Лебедева Екатерина Александровна
Подписано цифровой подписью: Лебедева Екатерина Александровна
Дата: 2026.06.25 15:58:45 +03'00'

Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДЭ.04.01 Регуляторика и комплаенс высокорисковых ИИ-систем

(индекс, наименование дисциплины в соответствии с учебным планом)

40.04.01 "Юриспруденция"
(Специализированное высшее образование в сфере Юридического консалтинга)
(код, наименование направления подготовки)

Правовое обеспечение использования искусственного интеллекта
(наименование образовательной программы)

Очная форма обучения
(форма обучения)

Год набора – 2026
Нижний Новгород, 2026 г.

Автор(ы)-составитель(и) РПД:

Калинина Евгения Валерьевна, доктор юридических наук, доцент, заведующая кафедрой гражданского и международного права

Заведующий кафедрой:

Калинина Евгения Валерьевна, доктор юридических наук, доцент, заведующая кафедрой гражданского и международного права

Рабочая программа дисциплины Б1.В.ДЭ.04.01 «Регуляторика и комплаенс высокорисковых ИИ-систем» одобрена на заседании кафедры гражданского и международного права

протокол № 6 от «4» марта 2026 г

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы
2. Объем и место дисциплины в структуре образовательной программы
3. Содержание и структура дисциплины
4. Типы оценочных материалов, показатели, критерии, шкалы оценивания
5. Формы аттестации и типовые оценочные материалы для текущего контроля успеваемости обучающихся
6. Формы промежуточной аттестации по дисциплине, типы оценочных материалов, показатели, критерии, шкалы оценивания
7. Методические материалы по освоению дисциплины
8. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет»
9. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Дисциплина Б1.В.ДЭ.04.01 «Регуляторика и комплаенс высокорисковых ИИ-систем» обеспечивает формирование у обучающихся следующих профессиональных компетенций:

ОТФ/ТФ и реквизиты ПС *(при наличии)*	**Код компетенции**	**Наименование компетенции**	**Код индикатора достижения компетенций**	**Наименование индикатора достижения компетенций**	**Образовательный результат**
	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**ИУК-1.2**	Выявляет и оценивает комплексные технологические и правовые риски в проектах с использованием искусственного интеллекта.	**ИУК-1.2 З-1 (High-Risk AI).** Знает: методологии идентификации и оценки рисков (risk assessment) применительно к высокорисковым ИИ-системам; критерии отнесения ИИ-систем к категории высокорисковых в различных правопорядках (EU AI Act, подходы РФ); типовые сценарии реализации рисков (алгоритмическая предвзятость, сбои, нарушение фундаментальных прав). **ИУК-1.2 У-1 (High-Risk AI).** Умеет: проводить системную декомпозицию высокорискового ИИ-проекта для выявления «узких мест» с точки зрения регуляторики; ранжировать выявленные риски по вероятности и потенциальному ущербу для целей построения системы комплаенс.
ОТФ-D/7: Правовое сопровождение и консультирование в сфере разработки и внедрения технологий искусственного интеллекта ТФ D/02.7 Обеспечение аналитического и консультационного сопровожде	**ПКс-ИИ-1** (проф. спец.)	Способен анализировать правовые риски и разрабатывать юридические модели внедрения и эксплуатации систем искусственного интеллекта (ИИ) в бизнес-процессы организации	**ИПКс-ИИ-1.2**	Проводит сравнительный анализ регуляторных требований к ИИ в разных юрисдикциях (EU AI Act, US подход, Китай) и разрабатывает стратегию глобального комплаенса для транснациональных ИИ-проектов.	**ИПКс-ИИ-1.2 З-1 (High-Risk AI).** ***Знает:*** ключевые положения основных зарубежных регуляторных актов в сфере высокорискового ИИ (классификация, требования к системам, обязанности поставщиков и пользователей); методологию построения глобальных карт соответствия (global compliance mapping) для мультиюрисдикционных проектов. **ПКс-ИИ-1.2 У-1 (High-Risk AI).** ***Умеет:*** выявлять коллизии и дополнительные требования разных правовых систем при выводе высокорискового ИИ-продукта на международные рынки; формулировать рекомендации по адаптации архитектуры ИИ-системы и

ния мероприятий по введению в оборот прав на РИД и СИ ТФ С/02.7 Информационное и аналитическое сопровождение мероприятий по защите прав на ИС, в том числе за рубежом (40.001 Специалист по патентоведению утв. приказом Министерства труда и социальной защиты РФ от 21.10.2021 № 748н)					потоков данных для минимизации регуляторных барьеров.
ОТФ С/7 Правовое обеспечение охраны и защиты прав на РИД и СИ ТФ С/01.7 Правовое обеспечение охраны, осуществления прав на РИД и СИ, а также распоряжения этими правами и их защиты ТФ С/02.7 Информационное и аналитическое сопровождение мероприятий по защите	**ПКс-ИИ-3** (проф. спец.)	Способен представлять интересы клиентов в спорах, связанных с причинением вреда решениями ИИ, защитой интеллектуальных прав на AI-модели и данные, а также в административных процедурах, связанных с регулированием инновационных технологий	**ИПКс-ИИ-3.2**	Разрабатывает и реализует правовую стратегию защиты интересов клиента при расследовании инцидентов, связанных с ИИ (утечка данных, дискриминационные решения, причинение вреда), включая взаимодействие с органами власти и подготовку структурированных документов, определяющих шаги по устранению причин выявленных несоответствий, ошибок или жалоб.	**ИПКс-ИИ-3.2 З-1 (High-Risk AI).** ***Знает:*** административные процедуры и полномочия регуляторов (Роскомнадзор, ФСТЭК, ФАС, Банк России, уполномоченные органы в сфере ИИ) при расследовании инцидентов с высокорисковыми ИИ-системами; требования к планам корректирующих мероприятий и отчетности по комплаенсу. **ИПКс-ИИ-3.2 У-1 (High-Risk AI).** ***Умеет:*** разрабатывать внутренние документы (политики, регламенты, карты рисков), обеспечивающие соответствие деятельности клиента регуляторным требованиям к высокорисковому ИИ; выстраивать коммуникацию с регуляторами и готовить структурированные ответы на запросы и предписания, связанные с расследованием инцидентов в высокорисковых сферах.

прав на ИС, в том числе за рубежом (40.001 Специалист по патентоведению утв. приказом Министерства труда и социальной защиты РФ от 21.10.2021 № 748н)					

2. Объем и место дисциплины (модуля) в структуре образовательной программы

Общая трудоемкость дисциплины составляет 72 а.ч. (2 з.е.)
Количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся: 4 сем. - лекции – 12 а.ч., практические занятия – 12 а.ч., самостоятельная работа – 44 а.ч., контактная работа на аттестацию в период экзаменационных сессий – 4 часа.

Дисциплина *«Регуляторика и комплаенс высокорисковых ИИ-систем»* относится к дисциплинам части, формируемой участниками образовательных отношений (элективные дисциплины ДЭ.04). Изучается на очной форме обучения - на 2 курсе.

Для освоения дисциплины «*Регуляторика и комплаенс высокорисковых ИИ-систем»* обучающиеся используют знания, умения, навыки, способы деятельности и установки, сформированные в ходе изучения дисциплины *«Информационное право», «Информационные технологии в юридической деятельности»*.

Форма промежуточной аттестации в соответствии с учебным планом:
Очная форма обучения – зачет.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Очная форма обучения

№ п/п	Наименование тем и (или) разделов	ВСЕГО	Объем дисциплины, ак.час											Форма текущего контроля успеваемости, промежуточной аттестации
			Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа		
			Период теоретического обучения						Период промежуточной аттестации (сессия)					
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Кат тэк	Контроль	СРкр	СРэк	СР
			Л	ВЛ	ЛР	ПЗ								
Тема 1.	Введение в регуляторику ИИ. Риск-ориентированный подход	11	2	0	0	2	0	0	0	0		0	0	7	Устный опрос, Ситуационная задача
Тема 2.	Система комплаенс высокорисковых ИИ-систем	12	2	0	0	2	0	0	0	0		0	0	8	Устный опрос, Ситуационная задача
Тема 3.	Управление данными и	11	2	0	0	2	0	0	0	0		0	0	7	Устный опрос, Ситуационная

	техническая документация													задача
Тема 4.	Этический комплаенс: прозрачность, недискриминация и справедливость	11	2	0	0	2	0	0	0	0	0	0	7	Устный опрос, Ситуационная задача
Тема 5.	Комплаенс на всем жизненном цикле: мониторинг, инциденты и надзор	11	2	0	0	2	0	0	0	0	0	0	7	Устный опрос, Ситуационная задача
Тема 6.	Трансграничный комплаенс и управление рисками третьих сторон	12	2	0	0	2	0	0	0	0	0	0	8	Устный опрос, Ситуационная задача
Промежуточная аттестация		4								4				Зачет
Итого		72	12	0	0	12	0	0	0	4	0	0	44	

Используемые сокращения:

Л – лекции - занятия, предусматривающие преимущественную передачу учебной информации обучающимся педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях,).

