

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.21
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Правовые и этические аспекты искусственного интеллекта

(наименование дисциплины)

по направлению подготовки
09.03.04 Программная инженерия

направленность (профиль)
Программная инженерия с применением ИИ-технологий

Форма обучения: заочная

Год набора: 2024

Общая трудоемкость: 3 ЗЕ

Распределение часов дисциплины по семестрам

Семестр		7	Итого
Вид занятий	Форма контроля	зачет с оценкой	
Лекции		4	4
Лабораторные			
Практические			
Руководство: курсовые работы (проекты) / РГР			
Промежуточная аттестация		0,25	0,25
Контактная работа		4,25	4,25
Самостоятельная работа		100	100
Контроль		3,75	3,75
Итого		108	108

Рабочую программу составил(и):

доцент института цифровых технологий, канд. пед. наук, доцент Гущина О.М.

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:



Отсутствует



Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки

09.03.04 Программная инженерия

Срок действия рабочей программы дисциплины до «31» августа 2031 г.

УТВЕРЖДЕНО

На заседании института цифровых технологий

(протокол заседания № 1 от «05» сентября 2025 г.).

1. Цель освоения дисциплины

Цель освоения дисциплины – формирование у обучающихся системного понимания правового поля, этических принципов и нормативных требований, связанных с разработкой, развертыванием и использованием систем искусственного интеллекта для создания ответственных, надежных и законных ИИ-решений.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина: «Системы искусственного интеллекта».

Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее: «Практикум по машинному обучению и анализу данных», «Выполнение и защита выпускной квалификационной работы».

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
ПК-11. Способен разрабатывать и оптимизировать нейросетевые архитектуры для анализа данных	ПК-11.1. Знает виды нейросетевых архитектур	Знать: основные архитектуры нейронных сетей (полносвязные, сверточные - CNN, рекуррентные - RNN/LSTM, трансформеры, автокодировщики). Уметь: выбирать тип архитектуры для задач компьютерного зрения, обработки естественного языка (NLP) и т.д. Владеть: терминологией в области глубокого обучения.
	ПК-11.2. Умеет оптимизировать нейросетевые архитектуры для анализа данных	Знать: методы оптимизации обучения нейросетей; методы аугментации данных. Уметь: подбирать параметры, проводить тонкую настройку предобученных моделей. Владеть: навыками использования фреймворков глубокого обучения для обучения и оптимизации моделей.
	ПК-11.3. Владеет навыками разработки нейросетевых архитектур для анализа данных	Знать: передовые нейросетевые архитектуры, применяемые для анализа данных. Уметь: проектировать новые или модифицировать существующие архитектуры для решения нестандартных задач. Владеть: практическими навыками создания и обучения сложных нейросетевых моделей с нуля.

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1. Интеллектуальная собственность и данные	Лек 1	Тема 1. Введение в правовые и этические вызовы ИИ. Интеллектуальная собственность	7	2	–	–	
	Ср	Самостоятельное изучение методических рекомендаций при подготовке к практическим работам.	7	10	–	–	
	Ср	ПР 1. Анализ лицензионной совместимости в AI-проекте	7	2	8	–	Отчет по практической работе № 1
Модуль 2. Ответственность и приватность	Лек 2	Тема 2. Ответственность за решения ИИ. Защита персональных данных.	7	2	–	–	
	Ср	Самостоятельное изучение методических рекомендаций при подготовке к практическим работам.	7	10	–	–	
	Ср	ПР 2. Составление карты данных и легальной основы для их обработки (часть 1)	7	2	8	–	Отчет по практической работе № 2
	Ср	ПР 2. Составление карты данных и легальной основы для их обработки» (часть 2)	7	2	–	–	
Модуль 3. Этика и безопасность AI-систем	Ср	Тема 3. Этические принципы и смещение в алгоритмах	7	2	–	–	
	Ср	Тема 4. Безопасность и киберустойчивость AI-систем		2	–	–	
	Ср	Самостоятельное изучение методических рекомендаций при подготовке к практическим работам.	7	10	–	–	
	Ср	ПР 3. Проведение аудита смещения (Bias Audit) датасета и модели (часть 1)	7	2	8	–	Отчет по практической работе № 3
	Ср	ПР 3. Проведение аудита смещения (Bias Audit) датасета и модели (часть 2)	7	2	–	–	
	Ср	ПР 4. Моделирование и защита от adversarial атаки. (часть 1)	7	2	8	–	Отчет по практической работе № 4
	Ср	ПР 4. Моделирование и защита от adversarial атаки. (часть 2)	7	2	–	–	
Модуль 4. Регулирование и прикладная этика	Ср	Тема 5. Национальные стратегии и регулирование ИИ	7	2	–	–	
	Ср	Тема 6. Правовой статус AI-агентов и генеративных моделей	7	2	–	–	

