

Этика и безопасность в ИИ

Правильно и ответственно использование ИИ

Цели модуля

1. Познакомить учителей с основными этическими вопросами, связанными с применением ИИ.

2. Разобраться, какие меры безопасности нужно принимать при работе с ИИ в образовательной среде.

3. Рассмотреть примеры этических дилемм и как их можно избежать.

4. Ознакомить с законодательными нормами, касающимися конфиденциальности и защиты данных.

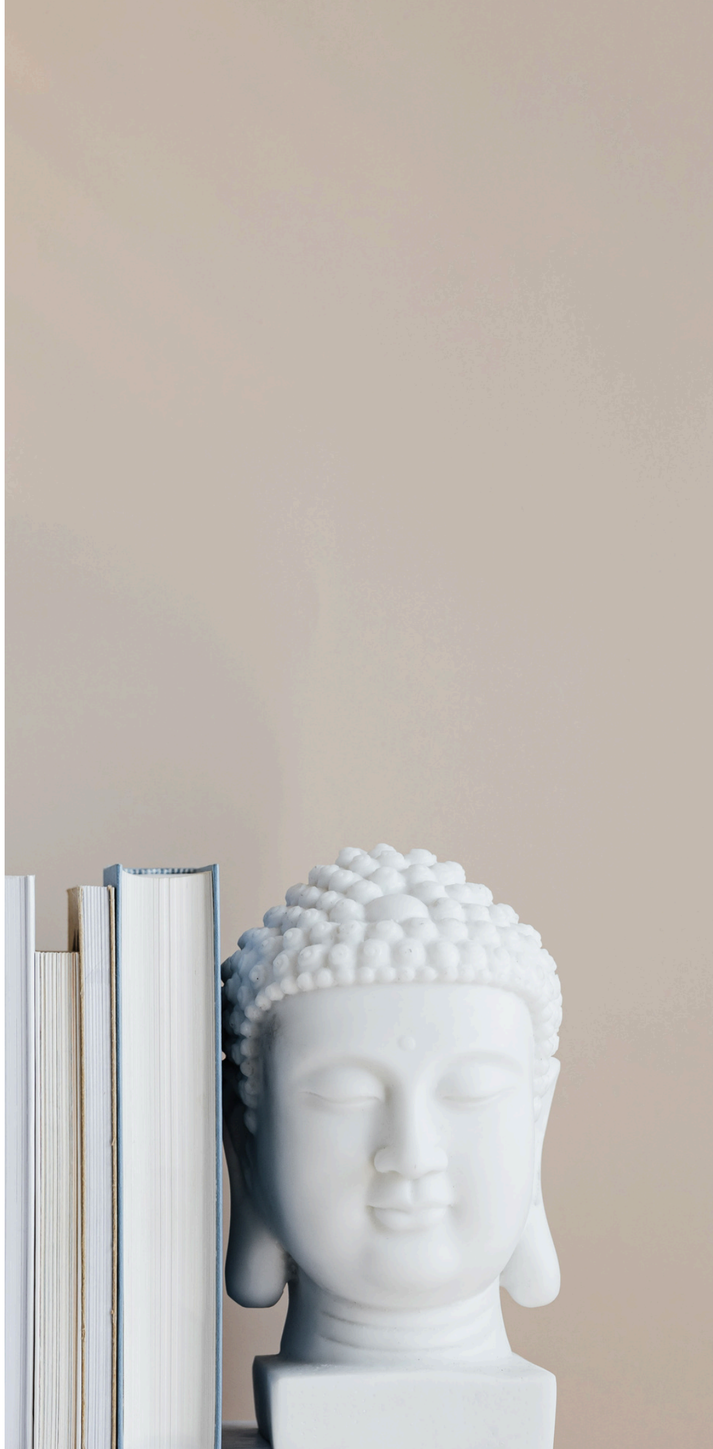
Основы этики в ИИ

Что такое этика в контексте ИИ?

Этика ИИ — это набор принципов, направленных на обеспечение ответственного использования технологий искусственного интеллекта. Она включает в себя рассмотрение того, как ИИ должен взаимодействовать с людьми, как избежать вреда и какие ограничения следует применять, чтобы защитить людей от неправильного использования ИИ.



Основные этические принципы ИИ



Прозрачность:

- Учителя, использующие ИИ, должны понимать, как и на основе чего работают системы, которые они применяют. Это особенно важно, чтобы ученики и их родители знали, как принимаются решения на основе данных, и могли доверять процессу.

  - Пример: Если ИИ используется для оценки знаний, то учитель должен быть готов объяснить, каким образом система пришла к такому результату и почему оценка справедлива.



Ответственность:



Несмотря на то что ИИ способен принимать решения на основе данных, ответственность за его использование всегда остается на учителях. Учителя должны проверять результаты ИИ и следить за тем, чтобы они соответствовали реальной ситуации.

- Пример: Если система ИИ автоматически оценивает работу ученика, учитель должен убедиться, что оценка справедлива, и при необходимости вмешаться в процесс.