ВЛ – видео лекции.

ЛР – лабораторные работы.

ПЗ – практические занятия (за исключением лабораторных работ).

ИК – индивидуальные консультации.

КСР – контроль самостоятельной работы

КЭ – консультации перед экзаменом

Каттэк – контактная работа на аттестацию в период экзаменационных сессий

СРкр – самостоятельная работа на подготовку курсовой работы/ курсового проекта.

СРэк – самостоятельная работа на подготовку к экзамену.СР – самостоятельная работа в семестре на подготовку к учебным занятиям.

3.2 Содержание дисциплины

Тема 1. Введение в регуляторику ИИ. Риск-ориентированный подход. УК-1.1

Обзор нормативного ландшафта: анализ ключевых мировых и национальных стратегий регулирования ИИ (ЕС AI Act, документы ОЭСР, российское законодательство в сфере ИИ).

Сущность риск-ориентированного подхода: классификация систем ИИ по уровням риска (неприемлемый, высокий, ограниченный, минимальный) и определение критериев отнесения к высокорисковым системам.

Правовые последствия классификации: описание требований, запретов и санкций, применяемых к системам в зависимости от присвоенной категории риска.

Зоны ответственности участников оборота: разграничение ролей и обязательств провайдеров (разработчиков) и пользователей (имплементаторов) высокорисковых ИИ-систем.

Тема 2. Система комплаенс высокорисковых ИИ-систем. ПКс-ИИ-1.1

Формирование политики комплаенса: разработка внутренних регламентов, кодексов этики ИИ и стандартов организации, соответствующих применимому праву.

Организационная структура и роли: создание органов управления (комитеты по этике ИИ), назначение ответственных лиц и распределение полномочий в области контроля за ИИ.

Процедуры должной осмотрительности: внедрение скрининговых процедур для проверки новых разработок и партнеров на соответствие регуляторным требованиям до вывода системы на рынок.

Внутренний контроль и аудит: разработка механизмов периодической проверки соответствия (комплаенс-аудиты), включая проверку документации, процессов и эффективности применяемых мер.

Тема 3. Управление данными и техническая документация. ПКс-ИИ-3.1

Требования к качеству данных: установление критериев репрезентативности, полноты и актуальности обучающих, валидационных и тестовых наборов данных для предотвращения ошибок модели.

Управление жизненным циклом данных: регламентация процессов сбора, очистки, маркировки, хранения и обновления данных с соблюдением конфиденциальности и защиты персональных данных.

Состав и ведение технической документации: формирование исчерпывающего пакета документов, описывающего архитектуру системы, методы разработки, логику работы и результаты тестирования (требование прослеживаемости).

Автоматизация документирования: использование инструментов для ведения логов и версионирования как моделей, так и данных для обеспечения воспроизводимости результатов и доказательной базы для регуляторов.

Тема 4. Этический комплаенс: прозрачность, недискриминация и справедливость. ПКс-ИИ-3.1

Обеспечение прозрачности и информирования: разработка политик раскрытия информации о взаимодействии с ИИ-системой (объяснимость результатов) и понятных пользовательских соглашений.

Выявление и смягчение алгоритмической предвзятости: применение методов тестирования моделей на наличие дискриминационных факторов по признакам пола, расы, возраста и другим защищенным категориям.

Принципы справедливости и равноправия: интеграция метрик справедливости (fairness metrics) в процесс разработки и валидации модели для обеспечения равного качества сервиса для всех групп пользователей.

Механизмы человеческого контроля: реализация возможности human-in-the-loop (участие человека в принятии решений) для критически важных сценариев и процедура пересмотра решений, вынесенных ИИ.

Тема 5. Комплаенс на всем жизненном цикле: мониторинг, инциденты и надзор. ПКс-ИИ-3.1, УК-1.1

Пострегистрационный мониторинг: организация системы непрерывного наблюдения за работой ИИ-системы в реальных условиях для выявления отклонений в производительности и точности.

Управление инцидентами: создание протоколов выявления, классификации, расследования и устранения инцидентов (сбои, ошибки, неэтичное поведение), связанных с работой ИИ.

Взаимодействие с надзорными органами: определение порядка уведомления регуляторов о серьезных инцидентах и предоставления отчетности по запросу.

Адаптивное обновление системы: разработка регламента внесения изменений в модель (дообучение, смена версии) с обязательной повторной оценкой соответствия требованиям безопасности и эффективности.

Тема 6. Трансграничный комплаенс и управление рисками третьих сторон. ПКс-ИИ-1.1 + ПКс-ИИ-3.1

Анализ юрисдикционных требований: сопоставление законодательства стран присутствия (например, экстерриториальное действие GDPR и EU AI Act) и выявление коллизий норм.

Управление цепочкой поставок ИИ: проведение due diligence в отношении поставщиков технологий, облачных провайдеров и вендоров, предоставляющих готовые ИИ-решения или данные.

Контрактное распределение рисков: включение в договоры с третьими сторонами положений об ответственности за соответствие продукции, аудиторских правах и гарантиях качества используемых компонентов.

Локализация vs. унификация: поиск баланса между требованиями локализации данных в отдельных странах и необходимостью унификации комплаенс-процедур глобальной компании.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.В.ДЭ.04.01 «Регуляторика и комплаенс высокорисковых ИИ-систем» входят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляют фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с целью оценивания достижения обучающимися планируемых результатов обучения.

4.2. ФОС разработан как комплекс проверочных заданий различного типа и уровня сложности, включает критерии и шкалы оценивания, а также «ключи» правильных ответов. ФОС формируется как отдельный документ и хранится в электронном виде, доступ к ФОС предоставлен ограниченному кругу лиц.

4.3. Для самостоятельной работы обучающихся при подготовке к текущему контролю успеваемости и промежуточной аттестации в рабочих программах дисциплин размещены типовые проверочные задания, которые можно условно разделить на задания закрытого, комбинированного и открытого типов.

Задания закрытого типа — это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или

несколько правильных.

Задания комбинированного типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных и обосновать свой выбор.

Задания открытого типа — это задания, в которых на каждый вопрос должен быть предложен развернутый обоснованный ответ.

В зависимости от типа задания рекомендованы определенная последовательность выполнения и система оценивания выполнения заданий.

4.4. Типы заданий, сценарии выполнения, критерии оценивания

ТИП ЗАДАНИЯ	ИНСТРУКЦИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	КРИТЕРИИ ОЦЕНИВАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	Прочитайте текст, выберите правильный ответ	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	Ответ считается верным, если правильно указана цифра или буква
Задание закрытого типа на установление соответствия	Прочитайте текст и установите соответствие	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).	Ответ считается верным, если правильно указаны цифры или буквы
Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных	Прочитайте текст, выберите правильные ответы	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать несколько правильных ответов. 4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г).	Ответ считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)
Задание закрытого типа на установление последовательности	Прочитайте текст и установите последовательность	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов. 2. Внимательно прочитать предложенные варианты ответа. 3. Построить верную последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).	Ответ считается верным, если правильно указана вся последовательность цифр
Задание комбинированного типа с	Прочитайте текст, выберите правильный	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных	Ответ считается верным, если правильно указана цифра или буква

выбором одного правильного ответа из предложенных и обоснованием выбора	ответ и запишите аргументы, обосновывающие выбор ответа	вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	и приведены корректные аргументы, используемые при выборе ответа
Задание открытого типа с развернутым ответом	Прочитайте текст и запишите развернутый обоснованный ответ	1. Внимательно прочитать текст задания и понять суть вопроса. 2.Продумать логику и полноту ответа. 3.Записать ответ, используя четкие компактные формулировки. 4.В случае расчетной задачи, записать решение и ответ	Ответ считается верным: 1. Отсутствие фактических ошибок. 2. Раскрытие объема используемых понятий (полнота ответа). 3.Обоснованность ответа (наличие аргументов). 4. Логическая последовательность излагаемого материала.

4.5. Общая шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся с применением БРС

Итоговая балльная оценка	**Традиционная система**	**Бинарная система**	**ECTS**	
			Для традиционной системы	**Для бинарной системы**
95-100	Отлично	Зачтено	A	P/ Passed
85-94			B	P/ Passed
75-84	Хорошо		C	P/ Passed
65-74			D	P/ Passed
55-64	Удовлетворительно		E	P/ Passed
0-54	Неудовлетворительно	Не зачтено	F	F/Failed

Соотношение баллов за текущий контроль успеваемости и промежуточную аттестацию, а также повторную промежуточную аттестацию:

Максимальная сумма баллов за текущий контроль успеваемости	Максимальная сумма баллов за промежуточную аттестацию	Максимальная итоговая балльная оценка	Максимальная сумма баллов за повторную промежуточную аттестацию
60 баллов	40 баллов	100 баллов	100 баллов

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

5.1. В ходе реализации дисциплины Б1.В.ДЭ.04.01 «Регуляторика и комплаенс высокорисковых ИИ-систем» используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

Устный опрос, ситуационная задача, тестирование.