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
	Ср	Самостоятельное изучение методических рекомендаций при подготовке к практическим работам.	7	10	–	–	
	Ср	ПР 5. Экспертиза AI-системы по критериям EU AI Act. (часть 1)	7	2	8	–	Отчет по практической работе № 5
	Ср	ПР 5. Экспертиза AI-системы по критериям EU AI Act. (часть 2)	7	2	–	–	
	Ср	ПР 6. Анализ комплексного кейса "Генеративный ИИ в медиа"(часть 1)	7	2	8	–	Отчет по практической работе № 6
	Ср	ПР 6. Анализ комплексного кейса "Генеративный ИИ в медиа"(часть 2)	7	2	–	–	
Модуль 5. Интеграция знаний в жизненный цикл разработки	Ср	Тема 7. Интеграция правовых и этических аспектов в жизненный цикл разработки (MLOps)	7	2	–	–	
	Ср	Тема8. Воркшоп "Ответственный AI": разбор сквозного примера	7	2	–	–	
	Ср	Самостоятельное изучение методических рекомендаций при подготовке к практическим работам.	7	10	–	–	
	Ср	ПР 7. Разработка раздела "Правовые и этические риски" в ТЗ на AI-продукт. (часть 1)	7	2	6	–	Отчет по практической работе № 7
	Ср	ПР 7. Разработка раздела "Правовые и этические риски" в ТЗ на AI-продукт. (часть 2)	7	2	–	–	
	Ср	ПР 8. Финальный проект: Создание "Этического паспорта" для AI-продукта. (часть 1)	7	2	6	–	Отчет по практической работе № 8
	Ср	ПР 8. Финальный проект: Создание "Этического паспорта" для AI-продукта. (часть 2)	7	2	–	–	
	Ср	Подготовка к зачету	7	9,75	–	–	
	ПА	Промежуточная аттестация	7	0,25	–	–	
	Контроль	Зачет с оценкой	7	3,75	40	–	Итоговый тест
ИТОГО:				180			

5. Образовательные технологии

В рамках учебного курса предусмотрены следующие образовательные технологии:

- технология традиционного обучения: лекции, практические работы, самостоятельная работа;
- технология проектного обучения: реализация и защита отчетов по практическим работам.

Для обучающихся всех форм обучения предусмотрено получение консультационной помощи. Особое внимание необходимо уделить самостоятельному изучению нормативных источников и рекомендованной литературы.

В качестве текущего контроля при изучении курса предусмотрены защиты отчетов по практическим работам.

6. Методические указания по освоению дисциплины

Самостоятельная работа обучающихся (СРС) – работа с лекционным материалом, подготовка к практическим занятиям, изучение методических рекомендаций по выполнению практических заданий; подготовка к зачету.

Самостоятельная работа обучающихся проводится с целью углубления и расширения теоретических знаний; развития познавательных способностей и активности обучающихся; самостоятельности, ответственности и организованности, творческой инициативы; формирования самостоятельности мышления, способности к саморазвитию, самосовершенствованию и самореализации.

6.1. Рекомендации по подготовке к практическим занятиям

Обучающимся следует:

- при подготовке к практическим занятиям следует обязательно использовать не только лекции, учебную литературу, но и другие источники;
- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;
- на занятии доводить задания практической работы до окончательного решения, демонстрировать выполненные задания, в случае затруднений обращаться к преподавателю.

Для того чтобы практические занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по рассмотренному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться обучающимся на практических занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях обучающийся не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

6.2. Рекомендации по подготовке к зачету

Подготовка к зачету способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к зачету, обучающийся ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На зачете обучающийся демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

На консультации перед зачетом обучающиеся должны быть ознакомлены с основными требованиями и получить ответы на возникающие в процессе подготовки вопросы.

Необходимо ориентировать обучающихся на систематическую подготовку к занятиям в течение семестра, что позволит использовать время экзаменационной сессии для систематизации знаний.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
7	ПК-11	Отчеты по практическим работам 1-8 Вопросы к зачету 1-150

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1. Пример практической работы

Практическая работа 1. Анализ лицензионной совместимости в AI-проекте

Цель работы: Сформировать у обучающихся устойчивые практические навыки анализа лицензионных соглашений программного обеспечения и данных, используемых в AI-проекте. Научить выявлять правовые риски, связанные с лицензионной несовместимостью, и разрабатывать стратегию по их минимизации для успешной и легальной реализации коммерческого или научного проекта.

