/или СИИ.

2.3.2. Контент, созданный или существенно изменённый с применением ИИ, подлежит обязательной маркировке.

2.3.3. По запросу пользователя ОО обеспечивает предоставление понятного объяснения логики и ключевых факторов, повлиявших на результат.

2.4. Человеческий контроль и право на обжалование

2.4.1. Значимые решения (приём/отчисление, допуск к аттестации, дисциплинарные меры) принимаются уполномоченным работником. Исключительно автоматизированные решения не допускаются, если иное не установлено законом (HITL).

2.4.2. В ОО устанавливается обязательный порядок апелляции и пересмотра решений, принятых с использованием ИИ. Порядок предусматривает сроки, уполномоченные органы, форму и содержание обращения.

2.4.3. Пользователь вправе отказаться от исключительно автоматизированного решения; в этом случае применяется альтернативная процедура, если иное не предусмотрено законом.

2.4.4. Пользователь имеет право на получение объяснения в понятной форме в течение 5 рабочих дней с момента запроса.

2.4.5. При неудовлетворенности данным объяснением пользователь может запросить дополнительное разъяснение с привлечением независимого эксперта.

2.4.6. Право на градацию объяснений по сложности (упрощенная версия для детей/родителей, техническая для специалистов).

2.4.7. Право на «забвение» - возможность удаления всех данных и результатов оценки ИИ по запросу пользователя после завершения образовательного цикла.

2.5. Безопасность и надёжность

2.5.1. ИС и СИИ эксплуатируются в соответствии с Законом РК «Об информатизации» и НПА в области ИБ. Подтверждение соответствия (сертификация, протоколы/акты испытаний) осуществляется профильными госорганами и/или вендором. ОО проверяет включение решения в

реестры/перечни, указанные уполномоченными органами, и не проводит собственных техиспытаний.

2.5.2. В организации применяются технические и организационные меры защиты: разграничение прав доступа, аутентификация (в т.ч. MFA, где доступна), ведение журналов, резервное копирование, минимизация и обезличивание данных, работа только с утверждёнными инструментами и настройками по умолчанию.

2.5.3. Сценарии применения классифицируются по уровню риска; для высокого риска обязательны усиленные меры: пилот на ограниченной выборке, HITL при принятии значимых решений, альтернатива без ИИ, дополнительные уведомления и хранение артефактов для пересмотра.

2.6. Качество данных и источников

2.6.1. Используются правомерно полученные наборы данных известного происхождения; происхождение и условия использования документируются (лицензии, согласия, договоры).

2.6.2. Обеспечиваются актуальность, полнота и репрезентативность данных для целей обработки, включая языковые и возрастные группы, релевантные образовательной задаче.

2.6.3. Запрещается использовать данные из недобросовестных источников (полученные с нарушением закона, прав ИС или СИИ, приватности или договорных условий); такие наборы подлежат исключению и удалению по зафиксированной процедуре.

2.7. Минимизация, целевое использование и ограничение сроков

2.7.1. Обрабатываются только те данные и в таком объёме, которые объективно необходимы для заявленной цели.

2.7.2. Цель обработки формулируется до начала обработки и фиксируется в локальных документах (уведомлениях/перечнях операций). Изменение цели требует отдельного обоснования.

2.7.3. Повторное использование данных вне первоначальной цели допускается при наличии правового основания и информирования пользователей в установленном порядке.

2.7.4. Сроки хранения устанавливаются по категориям данных и ограничиваются необходимым периодом для достижения цели и исполнения обязанностей организации.

2.7.5. По истечении сроков хранения данные подлежат безопасному удалению или обезличиванию с фиксацией факта в журнале.

2.7.6. Запрещается сбор специальных категорий данных и избыточных атрибутов при отсутствии правового основания и необходимости для цели.

2.7.7. При проектировании процессов применяется принцип «конфиденциальность по умолчанию и через дизайн»: отключаются необязательные поля/сбор телеметрии, ограничиваются доступы, исключается дообучение моделей на пользовательских данных без отдельного согласия.

2.7.8. Ответственные лица обеспечивают контроль соблюдения

2.7.1–2.7.7 и ведут учёт сроков хранения.

2.8. Пропорциональность и педагогическая уместность

2.8.1. Применение ИС и/или СИИ допускается, если доказана образовательная ценность по сравнению с альтернативами без ИИ.

2.8.2. Технологии не подменяют педагогическое взаимодействие в частях, критичных для формирования знаний, навыков и оценивания результатов.

2.8.3. Выбирается наименее инвазивное средство, способное достигнуть цели (тест пропорциональности: цель - необходимость - соразмерность - отсутствие менее рискового средства).

2.8.4. Практики, эксплуатирующие уязвимость детей, давление или манипуляцию поведением, не допускаются.

2.8.5. Инструменты и сценарии соответствуют возрасту и уровню развития обучающихся; при необходимости предусматриваются альтернативные задания без ИИ сопоставимой сложности.

2.8.6. Для высокорисковых сценариев проводится ограниченное пилотирование с оценкой образовательного эффекта и рисков; итоги пилота документируются и учитываются при принятии решения о масштабировании.

2.8.7. Недоступность технологии или несогласие на её использование не ухудшают положение обучающегося; предоставляется эквивалентная альтернатива.

2.9. Доступность и инклюзия

2.9.1. ИС и СИИ обеспечивают доступность для обучающихся с инвалидностью и ООП, включая совместимость с ассистивными технологиями.

2.9.2. Материалы и интерфейсы предоставляются на государственном и распространённых языках обучения в организации.

2.9.3. По запросу обучающегося предоставляются разумные приспособления: альтернативные форматы материалов, способы ввода/вывода, дополнительные инструкции.

2.9.4. Выявленные барьеры доступности устраняются; до устранения предоставляется функционально эквивалентный альтернативный формат выполнения задания/оценивания.

2.9.5. Использование ИИ не приводит к дискриминации, снижению качества или доступности обучения для отдельных групп; соответствующие риски идентифицируются и минимизируются до начала применения.

2.9.6. Факты исполнения требований

2.9.1–2.9.5 документируются в локальных материалах (перечень инструментов, инструкции, форма задания).

2.10. Академическая добросовестность

2.10.1. Запрещается представлять сгенерированный ИИ контент как собственную работу.

2.10.2. Факт использования генеративных средств подлежит раскрытию в порядке, установленном настоящим Стандартом и локальными актами.

2.10.3. Выводы детекторов ИИ носят вероятностный характер и используются только как вспомогательная информация; они не подменяют проверку преподавателем и не являются самостоятельным доказательством.

2.11. Ответственность и подотчётность

2.11.1. В организации определяются и закрепляются ответственные роли за этичное применение ИС и СИИ и защиту данных

2.11.2. Ведётся учёт используемых ИС и СИИ, целей и правовых оснований обработки, категорий и сроков хранения данных

2.11.3. Нарушения фиксируются, расследуются и устраняются в установленном порядке; результаты и принятые меры документируются.

2.12. Экологическая и социальная устойчивость

2.12.1. При выборе и эксплуатации ИС и СИИ приоритет отдается решениям с обоснованными вычислительными и энергетическими затратами при сохранении образовательной ценности.¶

2.12.2. Публичные коммуникации об ИИ ведутся корректно и проверяемо; вводящие в заблуждение утверждения не допускаются.

Раздел 3. Запрещенные практики

3.1. Наблюдение и данные

3.1.1. Запрещается скрытый сбор аудио, видео, изображений экрана, кейстроков и сетевой активности обучающихся и работников.

3.1.2. Запрещается массовая либо постоянная биометрическая идентификация/трекинг (распознавание лиц, походки, голоса) в учебной среде.

3.1.3. Запрещается сбор, хранение или использование биометрии несовершеннолетних для учета посещаемости, оценивания или дисциплины.

3.1.4. Запрещается трансграничная передача персональных данных при отсутствии правового основания и договорных гарантий защиты.

3.1.5. Запрещается использование учебных данных для рекламы, коммерческого профилирования или продажи.

3.2. Эмоции, поведение, скоринг

3.2.1. Запрещается эмоциональное распознавание и вывод психологических характеристик по лицу, голосу, тексту или физиологии.

3.2.2. Запрещается социальное скорингование обучающихся и работников.

3.2.3. Запрещается формирование поведенческих профилей, влияющих на доступ к образованию, ресурсам, поощрениям или дисциплинарным мерам.

3.3. Автоматизированные решения

3.3.1. Запрещаются исключительно автоматизированные решения по приёму, отчислению, допуску к аттестации, выдаче документов и дисциплинарным взысканиям.

3.3.2. Запрещается использовать детекторы «ИИ/не ИИ» как единственное основание для обвинений в недобросовестности.

3.4. Оценивание и прокторинг

3.4.1. Запрещается прокторинг с применением эмо-ИИ, анализа мимики/голоса, а также постоянного доступа к микрофону/камере вне периода экзамена.