5.2. Типовые оценочные материалы для текущего контроля успеваемости обучающихся (вне контрольных точек):

Тема 1. Введение в регуляторику ИИ. Риск-ориентированный подход. УК-1.1

Подготовка к практическому занятию:

- внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;
- подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;
- понять, что осталось неясными и постараться получить на них ответ заранее;
- готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Обзор нормативного ландшафта: анализ ключевых мировых и национальных стратегий регулирования ИИ (ЕС AI Act, документы ОЭСР, российское законодательство в сфере ИИ).
2. Сущность риск-ориентированного подхода: классификация систем ИИ по уровням риска (неприемлемый, высокий, ограниченный, минимальный) и определение критериев отнесения к высокорисковым системам.
3. Правовые последствия классификации: описание требований, запретов и санкций, применяемых к системам в зависимости от присвоенной категории риска.
4. Зоны ответственности участников оборота: разграничение ролей и обязательств провайдеров (разработчиков) и пользователей (имплементаторов) высокорисковых ИИ-систем.

Ситуационные задачи

Задача 1. Классификация системы «Психологический профайлинг»

Ситуация: Российский стартап разработал ИИ-систему для HR-департаментов. Система анализирует видео с собеседований (мимика, тембр голоса, выбор слов) и выдает заключение о психологическом типе кандидата, его склонности к конфликтам и прогнозируемой лояльности. Система также оценивает "честность" ответов (детектор лжи). Стартап планирует продавать решение в Европу.

Задание: *Используя риск-ориентированный подход EU AI Act, проведите анализ системы как целостной проблемной ситуации. К какому классу риска относится система? Подпадает ли она под запрещенные практики? Какие требования к ней будут применяться?*

Задача 2. Применимость российского и европейского права

Ситуация: Банк (головной офис в Москве) использует ИИ-систему для кредитного скоринга. Система обучена на данных российских заемщиков. Банк открывает отделение в Казахстане и планирует использовать ту же систему для скоринга граждан Казахстана. В России система работает в рамках Экспериментального правового режима (ЭПР) и не подпадает под все требования общего регулирования.

Задание: *Проанализируйте регуляторную ситуацию как систему. Какие нормы (российские, казахстанские, ЕС) и в какой комбинации будут применимы к деятельности банка в Казахстане? Будет ли иметь значение, что серверы с данными остаются в Москве?*

Тема 2. Система комплаенс высокорисковых ИИ-систем. ПКс-ИИ-1.1

Подготовка к практическому занятию:

- внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;
- подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;
- понять, что осталось неясными и постараться получить на них ответ заранее;
- готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Формирование политики комплаенса: разработка внутренних регламентов, кодексов этики ИИ и стандартов организации, соответствующих применимому праву.
2. Организационная структура и роли: создание органов управления (комитеты по этике ИИ), назначение ответственных лиц и распределение полномочий в области контроля за ИИ.
3. Процедуры должной осмотрительности: внедрение скрининговых процедур для проверки новых разработок и партнеров на соответствие регуляторным требованиям до вывода системы на рынок.
4. Внутренний контроль и аудит: разработка механизмов периодической проверки соответствия (комплаенс-аудиты), включая проверку документации, процессов и эффективности применяемых мер.

Ситуационные задачи.

Задача 1. Разработка Политики для медицинского учреждения

Ситуация: Сеть частных клиник "Здоровье+" начинает внедрение ИИ-системы для анализа рентгеновских снимков (флюорография, маммография). Система помогает рентгенологу расставлять метки "подозрительные области" и приоритезировать очередь снимков. Главный врач поручил комплаенс-менеджеру разработать Политику использования ИИ в клинической практике.

Задание: *Разработайте структуру и ключевые положения Политики (ПКс-ИИ-1.1). Какие разделы обязательно должны быть включены? Определите зоны ответственности ключевых сотрудников.*

Задача 2. Процедура валидации модели перед внедрением

Ситуация: Финансовая компания "Кредит-Капитал" закупила ИИ-модель для оценки кредитоспособности малого бизнеса. Модель разработана сторонним вендором. Перед запуском в промышленную эксплуатацию необходимо провести ее валидацию и утвердить процедуру ввода в эксплуатацию.

Задание: *Опишите процедуру (алгоритм действий), которую компания должна закрепить в своем регламенте для проверки и запуска высокорисковой ИИ-системы, приобретенной у стороннего поставщика (ПКс-ИИ-1.1).*

Тема 3. Управление данными и техническая документация. ПКс-ИИ-3.1

Подготовка к практическому занятию:

– внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;

– подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;

– понять, что осталось неясными и постараться получить на них ответ заранее;

– готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Требования к качеству данных: установление критериев репрезентативности, полноты и актуальности обучающих, валидационных и тестовых наборов данных для предотвращения ошибок модели.

2. Управление жизненным циклом данных: регламентация процессов сбора, очистки, маркировки, хранения и обновления данных с соблюдением конфиденциальности и защиты персональных данных.

3. Состав и ведение технической документации: формирование исчерпывающего пакета документов, описывающего архитектуру системы, методы разработки, логику работы и результаты тестирования (требование прослеживаемости).

4. Автоматизация документирования: использование инструментов для ведения логов и версионирования как моделей, так и данных для обеспечения воспроизводимости результатов и доказательной базы для регуляторов.

Ситуационные задачи.

Задача 1. Аудит датасета на предмет репрезентативности

Ситуация: Разрабатывается ИИ-система для автоматического отбора резюме в крупной IT-компании. Датасет для обучения состоял из 100 000 резюме, поданных за последние 3 года. Анализ показал: 80% успешных кандидатов в датасете — мужчины, 70% — выпускники топ-5 московских вузов, средний возраст — 27 лет. Компания нанимает сотрудников по всей России, включая удаленных сотрудников из регионов, и ставит цель diversity (разнообразие).

Задание (ПКс-ИИ-3.1): *выявите риски использования данного датасета. Какие меры по управлению рисками вы предложите? Какие записи необходимо внести в техническую документацию относительно ограничений модели?*

Задача 2. Дефекты технической документации при проверке

Ситуация: Компания-интегратор проверяет техническую документацию на ИИ-систему "Цифровой юрист" (помощник для составления исковых заявлений), предоставленную вендором. В документации есть общее описание, но отсутствуют: описание валидационной выборки, метрики качества (точность классификации статей, F1-score), а также не приложена инструкция для пользователя. Вместо инструкции — короткий файл README.TXT с тремя строчками.

Задание: *составьте мотивированный отказ в приемке документации (дефектовочный акт) со ссылками на то, какие требования нарушены и какую информацию необходимо дозапросить у вендора (ПКс-ИИ-3.1).*

Тема 4. Этический комплаенс: прозрачность, недискриминация и справедливость. ПКс-ИИ-3.1

Подготовка к практическому занятию:

– внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;

– подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;

– понять, что осталось неясными и постараться получить на них ответ заранее;

– готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Обеспечение прозрачности и информирования: разработка политик раскрытия информации о взаимодействии с ИИ-системой (объяснимость результатов) и понятных пользовательских соглашений.

2. Выявление и смягчение алгоритмической предвзятости: применение методов тестирования моделей на наличие дискриминационных факторов по признакам пола, расы, возраста и другим защищенным категориям.

3. Принципы справедливости и равноправия: интеграция метрик справедливости (fairness metrics) в процесс разработки и валидации модели для обеспечения равного качества сервиса для всех групп пользователей.

4. Механизмы человеческого контроля: реализация возможности human-in-the-loop (участие человека в принятии решений) для критически важных сценариев и процедура пересмотра решений, вынесенных ИИ.

Ситуационные задачи.

Задача 1. Выявление и смягчение предвзятости в рекрутинге

Ситуация: После запуска ИИ-системы для отбора резюме (см. задачу 3.1) комплаенс-отдел через три месяца провел мониторинг. Статистика показала: система отсеивает 65% кандидатов старше 45 лет, хотя их доля в общем потоке резюме составляет всего 30%. Доля женщин, прошедших первый этап отбора, снизилась на 20% по сравнению с периодом до внедрения ИИ.

Задание: *Как специалист по комплаенс, предложите план действий по управлению выявленным риском дискриминации. Какие меры могут быть техническими, а какие — организационными?*

Задача 2. Дизайн интерфейса для человеческого контроля

Ситуация: Разрабатывается интерфейс для судей (помощник судьи), где ИИ предлагает меру пресечения (подписка о невыезде, залог, арест) на основе вводных данных по делу. Система выдает одну рекомендацию и процент уверенности.

Задание: *Предложите, как должен быть спроектирован интерфейс, чтобы обеспечить эффективный человеческий контроль (human oversight) и соответствовать этическим требованиям прозрачности. Какие элементы обязательны?*

Тема 5. Комплаенс на всем жизненном цикле: мониторинг, инциденты и надзор. ПКс-ИИ-3.1, УК-1.1

Подготовка к практическому занятию:

– внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;

– подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;

– понять, что осталось неясными и постараться получить на них ответ заранее;

– готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Пострегистрационный мониторинг: организация системы непрерывного наблюдения за работой ИИ-системы в реальных условиях для выявления отклонений в производительности и точности.