Порядок выполнения работы:

- Внимательно прочитайте описание одного из предложенных кейсов. Если вы используете собственный проект, составьте его краткое описание (1-2 абзаца), указав цель, основной функционал и планируемую модель распространения (коммерческая/некоммерческая, открытая/проприетарная).
 - Кейс А: "Разработка коммерческого SaaS-продукта для анализа эмоций по видео. Стек технологий: бэкенд на Python, использование библиотек NumPy (лицензия BSD), TensorFlow (Apache 2.0), коммерческая библиотека для обработки видео от стороннего вендора (проприетарная EULA), а также модифицированная версия библиотеки с открытым исходным кодом, распространяемой под лицензией GNU GPLv3".
 - Кейс Б: "Создание открытого исследовательского ИИ-инструмента для генерации поэзии. Используется фреймворк PyTorch (лицензия BSD), датасет из текстов, размещенных под лицензией Creative Commons Attribution-ShareAlike (CC BY-SA), и подключаемый модуль, распространяемый под лицензией MIT".
- Создайте таблицу в Excel или Google Sheets. Внесите в нее все ключевые компоненты вашего проекта, которые не были созданы вами с нуля.
- Разделите компоненты на две категории: "Программное обеспечение (библиотеки, фреймворки)" и "Данные (датасеты, модели)".
- Для каждого компонента укажите:
 - Точное название.
 - Версию (если применимо).
 - Ссылку на официальный источник (сайт, GitHub репозиторий).
 - Тип лицензии. Найдите текст лицензии. Обычно он находится в файле LICENSE, COPYING в корне репозитория или на сайте проекта.
- Для каждого компонента из таблицы проведите детальный разбор лицензионного соглашения. Выпишите ключевые условия и ограничения. Используйте для этого следующую таблицу-шаблон:

Название компонента	Лицензия	Условия коммерческого использования	Требования к раскрытию исходного кода (Копилефт)	Требования к атрибуции (указанию автора)	Другие важные ограничения (запрет на патентные иски, запрет на использование в военных целях и т.д.)
---------------------	----------	-------------------------------------	--	--	--

<i>TensorFlow</i>	<i>Apache 2.0</i>	<i>Разрешено</i>	<i>Нет. Разрешающая лицензия.</i>	<i>Да. Необходимо включить уведомление об авторских правах, текст лицензии и изменение файла NOTICE в распространяемых копиях.</i>	<i>Предоставляет патентную лицензию, но она прекращается при подаче патентного иска.</i>
<i>Библиотека X</i>	<i>GPLv3</i>	<i>Разрешено</i>	<i>Да. Любая производная работа должна распространяться на условиях GPLv3.</i>	<i>Да</i>	<i>Защищает права пользователей против патентных исков и ограничения аппаратного обеспечения (tivoization).</i>
<i>Datascet Y</i>	<i>CC BY-NC</i>	<i>Запрещено</i>	<i>Не применимо</i>	<i>Да</i>	<i>Запрещено коммерческое использование.</i>

6. Особое внимание уделите "сильным" копиелефт-лицензиям (GPL). Помните: если ваш проект динамически линкует или иным образом образует единое целое с кодом под GPL, то весь ваш проект может подпадать под требование раскрытия исходного кода на условиях GPL.
7. Проверьте совместимость лицензий между собой. Сфокусируйтесь на самых "строгих" лицензиях в вашем стеке.
 - Используйте официальные ресурсы, например, матрицу совместимости лицензий от GNU.
 - Ответьте на ключевые вопросы:
 - Совместима ли разрешающая лицензия (MIT, BSD, Apache 2.0) с копиелефт (GPL)? *Да, обычно они могут быть использованы в проекте под GPL, но не наоборот.*
 - Совместима ли лицензия, запрещающая коммерческое использование (CC BY-NC), с вашим коммерческим проектом? *Нет.*
 - Можно ли использовать код под лицензией Apache 2.0 в проекте под GPLv3? *Да.*
8. Сформулируйте конкретные правовые риски. Например: "Использование библиотеки под GPLv3 в нашем проприетарном коммерческом продукте приведет к нарушению лицензии и требованию раскрыть весь исходный код продукта".
9. На основе анализа дайте четкий ответ: можно ли использовать выбранный стек технологий для поставленных целей?
10. Если нет, предложите альтернативы. Например: "Вместо библиотеки под GPLv3 рекомендуется найти аналог с разрешающей лицензией (например, BSD или MIT)".
11. Если да, составьте список обязательных действий для compliance. Например: "Для соблюдения лицензии Apache 2.0 необходимо включить текст лицензии и уведомление об авторских правах в документацию к нашему продукту".

Содержание отчета:

1. Титульный лист.
2. Описание выбранного кейса и целей проекта.
3. Таблица с анализом лицензий компонентов.
4. Аналитический раздел с оценкой лицензионной совместимости и выявленными рисками.
5. Список конкретных рекомендаций для разработческой команды.
6. Выводы.