3.4.2. Запрещается сканирование помещения и окружающих лиц сверх минимально необходимого объёма и без предоставления альтернативного формата сдачи.

3.5. Контент и коммуникации

3.5.1. Запрещается создание и распространение дипфейков о реальных лицах без их согласия и без явной маркировки синтетического происхождения.

3.5.2. Запрещается генерация контента, нарушающего права ребёнка, включая сексуализированные изображения/описания несовершеннолетних, травлю и иные формы насилия.

3.5.3. Запрещается использование манипулятивных интерфейсов (dark patterns), побуждающих к раскрытию избыточных данных или формирующих зависимое поведение.

3.5.4 Запрещается использование техник, формирующих зависимость или навязчивое использование (бесконечная лента, игрофикация с негативными последствиями при прекращении).

3.5.5. Запрещается персонализированная реклама и коммерческие предложения, встроенные в образовательный контент.

3.5.6. Запрещаются алгоритмы, эксплуатирующие детскую импульсивность и незрелость принятия решений.

3.6. Психодиагностика и поддержка

3.6.1. Запрещается применение ИИ для психодиагностики и скрининга без лицензированных методик и участия квалифицированного специалиста.

3.6.2. Запрещается подмена профессиональной психологической или медицинской помощи чат-сервисами ИИ без предупреждения пользователя и без маршрутизации к специалисту.

3.7. Трудовые отношения

3.7.1. Запрещается оценка эффективности педагогов и иного персонала на основе эмо-ИИ или социального скоринга.

3.7.2. Запрещается скрытый мониторинг работников с применением ИИ вне их трудовых обязанностей и без уведомления.

3.8. Безопасность и целостность систем

3.8.1. Запрещается внедрение информационных систем и (или) систем ИИ,

не прошедших проверку на уязвимости и предвзятость для целевых языков обучения в установленном порядке.

3.8.2. Запрещается обход установленных политик и технических ограничений через сторонние ИИ-сервисы или «теневые» аккаунты.

Раздел 4. Академическая честность и использование генеративного ИИ

4.1. Базовые правила

4.1.1. Обучающиеся и педагоги обязаны соблюдать академическую честность: обеспечивать самостоятельность выполнения, оригинальность результата, корректное цитирование и ссылки на источники.

4.1.2. Любое использование генеративного искусственного интеллекта (GenAI) в учебных и служебных материалах подлежит раскрытию и маркировке в порядке раздела 8 и п. 4.4.

4.1.3. Не допускается представление сгенерированного ИИ контента как результата собственного труда.

4.1.4. Нарушения подпунктов 4.1.1–4.1.3 квалифицируются как нарушение академической честности и влекут меры по п. 4.7.

4.2. Разрешено при условии раскрытия

Использование GenAI допускается при одновременном выполнении условий: отсутствие ввода персональных данных, соблюдение требований раздела 8 к маркировке и п. 4.5 к доказательности процесса, проверка фактов и корректности автором. В указанных пределах разрешается:

4.2.1. Генерация идей, планов, вопросов и уточняющих формулировок по теме задания.

4.2.2. Языковая правка: орфография, пунктуация, стилистическое упрощение без изменения смысла авторского текста.

4.2.3. Использование тренажёров и примеров решений с последующей самостоятельной переработкой результата обучающимся.

4.2.4. Рефакторинг и форматирование кода с обязательным указанием источника и последующей проверкой работоспособности автором.

4.2.5. По требованию педагога автор предоставляет «следы процесса» по п. 4.5 (промпты, ключевые ответы, скриншоты либо краткую записку).

4.3. Запрещено Следующие действия не допускаются при выполнении

учебных заданий и оценочных работ:

4.3.1. Генерация готовых ответов или работ «под ключ» вместо самостоятельного выполнения.

4.3.2. Автоматизированный перевод без анализа и доработки в заданиях, направленных на проверку языковой компетенции.

4.3.3. Использование авто-решателей тестов, а также технических и программных средств обхода установленных правил проведения контроля и прокторинга.

4.3.4. Создание и распространение дипфейков и иного манипулятивного контента.

4.3.5. Передача выполнения задания третьим лицам, включая платные сервисы «под ключ» и иные формы аутсорсинга.

4.4. Атрибуция в работах

4.4.1. Любое использование генеративного ИИ подлежит обязательной атрибуции. Атрибуция размещается в конце работы. Указывается: наименование инструмента, версия/модель (если известна), перечень задач, для которых применялся ИИ, и степень его влияния.

4.4.2. Рекомендуемая формулировка: «Использован GenAI <сервис>, модель <модель>, для: <правка языка/генерация идей/проверка кода>. Ключевые подсказки и ответы - в приложении».

4.4.3. При существенном заимствовании контента с указанием конкретных ответов/фрагментов ИИ приводятся внутритекстовые ссылки на соответствующие места работы или на приложение с промптами/скриншотами.

4.4.4. Требования к оформлению меток и расширенной декларации (для итоговых работ и публичных материалов) применяются по локальным правилам маркировки организации образования.

4.4.5. Отсутствие атрибуции при фактическом использовании ИИ рассматривается как нарушение правил академической добросовестности и влечет меры по п. 4.7 Стандарта.

4.5. Доказательность процесса

4.5.1. По запросу педагога или уполномоченной комиссии обучающийся обязан предоставить артефакты процесса: черновики, историю версий, заметки, расчёты, исходный код и (при наличии) файл с промптами и ключевыми ответами ИИ, скриншоты диалога или краткую записку о распределении ролей «что сделал ИИ/что сделал автор».

4.5.2. Для подтверждения авторства педагог вправе назначить устную защиту; её результаты фиксируются в материалах задания.

4.5.3. Сроки хранения артефактов и материалов защиты определяются разделом о данных и локальными актами организации образования; избыточная фиксация не допускается.

4.6. Проверка подозрений

4.6.1. Использование детекторов «ИИ/не ИИ» допускается только как

сигнальный индикатор и не является самостоятельным доказательством нарушения.

4.6.2. Основаниями для проверки являются, в том числе: явное несоответствие уровня работы обычным результатам обучающегося, отсутствие артефактов процесса, неудовлетворительная устная защита, установленные совпадения источников. Факты и время фиксируются педагогом.

4.6.3. При наличии оснований педагог запрашивает у обучающегося артефакты процесса и/или проводит краткую устную проверку. При сохранении сомнений материалы передаются на рассмотрение школьной комиссии, определённой локальным актом (как правило, Этический совет по ИИ).

4.6.4. Решение по делу принимает комиссия. В акте указываются мотивировка и доказательства; сведения хранятся по срокам локальных актов. Право на апелляцию реализуется в порядке, установленном положением о комиссии.

4.7. Санкции (градации)

4.7.1. Квалификация нарушений

1. **Уровень 0 (без умысла)**: нераскрыто разрешённое использование СИИ; ошибки маркировки/атрибуции без подмены содержания.
2. **Уровень А (частичная подмена)**: отдельные фрагменты/элементы работы созданы СИИ вопреки правилам задания, но ядро задания выполнено самостоятельно.
3. **Уровень В (значимая подмена)**: ключевые части работы или итоговый ответ созданы СИИ; цель оценивания утрачена.
4. **Уровень С (тяжёлое/систематическое)**: повтор в течение учебного года; групповая организация; умышленная маскировка следов процесса; коммерческая передача задания третьим лицам.

4.7.2. Меры воздействия по уровням

1. **Уровень 0**: письменное предупреждение; дооформление атрибуции и маркировки в срок до 2 рабочих дней; разъяснение правил.
2. **Уровень А**: пересдача задания в альтернативном формате; снижение балла в пределах опубликованных критериев задания.
3. **Уровень В**: оценка «0» за работу; по решению комиссии - пересдача темы/модуля (курса) в установленном порядке.
4. **Уровень С**: меры дисциплинарного взыскания по уставу/локальным актам; при повторе - ужесточение вплоть до максимальных мер, допускаемых уставом и другими внутрий школьными нормативными документами.

4.7.3. Процедура принятия решения

1. Основания фиксируются: материалы задания, «следы процесса», мотивировка (см. п. 7.6).
2. Обучающийся (и законный представитель) до решения даёт письменные объяснения; при необходимости проводится устная защита.
3. Решение по уровням 2–3 принимает школьная комиссия/Этический совет;

по уровням 0–1 - педагог с записью обоснования.

4. Итог оформляется актом: квалификация уровня, меры, сроки исполнения, порядок обжалования (см. разд. 4.12).

4.7.4. Смягчающие и отягчающие обстоятельства

1. Смягчающие: добровольное раскрытие, содействие, первый случай, техническая ошибка маркировки - допускается понижение уровня.
2. Отягчающие: повторность, групповая координация, преднамеренная маскировка, использование платных «под ключ» сервисов - допускается повышение уровня.