2. Управление инцидентами: создание протоколов выявления, классификации, расследования и устранения инцидентов (сбои, ошибки, неэтичное поведение), связанных с работой ИИ.

3. Взаимодействие с надзорными органами: определение порядка уведомления регуляторов о серьезных инцидентах и предоставления отчетности по запросу.

4. Адаптивное обновление системы: разработка регламента внесения изменений в модель (дообучение, смена версии) с обязательной повторной оценкой соответствия требованиям безопасности и эффективности.

Ситуационные задачи:

Задача 1. Расследование инцидента с беспилотным такси

Ситуация: Беспилотное такси (автономный автомобиль) компании "Авто-Тех" попало в ДТП в центре города. Автомобиль совершил наезд на велосипедиста, который двигался по велодорожке, но неожиданно выехал на проезжую часть. Система распознала объект, но неверно предсказала его траекторию и скорость, в результате чего торможение началось слишком поздно. Велосипедист получил тяжелые травмы.

Задание: *Как руководитель отдела комплаенс, составьте план расследования инцидента и определите порядок взаимодействия с внешними сторонами (полиция, регулятор, СМИ). Какие данные необходимо собрать в первую очередь?*

Задача 2. Пост-рыночный мониторинг и отклонение метрик

Ситуация: Медицинская ИИ-система для выявления пневмонии по рентгеновским снимкам успешно прошла валидацию и была внедрена в 10 клиниках. Система ежемесячно присылает агрегированные метрики в центр мониторинга. В отчете за апрель обнаружено, что показатель точности (precision) упал с 94% до 87%, а количество ложноположительных срабатываний выросло на 30% в трех клиниках из десяти.

Задание: *предложите процедуру действий по пост-рыночному мониторингу. Каков может быть алгоритм расследования данного отклонения? Какие гипотезы необходимо проверить?*

Тема 6. Трансграничный комплаенс и управление рисками третьих сторон.

ПКс-ИИ-1.1, ПКс-ИИ-3.1

Подготовка к практическому занятию:

– внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;

– подготовить развернутые ответы на вопросы для проведения опроса по теме практического занятия;

– понять, что осталось неясными и постараться получить на них ответ заранее;

– готовиться к практическому занятию можно как индивидуально, так и в составе малой группы.

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Анализ юрисдикционных требований: сопоставление законодательства стран присутствия (например, экстерриториальное действие GDPR и EU AI Act) и выявление коллизий норм.

2. Управление цепочкой поставок ИИ: проведение due diligence в отношении поставщиков технологий, облачных провайдеров и вендоров, предоставляющих готовые ИИ-решения или данные.

3. Контрактное распределение рисков: включение в договоры с третьими сторонами положений об ответственности за соответствие продукции, аудиторских правах и гарантиях качества используемых компонентов.

4. Локализация vs. унификация: поиск баланса между требованиями локализации данных в отдельных странах и необходимостью унификации комплаенс-процедур глобальной компании.

Ситуационные задачи.

Задача 1. Due diligence китайского поставщика камер с распознаванием лиц

Ситуация: Российская сеть магазинов "Перекресток Плюс" планирует закупить у китайской компании "VisionTech" систему видеоаналитики с функцией распознавания лиц для выявления известных магазинных воров. Система также собирает статистику по полу и возрасту посетителей. Отдел безопасности доволен, но юридический департамент обеспокоен комплаенс-рисками.

Задание: *составьте чек-лист для проверки (due diligence) китайского поставщика с точки зрения комплаенс. Какие риски необходимо проверить в первую очередь и как их можно минимизировать в договоре (ПКс-ИИ-1.1, ПКс-ИИ-3.1)?*

Задача 2. Составление протокола разногласий к договору на ИИ-решение

Ситуация: Российский банк получает от европейского вендора проект договора на поставку системы AML (противодействие отмыванию денег) с элементами ИИ. В договоре есть следующие пункты:

П. 5.1: "Поставщик не несет ответственности за убытки, вызванные ошибками работы ИИ-алгоритмов, так как они носят вероятностный характер".

П. 8.3: "Заказчик не вправе проводить аудит исходного кода или алгоритмов работы системы".

П. 10.2: "Применимое право — право Англии. Споры рассматриваются в Лондонском международном арбитражном суде (LCIA)".

Задание: *составьте протокол разногласий (мотивированные возражения) к данным пунктам. Предложите свои редакции, защищающие интересы банка (ПКс-ИИ-1.1, ПКс-ИИ-3.1).*

5.3. Один или несколько тематических блоков дисциплины завершаются контрольной точкой (далее – КТ). Текущий контроль успеваемости по дисциплине предусматривает не менее 2 (двух) и не более 10 (десяти) КТ в течение периода освоения дисциплины.

Максимальное количество баллов за любой тип работ в рамках КТ составляет 100 (сто) баллов.

Распределение весовых коэффициентов по КТ в рамках текущего контроля успеваемости по дисциплине и формулы расчета:

Наименование контрольной точки	Максимальное количество баллов за работу в рамках КТ, которое может набрать обучающийся	Коэффициент веса контрольной точки	Результат контрольной точки, участвующий в формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО)
КТ 1	100	0,1	10
КТ 2	100	0,2	20
КТ 3	100	0,3	30
Итого:	x	0,6	60

Формула расчета результата контрольной точки:

Результат контрольной точки = Количество баллов за работу в рамках КТ X Коэффициент веса контрольной точки.

5.4. Формы текущего контроля успеваемости обучающихся в рамках КТ и типовые оценочные материалы:

КТ – 1.

Тема 1-6.

Доклад.

Тематика докладов:

Тема 1. Введение в регуляторику ИИ. Риск-ориентированный подход. УК-1.1

1. Обзор нормативного ландшафта: анализ ключевых мировых и национальных стратегий регулирования ИИ (ЕС AI Act, документы ОЭСР, российское законодательство в сфере ИИ).
2. Сущность риск-ориентированного подхода: классификация систем ИИ по уровням риска (неприемлемый, высокий, ограниченный, минимальный) и определение критериев отнесения к высокорисковым системам.
3. Правовые последствия классификации: описание требований, запретов и санкций, применяемых к системам в зависимости от присвоенной категории риска.
4. Зоны ответственности участников оборота: разграничение ролей и обязательств провайдеров (разработчиков) и пользователей (имплементаторов) высокорисковых ИИ-систем.

Тема 2. Система комплаенс высокорисковых ИИ-систем. ПКс-ИИ-1.1

5. Формирование политики комплаенса: разработка внутренних регламентов, кодексов этики ИИ и стандартов организации, соответствующих применимому праву.

6. Организационная структура и роли: создание органов управления (комитеты по этике ИИ), назначение ответственных лиц и распределение полномочий в области контроля за ИИ.

7. Процедуры должной осмотрительности: внедрение скрининговых процедур для проверки новых разработок и партнеров на соответствие регуляторным требованиям до вывода системы на рынок.

8. Внутренний контроль и аудит: разработка механизмов периодической проверки соответствия (комплаенс-аудиты), включая проверку документации, процессов и эффективности применяемых мер.

Тема 3. Управление данными и техническая документация. ПКс-ИИ-3.1

9. Требования к качеству данных: установление критериев репрезентативности, полноты и актуальности обучающих, валидационных и тестовых наборов данных для предотвращения ошибок модели.

10. Управление жизненным циклом данных: регламентация процессов сбора, очистки, маркировки, хранения и обновления данных с соблюдением конфиденциальности и защиты персональных данных.

11. Состав и ведение технической документации: формирование исчерпывающего пакета документов, описывающего архитектуру системы, методы разработки, логику работы и результаты тестирования (требование прослеживаемости).

12. Автоматизация документирования: использование инструментов для ведения логов и версионирования как моделей, так и данных для обеспечения воспроизводимости результатов и доказательной базы для регуляторов.

Тема 4. Этический комплаенс: прозрачность, недискриминация и справедливость. ПКс-ИИ-3.1

13. Обеспечение прозрачности и информирования: разработка политик раскрытия информации о взаимодействии с ИИ-системой (объяснимость результатов) и понятных пользовательских соглашений.

14. Выявление и смягчение алгоритмической предвзятости: применение методов тестирования моделей на наличие дискриминационных факторов по признакам пола, расы, возраста и другим защищенным категориям.

15. Принципы справедливости и равноправия: интеграция метрик справедливости (fairness metrics) в процесс разработки и валидации модели для обеспечения равного качества сервиса для всех групп пользователей.

16. Механизмы человеческого контроля: реализация возможности human-in-the-loop (участие человека в принятии решений) для критически важных сценариев и процедура пересмотра решений, вынесенных ИИ.

Тема 5. Комплаенс на всем жизненном цикле: мониторинг, инциденты и надзор. ПКс-ИИ-3.1, УК-1.1

17. Пострегистрационный мониторинг: организация системы непрерывного наблюдения за работой ИИ-системы в реальных условиях для выявления отклонений в производительности и точности.