Процедура оценивания

Оценка выполненной практической работы проводится по следующим критериям:

1. Наличие всей существенной информации по работе
2. Точность и полнота предоставляемых сведений
3. Непротиворечивость приводимой информации
4. Правильность интерпретаций и выводов, которые сделаны по результатам работы
5. Степень достижения обучающимся поставленной цели

6. Обоснованность применяемого решения
7. Грамотность (содержательная) используемых формулировок

Критерии оценки за отчеты по практическим работам:

Формы текущего контроля	Критерии и нормы оценки
Отчеты по практическим работам 1-6	7-8 баллов – задание выполнено в полном объеме 5-6 баллов – задание выполнено в объеме 70%, 3-4 баллов – задание выполнено в объеме 50%, 1-2 балла – задание выполнено в объеме менее 50%, 0 баллов – задание не выполнено.
Отчеты по практическим работам 7-8	5-6 баллов – задание выполнено в полном объеме 3-4 балла – задание выполнено в объеме 70%, 2-3 балла – задание выполнено в объеме 50%, 1 балл – задание выполнено в объеме менее 50%, 0 баллов – задание не выполнено.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр седьмой

№	Вопросы к зачету
1.	Дайте определение интеллектуальной собственности (ИС) в контексте искусственного интеллекта.
2.	Назовите основные объекты ИС, которые могут возникать на разных этапах жизненного цикла AI-системы.
3.	Кто является автором и правообладателем произведения, созданного с помощью ИИ? Проанализируйте разные точки зрения.
4.	В чем заключаются основные проблемы охраноспособности произведений, созданных ИИ?
5.	Каков правовой статус данных, используемых для обучения моделей машинного обучения?
6.	Что такое "исходные данные для обучения" и "результатирующие данные" (модель) с правовой точки зрения?
7.	Объясните, что такое "лицензионная совместимость" (license compatibility).
8.	Какие основные типы лицензий на программное обеспечение и данные вы знаете? (например, открытые, проприетарные, копилефт).
9.	Какие правовые риски возникают при использовании открытых датасетов для коммерческого AI-проекта?
10.	Что такое "добросовестное использование" (fair use) и как оно может применяться к обучению ИИ?
11.	Какие условия должны быть соблюдены для правомерного использования произведений в качестве данных для обучения?
12.	Опишите процедуру анализа лицензионной совместимости при использовании нескольких библиотек с разными лицензиями.
13.	Каковы последствия нарушения лицензионных соглашений при использовании чужого кода или данных в AI-проекте?
14.	Может ли AI-модель быть запатентована? Какие есть ограничения?

№	Вопросы к зачету
15.	Как защищается обученная модель как ноу-хау (коммерческая тайна)?
16.	В чем разница между авторским правом и патентом применительно к алгоритмам?
17.	Какие этические вызовы связаны с использованием данных из публичных источников (например, социальных сетей) для обучения ИИ?
18.	Что такое "право на обезличенение" и как оно связано с обучением моделей?
19.	Как законодательство о базах данных (sui generis) может влиять на использование датасетов?
20.	Сформулируйте основные шаги для минимизации правовых рисков, связанных с ИС, на старте AI-проекта.
21.	Какие существуют международные инициативы по регулированию ИС в сфере ИИ (ВОИС, EU AI Act)?
22.	Проанализируйте кейс: компания использует код под лицензией GPL для создания проприетарной AI-системы. Правомерно ли это?
23.	Что такое "открытая лицензия" и в чем ее преимущества и риски для разработчика?
24.	Как лицензия Creative Commons может применяться к датасетам?
25.	Объясните, что такое "производное произведение" в контексте outputs генеративного ИИ.
26.	Какие права имеют пользователи на контент, сгенерированный для них AI-системой?
27.	Кто несет ответственность за нарушение авторских прав, если AI-модель генерирует контент, похожий на охраняемое произведение?
28.	В чем специфика правового регулирования больших данных (Big Data) как объекта ИС?
29.	Что такое "Data Governance" и как оно связано с управлением ИС в компании?
30.	Подготовьте краткий чек-лист для проверки легальности использования данных и ПО в AI-проекте.
31.	Дайте определение персональным данным (ПД) согласно законодательству (например, GDPR/ФЗ-152).
32.	Назовите и охарактеризуйте принципы обработки персональных данных.
33.	Кто является оператором, обработчиком и субъектом персональных данных в контексте AI-системы?
34.	Какие правовые основания для обработки ПД вы знаете? Какие из них наиболее применимы для ИИ?
35.	Что такое "картирование данных" (data mapping) и какова его цель?
36.	Опишите структуру и содержание "легальной основы" (legal basis) для обработки ПД.
37.	Какие специальные категории персональных данных запрещены к обработке? Существуют ли исключения для ИИ?
38.	Что такое "профилирование" в контексте ИИ и какие правовые требования к нему предъявляются?
39.	Каковы права субъектов ПД при их обработке с помощью ИИ (право на доступ, объяснение, исправление, забвение)?
40.	В чем заключаются особенности ответственности за решения, принятые AI-системой?
41.	Объясните разницу между "продуктовой" и "деликтной" (внедоговорной) ответственностью в контексте ИИ.
42.	Кто несет ответственность за вред, причиненный автономной AI-системой: разработчик, владелец, пользователь?
43.	Что такое "презумпция виновности оператора" в некоторых случаях утечки ПД?
44.	Какие технические и организационные меры защиты ПД должны быть реализованы в AI-проекте?
45.	Что такое "Privacy by Design" и "Privacy by Default"? Как эти принципы