4.7.5. Повторность

1. Повтор в пределах учебного года переводит нарушение на следующий уровень.
2. Снятие статуса «повторности» - по истечении учебного года.

4.7.6. Фиксация и хранение

1. Акт, материалы рассмотрения и уведомления хранятся: не менее 12 месяцев; если влияет на итоговую оценку - до выставления итоговой оценки за период + 3 месяца, но не менее 12 месяцев.
2. Записи ведутся без избыточных персональных данных, с соблюдением раздела 5.

4.7.7. Апелляция

Решение и меры могут быть обжалованы в порядке раздела 4.12 в установленные сроки.

4.8. Проектирование оценивания

4.8.1. Оценивание процесса и результата.

а) Оцениванию подлежат как итоговый продукт, так и процесс его выполнения.

б) Обучающийся вместе с работой представляет «следы процесса» из перечня, определяемого педагогом: план/структура, черновики/версии, промпты и ключевые ответы ИИ (либо скриншоты), исходные файлы кода/расчётов, краткая рефлексия (100–150 слов) с разграничением вклада ИИ и обучающегося и указанием способов проверки.

в) «Следы процесса» не должны содержать персональные данные.

г) Представленные материалы используются для подтверждения авторства и хранятся в сроки, установленные настоящим Стандартом.

4.8.2. Локализация заданий и устная проверка.

а) Задания формулируются с привязкой к изученным темам и локальным материалам, предоставленным педагогом (наборы данных, кейсы школы/города, наблюдения с уроков), без использования персональных данных.

б) Для подтверждения авторства может проводиться краткая устная проверка и/или защита ключевых частей работы.

в) Допускается вариативность условий и различие исходных данных для групп/обучающихся с целью снижения риска подмены.

4.8.3. Правила использования генеративного ИИ в задании.

а) До выдачи задания педагог в явном виде определяет: что разрешено, что запрещено, и что допускается под контролем педагога при использовании ИИ; требования к маркировке и атрибуции вклада ИИ; состав «следов процесса», подлежащих сдаче.

б) Прозрачность использования ИИ включается в критерии оценивания.

в) Пример формулировки: «разрешено - идеи/план/языковая правка; под контролем - автопроверка черновиков; запрещено - генерация финального ответа».

г) Настоящие требования применяются совместно с нормами об атрибуции (п. 4.4), доказательности процесса (п. 4.5) и ограничениях детекторов (п. 4.6).

4.9. Экзамены и контрольные

4.9.1. Организация образования (далее - ОО) заблаговременно публикует перечни разрешенных и запрещенных средств, в том числе ИИ-инструментов, для каждого экзамена и контрольной работы; перечни доводятся до обучающихся, родителей или законных представителей.

4.9.2. При дистанционном проведении применяется принцип минимального вмешательства: используются только средства, необходимые для обеспечения академической честности. При недоступности требуемых технологий обучающемуся предоставляется равнозначная альтернатива.

4.9.3. Запрещается применение эмо-ИИ, а также непрерывный доступ к камере, микрофону и иным устройствам вне времени проведения экзамена или контрольной работы.

4.10. Практики педагогов

4.10.1. Педагогу разрешается использовать генеративный ИИ для подготовки черновиков планов уроков, рубрик и учебных примеров при условии последующей экспертной проверки и личной ответственности за содержание.

4.10.2. Запрещается загрузка персональных данных обучающихся и педагогов во внешние модели и сервисы без правового основания и утвержденного порядка.

4.10.3. Материалы, созданные с использованием генеративного ИИ, подлежат маркировке и обязательной доработке педагогом до использования в учебном процессе или публичного размещения.

4.11. Поддержка обучающихся

4.11.1. ОО обеспечивает инструктаж обучающихся по честному использованию генеративного ИИ, по правилам атрибуции и маркировки.

4.11.2. ОО обеспечивает доступ к безопасным инструментам и примерам корректного раскрытия вклада ИИ.

4.12. Апелляции

4.12.1. Право и основания

1. Право на апелляцию имеют обучающийся, родитель или законный представитель.
2. Обжалованию подлежат решения, принятые с участием (использованием) систем искусственного интеллекта, либо повлиявшее на оценку, допуск к аттестации или дисциплинарные меры.
3. Основания: а) процедурная ошибка; б) новые существенные обстоятельства.
4. Выводы детекторов «ИИ/не ИИ» не являются самостоятельным доказательством.
5. Значимые решения принимаются с участием человека и подлежат пересмотру в порядке апелляции.

4.12.2. Подача и срок

1. Апелляция подается в письменной форме на имя председателя Этического совета ОО по ИИ через официальный электронный адрес школы, опубликованный для обращений.
2. Срок подачи - 10 рабочих дней с момента, когда заявителю стало известно о решении.
3. Секретарь Совета регистрирует апелляцию в день поступления.

4.12.3. Приложения к апелляции

1. Краткое изложение сути спора и требований.
2. Копия оспариваемого решения или оценочного листа.
3. Материалы, подтверждающие процесс выполнения задания: черновики, история версий, промпты и ключевые ответы ИИ, скриншоты диалога, либо краткая записка «что делал ИИ/что выполнял автор».
4. Иные документы, подтверждающие доводы заявителя.

Примечание: рассмотрение апелляции и сроки ее разрешения осуществляются Советом по порядку, установленному Положением об Этическом совете по ИИ, принятым в ОО.

4.12.4. Рассмотрение

Секретарь Совета регистрирует апелляцию в день поступления и включает её в повестку ближайшего заседания; при необходимости Председатель созывает внеочередное заседание.

1. Совет изучает материалы задания и мотивировку оспариваемого решения; при необходимости приглашает заявителя для кратких устных пояснений.

2. Член Совета при наличии конфликта интересов заявляет самоотвод, в обсуждении и голосовании не участвует; факт фиксируется в протоколе.

3. Срок рассмотрения составляет не более 20 рабочих дней со дня регистрации апелляции.

4.12.5. Варианты решения

1. Оставить первоначальное решение без изменений.
2. Изменить оценку/решение с указанием причин.
3. Назначить пересдачу, устную защиту либо альтернативное задание.
4. Отменить санкции и удалить запись о нарушении.
5. Окончательное решение на уровне организации принимает комиссия на основании заключения Совета; решение оформляется приказом.

4.12.6. Оформление и уведомление

1. Решение оформляется письменно и включает: резолютивную часть, краткую мотивировку, перечень рассмотренных материалов, дату и подписи.
2. Копия решения направляется заявителю тем же каналом, которым подана апелляция.

4.12.7. Хранение

а) Решение по апелляции и все материалы рассмотрения хранятся в школьном деле не менее 12 месяцев.

б) Если апелляция влияет на итоговую оценку, хранение до выставления итоговой оценки за соответствующий период плюс 3 месяца. Срок не может быть меньше 12 месяцев.

4.12.8. Защита заявителя

а) Любые формы давления на заявителя и ухудшение его положения в связи с апелляцией запрещены.

б) Сообщения о давлении и иных нарушениях регистрируются и рассматриваются по общему порядку инцидентов. При подтверждении применяются меры ответственности в пределах компетенции организации.

Короткий шаблон апелляции (1 страница)

1. ФИО, класс/группа, контакты.
2. Какое решение обжалуется, дата.
3. Основание: процедурная ошибка / новые обстоятельства (нужное подчеркнуть).
4. Суть несогласия кратко (до 150 слов).
5. Требование: пересмотр оценки / пересдача / отмена санкций / иное.
6. Перечень приложений: работа, «следы процесса», иное.
7. Дата, подпись.

Раздел 5. Порядок внедрения и меры контроля

5.1. Принцип разделения ответственности

5.1.1. Уполномоченный орган в сфере образования устанавливает отраслевые правила и критерии допустимости применения ИИ, проводит педагогико-этическую и правовую оценку и принимает решение о включении системы в Реестр на основании заключений уполномоченных государственных органов в области цифровизации и защиты персональных данных.

5.1.2. Техническая экспертиза, сертификация соответствия требованиям информационной безопасности, испытания на уязвимости и проверка соответствия ИТ-стандартам осуществляются компетентными государственными органами и их подведомственными организациями. Уполномоченный орган учитывает их заключения при принятии решения о включении системы в Реестр.

5.1.3. Уполномоченный орган организует регулярные консультации с разработчиками ИИ-систем и образовательным сообществом для обеспечения баланса между инновациями и безопасностью.

5.1.4. При внесении изменений в требования проводится оценка экономического воздействия на действующие системы и устанавливаются переходные периоды продолжительностью 12-18 месяцев.

5.1.5. ОО отвечает за локальное внедрение одобренных систем, соблюдение настоящего Стандарта, информирование пользователей и рассмотрение апелляций. Технические испытания программного обеспечения и аудит поставщика организацией образования не проводятся, за исключением случаев, прямо предусмотренных законодательством Республики Казахстан.