18. Управление инцидентами: создание протоколов выявления, классификации, расследования и устранения инцидентов (сбои, ошибки, неэтичное поведение), связанных с работой ИИ.

19. Взаимодействие с надзорными органами: определение порядка уведомления регуляторов о серьезных инцидентах и предоставления отчетности по запросу.

20. Адаптивное обновление системы: разработка регламента внесения изменений в модель (дообучение, смена версии) с обязательной повторной оценкой соответствия требованиям безопасности и эффективности.

Тема 6. Трансграничный комплаенс и управление рисками третьих сторон. ПКс-ИИ-1.1 + ПКс-ИИ-3.1

21. Анализ юрисдикционных требований: сопоставление законодательства стран присутствия (например, экстерриториальное действие GDPR и EU AI Act) и выявление коллизий норм.
22. Управление цепочкой поставок ИИ: проведение due diligence в отношении поставщиков технологий, облачных провайдеров и вендоров, предоставляющих готовые ИИ-решения или данные.
23. Контрактное распределение рисков: включение в договоры с третьими сторонами положений об ответственности за соответствие продукции, аудиторских правах и гарантиях качества используемых компонентов.
24. Локализация vs. унификация: поиск баланса между требованиями локализации данных в отдельных странах и необходимостью унификации комплаенс-процедур глобальной компании.

Методические рекомендации по подготовке доклада.

Подготовка доклада способствует формированию навыков исследовательской работы, расширяет познавательные интересы, приучает критически мыслить. При написании доклада по заданной теме составляется план, подбираются основные источники. В процессе работы с источниками, систематизируют полученные сведения, делают выводы и обобщения.

Подготовка доклада требует от обучающегося большой самостоятельности и серьезной интеллектуальной работы, которая принесет наибольшую пользу, если будет включать с себя следующие этапы: изучение наиболее важных научных работ по данной теме, перечень которых дает сам преподаватель; анализ изученного материала, выделение наиболее значимых для раскрытия темы фактов, мнений разных ученых и научных положений; обобщение и логическое построение материала доклада, например, в форме развернутого плана; написание текста доклада с соблюдением требований научного стиля.

Построение доклада включает три части: вступление, основную часть и заключение. Во вступлении указывается тема доклада, устанавливается логическая связь ее с другими темами или место рассматриваемой проблемы среди других проблем, дается краткий обзор источников, на материале которых раскрывается тема и т. п. Основная часть должна иметь четкое логическое построение, в ней должна быть раскрыта тема доклада. В заключении обычно подводятся итоги, формулируются выводы, подчеркивается значение рассмотренной проблемы и т. п.

Критерии оценивания доклада:

Критерии оценки	Диапазон баллов	Описание критерия
Содержание и раскрытие темы	0-20	Детальное, последовательное описание всех этапов с конкретными примерами
Грамотность изложения	0-20	Соблюдены все правила грамматики, орфографии и пунктуации
Стилистика	0-20	Единый стиль изложения, точные формулировки, уместное использование

		терминов, лаконичность
Логика изложения	0-20	Чёткая последовательность изложения, логические связи между частями текста, аргументы подтверждают выводы
Оригинальность	0-20	Уникальный подход к теме, нестандартные решения, инновационные идеи, собственная позиция автора
Итого максимально:	100	

КТ – 2.

Темы 1-6

Устный опрос:

Вопросы для опроса:

№ п.п.	Содержание вопроса
1.	1. Сущность риск-ориентированного подхода: классификация систем ИИ по уровням риска (неприемлемый, высокий, ограниченный, минимальный) и определение критериев отнесения к высокорисковым системам.
2.	2. Зоны ответственности участников оборота: разграничение ролей и обязательств провайдеров (разработчиков) и пользователей (имплементаторов) высокорисковых ИИ-систем.
3.	3. Формирование политики комплаенса: разработка внутренних регламентов, кодексов этики ИИ и стандартов организации, соответствующих применимому праву.
4.	4. Процедуры должной осмотрительности: внедрение скрининговых процедур для проверки новых разработок и партнеров на соответствие регуляторным требованиям до вывода системы на рынок.
5.	5. Требования к качеству данных: установление критериев репрезентативности, полноты и актуальности обучающих, валидационных и тестовых наборов данных для предотвращения ошибок модели.
6.	6. Состав и ведение технической документации: формирование исчерпывающего пакета документов, описывающего архитектуру системы, методы разработки, логику работы и результаты тестирования (требование прослеживаемости).
7.	7. Обеспечение прозрачности и информирования: разработка политик раскрытия информации о взаимодействии с ИИ-системой (объяснимость результатов) и понятных пользовательских соглашений.
8.	8. Выявление и смягчение алгоритмической предвзятости: применение методов тестирования моделей на наличие дискриминационных факторов по признакам пола, расы, возраста и другим защищенным категориям.
9.	9. Принципы справедливости и равноправия: интеграция метрик справедливости (fairness metrics) в процесс разработки и валидации модели для обеспечения равного качества сервиса для всех групп пользователей.
10.	10. Механизмы человеческого контроля: реализация возможности human-in-the-loop (участие человека в принятии решений) для критически важных сценариев и

	процедура пересмотра решений, вынесенных ИИ.
11.	11. Управление инцидентами: создание протоколов выявления, классификации, расследования и устранения инцидентов (сбои, ошибки, неэтичное поведение), связанных с работой ИИ.
12.	12. Анализ юрисдикционных требований: сопоставление законодательства стран присутствия (например, экстерриториальное действие GDPR и EU AI Act) и выявление коллизий норм.
13.	13. Контрактное распределение рисков: включение в договоры с третьими сторонами положений об ответственности за соответствие продукции, аудиторских правах и гарантиях качества используемых компонентов.
14.	14. Локализация vs. унификация: поиск баланса между требованиями локализации данных в отдельных странах и необходимостью унификации комплаенс-процедур глобальной компании.

Критерии оценивания опроса:

Диапазон баллов	Описание критерия
85-100	Обучающийся полно излагает материал (отвечает на вопрос), дает правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка.
65-84	Обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.
55-64	Обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
0-54	Обучающийся обнаруживает незнание вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

КТ – 3.
Темы 1-6

Тестирование

1. Какой принцип НЕ относится к основным принципам регулирования ИИ?
A) Приоритет прав и безопасности человека
B) Прозрачность и объяснимость
C) Максимизация прибыли разработчика
D) Подконтрольность человеку

2. Что означает экстерриториальное действие EU AI Act?
A) Действие акта только на территории Европейского Союза
B) Распространение норм акта на разработчиков и пользователей за пределами ЕС, если результаты работы ИИ затрагивают лиц на территории ЕС
C) Обязательность применения акта только в странах-членах НАТО
D) Действие акта исключительно в отношении европейских компаний

3. Какой штраф предусмотрен EU AI Act за нарушение требований к высокорисковым системам?
A) До 1 млн евро
B) До 10 млн евро или 2% оборота
C) До 30 млн евро или 6% глобального годового оборота
D) Штраф не предусмотрен

4. Какой коллегиальный орган обычно создается для рассмотрения сложных этических вопросов при разработке ИИ?
A) Совет директоров
B) Комитет по этике ИИ
C) Профсоюзный комитет
D) Технический совет

5. Что означает требование репрезентативности данных?
A) Данные должны быть собраны только из одного источника
B) Данные должны отражать целевую аудиторию и условия применения системы
C) Данные должны быть засекречены
D) Данные должны быть минимальны по объему

6. Что такое дрейф данных (data drift)?
A) Физическое перемещение данных между серверами
B) Изменение статистических характеристик входных данных в реальном использовании по сравнению с обучающей выборкой
C) Намеренное искажение данных злоумышленником
D) Процесс архивации устаревших данных

7. Что означает принцип прозрачности в контексте ИИ?
A) Публикация исходного кода всех систем
B) Информирование о взаимодействии с ИИ и предоставление понятных объяснений решений
C) Полная секретность всех алгоритмов
D) Трансляция процесса разработки в прямом эфире

8. Что такое алгоритмическая предвзятость (bias)?
A) Высокая точность модели
B) Систематическое несправедливое отношение к отдельным лицам или группам лиц
C) Способность модели обучаться на новых данных
D) Защита модели от взлома

9. Что такое инцидент в сфере ИИ?
A) Любое событие, связанное с работой ИИ
B) Событие, которое привело или могло привести к причинению вреда либо к нарушению обязательных требований
C) Успешное завершение обучения модели

D) Регулярное обновление программного обеспечения

10. Что такое "существенное изменение" (significant modification) ИИ-системы?
A) Любое изменение, даже исправление опечатки в документации
B) Изменение, которое может повлиять на соответствие системы требованиям или изменить предполагаемое назначение
C) Изменение цвета интерфейса
D) Обновление версии операционной системы на сервере

11. На кого распространяется GDPR (Общий регламент о защите данных ЕС)?
A) Только на европейские компании
B) На любые компании мира, обрабатывающие персональные данные резидентов ЕС при предложении товаров/услуг или мониторинге поведения
C) Только на компании из США
D) Только на государственные учреждения

12. Какая стратегия позволяет сочетать унификацию и локализацию?
A) Игнорирование локальных требований
B) Создание полностью разных продуктов для каждой страны
C) Разработка единого ядра продукта с возможностью локальных адаптаций
D) Ведение бизнеса только в одной стране

Критерии оценивания тестовых заданий:

Диапазон баллов	Описание критерия	
85-100	Свыше 80% правильных ответов.	Обучающийся демонстрирует глубокое познание в освоенном материале.
65-84	Свыше 70% правильных ответов.	Обучающимся материал освоен полностью, без существенных ошибок.
55-64	Свыше 50% правильных ответов.	Обучающимся материал освоен не полностью, имеются значительные пробелы в знаниях.
0-54	Менее 50% правильных ответов.	Обучающимся материал не освоен, знания обучающегося ниже базового уровня.