№	Вопросы к зачету
	интегрируются в жизненный цикл AI-системы?
46.	Какие требования к трансграничной передаче ПД вы знаете?
47.	Опишите процесс проведения оценки воздействия на защиту данных (DPIA / Data Protection Impact Assessment).
48.	В каких случаях использование AI-системы обязательно требует проведения DPIA?
49.	Что такое "анонимизация" и "псевдонимизация" данных? Как они помогают снизить риски?
50.	Каковы потенциальные риски для приватности при использовании генеративных моделей?
51.	Как законодательство о защите ПД регулирует использование биометрических данных в ИИ?
52.	Проанализируйте кейс: банк отказывает в кредите на основе скоринговой AI-модели. Какие требования к прозрачности и объяснимости должны быть выполнены?
53.	Что такое "объяснимый ИИ" (XAI) и как он связан с правовыми требованиями?
54.	Какие существуют модели распределения ответственности за ИИ в мире (например, строгая ответственность, страхование)?
55.	Как доказать, что вред был причинен именно дефектом AI-модели, а не действиями пользователя?
56.	Каковы обязанности оператора при утечке данных, ставшей известной в ходе обучения модели?
57.	Что такое "функциональное назначение" модели и как оно влияет на оценку рисков для приватности?
58.	Как осуществляется надзор за соблюдением законодательства о защите ПД (роль регуляторов)?
59.	Составьте примерный перечень сведений, которые должны быть отражены в карте данных для AI-проекта.
60.	Какие этические дилеммы возникают на стыке приватности и развития ИИ?
61.	Дайте определение "смещения" (bias) в алгоритмах и данных.
62.	Назовите и охарактеризуйте основные типы алгоритмических смещений (selection, confirmation, automation bias и др.).
63.	Каковы источники смещений в датасетах и моделях машинного обучения?
64.	Какие этические последствия влечет за собой наличие смещений в AI-системах?
65.	Опишите процесс проведения аудита смещения (Bias Audit).
66.	Какие метрики и методы используются для выявления и измерения смещений?
67.	Что такое "справедливость" (fairness) в машинном обучении? Назовите ее виды (например, demographic parity, equality of opportunity).
68.	Какие существуют подходы к смягчению (mitigation) смещений на разных этапах ML-цикла?
69.	Сформулируйте основные этические принципы, применяемые к ИИ (например, справедливость, прозрачность, подотчетность, ненанесение вреда).
70.	Что такое "Этический паспорт" AI-продукта и какова его структура?
71.	Дайте определение кибербезопасности AI-систем.
72.	Что такое "adversarial атаки"? Назовите их основные типы (белые/серые/черные ящики, целевые/нецелевые).
73.	Опишите механизм adversarial атаки на примере классификации изображений.
74.	Какие уязвимости AI-моделей используют adversarial атаки?
75.	Назовите и охарактеризуйте основные методы защиты от adversarial атак (обучение с подкреплением, обнаружение, сертифицированная Robustness).
76.	Что такое "конфиденциальность обучения" (Privacy-Preserving ML) и какие методы она включает (федеративное обучение, дифференциальная приватность, гомоморфное шифрование)?