5.2. Использование Реестра

5.2.1. Организация образования вправе внедрять и использовать только ИС / СИИ, включенные в Реестр, утвержденный Уполномоченным органом.

5.2.2. Запись Реестра содержит сведения о назначении системы, результатах экспертизы, присвоенном уровне риска и обязательных мерах по его снижению, доводимые до ОО.

5.2.3. По каждому одобренному сценарию в записи Реестра размещается форма R-1; к использованию допускаются только системы с актуальной формой R-1.

5.3. Классификация риска на уровне организации

5.3.1. До начала эксплуатации одобренной СИИ организация образования классифицирует каждый конкретный сценарий использования по уровням риска в соответствии с Приложением А.

5.4. Общие меры контроля (для всех уровней риска)

5.4.1. Назначается ответственное лицо за соблюдение настоящего Стандарта.

5.4.2. Все пользователи (работники, обучающиеся, законные представители) уведомляются о факте, целях и правилах применения СИИ.

5.4.3. Обеспечивается маркировка контента, созданного с использованием ИИ, в учебном процессе.

5.4.4. Настраивается ролевой доступ и ведётся учёт использования системы.

5.5. Дополнительные меры контроля (для среднего и высокого риска)

5.5.1. Ответственное лицо организации образования изучает сведения из Реестра по соответствующей СИИ и утверждает внутренний план реализации обязательных мер по снижению рисков.

5.5.2. Организация устанавливает и доводит до всех пользователей порядок апелляции и пересмотра результатов, выданных ИС или СИИ.

5.5.3. Для сценариев высокого риска:

5.5.3.1. Любое значимое решение, влияющее на оценку, допуск к аттестации или применение дисциплинарных мер, принимает уполномоченный сотрудник. Вывод ИИ носит вспомогательный характер.

5.5.3.2. Внедрение нового сценария начинается с пилотного проекта на ограниченной аудитории. По итогам пилота фиксируются показатели эффективности и безопасности по метрикам, установленным в Приложении D, с последующим решением о продолжении или прекращении применения.

5.6. Педагогическая уместность и безопасность

5.6.1. Применение ИС и/или СИИ допускается при наличии педагогического обоснования и не подменяет педагогическое взаимодействие в ситуациях, критичных для результата обучения и развития обучающихся.¶

5.6.2. Во всех сценариях оценивания и аттестации обучающимся предлагается альтернативная форма сдачи без использования ИИ. Альтернатива обязательна при недоступности технологии или непропорциональном вмешательстве в приватность.

5.6.3. Используемые инструменты и сценарии соответствуют возрасту и психофизиологическим особенностям обучающихся.

5.6.4. Организация обеспечивает доступность ИИ-инструментов для обучающихся с инвалидностью и особыми образовательными потребностями, в том числе за счет разумных приспособлений.

5.7. Экспериментальные режимы (пилотные проекты, регуляторные песочницы и иные формы)

5.7.1. В целях апробации инновационных образовательных решений допускается проведение ограниченных пилотных проектов сроком до 6 месяцев. Для таких проектов устанавливается упрощенная процедура включения в Реестр с присвоением статуса «Пилотный проект».

5.7.2. Участие в пилотных проектах осуществляется исключительно на основании добровольного информированного согласия с правом прекращения участия в любое время без неблагоприятных последствий.

5.7.3. Результаты пилотных проектов подлежат оценке независимой комиссией с обязательным участием педагогических работников и представителей родителей (законных представителей).

5.7.4. Заявки отечественных разработчиков образовательных ИИ-решений рассматриваются в первоочередном порядке.

5.7.5. На региональном уровне назначается независимый омбудсмен по вопросам ИИ для рассмотрения жалоб и обращений участников пилотных проектов.

Раздел 6. Данные и приватность

6.1. Основные принципы

6.1.1. При использовании ИС и/или СИИ ОО является оператором персональных данных (ПД) обучающихся и работников и несет ответственность за их защиту в пределах своей компетенции.

6.1.2. Обработка ПД с применением ИС и/или СИИ осуществляется на законном основании и исключительно в пределах заранее определенных образовательных или управленческих целей. Основания: требование закона, договор, согласие субъекта ПД (либо законного представителя несовершеннолетнего).

6.1.3. Применяется принцип «защита данных по проектированию и по умолчанию» (privacy by design/default): сбор и обработка данных, не являющихся строго необходимыми для заявленной цели, по умолчанию отключены.

6.2. Роль Уполномоченного органа в обеспечении приватности

6.2.1. Уполномоченный орган проводит оценку воздействия на защиту данных (DPIA) для всех ИС и/или СИИ с высоким уровнем риска до включения в Реестр и при каждом существенном изменении таких систем.

6.2.2. Методики и типовые формы DPIA утверждает Уполномоченный орган; при необходимости привлекаются профильные государственные органы в сфере цифровизации и защиты ПД.

6.2.3. По итогам DPIA Уполномоченный орган устанавливает обязательные условия и ограничения использования, меры по снижению рисков, требования к уведомлениям, срокам хранения и обезличиванию данных; соответствующие сведения вносятся в запись Реестра и доводятся до ОО.

6.2.4. Уполномоченный орган организует этико-правовую оценку воздействия (AIA) для отраслевых систем среднего и высокого риска и координирует её с DPIA.

6.2.5. Допустимость и условия трансграничной передачи ПД по каждой системе определяет уполномоченный орган в сфере защиты ПД; Уполномоченный орган учитывает эти условия в Реестре и при установлении отраслевых ограничений использования.

6.2.6. ОО не проводят DPIA; они исполняют меры контроля, указанные в записи Реестра и в настоящем Стандарте, и по запросу предоставляют сведения, необходимые для проведения DPIA Уполномоченным органом.

6.3. Обязанности ОО

6.3.1. ОО до начала использования ИС и/или СИИ уведомляет пользователей и, где это требуется законом, получает согласие законных представителей несовершеннолетних по типовым формам, утверждённым Уполномоченным органом.

6.3.2. ОО обеспечивает минимизацию персональных данных: собираются только данные, необходимые для цели, одобренной для конкретной ИС и/или СИИ; необязательные поля в формах отключаются.

6.3.3. ОО настраивает ролевую модель доступа по принципу наименьших привилегий; административный доступ защищается многофакторной аутентификацией (МФА).

6.3.4. ОО соблюдает сроки хранения по категориям данных, утверждённые Уполномоченным органом; по окончании сроков данные подлежат безопасному удалению либо анонимизации.

6.3.5. ОО организует «единое окно» для запросов субъектов данных о доступе, исправлении и удалении персональных данных и исполняет их в порядке и сроки, установленные законодательством РК.

6.4. Обращение с особыми категориями данных

6.4.1. По умолчанию сбор и обработка биометрических данных и данных о здоровье с применением ИС и/или СИИ в ОО не допускаются.

6.4.2. Исключения возможны только в случаях, прямо предусмотренных отраслевым законодательством, и применяются исключительно к сценариям из Реестра при выполнении специальных мер защиты, установленных Уполномоченным органом. Условия фиксируются локальным актом ОО.

6.5. Безопасность данных

6.5.1. Поставщик ИС и/или СИИ обеспечивает техническую защиту платформы (включая шифрование, управление уязвимостями, тесты на проникновение) в соответствии с Законом РК «Об информатизации» и договорными обязательствами.

6.5.2. ОО обеспечивает организационные и технические меры на своей стороне: управление доступами, антивирусную защиту, обучение пользователей цифровой гигиене, реагирование на инциденты.

6.5.3. Использование реальных персональных данных в тестовых, демонстрационных и пилотных средах, не вошедших в Реестр, запрещается; применяются синтетические либо полностью обезличенные данные.

6.6. Использование данных в генеративных ИИ

6.6.1. Ввод персональных данных обучающихся и работников в общедоступные внешние генеративные модели запрещается.

6.6.2. В СИИ из Реестра опция использования пользовательских данных для дообучения глобальных моделей отключается по умолчанию; её включение допускается только при наличии отдельного, информированного и свободно

данного согласия пользователя (законного представителя), с возможностью отказа без ухудшения условий получения услуги/услуги обучения.

6.6.3. Разрешается использование корпоративных версий генеративных ИИ-сервисов с гарантированной изоляцией данных и соглашениями о неразглашении.

Раздел 7. Прозрачность, объяснимость и маркировка

7.1. Уведомление о применении СИИ

7.1.1. До начала обработки ОО предоставляет пользователю понятное уведомление с указанием: цели; правового основания; категорий данных; сроков и места хранения; основных рисков; прав пользователя и порядка их реализации; контактного адреса.

7.1.2. Для экзаменов, прокторинга, аналитики успеваемости и мониторинга работников оформляются отдельные уведомления с описанием особенностей обработки и сроков хранения.