5.5. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий (*при необходимости*).

Для ответа на вопросы студенту разрешается использование нормативно-правовых актов.

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

6.1. Промежуточная аттестация (зачет, экзамен) проводится в устной форме. Обучающийся получает экзаменационный билет и готовится к устному ответу.

6.2. Типовые оценочные материалы промежуточной аттестации

Типовые проверочные задания для самоподготовки обучающегося к промежуточной

аттестации:

Тема 1. Введение в регуляторику ИИ. Риск-ориентированный подход. УК-1.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Обзор нормативного ландшафта: анализ ключевых мировых и национальных стратегий регулирования ИИ (ЕС AI Act, документы ОЭСР, российское законодательство в сфере ИИ).
2.	Сущность риск-ориентированного подхода: классификация систем ИИ по уровням риска (неприемлемый, высокий, ограниченный, минимальный) и определение критериев отнесения к высокорисковым системам.
3.	Правовые последствия классификации: описание требований, запретов и санкций, применяемых к системам в зависимости от присвоенной категории риска.
4.	Зоны ответственности участников оборота: разграничение ролей и обязательств провайдеров (разработчиков) и пользователей (имплементаторов) высокорисковых ИИ-систем.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	В соответствии с EU AI Act, системы ИИ для кредитного скоринга и оценки кредитоспособности физических лиц относятся к категории: а) недопустимого риска (запрещены); б) высокого риска, что влечёт наиболее строгие требования к оценке соответствия и управлению рисками на всём жизненном цикле; в) ограниченного риска, требующего лишь информирования пользователя; г) минимального риска, не подпадающего под специальное регулирование.		
2.	Российская Национальная стратегия развития ИИ до 2030 года (утв. Указом Президента № 490) в отличие		

	от EU AI Act делает акцент на: а) запрете социального скоринга как приоритетном направлении; б) создании комплексной системы регулирования общественных отношений, возникающих в связи с развитием и использованием технологий ИИ, с приоритетом поддержки инноваций; в) введении оборотных штрафов за любые нарушения в сфере ИИ с 2025 года; г) полном копировании европейского риск-ориентированного подхода.		

3. Задания закрытого типа.

Тестовые задания.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

1. Какой принцип НЕ относится к основным принципам регулирования ИИ?
A) Приоритет прав и безопасности человека
B) Прозрачность и объяснимость
C) Максимизация прибыли разработчика
D) Подконтрольность человеку

2. Что означает экстерриториальное действие EU AI Act?
A) Действие акта только на территории Европейского Союза
B) Распространение норм акта на разработчиков и пользователей за пределами ЕС, если результаты работы ИИ затрагивают лиц на территории ЕС
C) Обязательность применения акта только в странах-членах НАТО
D) Действие акта исключительно в отношении европейских компаний

3. Какая категория риска предусматривает запрет на использование ИИ-систем?
A) Высокий риск
B) Ограниченный риск
C) Неприемлемый риск
D) Минимальный риск

4. К какому виду юридических фактов относится наступление вреда вследствие работы ИИ-системы?
A) Действие

B) Событие
C) Правопрекращающий факт
D) Фикция

Тема 2. Система комплаенс высокорисковых ИИ-систем. ПКс-ИИ-1.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Формирование политики комплаенса: разработка внутренних регламентов, кодексов этики ИИ и стандартов организации, соответствующих применимому праву.
2.	Организационная структура и роли: создание органов управления (комитеты по этике ИИ), назначение ответственных лиц и распределение полномочий в области контроля за ИИ.
3.	Процедуры должной осмотрительности: внедрение скрининговых процедур для проверки новых разработок и партнеров на соответствие регуляторным требованиям до вывода системы на рынок.
4.	Внутренний контроль и аудит: разработка механизмов периодической проверки соответствия (комплаенс-аудиты), включая проверку документации, процессов и эффективности применяемых мер.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	В соответствии со статьей 17 EU AI Act, поставщик высокорисковой ИИ-системы обязан внедрить систему менеджмента качества (quality management system). Что из перечисленного является обязательным элементом такой системы? а) Ежегодный аудит финансовой отчётности компании; б) Стратегия взаимодействия с общественностью и СМИ; в) Политика управления данными (data governance policy), процедуры контроля и документирования послепродажного		

	мониторинга; г) Маркетинговая стратегия продвижения ИИ-системы.		
2.	Новый российский стандарт ГОСТ Р ИСО/МЭК 42001-2024 «Системы менеджмента искусственного интеллекта» (AIMS) устанавливает требования к: а) исключительно техническим характеристикам моделей машинного обучения; б) формированию политик, ролей, процедур оценки рисков ИИ и непрерывного улучшения системы управления ИИ в организации; в) дизайну пользовательского интерфейса ИИ-приложений; г) алгоритмам шифрования данных, используемых для обучения.		

3. Задания закрытого типа.

Тестовые задания.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

1. Какой штраф предусмотрен EU AI Act за нарушение требований к высокорисковым системам?
A) До 1 млн евро
B) До 10 млн евро или 2% оборота
C) До 30 млн евро или 6% глобального годового оборота
D) Штраф не предусмотрен

2. Какой коллегиальный орган обычно создается для рассмотрения сложных этических вопросов при разработке ИИ?
A) Совет директоров
B) Комитет по этике ИИ
C) Профсоюзный комитет
D) Технический совет

3. Кто несет ответственность за ненадлежащее использование ИИ-системы, если она используется не по назначению?
A) Провайдер (разработчик)
B) Пользователь (имплементатор)

C) Регулятор
D) Разработчик алгоритмов машинного обучения

4. Какова правильная последовательность процесса оценки рисков?
A) Обработка → Идентификация → Анализ → Оценка → Мониторинг
B) Идентификация → Анализ → Оценка → Обработка → Мониторинг
C) Мониторинг → Идентификация → Анализ → Обработка → Оценка
D) Анализ → Идентификация → Мониторинг → Обработка → Оценка

Тема 3. Управление данными и техническая документация. ПКс-ИИ-3.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Требования к качеству данных: установление критериев репрезентативности, полноты и актуальности обучающих, валидационных и тестовых наборов данных для предотвращения ошибок модели.
2.	Управление жизненным циклом данных: регламентация процессов сбора, очистки, маркировки, хранения и обновления данных с соблюдением конфиденциальности и защиты персональных данных.
3.	Состав и ведение технической документации: формирование исчерпывающего пакета документов, описывающего архитектуру системы, методы разработки, логику работы и результаты тестирования (требование прослеживаемости).
4.	Автоматизация документирования: использование инструментов для ведения логов и версионирования как моделей, так и данных для обеспечения воспроизводимости результатов и доказательной базы для регуляторов.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Согласно требованиям к высокорисковым ИИ-системам, ключевым элементом управления данными (data governance) является обеспечение того, чтобы обучающие, валидационные и тестовые наборы данных были: а) максимально большими по объёму, независимо от качества; б) релевантными, репрезентативными, свободными от ошибок и полными с учётом		

	предполагаемого назначения системы, а также характеризовались соответствующими статистическими свойствами; в) исключительно синтетическими, не содержащими персональных данных; г) загружены в единую базу данных компании до начала разработки.		
2.	Прослеживаемость происхождения данных (data lineage) для высокорисковой ИИ-системы необходима, главным образом, для: а) ускорения процесса обучения модели; б) демонстрации регулятору и аудиторам того, как были получены и преобразованы данные, какие наборы использовались для обучения, и обеспечения готовности к комплаенс-проверкам и расследованию инцидентов; в) удешевления хранения данных; г) автоматического патентования модели.		

3. Задания закрытого типа.