№	Вопросы к зачету
77.	Как связаны безопасность модели и защита персональных данных?
78.	Что такое "модель угроз" (threat model) для AI-системы и как ее построить?
79.	Какие существуют риски, связанные с безопасностью данных в MLOps-конвейере?
80.	Как обеспечить подотчетность (accountability) и контроль за AI-системой?
81.	Что такое "интерпретируемость" (interpretability) и "объяснимость" (explainability) моделей?
82.	Каковы этические аспекты создания автономных систем, способных наносить физический вред (автономное оружие, беспилотные автомобили)?
83.	Как смещение в алгоритмах может усиливать социальное неравенство? Приведите пример.
84.	Что такое "этическая экспертиза" AI-системы и кто должен ее проводить?
85.	Каковы обязанности разработчика по обеспечению безопасности и этики AI-продукта?
86.	Проанализируйте кейс: рекрутинговая AI-система дискриминирует кандидатов по гендерному признаку. Каковы вероятные причины и способы устранения?
87.	Как adversarial атаки могут быть использованы для манипуляции поведением AI-системы в реальном мире?
88.	В чем разница между "надежностью" (reliability) и "устойчивостью" (robustness) AI-модели?
89.	Какие международные стандарты и руководства по этике ИИ вы знаете (например, от IEEE, OECD, UNESCO)?
90.	Разработайте план по внедрению принципов "Ethics by Design" в процесс разработки вашей AI-команды.
91.	Охарактеризуйте основные подходы к регулированию ИИ в мире (жесткий vs. мягкий, риск-ориентированный).
92.	Каковы ключевые положения "Закона об ИИ" Европейского Союза (EU AI Act)?
93.	Что такое "риск-ориентированный подход" (risk-based approach) в EU AI Act? Назовите уровни риска.
94.	Какие практики и системы ИИ запрещены согласно EU AI Act?
95.	Какие требования предъявляются к системам "высокого риска" (high-risk AI systems)?
96.	Опишите обязанности поставщиков и пользователей (deployers) систем высокого риска.
97.	Каков правовой статус "генеративных моделей" (general-purpose AI models) и "генеративных ИИ-систем" в EU AI Act?
98.	Какие требования к прозрачности установлены для генеративного ИИ?
99.	Сравните регулирование ИИ в ЕС, США и Китае. В чем основные различия в подходах?
100.	Каковы основные положения Национальной стратегии развития ИИ в вашей стране (если применимо)?
101.	Какие этические вопросы возникают при использовании генеративного ИИ в креативных индустриях и медиа?
102.	Кто должен нести ответственность за распространение дезинформации, созданной генеративным ИИ?
103.	Что такое "глубокие подделки" (deepfakes) и как они регулируются?
104.	Каковы проблемы с установлением авторства и оригинальности контента, созданного генеративным ИИ?
105.	Как генеративный ИИ влияет на рынок труда и каковы этические последствия этого влияния?
106.	Что такое "правосубъектность" (legal personality) ИИ? Существуют ли предложения по ее признанию?
107.	Может ли AI-агент быть стороной договора? Проанализируйте возможные модели.

№	Вопросы к зачету
108.	Какие существуют проблемы с использованием ИИ в судебной системе и государственном управлении?
109.	Как регулируются системы социального скоринга в разных странах?
110.	Что такое "песочницы регулятивных норм" (regulatory sandboxes) для тестирования ИИ?
111.	Опишите процедуру проведения экспертизы AI-системы на соответствие критериям EU AI Act.
112.	Какие документы и доказательства необходимо подготовить для вывода системы высокого риска на рынок ЕС?
113.	Каковы потенциальные риски использования ИИ в медицине и здравоохранении с точки зрения регулирования?
114.	Как законодательство о защите прав потребителей применяется к продуктам с ИИ?
115.	Каковы этические и правовые аспекты создания "цифровых бессмертных" личностей на основе ИИ?
116.	Проанализируйте кейс: новостное издание использует генеративный ИИ для написания статей. Какие риски и как должны быть минимизированы?
117.	Какие требования к маркировке (labeling) AI-генерируемого контента вводятся в разных странах?
118.	Как международное право регулирует применение автономных систем в военных целях?
119.	Каковы глобальные вызовы, связанные с согласованием регулирования ИИ между странами?
120.	Подготовьте презентацию для руководства компании о ключевых изменениях, которые повлечет за собой вступление в силу EU AI Act для вашего AI-продукта.
121.	Что такое MLOps и как он связан с управлением правовыми и этическими рисками?
122.	Опишите жизненный цикл разработки AI-продукта (от идеи до вывода на рынок и мониторинга).
123.	На каких этапах жизненного цикла необходимо внедрять проверки на соблюдение правовых и этических норм?
124.	Что такое "Ответственный ИИ" (Responsible AI) как сквозная практика?
125.	Какие роли и зоны ответственности за внедрение Ответственного ИИ должны быть в команде (Data Scientist, ML Engineer, Юрист, Менеджер по продукту)?
126.	Опишите структуру и содержание раздела "Правовые и этические риски" в техническом задании (ТЗ) на AI-продукт.
127.	Какие ключевые риски должны быть отражены в таком разделе (ИС, данные, приватность, смещения, безопасность, регулирование)?
128.	Как интегрировать оценку соответствия EU AI Act в процесс разработки?
129.	Что такое "Этический паспорт" (Ethics Card, Model Card) AI-продукта и каково его практическое применение?
130.	Из каких основных разделов состоит "Этический паспорт"?
131.	Какая информация о данных (прозрачность датасета) должна быть включена в паспорт?
132.	Как отразить в паспорте информацию о тестировании на смещения и ограничениях модели?
133.	Каковы лучшие практики по документированию процесса принятия решений моделью?
134.	Как организовать процесс регулярного аудита и мониторинга развернутой модели на предмет новых рисков?
135.	Что такое "управление моделью" (Model Governance) и какие процессы оно включает?
136.	Как обеспечить воспроизводимость (reproducibility) и прослеживаемость