7.1.3. Уведомления доступны на государственном и русском языках, а также в доступных форматах для лиц с инвалидностью.

7.1.4. Факт информирования фиксируется и хранится в сроки, установленные разделом 5.

7.1.5. Применяются типовые формы уведомлений по Приложению В.

7.2. Самоидентификация СИИ

7.2.1. Чат-боты и ассистенты в интерфейсе явно сообщают, что они являются СИИ.

7.2.2. Запрещены формулировки и элементы интерфейса, создающие видимость участия человека при его отсутствии.

7.2.3. Текст самоидентификации размещается до начала взаимодействия и остается видимым во время сессии.

7.2.4. Применяются типовые формулировки по Приложению В.

7.3. Маркировка сгенерированного контента

7.3.1. Любой контент, созданный или доработанный с применением СИИ в учебных и управленческих процессах, подлежит визуальной маркировке и, при технической возможности, меткам в метаданных.

7.3.2. Синтетические медиа и дипфейки маркируются как синтетические; их использование допускается только при наличии правового основания и необходимых согласий.

7.3.3. При обмене и экспорте материалов сохраняются сведения о происхождении (provenance); необоснованное удаление метаданных не допускается.

7.3.4. Форматы и примеры меток устанавливаются Приложением С.

7.4. Раскрытие логики и факторов

7.4.1. По запросу пользователя ОО обеспечивает краткое объяснение

результата СИИ: цель обработки, основные входные данные, ключевые факторы, известные ограничения, дата и версия модели.

7.4.2. Для значимых решений указываются уровень уверенности и применённые пороги.

7.4.3. При технической невозможности полного объяснения алгоритма предоставляется описание основных принципов работы системы, факторов риска и способов минимизации ошибок

7.4.4. Объяснения адаптируются к аудитории: упрощенные версии для обучающихся и родителей, технические для специалистов

7.5. Документация для пользователей

7.5.1. В открытом доступе размещается краткая карта СИИ: назначение, недопустимые использования, типы данных, метрики качества (по Приложению D), известные риски и меры их снижения.

7.5.2. Указывается порядок апелляции и контакт ответственного лица.

7.6. Раскрытие потоков данных

7.6.1. Раскрываются категории обрабатываемых данных, источники, получатели, место хранения, сроки хранения, факты и основания трансграничной передачи.

7.6.2. Если СИИ поставляется вендором, первичное раскрытие выполняет вендор; ОО публикует ссылку или заверенную выписку и поддерживает её актуальность.

7.6.3. Использование данных для обучения моделей раскрывается отдельно.

7.7. Подрядчики и субобработчики

7.7.1. Обеспечивается доступ к перечню поставщиков, субобработчиков и юрисдикций хранения, раскрытому вендором.

7.7.2. Изменения перечня доводятся до пользователей заблаговременно с указанием даты вступления в силу.

7.8. Доступ к материалам решения

7.8.1. По запросу предоставляется выписка из журнала операций и описание причинно-следственных факторов без раскрытия коммерческой тайны и уязвимостей.

7.8.2. Хранятся артефакты, достаточные для пересмотра (входы, выводы, ключевые параметры) в сроки, установленные разделом 6.

7.9. Ясность формулировок

7.9.1. Тексты уведомлений составляются простым языком без избыточной юридической терминологии.

7.9.2. Для несовершеннолетних и их законных представителей готовятся адаптированные версии.

7.10. Изменения и версии

7.10.1. Существенные изменения целей обработки, категорий данных, используемых моделей СИИ или уровней риска подлежат предварительному опубликованию не позднее даты ввода в действие.

7.10.2. Ведётся журнал версий уведомлений и политик: номер/дата версии, краткое описание изменений, ссылка на основание (приказ/уведомление). Журнал хранится по срокам раздела 6.

7.11. Ограничения детекторов ИИ

7.11.1. При использовании детекторов ИИ указывается, что их выводы носят вероятностный характер и не являются единственным и достаточным основанием для дисциплинарных мер. Окончательное решение принимает уполномоченный сотрудник на основе совокупности доказательств.

7.12. Канал обратной связи

7.12.1. Обеспечивается доступный канал (веб-форма/официальный e-mail) для вопросов и жалоб по прозрачности с установленными в локальном акте сроками ответа.

7.12.2. Публикуется агрегированная статистика обращений и решений без персональных данных с периодичностью, установленной локальным актом.

7.13. Фиксация уведомления и согласий

7.13.1. Факт информирования и, где требуется, согласий фиксируется и хранится в сроки, определённые разделом 6.

7.13.2. Применяется принцип минимизации: фиксируются только сведения, необходимые для подтверждения факта информирования/согласия. Избыточная фиксация не допускается.

Раздел 8. Управление, роли и подотчётность

8.1. Принцип разделения ответственности

8.1.1. Уполномоченный орган:

а) устанавливает обязательные правила и критерии допустимости применения СИИ;

б) формирует и ведёт Реестр, разрабатывает типовые документы и программы обучения;

в) организует внешний мониторинг соблюдения Этического стандарта, включая анализ форм R-1 по Приложению D, учёт результатов проверок профильных органов и обезличенных данных ОО;

г) собственных технических испытаний не проводит;

д) по итогам мониторинга вправе ограничивать сценарии применения, приостанавливать или прекращать включение СИИ в Реестр.

8.1.2. ОО:

а) обеспечивает локальное внедрение одобренных ИС и/или СИИ;

б) контролирует педагогическую уместность сценариев;

в) организует обучение пользователей в Реестре и настоящем Стандарте.

г) исполняет обязатель

8.2. Роли и ответственность на уровне организации

8.2.1. Руководитель организации:

а) утверждает локальные правила использования ИС и/или СИИ на основе настоящего Стандарта;

б) назначает Ответственного за внедрение ИС и/или СИИ;

в) утверждает состав Этического совета.

8.2.2. Ответственный за внедрение ИС и/или СИИ:

а) ведёт внутренний журнал использования ИС и/или СИИ;

б) организует работу Этического совета;

в) является контактным лицом по вопросам, связанным с ИС и/или СИИ;

г) контролирует прохождение обучения сотрудниками и обучающимися.

8.2.3. Этический совет по ИИ - выполняет функции согласно пункту 8.3 и связанному положению.

8.2.4. Педагоги и сотрудники:

а) используют только одобренные ИС и/или СИИ в рамках разрешённых сценариев;

б) соблюдают правила академической честности и защиты данных.

8.2.5. Вендор ИС и/или СИИ:

а) соответствие требованиям настоящего Стандарта подтверждается фактом включения продукта в Реестр Уполномоченным органом;

б) ОО самостоятельный аудит вендора не проводит.

8.3. Этический совет по ИИ в ОО

8.3.1. Состав Совета:

1. представитель школьной администрации (но не Директор), председатель;
2. ответственное лицо за ИТ;
3. педагог-психолог либо социальный педагог;
4. представитель педагогического коллектива;
5. по возможности представитель родительского сообщества;
6. по возможности представитель обучающихся старших классов.

8.3.2. Полномочия Совета:

1. рассмотрение и утверждение конкретных сценариев использования СИИ, включённых в Реестр;
2. рассмотрение жалоб и апелляций пользователей на решения и действия с участием СИИ;
3. участие в разборе локальных инцидентов, связанных с применением СИИ.

8.4. Учёт и документация на уровне организации

8.4.1. ОО ведёт внутренний Журнал использования ИС и/или СИИ с фиксацией:

1. наименования СИИ по записи Реестра;

2. одобренного Советом сценария использования;
3. ответственного подразделения либо должностного лица;
4. даты и номера протокола решения Совета.

8.4.2. ОО не хранит и не анализирует техническую документацию поставщиков и Уполномоченного органа, кроме сведений, необходимых для исполнения настоящего Стандарта и ведения Журнала.

8.5. Повышение компетенций

8.5.1. ОО обеспечивает прохождение всеми сотрудниками и обучающимися обязательных программ по ИТ- и ИИ-грамотности, разработанных и утверждённых Уполномоченным органом.

8.5.2. Факт прохождения и результаты обучения фиксируются в установленных системах учёта.

Раздел 9. Мониторинг, аудит и инциденты

9.1. Цели мониторинга на уровне организации

9.1.1. Контроль соблюдения сотрудниками и обучающимися правил использования одобренных СИИ.

9.1.2. Своевременное выявление и реагирование на локальные инциденты (в т.ч. случаи академической недобросовестности, утечки данных по вине пользователя).

9.1.3. Сбор обратной связи и данных об эффективности применения СИИ для последующей передачи Уполномоченному органу.