Тестовые задания.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

1. Что означает требование репрезентативности данных?
A) Данные должны быть собраны только из одного источника
B) Данные должны отражать целевую аудиторию и условия применения системы
C) Данные должны быть засекречены
D) Данные должны быть минимальны по объему

2. Что такое дрейф данных (data drift)?
A) Физическое перемещение данных между серверами

B) Изменение статистических характеристик входных данных в реальном использовании по сравнению с обучающей выборкой
C) Намеренное искажение данных злоумышленником
D) Процесс архивации устаревших данных

3. Что должно быть включено в общее описание системы в технической документации?
A) Исходный код всех программ
B) Назначение, цели использования, границы и ограничения системы
C) Персональные данные всех тестировщиков
D) Маркетинговый бюджет

4. Что означает прослеживаемость (traceability) в контексте ИИ?
A) Отслеживание местоположения пользователей
B) Способность воспроизвести процесс разработки и установить причины конкретных решений или инцидентов
C) Установка GPS-трекеров на серверы
D) Мониторинг физического доступа в офис

Тема 4. Этический комплаенс: прозрачность, недискриминация и справедливость. ПКс-ИИ-3.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Обеспечение прозрачности и информирования: разработка политик раскрытия информации о взаимодействии с ИИ-системой (объяснимость результатов) и понятных пользовательских соглашений.
2.	Выявление и смягчение алгоритмической предвзятости: применение методов тестирования моделей на наличие дискриминационных факторов по признакам пола, расы, возраста и другим защищенным категориям.
3.	Принципы справедливости и равноправия: интеграция метрик справедливости (fairness metrics) в процесс разработки и валидации модели для обеспечения равного качества сервиса для всех групп пользователей.
4.	Механизмы человеческого контроля: реализация возможности human-in-the-loop (участие человека в принятии решений) для критически важных сценариев и процедура пересмотра решений, вынесенных ИИ.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	В рамках комплаенса высокорисковых ИИ-систем, используемых для найма персонала, требование		

	«недискриминации» (non-discrimination) обязывает поставщика: а) гарантировать, что алгоритм никогда не откажет кандидату по признаку пола или возраста; б) внедрить процедуры выявления, оценки и минимизации рисков предвзятости (bias) на протяжении всего жизненного цикла системы, включая тестирование на репрезентативных данных и регулярный аудит результатов; в) полностью исключить участие человека в процессе отбора кандидатов; г) использовать только те данные о кандидатах, которые были собраны до 2020 года.		
2.	Требование «прозрачности» (transparency) для высокорисковых ИИ-систем означает, что поставщик обязан: а) опубликовать исходный код системы в открытом доступе; б) предоставить развертывающей организации (deployer) инструкцию по эксплуатации, понятную для пользователей, и информацию о характеристиках, ограничениях и показателях точности системы, достаточную для обеспечения человеческого контроля; в) раскрыть все коммерческие договорённости с контрагентами; г) обеспечить публичный доступ к логам работы системы в реальном времени.		

3. Задания закрытого типа.

Тестовые задания.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

1. Что означает принцип прозрачности в контексте ИИ?
A) Публикация исходного кода всех систем
B) Информирование о взаимодействии с ИИ и предоставление понятных объяснений решений
C) Полная секретность всех алгоритмов
D) Трансляция процесса разработки в прямом эфире

2. Что такое алгоритмическая предвзятость (bias)?
A) Высокая точность модели
B) Систематическое несправедливое отношение к отдельным лицам или группам лиц
C) Способность модели обучаться на новых данных
D) Защита модели от взлома

3. Что требует метрика "демографический паритет" (demographic parity)?
A) Доля положительных решений должна быть одинаковой для всех групп
B) Точность предсказаний должна быть 100%
C) Модель должна учитывать пол пользователя
D) Все решения должны быть отрицательными

4. Что означает режим "human-in-the-loop" (HITL)?
A) Человек не участвует в принятии решений
B) Человек участвует в каждом цикле принятия решения, утверждая или отклоняя предложения ИИ
C) Система работает полностью автономно
D) Человек только наблюдает за работой системы

Тема 5. Комплаенс на всем жизненном цикле: мониторинг, инциденты и надзор. ПКс-ИИ-3.1, УК-1.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Пострегистрационный мониторинг: организация системы непрерывного наблюдения за работой ИИ-системы в реальных условиях для выявления отклонений в производительности и точности.
2.	Управление инцидентами: создание протоколов выявления, классификации, расследования и устранения инцидентов (сбои, ошибки, неэтичное поведение), связанных с работой ИИ.
3.	Взаимодействие с надзорными органами: определение порядка уведомления регуляторов о серьезных инцидентах и предоставления отчетности по запросу.
4.	Адаптивное обновление системы: разработка регламента внесения изменений в

	модель (дообучение, смена версии) с обязательной повторной оценкой соответствия требованиям безопасности и эффективности.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Обязанность поставщика высокорисковой ИИ-системы по послепродажному мониторингу (post-market monitoring) предполагает: а) однократную проверку системы перед выпуском на рынок; б) активный и систематический сбор и анализ данных о работе системы на протяжении всего её жизненного цикла для выявления необходимости принятия корректирующих мер; в) опрос пользователей об их удовлетворённости дизайном интерфейса раз в год; г) полное прекращение поддержки системы после её продажи.		
2.	В российских стандартах (ГОСТ Р ИСО/МЭК 27000-2021) инцидент информационной безопасности определяется как: а) любое событие, которое пользователь посчитал неудобным; б) одно или несколько нежелательных или неожиданных событий ИБ, которые с высокой вероятностью могут привести к нарушению процессов и угрозам безопасности информации; в) технический сбой оборудования; г) получение компанией		

	претензии от контролирующего органа.		

3. Задания закрытого типа.

Тестовые задания.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

1. Какова основная цель пострегистрационного мониторинга?
A) Сбор статистики для маркетинга
B) Выявление отклонений и новых рисков после вывода системы на рынок
C) Увеличение стоимости акций компании
D) Спам-рассылка пользователям

2. Что такое инцидент в сфере ИИ?
A) Любое событие, связанное с работой ИИ
B) Событие, которое привело или могло привести к причинению вреда либо к нарушению обязательных требований
C) Успешное завершение обучения модели
D) Регулярное обновление программного обеспечения

3. Что могут делать надзорные органы в ходе проверки (инспекции)?
A) Только направлять письменные запросы
B) Изучать документацию, проводить тестирование системы, посещать помещения
C) Только беседовать с руководством
D) Ничего, кроме наблюдения

4. Что такое "существенное изменение" (significant modification) ИИ-системы?
A) Любое изменение, даже исправление опечатки в документации
B) Изменение, которое может повлиять на соответствие системы требованиям или изменить предполагаемое назначение
C) Изменение цвета интерфейса
D) Обновление версии операционной системы на сервере

Тема 6. Трансграничный комплаенс и управление рисками третьих сторон. ПКс-ИИ-1.1, ПКс-ИИ-3.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Анализ юрисдикционных требований: сопоставление законодательства стран присутствия (например, экстерриториальное действие GDPR и EU AI Act) и выявление коллизий норм.
2.	Управление цепочкой поставок ИИ: проведение due diligence в отношении

	поставщиков технологий, облачных провайдеров и вендоров, предоставляющих готовые ИИ-решения или данные.
3.	Контрактное распределение рисков: включение в договоры с третьими сторонами положений об ответственности за соответствие продукции, аудиторских правах и гарантиях качества используемых компонентов.
4.	Локализация vs. унификация: поиск баланса между требованиями локализации данных в отдельных странах и необходимостью унификации комплаенс-процедур глобальной компании.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Согласно EU AI Act, российская IT-компания, разрабатывающая высокорисковую ИИ-систему, должна выполнить требования Регламента даже при отсутствии представительства в ЕС, если: а) компания использует серверы, расположенные на территории ЕС; б) выходные данные (output) этой системы используются на территории ЕС; в) компания зарегистрировала домен в зоне .eu; г) хотя бы один из сотрудников компании говорит по-английски.		
2.	При управлении рисками, связанными с третьими сторонами (поставщиками данных, облачными провайдерами, разработчиками библиотек), в рамках комплаенса ИИ-системы критически важно: а) требовать от всех контрагентов нотариально заверенного обещания не нарушать закон; б) включить в договоры с третьими сторонами обязательства о соблюдении применимых требований к данным, безопасности и		

	конфиденциальности, а также право на аудит и проверку их комплаенс-статуса; в) полностью отказаться от услуг любых внешних поставщиков; г) застраховать ответственность всех третьих сторон за свой счёт.		

3. Задания закрытого типа.

Тестовые задания.

Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

1. На кого распространяется GDPR (Общий регламент о защите данных ЕС)?
A) Только на европейские компании
B) На любые компании мира, обрабатывающие персональные данные резидентов ЕС при предложении товаров/услуг или мониторинге поведения
C) Только на компании из США
D) Только на государственные учреждения

2. Кто несет ответственность за соответствие конечной системы требованиям, если использовались компоненты третьих сторон?
A) Поставщик компонента несет полную ответственность
B) Провайдер (разработчик) конечной системы
C) Ответственность не несет никто
D) Регулятор

3. Что означает условие об indemnification (возмещении потерь) в договоре?
A) Обязанность поставщика поставить товар в срок
B) Обязанность поставщика возместить убытки заказчика, если к заказчику предъявлены претензии из-за дефекта компонента поставщика
C) Право заказчика не платить
D) Обязанность заказчика застраховать поставщика

4. Какая стратегия позволяет сочетать унификацию и локализацию?
A) Игнорирование локальных требований
B) Создание полностью разных продуктов для каждой страны
C) Разработка единого ядра продукта с возможностью локальных адаптаций
D) Ведение бизнеса только в одной стране

6.3. Критерии и шкала оценивания на основе БРС.