№	Вопросы к зачету
	(traceability) экспериментов и решений модели?
137.	Какие инструменты и платформы могут помочь во внедрении практик Ответственного ИИ в MLOps?
138.	Разработайте чек-лист для "воротеста" (gate review) перед выводом AI-модели в продакшен.
139.	Как коммуницировать правовые и этические ограничения модели конечным пользователям и стейкхолдерам?
140.	Опишите процесс создания "сквозного примера" (end-to-end example) для воркшопа по Ответственному ИИ.
141.	Какие сценарии чаще всего разбирают на таких воркшопах?
142.	Какова роль "красных команд" (Red Teaming) в оценке безопасности и этики AI-систем?
143.	Что такое "канарейки" (canaries) в контексте мониторинга моделей на предмет смещений и дрейфа?
144.	Как планировать обновления модели с учетом изменений в законодательстве (например, вступление в силу нового закона)?
145.	Какие метрики "второго порядка" (качество данных, справедливость, объяснимость) нужно отслеживать в продакшене?
146.	Проанализируйте кейс: при обновлении модели ее результаты стали дискриминационными. Опишите план действий.
147.	Как интегрировать оценку воздействия на приватность (DPIA) в процесс разработки?
148.	Каковы обязанности Product Manager'a по управлению правовыми и этическими рисками продукта?
149.	Подготовьте шаблон для краткого "Этического паспорта" для внутреннего использования в вашей команде.
150.	Предложите дорожную карту (roadmap) по внедрению фреймворка Ответственного ИИ в стартапе из 10 человек.

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
7	Зачет с оценкой	«отлично»	рейтинговый балл 85-100
		«хорошо»	рейтинговый балл 70-84
		«удовлетворительно»	рейтинговый балл 55-69
		«неудовлетворительно»	рейтинговый балл 0-54

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1.	Е. С. Митяков, А. Г. Шмелева, А. И. Ладынин	Искусственный интеллект и машинное обучение : учебное пособие для вузов / Е. С. Митяков, А. Г. Шмелева, А. И. Ладынин. — 2-е изд., стер. — Санкт-Петербург : Лань, 2026. — 252 с. — ISBN 978-5-507-51198-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/507451 (дата обращения: 30.11.2025). — Режим доступа: для авториз. пользователей.	учебное пособие для вузов	2026	ЭБС Лань
2.	А. Н. Баланов	Машинное обучение и искусственный интеллект : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 172 с. — ISBN 978-5-507-52891-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/462248 (дата обращения: 30.11.2025). — Режим доступа: для авториз. пользователей.	учебное пособие для вузов	2025	ЭБС Лань
3.	А. А. Тюгашев	Компьютерные средства искусственного интеллекта : учебное пособие / А. А. Тюгашев. — Самара : Самарский государственный технический университет, ЭБС АСВ, 2020. — 270 с. — ISBN 978-5-7964-2293-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/105021.html (дата обращения: 30.11.2025). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/105021	учебное пособие	2020	ЭБС IPRbooks
4.	А. О. Подкопаев	Системы искусственного интеллекта и машинное обучение : учебное пособие / А. О. Подкопаев. — Новосибирск : Новосибирский государственный технический университет, 2024. — 66 с. — ISBN 978-5-7782-5163-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL:	учебное пособие	2024	ЭБС IPRbooks

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
		https://www.iprbookshop.ru/155681.html (дата обращения: 30.11.2025). — Режим доступа: для авторизир. пользователей			
5.	М. В. Захарова, С. Н. Гриняев, Т. В. Исаева [и др.]	Международная безопасность в эпоху искусственного интеллекта. Том 1 : учебник для вузов / М. В. Захарова, С. Н. Гриняев, Т. В. Исаева [и др.] ; под ред. М. В. Захаровой, А. И. Смирнова. - Москва : Издательство «Аспект Пресс», 2024. - 401 с. - ISBN 978-5-7567-1319-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2188451 (дата обращения: 30.11.2025). – Режим доступа: по подписке.	учебник для вузов	2024	ЭБС znanium.com
6.	А.В. Андрейчиков, О.Н. Андрейчикова	Интеллектуальные информационные системы и методы искусственного интеллекта : учебник / А.В. Андрейчиков, О.Н. Андрейчикова. — Москва : ИНФРА-М, 2025. — 530 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI 10.12737/1009595. - ISBN 978-5-16-020880-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2194412 (дата обращения: 30.11.2025). – Режим доступа: по подписке.	учебник	2025	ЭБС znanium.com