9.2. Мониторинг и аудит со стороны Уполномоченного органа

9.2.1. Уполномоченный орган осуществляет внешний мониторинг соблюдения Этического стандарта в отношении СИИ из Реестра без проведения собственных технических испытаний; основой мониторинга являются:

9.2.1.1. отчёты и декларации вендора по безопасности, качеству и предвзятости;

9.2.1.2. заключения профильных государственных органов;

9.2.1.3. обезличенные журналы использования и инцидентов, предоставляемые ОО.

9.2.2. По итогам мониторинга Уполномоченный орган вправе выдать предписание об ограничении или приостановке применения СИИ в отдельных сценариях до устранения нарушений, а также обновить записи Реестра; ОО по запросу обязана предоставлять обезличенные данные и документацию, необходимую для мониторинга.

9.2.3. Вендор обновляет форму R-1 не реже одного раза в год и при мажорных изменениях модели или данных; обновления публикуются в Реестре.

9.3. Внутренний мониторинг в организации

9.3.1. Ответственный за внедрение СИИ совместно с Этическим советом проводит внутренний мониторинг не реже одного раза в полугодие. 9.3.2.

Объекты мониторинга:

9.3.2.1. журнал использования СИИ;

9.3.2.2. журналы апелляций и жалоб;

9.3.2.3. статистика инцидентов (в т.ч. зафиксированных случаев использования СИИ с нарушением правил);

9.3.2.4. результаты обучения персонала.

9.3.3. По итогам мониторинга формируется краткий отчёт для руководителя организации с предложениями по улучшению практик использования СИИ.

9.4 Управление инцидентами

9.4.1. ОО утверждает План реагирования на инциденты, включающий: роли и порядок эскалации; критерии уровней 1–3; контакты для срочной связи (вендор, Уполномоченный орган, иные государственные органы); формы фиксации и уведомлений; порядок восстановления и профилактики.

9.4.2. Классификация инцидентов:

Уровень А (низкий) - единичное нарушение без существенных последствий (например, некорректная атрибуция GenAI).

Уровень В (средний) - затронуты права, оценки или данные нескольких лиц (например, серьёзный случай плагиата, жалоба на предвзятость вывода СИИ).

Уровень С (высокий) - критический инцидент: массовая утечка ПД, системный сбой ИС и/или СИИ, создающий высокий риск вреда.

9.4.3. Реагирование по уровням:

Уровень А: педагог проводит разъяснение; факт фиксируется в Журнале инцидентов; при необходимости - дооформление работы и атрибуции.

Уровень В: регистрация у Ответственного за внедрение; рассмотрение Этическим советом; оформляется решение с мотивировкой и, при необходимости, предоставляется право апелляции по установленному порядку.

Уровень С: немедленная приостановка использования соответствующей ИС и/или СИИ; активация Плана реагирования; безотлагательное уведомление Уполномоченного органа и, при необходимости, иных государственных органов в сфере защиты ПД и ИБ; фиксация и сохранение журналов; организация резервных процедур обучения/оценивания.

9.4.4. Для каждого инцидента оформляется запись: дата/время обнаружения, уровень, описание, задействованная ИС и/или СИИ, принятые меры, результат, дальнейшие действия по предотвращению повторения. Сроки хранения - по разделу 5.

9.4.5. По итогам Уровня В–С Ответственный за внедрение готовит краткий отчёт для руководителя ОО с мерами профилактики; при Уровне 3 - план корректирующих действий с контрольными сроками.

9.5 Взаимодействие с поставщиком (вендором)

9.5.1. При технических сбоях или инцидентах в зоне ответственности вендора ОО незамедлительно обращается в службу поддержки поставщика по

утверждённым каналам эскалации, указывает номер инцидента и требует подтверждения получения.

9.5.2. Для каждой ИС и/или СИИ из Реестра у Ответственного за внедрение хранятся: контакты поддержки и эскалации, SLA/SLO (при наличии), порядок приостановки сервиса по требованию директора.

9.5.3. По инцидентам Уровня B-C ОО запрашивает у вендора: описание причины, затронутые функции/данные, временные и постоянные исправления, факт отключения дообучения на пользовательских данных (если применимо), подтверждение удаления/анонимизации затронутых данных, рекомендуемые меры на стороне ОО.

9.5.4. При риске для прав обучающихся и/или утечке ПД директор ОО вправе приостановить использование сервиса до устранения причин и получения от вендора подтверждений безопасности.

Раздел 10. Обучение, компетенции и возрастные меры

10.1. Цели обучения

10.1.1. Обеспечение безопасных и добросовестных практик применения ИИ.

10.1.2. Формирование базовой ИТ- и ИИ-грамотности всех участников образовательного процесса.

10.1.3. Подготовленность к рискам и инцидентам, предусмотренным настоящим Стандартом.

10.2. Норматив объёма и учёт

10.2.1. Минимальные объёмы и периодичность обучения утверждаются Уполномоченным органом.

10.2.2. ОО обеспечивает прохождение обучения в установленных объёмах всеми категориями пользователей и фиксирует результаты в учётных системах.

10.2.3. ОО хранит подтверждающие документы об обучении в сроки, установленные локальными актами и настоящим Стандартом.

10.3. Компетенции педагогов

Педагог обязан:

10.3.1. Знать ограничения генеративного ИИ (GenAI), правила атрибуции и требования академической добросовестности.

10.3.2. Проектировать задания с учётом возможностей GenAI, указывать допустимые формы помощи, обеспечивать альтернативы без применения ИИ.

10.3.3. Обеспечивать защиту данных обучающихся, применять минимизацию данных и иные меры, установленные разделами 5–6.

10.3.4. Выявлять предвзятость и ошибки вывода, инициировать процедуры апелляции и пересмотра в случаях, предусмотренных разделом 7.

10.3.5. Действовать по процедурам информирования, маркировки и реагирования на инциденты, установленным разделами 6 и 9.

10.4. Компетенции администрации, ИТ и ИБ

10.4.1. Вести на уровне ОО реестры используемых ИС и/или СИИ, применять матрицу порогов из Приложения А для локальной классификации рисков, фиксировать решения Этического совета.

10.4.2. Обеспечивать поддержку централизованной DPIA, проводимой Уполномоченным органом для систем/сценариев среднего и высокого риска: своевременно предоставлять сведения и артефакты по запросу, исполнять установленные условия и меры, доводить их до пользователей, вести учет исполнения. Локальные DPIA в ОО не проводятся.

10.4.3. Настраивать доступы и роли по принципу наименьших привилегий, обеспечивать журналирование и реагирование на инциденты по разделу 9, предоставлять альтернативные форматы без ИИ там, где это требуется.

10.4.4. Вести локальную документацию: выписки из записи Реестра по используемым системам, протоколы решений Этического совета, планы внедрения и перечни мер по снижению рисков. Сложные технические отчеты вендора не требуются; собственных технических испытаний администрация и ИТ-службы не проводят.

10.4.5. Вести выписки по форме R-1 и исполнять меры и ограничения из записи Реестра; подтверждать, что собственные технические испытания не проводятся; синхронизировать действия с централизованной DPIA.

10.5. Компетенции обучающихся

10.5.1. Понимать назначение ИИ, границы уместного использования и правила раскрытия вклада ИИ.

10.5.2. Проверять факты, распознавать дипфейки, знать ограничения детекторов ИИ.

10.5.3. Соблюдать приватность и не передавать персональные данные в промпты без правового основания.

10.5.4. Владеть базовыми навыками инженерии запросов в учебных целях.

10.6. Возрастная дифференциация

10.6.1. 1–4 классы: основы, безопасность, академическая честность, простые примеры.

10.6.2. 5–9 классы: критическое мышление, атрибуция, риски медиасреды.

10.6.3. 10–11 классы и колледж: правила GenAI, данные и приватность, порядок апелляций, базовые правовые рамки.

10.7. Родители и законные представители

10.7.1. ОО доводит до сведения родителей (законных представителей) краткие ориентиры по разрешённым и запрещённым практикам применения СИИ в учебном процессе.

10.7.2. ОО публикует порядок обращений по вопросам применения СИИ: официальный адрес для приёма вопросов и жалоб, сроки ответа, порядок апелляции (разделы 4, 9).

10.7.3. Обращения родителей (законных представителей) регистрируются

и рассматриваются в сроки, установленные локальными актами и законодательством; ответ направляется по указанному каналу.

10.8. Форматы и доступность

10.8.1. Программы обучения проводятся очно и (или) онлайн на государственном и русском языках.

10.8.2. Материалы предоставляются в доступных форматах с учётом потребностей обучающихся с инвалидностью и ООП.

10.8.3. Учебные материалы не содержат признаков лоббирования вендоров, имеют указание версии и даты актуализации.

10.9. Оценка усвоения

10.9.1. Оценка усвоения проводится с использованием пре- и пост-тестов, практических заданий и (или) артефактов обучения.

10.9.2. Для педагогов и сотрудников ИТ/ИБ применяются кейсы и симуляции, моделирующие инциденты и этические ситуации.