Непредвзятость:

- ИИ может неосознанно усиливать предвзятость в данных, особенно если алгоритмы обучены на некорректных или ограниченных данных. Учителя должны быть осторожны при использовании ИИ, чтобы не допускать дискриминации.



- Пример: Алгоритм может быть обучен на данных, которые не учитывают культурные или социальные различия. Это может привести к тому, что оценки или рекомендации, сгенерированные ИИ, будут не совсем точными для отдельных учеников.

Конфиденциальность и защита данных:

- Учителя должны следить за тем, чтобы данные учеников были защищены, а ИИ не использовался для сбора или передачи конфиденциальной информации без согласия. Это особенно важно в контексте школьных данных, где хранится информация о личных данных учеников.

- Пример: Использование ИИ для анализа успеваемости не должно нарушать конфиденциальность учеников. Данные должны храниться на защищенных серверах, и доступ к ним должен быть строго ограничен.





Этические вопросы в образовании

Предвзятость в оценке:



- Когда ИИ используется для автоматической оценки работ или тестов, существует риск, что система будет предвзята. Например, если ИИ обучен на ограниченных данных, он может неправильно оценивать ответы учеников из разных культурных или языковых групп.
- Как избежать: Учителя должны проверять результаты, предсказанные ИИ, и вводить корректировки, если алгоритм ошибается или выдает неоднозначные результаты.

Автоматизация и гуманизация процесса обучения:

- ИИ может автоматизировать многие аспекты обучения, но важно помнить, что технология не заменяет человеческое взаимодействие. Образование — это не только передача знаний, но и воспитание, эмоциональная поддержка и социализация.

- Как избежать: Используйте ИИ как помощника, но не как замену. Например, пусть ИИ помогает в рутинных задачах, таких как проверка тестов, но обратная связь от учителя должна оставаться ключевой.





Безопасность ИИ в образовательной среде

Опасности и риски при использовании ИИ

Нарушение конфиденциальности данных:

- При использовании ИИ важно защищать личные данные учеников. Множество ИИ-систем работают на основе анализа данных, и если безопасность этих данных не обеспечена, это может привести к утечке информации.

- Как предотвратить: Доступ к данным должен быть ограничен только для тех, кто непосредственно работает с ними. Все системы должны быть защищены паролями и шифрованием.

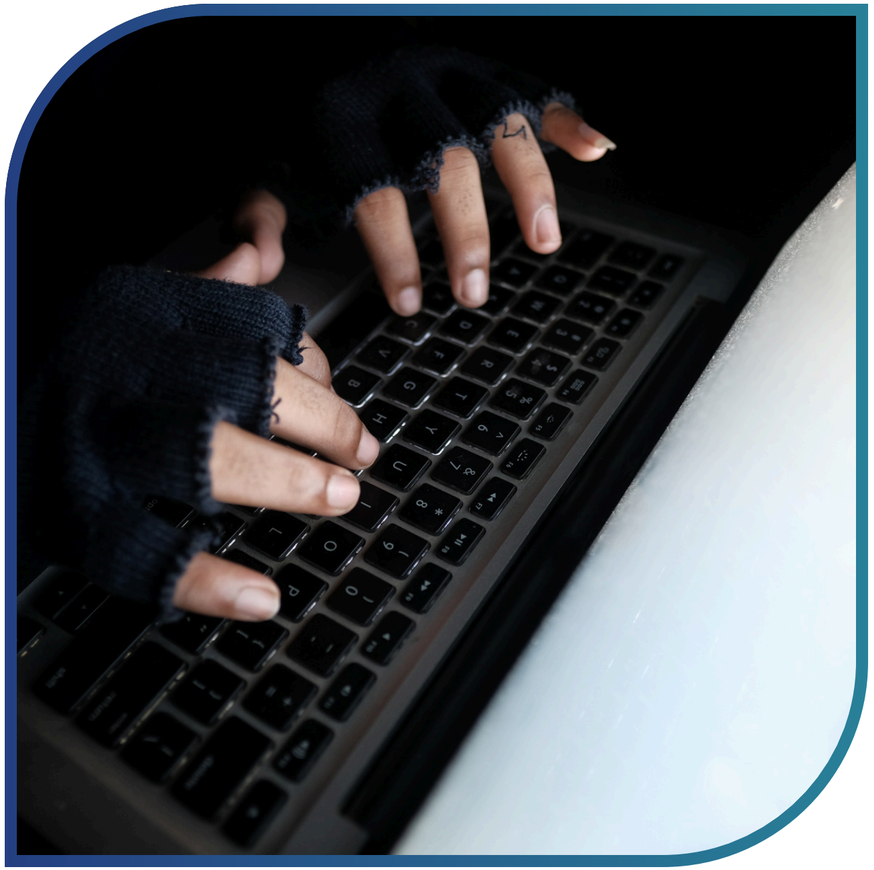




Кибератаки и взломы:

- С увеличением использования ИИ возрастает угроза кибератак. Образовательные платформы могут стать целью хакеров, стремящихся получить доступ к данным учеников и учителей.

- Как предотвратить: Используйте защищенные платформы для работы с данными. Все системы, где хранятся данные учеников, должны регулярно обновляться, чтобы избегать уязвимостей.