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1.	Золкин А. Л., Мунистер В. Д., Подолько П. М.	Машинное обучение и искусственный интеллект в медицине. Алгоритмы, приложения и перспективы» (Золкин, А. Л. Машинное обучение и искусственный интеллект в медицине. Алгоритмы, приложения и перспективы : учебник для вузов / А. Л. Золкин, В. Д.	учебник для вузов	2025	ЭБС Лань

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
		Мунистер, П. М. Подолько. — Санкт-Петербург : Лань, 2025. — ISBN 978-5-507-53095-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/505459 (дата обращения: 30.11.2025). — Режим доступа: для авториз. пользователей.			
2.	Д. А. Баяк, А. В. Попова	Правовые и этические проблемы искусственного интеллекта : учебник для магистратуры / Д. А. Баяк, А. В. Попова. — Москва : Прометей, 2022. — 300 с. — ISBN 978-5-00172-253-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/125621.html (дата обращения: 30.11.2025). — Режим доступа: для авторизир. пользователей	учебник для магистратуры	2022	ЭБС IPRbooks
3.	Т. Дейвенпорт	Внедрение искусственного интеллекта в бизнес-практику: Преимущества и сложности : практическое руководство / Т. Дейвенпорт. - Москва : Альпина Паблишер, 2026. - 320 с. - ISBN 978-5-9614-3952-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2235397 (дата обращения: 30.11.2025). – Режим доступа: по подписке.	практическое руководство	2026	ЭБС znanium.com
4.	С.О. Крамаров, О.Р. Попов, Л.В. Сахарова	Использование искусственного интеллекта в образовательном процессе / С.О. Крамаров, О.Р. Попов, Л.В. Сахарова: учебно-методическое пособие. — Москва : РИОР, ИНФРА-М, 2026. — 106 с. — (Наука и практика). — DOI: https://doi.org/10.29039/02169-9 . - ISBN 978-5-369-01995-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2218762 (дата обращения: 30.11.2025). – Режим доступа: по подписке.	учебно-методическое пособие	2026	ЭБС znanium.com
5.	Мишра, П.	Объяснимые модели искусственного интеллекта на Python. Модель искусственного интеллекта. Объяснения с использованием библиотек, расширений и фреймворков на основе языка Python : практическое руководство / П. Мишра ; пер. с англ. С. В. Минца. -	практическое руководство	2022	ЭБС znanium.com

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
		Москва : ДМК Пресс, 2022. - 298 с. - ISBN 978-5-93700-124-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/2109490 (дата обращения: 30.11.2025). – Режим доступа: по подписке.			

8.3. Перечень профессиональных баз данных и информационных справочных систем

№ пп	Наименование	Ссылка
1	Springer Nature (Полнотекстовая коллекция журналов)	https://www.springernature.com/gp/products
2	Springer eBooks (Полнотекстовая коллекция электронных книг издательства Springer Nature)	https://link.springer.com/
3	«Кодекс»	https://kodeks.ru/
4	ELIBRARY.RU (электронная библиотека научных публикаций)	http://elibrary.ru
5	"Гарант"	https://www.garant.ru/
6	"КонсультантПлюс"	https://www.consultant.ru/
7	Техэксперт	https://cntd.ru/

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	WinPro 10 RUS Upgrd OLP NL Acdmc	Договор № 757 от 04.07.2018, срок действия - бессрочно; Контракт № 1653 от 14.12.2018, срок действия – бессрочно
2	Office Stdandard 2013 Russian OLP NL AcademicEdition	Контракт № 690 от 19.05.2015, срок действия - бессрочно)
3	Python 3.11	Free Software
4	Visual Studio Code 1.75	Free Software
5	Django 1.11.29	Free Software

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Компьютерный класс. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для проведения лабораторных работ. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. (УЛК-407)	Компьютер (монитор Samsung Sync Master 943n 19", системный блок Intel (R) Core 2 Quad 2,40 GHz 1 Gb), столы лабораторные, стулья, доска 3-х секционная (меловая), стол преподавательский.
2	Помещение для самостоятельной работы обучающихся (УЛК-105)	Стол, стулья, стеллажи (в т.ч. выставочные) с книгами, компьютеры,

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
		мобильные рабочие места.
3	Помещение для самостоятельной работы обучающихся (УЛК-406)	Столы компьютерные, стулья, микрокомпьютеры raspberry pi 32 bit