10.9.3. Для обучающихся подтверждается понимание правил атрибуции и границ применения генерирующих функций СИИ.

10.10. Учёт и контроль качества

10.10.1. ОО ведёт учёт часов обучения, результатов тестирования и созданных артефактов в установленной системе.

10.10.2. Показатели эффективности включают не менее: охват целевых групп, результаты пост-тестов, динамику инцидентов, качество атрибуции в работах.

10.10.3. Программы обучения ежегодно актуализируются по результатам мониторинга и аудита (раздел 9).

Раздел 11. Эволюция Стандарта и дальнейшие шаги

11.1. Цели и приоритеты

а) Настоящий Стандарт направляет применение ИИ в образовании.

б) Приоритет имеют права и наилучшие интересы ребёнка, педагогическая ценность и безопасность.

в) Применяется принцип соразмерности; всеобщие запреты без необходимости не устанавливаются.

11.2. Статус документа

а) Стандарт является «живым» документом.

б) Стандарт подлежит регулярной актуализации для поддержания актуальности и эффективности с учётом развития технологий ИИ.

11.3. Пересмотр

11.3.1. Периодичность.

Комплексный пересмотр проводится не реже одного раза в два года.

11.3.2. Внеплановый пересмотр.

Допускается при появлении прорывных технологий либо значимых изменений рисков.

11.3.3. Основания пересмотра:

а) практика применения Стандарта в ОО и официальная обратная связь;

б) результаты национальных исследований и мониторинга в сфере образования;

в) появление новых технологических рисков и возможностей;

г) изменения законодательства Республики Казахстан и международных рекомендаций.

11.3.4. Организация процесса. Пересмотр координирует Уполномоченный орган с участием подведомственных организаций и профильных государственных органов.

11.3.5. Метрики. Метрики Приложения D могут быть пересмотрены по данным мониторинга.

11.4. Ответственность за реализацию

11.4.1. Уполномоченный орган

1. формирует и ведёт Реестр; устанавливает отраслевые требования, типовые формы и программы обучения;
2. проводит централизованные DPIA и AIA для сценариев среднего и высокого риска; по итогам устанавливает обязательные условия и ограничения применения (см. разд. 6 и 7);
3. организует внешний мониторинг исполнения Стандарта и при необходимости ограничивает, приостанавливает или прекращает применение конкретных сценариев (см. разд. 9);
4. не проводит собственных технических испытаний программного обеспечения; учитывает заключения профильных государственных органов.

11.4.2. Организация среднего образования (ОО)

1. внедряет одобренные в Реестре ИС и/или СИИ локально, соблюдает разделы 4–10 Стандарта;
2. обеспечивает информирование пользователей, маркировку контента, альтернативные форматы без ИИ, учёт и журналирование;
3. исполняет меры и ограничения из записи Реестра и решений Этического совета;
4. поддерживает централизованные DPIA/AIA предоставлением сведений и артефактов; локальные DPIA не проводит;
5. не проводит собственных технических испытаний и аудита вендора; контролирует соблюдение локальных правил.

11.4.3. Вендор ИС и/или СИИ

1. обеспечивает соответствие продукта требованиям допуска и условий записи Реестра, в том числе по ИБ, приватности, фильтрации контента и дообучению на данных;

2. отвечает за техническую безопасность платформы и за своевременные обновления;
3. ведёт и обновляет форму R-1 по Приложению D, уведомляет об изменениях, предоставляет поддержку при инцидентах;
4. не использует данные обучающихся и работников вне целей, обозначенных в записи Реестра и договоре.

11.4.4. Педагогические работники

1. применяют только одобренные ИС и/или СИИ в пределах разрешённых сценариев;
2. фиксируют в заданиях правила использования ИИ, требования к атрибуции и «следам процесса», проверяют метки;
3. соблюдают минимизацию данных и запрет ввода ПД во внешние сервисы без основания;
4. действуют по процедурам апелляций, мониторинга и реагирования на инциденты (разд. 4, 8, 9, 10).

11.4.5. Обучающиеся и их законные представители

1. соблюдают правила академической добросовестности, атрибуции и маркировки;
2. не передают персональные данные в промпты и материалы без правового основания;
3. используют установленные каналы для обращений и апелляций;
4. исполняют ограничения по возрастным режимам и доступности (разд. 7, 10).

11.4.6. Ответственность за нарушения

Ответственность за несоблюдение настоящего Стандарта и условий записи Реестра наступает в порядке, установленном законодательством РК и локальными актами ОО.

Приложение А (обязательное).

Матрица порогов риска сценариев использования ИИ

А.1. Назначение

А.1.1. Матрица порогов риска устанавливает единый порядок предварительной классификации сценариев использования ИИ по уровням риска до их внедрения в организациях образования (далее - ОО).

А.1.2. Матрица применяется исключительно к дозволенным сценариям в соответствии с настоящим Стандартом.

А.1.3. Практики, указанные в разделе 3 Стандарта как запрещенные, классификации не подлежат и в ОО не допускаются.

А.2. Матрица критериев и порогов риска

Критерий	Низкий риск	Средний риск	Высокий риск
Значимость решения	Не влияет на оценки и статус обучающихся.	Косвенное влияние на оценивание или образовательную траекторию.	Может повлиять на допуск, итоговую оценку, дисциплинарные меры.
Категории данных	Без персональных данных или полностью обезличенные данные.	Персональные данные без специальных категорий.	Чувствительные ПД детей, в том числе массовая обработка.
Объём и идентифицируемость	Малый объём, один класс; риск реидентификации исключён.	Уровень класса или параллели; применена псевдонимизация.	Уровень школы или колледжа; риск реидентификации существенен.
Уровень автономии	Справочная либо черновая помощь.	Рекомендации с обязательной проверкой человеком.	Рекомендации по значимым решениям; риск исключительно автоматизированного решения.
Возраст и уязвимость	Старшие классы или взрослые обучающиеся.	Смешанные по возрасту группы.	Младшие классы; обучающиеся с ОВЗ.
Трансграничность	Отсутствует.	Имеется, при наличии достаточных гарантий.	Имеется, оценка гарантий затруднена.

Новизна и стабильность модели	Зрелый инструмент из Реестра, устоявшийся сценарий.	Новая версия или новый сценарий применения.	Пилот ранее не применявшейся в школе технологии.

А.3. Правила классификации

А.3.1. Итоговый уровень риска сценария определяется по наивысшему уровню среди всех применимых критериев.

А.3.2. При отсутствии достаточных сведений по любому критерию применяется более высокий уровень риска.

А.3.3. Для детализированной оценки используются определения: «массовая обработка» - обработка данных значительной части обучающихся организации; «исключительно автоматизированное решение» - решение без участия человека, порождающее юридические или аналогично значимые последствия.

А.4. Требуемые меры по уровням риска

А.4.1. Низкий риск:

а) применяются общие меры контроля, установленные п. 5.4;

б) ведётся локальный журнал применения сценария (учёт случаев и целей использования).

А.4.2. Средний риск:

а) требуется решение Этического совета ОО о допустимости сценария;

б) осуществляется уведомление родителей (законных представителей) и обучающихся;

в) доводится до сведения порядок апелляции и рассмотрения жалоб;

г) исполняются условия и ограничения, указанные в записи Реестра;

д) применяются меры, предусмотренные п. 5.5 подпункты 1 и 2.

А.4.3. Высокий риск:

а) выполняются все меры, установленные для уровня «Средний»;

б) проводится пилотная эксплуатация на ограниченной аудитории (см. п. 5.7);

в) обеспечивается равнозначная альтернатива без применения ИИ;

г) подтверждается участие человека в принятии значимых решений (human-in-the-loop);

д) применяются меры, предусмотренные п. 5.5 подпункт 3.

А.5. Карта сценария (форма М-1)

А.5.1. Форма заполняется при классификации сценария и включает обязательные разделы:

1. наименование ИС/СИИ (по Реестру);
2. описание сценария применения;
3. оценка по каждому критерию матрицы риска;
4. итоговый уровень риска и обоснование;
5. перечень обязательных мер контроля;
6. решение Этического совета и срок пересмотра.

А.5.2. Карта сценария хранится у ОО, представляется уполномоченному органу и иным компетентным органам по их запросу.

Приложение В (обязательное).

Шаблоны уведомлений

В.0. Общие требования к уведомлениям

В.0.1. Уведомления доводятся до обучающихся и родителей на государственном и русском языках до начала обработки данных.

В.0.2. Уведомления содержат: цель обработки, правовое основание, категории данных, место и срок хранения, получателей и обработчиков, условия трансграничной передачи, описание участия человека, риски и ограничения, права субъекта данных и порядок апелляции, контакт ответственного.

В.0.3. Факт ознакомления фиксируется подписью или электронной отметкой с указанием даты и версии уведомления.