Мошенничество и плагиат:

- ИИ может быть использован учениками для мошенничества, например, с помощью чат-ботов для написания сочинений или ответов на тесты.

- Как предотвратить: Учителя должны быть осведомлены о возможностях ИИ и проверять оригинальность работ учеников. Существуют инструменты, такие как **Turnitin**, которые помогают выявлять плагиат и автоматические ответы.



Меры для обеспечения безопасности

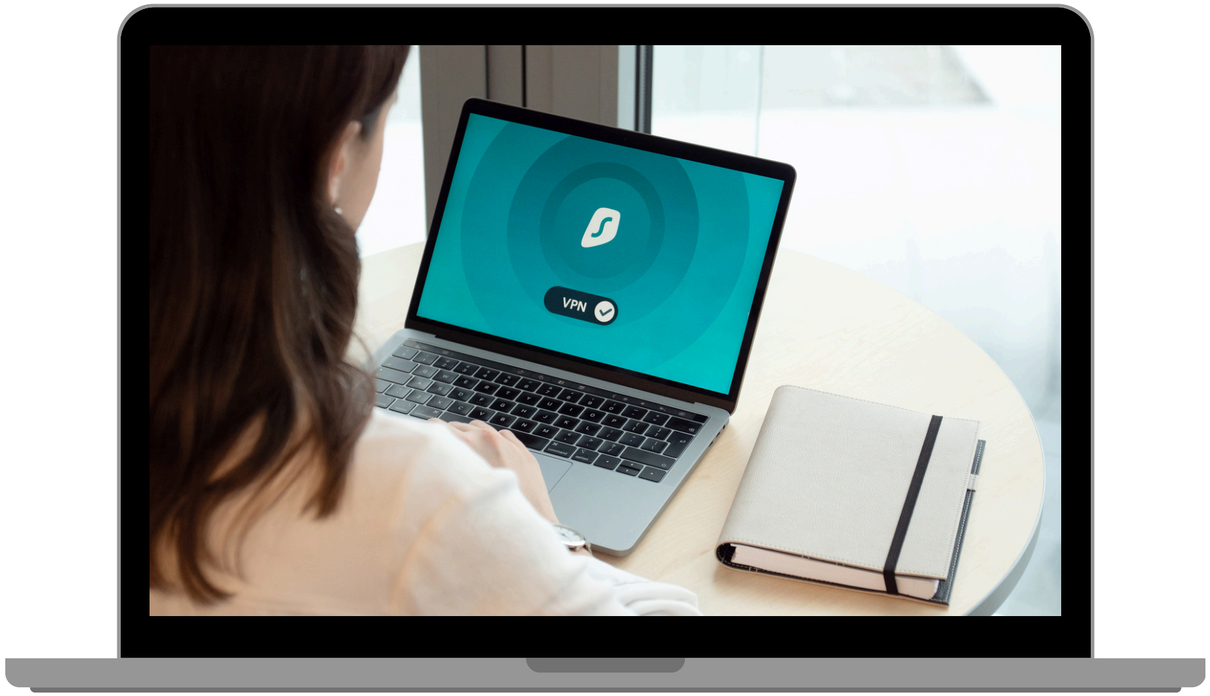
Шифрование данных:

- Все данные, передаваемые через интернет, должны быть зашифрованы. Это минимизирует риск утечек информации, если система будет взломана.
  - Пример: Использование HTTPS-протоколов и VPN для безопасного подключения к учебным системам.



Ограничение доступа:

- Только те, кто непосредственно работает с данными (учителя, администраторы), должны иметь доступ к личной информации учеников.
  - Пример: Установка многофакторной аутентификации для входа в систему.



Периодическое обновление и аудит системы безопасности:

- Необходимо регулярно обновлять программное обеспечение и проводить аудит безопасности систем, чтобы быть уверенными, что они соответствуют современным стандартам.
  - Пример: Ежеквартальные проверки IT-инфраструктуры школы на наличие уязвимостей.





Законодательные нормы и стандарты безопасности

Закон Республики Казахстан "О персональных данных и их защите":

- Этот закон регулирует обработку персональных данных и их защиту. Учителя и школы должны следовать его нормам при использовании ИИ для анализа данных учеников.

- Пример: Перед сбором данных от учеников и их родителей необходимо получать согласие на использование и обработку данных.



Международные стандарты безопасности (GDPR и др.):

- Если школа работает с международными платформами, важно учитывать также и международные стандарты безопасности данных, такие как GDPR (Общий регламент по защите данных в Европе).
  - Пример: При использовании международных сервисов для хранения данных необходимо убедиться, что они соответствуют нормам по защите данных.



Заключение

Итак, в этом модуле мы с вами обсудили ключевые вопросы этики и безопасности при использовании ИИ в образовательном процессе. Ответственное использование ИИ, защита данных учеников и понимание возможных рисков — всё это помогает создать безопасную и этичную среду для обучения с использованием современных технологий. Помните, что ИИ — это мощный инструмент, но его использование требует осознанного и внимательного подхода.

Спасибо за внимание!