В.0.4. Для отдельных кейсов применяются специальные уведомления. Перечень таких кейсов и формы утверждаются локальным актом ОО.

В.0.5. Содержание и порядок доведения уведомлений должны соответствовать пп. 7.1–7.3, 7.6–7.7, 7.9–7.13 настоящего Стандарта.

В.0.6. При изменении цели, правового основания, состава данных, получателей или сроков хранения уведомление подлежит актуализации и повторному доведению.

В.0.7. Если требуется согласие, к уведомлению прилагается форма согласия. Факт получения согласия фиксируется в порядке п. 7.13.

В.0.8. Уведомления сохраняются вместе с подтверждением ознакомления в порядке и сроки, установленные законодательством и локальными актами ОО.

В.1. Общее уведомление о применении ИИ в учебном процессе

Форма У-1

Заголовок: Уведомление о применении ИИ в [предмет/раздел].

Оператор обработки: [наименование организации образования, адрес, ИИН/БИН].

Цель обработки: [описание учебной цели].

Правовое основание: [норма закона и локального акта и/или договор и/или согласие*].

Используемая система: [наименование из Реестра], версия или модель: [ ], поставщик: [ ], ссылка на запись в Реестре: [идентификатор].

Категории данных: [перечень категорий данных или «не применяются»].

Место и срок хранения: [место хранения, ИС], срок: [конкретный срок или критерий].

Получатели и обработчики: [внутренние роли ОО; поставщик из Реестра; иные лица при наличии].

Трансграничная передача: [есть/нет; страна; правовые гарантии].

Участие человека: Итоговые решения принимает педагог. ИИ используется как вспомогательный инструмент.

Риски и ограничения: [краткое описание предусмотренных рисков и ограничений использования].

Права субъекта данных и порядок апелляции: [перечень прав, ссылка или контакты для обращения и апелляции].

Контакт ответственного: [ФИО должностного лица, телефон, электронная почта].

Фиксация ознакомления: [подпись или электронная отметка], дата: [ ], версия уведомления: [ ].

Приложения: [форма согласия при необходимости*; выдержка из Реестра; локальный порядок апелляции].

*Если требуется согласие, прикладывается форма согласия. Фиксация согласия осуществляется по п. 7.13.

В.2. Специальное уведомление: экзамен/прокторинг

Форма У-2. Дополнительно к У-1 указываются:

- Вид контроля, дата, время начала и длительность: [ ].
- Перечень и режим включения датчиков и доступов: камера [вкл/выкл], микрофон [вкл/выкл], доступ к экрану [вкл/выкл]. Доступ активируется только на период экзамена. Постоянный доступ вне экзамена запрещён.
- Альтернативный формат сдачи без ИИ с равнозначным оцениванием: [описание и порядок выбора].
- Эмо-ИИ не применяется.
- Контакт для оперативной связи в день экзамена: [ФИО, телефон, e-mail]. Соответствие: п. 3.4, п. 7.1.2 Стандарта.

В.3. Специальное уведомление: аналитика успеваемости и персонализация Форма У-3. Дополнительно к У-1 указываются:

- Набор показателей и метрик: [перечень].
- Источники данных: [ИС, журналы, тесты, иное].
- Метод обезличивания или псевдонимизации: [описание].
- Порог вмешательства человека и порядок пересмотра рекомендаций: условия триггера ручной проверки [ ], ответственный [ ], сроки пересмотра [ ].

Соответствие: п. 5.5, п. 7.4 Стандарта.

В.4. Специальное уведомление: мониторинг работников
Форма У-4. Дополнительно к У-1 указываются:

- Законные цели: [обеспечение трудовой дисциплины; безопасность и охрана труда; защита ИС и имущества; ИБ; контроль качества услуг; иное, конкретизировать].
- Перечень метрик и источников: [учёт рабочего времени; события вход/выход; логи ИС; использование служебных устройств и сетей; видеонаблюдение в обозначенных зонах; геолокация служебных устройств при необходимости; иное, конкретизировать].
- Сроки хранения журналов и носителей: [конкретный срок по каждой метрике], место хранения [ ], режим доступа [ ]. Принцип минимизации: хранение не дольше, чем необходимо для заявленной цели.
- Запрет скрытого наблюдения вне трудовых обязанностей: контроль ведётся только в рабочее время, в служебных зонах и/или на служебных устройствах; скрытая запись и слежение за личными устройствами, аккаунтами и в нерабочее время не допускаются. Зоны видеонаблюдения маркируются.

Соответствие: п. 3.7, п. 7.1.2 Стандарта.

Приложение С (обязательное).

Шаблоны атрибуции и маркировки

С.0. Общие требования.
Любое использование GenAI раскрывается; ИИ-контент маркируется

визуально и в метаданных. Соответствие п. 6.2–6.3 и п. 7.4.

C.1. Краткая атрибуция в письменной работе

«Использован GenAI [сервис], модель [модель/версия], для: [генерация идей / языковая правка / рефакторинг кода / иное]. Дата обращения: [дд.мм.гггг]. Ключевые подсказки и ответы отражены в приложении/ссылке.»
Шаблон соответствует п. 7.4 б.

C.2. Расширенная атрибуция (при существенном влиянии ИИ)

В конце работы приводится таблица: задача → подсказка → ответ ИИ → редакция автора → ссылка на источник/фрагмент.

C.3. Маркировка учебных материалов и управленческих документов

В шапке или под заголовком:

«Содержит материалы, сгенерированные ИИ: [сервис], [модель/версия], дата: [дд.мм.гггг]. Ответственный: [ФИО].»

Для синтетических медиа:

«СИНТЕТИЧЕСКОЕ ИЗОБРАЖЕНИЕ/АУДИО/ВИДЕО, создано ИИ: [сервис], [модель], [дата].»

Метаданные файла: поля CreatorTool/Software, AI-Generated: Yes, Model, ModelVersion, GenerationDate, ResponsibleContact. Соответствие п. 6.3.

C.4. Карточка атрибуции для презентации

Отдельный слайд «Использование ИИ»: инструмент, модель, задачи, степень влияния; ссылка на приложение с примерами подсказок.

C.5. Фиксация атрибуции в электронных системах

В форме сдачи работы добавляются поля: чекбокс «Использован ИИ», список задач, инструмент/модель, дата, ссылка на черновики. Соответствие п. 6.13 и п. 7.5.

Минимальные метрики и форма R-1 для Реестра доверенных ИС / СИИ

D.1. Общие правила

а) Метрики считает и подтверждает вендор. Школы метрики не считают.

б) Наборы тестов репрезентативны по казахскому и русскому языкам и ключевым категориям обучающихся. Реальные ПД детей в тестах не применяются.

в) Результаты публикуются в форме R-1 в записи Реестра. Статус: «в норме / под наблюдением / ограничить / приостановить». Решение принимает Уполномоченный орган.

D.2. Универсальные требования

Языковой паритет: разница ключевых метрик между казахским и русским ≤5 п.п.

- Контент-безопасность: доля нарушающих ответов ≤0.1%.
- Прозрачность: указание уровня уверенности и ограничений; пример объяснения вывода.

D.3. Генеративный учебный ассистент

- Фактологическая точность ≥85%.
- Галлюцинации ≤10%.
- Задержка ответа p95 ≤3 сек.
- Утечки ПД на неинвазивные промпты: 0 кейсов.

D.4. Автооценивание коротких ответов и эссе

- Сходимость с педагогам: QWK ≥0.80 или MAE ≤0.3 балла.
- Калибровка: средняя абсолютная ошибка ≤0.05.
- Ошибка «проход/непроход»: FPR ≤5%, FNR ≤15%.
- 100% человек-в-петле для значимых решений.

D.5. Персонализация и аналитика успеваемости

- Precision@K для риска отставания ≥0.75.
- FPR ≤10%.
- Явный порог вмешательства человека и порядок пересмотра рекомендаций.

D.6. Прокторинг сигналов (если применяется)

- Ложные срабатывания ≤5%.
- Пропуски нарушений ≤20%.
- 100% ручной пересмотр всех флагов.
- Запрет эмо-ИИ. Альтернатива без ИИ обязательна.

D.7. Периодичность подтверждения

- При включении в Реестр, затем ежегодно и при мажорных изменениях.

Форма R-1 (одна страница на сценарий)

1. Система: название, версия/модель, дата сборки, уровень риска.
2. Назначение и границы: допустимые и недопустимые применения.
3. Данные: категории, хранение, трансграничная передача, обезличивание в тестах.
4. Метрики и результаты: по разделам D.2–D.6.
5. Статус соответствия и срок на исправление при отклонениях.
6. Прозрачность: пример объяснения вывода, уровень уверенности, ссылка на «карту системы» из п. 6.5.
7. Меры для школ: обязательные меры из записи Реестра, включая человек-в-контуре и альтернативу без ИИ для высокого риска.
8. Контакты эскалации у вендора.