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ В БАЛЛАХ
Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал	40

знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок	
Дан развернутый ответ на поставленный вопрос, где обучающийся демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями.	30-39
Дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа и решении практических заданий.	20-29
Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено, т.е. обучающийся не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.	0-19

6.4. Для решения практических заданий обучающемуся разрешается использование нормативно-правовых актов.

7. Методические материалы по освоению дисциплины

Подготовка к лекциям.

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы. В основу его нужно положить рабочие программы изучаемых в семестре дисциплин. Каждому обучающемуся следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли

выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Самостоятельная работа на лекции.

Слушание и запись лекций – сложный вид вузовской аудиторной работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность обучающегося. Краткие записи лекций, их конспектирование помогает усвоить учебный материал. Конспект является полезным тогда, когда записано самое существенное, основное и сделано это самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лекции лучше подразделять на пункты, параграфы, соблюдая красную строку. Этому в большой степени будут способствовать пункты плана лекции, предложенные преподавателям. Принципиальные места, определения, формулы и другое следует сопровождать замечаниями «важно», «особо важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек. Лучше если они будут собственными, чтобы не приходилось просить их у однокурсников и тем самым не отвлекать их во время лекции. Целесообразно разработать собственную «маркографию» (значки, символы), сокращения слов. Не лишним будет и изучение основ стенографии. Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть знаниями.

Подготовка к практическим занятиям.

Подготовку к каждому практическому занятию каждый обучающийся должен начать с ознакомления с планом практического занятия, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала лекции, а затем изучения обязательной и дополнительной литературы, рекомендованную к данной теме. На основе индивидуальных предпочтений обучающемуся необходимо самостоятельно выбрать тему доклада по проблеме практического занятия и по возможности подготовить по нему презентацию. Если программой дисциплины предусмотрено выполнение практического задания, то его необходимо выполнить с учетом предложенной инструкции (устно или 10 письменно). Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса. Результат такой работы должен проявиться в способности обучающегося свободно ответить на теоретические вопросы практического занятия, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

Структура практического занятия:

В зависимости от содержания и количества отведенного времени на изучение каждой темы может практическое занятие состоять из четырех-пяти частей:

1. Обсуждение теоретических вопросов, определенных программой дисциплины.
2. Доклад и/ или выступление с презентациями по проблеме практического занятия.
3. Обсуждение выступлений по теме – дискуссия.
4. Выполнение практического задания с последующим разбором полученных результатов или обсуждение практического задания, выполненного дома, если это

предусмотрено программой.

5. Подведение итогов занятия.

Первая часть – обсуждение теоретических вопросов - проводится в виде фронтальной беседы со всей группой и включает выборочную проверку преподавателем теоретических знаний обучающихся. Примерная продолжительность — до 15 минут. Вторая часть — выступление обучающихся с докладами, которые должны сопровождаться презентациями с целью усиления наглядности восприятия, по одному из вопросов практического занятия. Обязательный элемент доклада – представление и анализ статистических данных, обоснование социальных последствий любого экономического факта, явления или процесса. Примерная продолжительность — 20-25 минут. После докладов следует их обсуждение – дискуссия. В ходе этого этапа практического занятия могут быть заданы уточняющие вопросы к докладчикам. Примерная продолжительность – до 15-20 минут. Если программой предусмотрено выполнение практического задания в рамках конкретной темы, то преподавателями определяется его содержание и дается время на его выполнение, а затем идет обсуждение результатов. Если практическое задание должно было быть выполнено дома, то на практическом занятии преподаватель проверяет его выполнение (устно или письменно). Примерная продолжительность – 15-20 минут. Подведением итогов заканчивается практическое занятие. Обучающимся должны быть объявлены оценки за работу и даны их четкие обоснования. Примерная продолжительность — 5 минут.

Работа с литературными источниками.

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на занятиях, выявить широкий спектр мнений по изучаемой проблеме.

Вопросы для самостоятельной подготовки к лекционным и практическим занятиям:

1. Обзор нормативного ландшафта: анализ ключевых мировых и национальных стратегий регулирования ИИ (ЕС AI Act, документы ОЭСР, российское законодательство в сфере ИИ).
2. Сущность риск-ориентированного подхода: классификация систем ИИ по уровням риска (неприемлемый, высокий, ограниченный, минимальный) и определение критериев отнесения к высокорисковым системам.
3. Правовые последствия классификации: описание требований, запретов и санкций, применяемых к системам в зависимости от присвоенной категории риска.
4. Зоны ответственности участников оборота: разграничение ролей и обязательств провайдеров (разработчиков) и пользователей (имплементаторов) высокорисковых ИИ-систем.
5. Формирование политики комплаенса: разработка внутренних регламентов, кодексов этики ИИ и стандартов организации, соответствующих применимому праву.
6. Организационная структура и роли: создание органов управления (комитеты по этике ИИ), назначение ответственных лиц и распределение полномочий в области контроля за ИИ.

7. Процедуры должной осмотрительности: внедрение скрининговых процедур для проверки новых разработок и партнеров на соответствие регуляторным требованиям до вывода системы на рынок.

8. Внутренний контроль и аудит: разработка механизмов периодической проверки соответствия (комплаенс-аудиты), включая проверку документации, процессов и эффективности применяемых мер.

9. Требования к качеству данных: установление критериев репрезентативности, полноты и актуальности обучающих, валидационных и тестовых наборов данных для предотвращения ошибок модели.

10. Управление жизненным циклом данных: регламентация процессов сбора, очистки, маркировки, хранения и обновления данных с соблюдением конфиденциальности и защиты персональных данных.

11. Состав и ведение технической документации: формирование исчерпывающего пакета документов, описывающего архитектуру системы, методы разработки, логику работы и результаты тестирования (требование прослеживаемости).

12. Автоматизация документирования: использование инструментов для ведения логов и версионирования как моделей, так и данных для обеспечения воспроизводимости результатов и доказательной базы для регуляторов.

13. Обеспечение прозрачности и информирования: разработка политик раскрытия информации о взаимодействии с ИИ-системой (объяснимость результатов) и понятных пользовательских соглашений.

14. Выявление и смягчение алгоритмической предвзятости: применение методов тестирования моделей на наличие дискриминационных факторов по признакам пола, расы, возраста и другим защищенным категориям.

15. Принципы справедливости и равноправия: интеграция метрик справедливости (fairness metrics) в процесс разработки и валидации модели для обеспечения равного качества сервиса для всех групп пользователей.

16. Механизмы человеческого контроля: реализация возможности human-in-the-loop (участие человека в принятии решений) для критически важных сценариев и процедура пересмотра решений, вынесенных ИИ.

17. Пострегистрационный мониторинг: организация системы непрерывного наблюдения за работой ИИ-системы в реальных условиях для выявления отклонений в производительности и точности.

18. Управление инцидентами: создание протоколов выявления, классификации, расследования и устранения инцидентов (сбои, ошибки, неэтичное поведение), связанных с работой ИИ.

19. Взаимодействие с надзорными органами: определение порядка уведомления регуляторов о серьезных инцидентах и предоставления отчетности по запросу.

20. Адаптивное обновление системы: разработка регламента внесения изменений в модель (дообучение, смена версии) с обязательной повторной оценкой соответствия требованиям безопасности и эффективности.

21. Анализ юрисдикционных требований: сопоставление законодательства стран присутствия (например, экстерриториальное действие GDPR и EU AI Act) и выявление коллизий норм.

22. Управление цепочкой поставок ИИ: проведение due diligence в отношении поставщиков технологий, облачных провайдеров и вендоров, предоставляющих готовые ИИ-решения или данные.

23. Контрактное распределение рисков: включение в договоры с третьими сторонами положений об ответственности за соответствие продукции, аудиторских правах и гарантиях качества используемых компонентов.

24. Локализация vs. унификация: поиск баланса между требованиями локализации данных в отдельных странах и необходимостью унификации комплаенс-процедур глобальной компании.

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Черепанова, В. А. Комплаенс-программа организации : практическое руководство / В. А. Черепанова. — 5-е изд., испр. — Москва : ИНФРА-М, 2026. — 285 с. — DOI 10.12737/1221793. - ISBN 978-5-16-016722-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2227301 (дата обращения: 08.06.2026). – Режим доступа: по подписке.

2. Крамаров, С. О. Разработка интеллектуальных аналитически-рекомендательных систем профессиональной ориентации на основе психофизического профилирования и алгоритмов ИИ : монография / С. О. Крамаров, Л. В. Сахарова, О. Р. Попов. – Москва : РИОР, 2026. - 200 с. – (Научная мысль). - ISBN 978-5-369-02184-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2251657 (дата обращения: 08.06.2026). – Режим доступа: по подписке.

3. Оценка регулирующего воздействия и регуляторная политика : учебное пособие / под общ. ред. И.Д. Тургель. — Москва : ИНФРА-М, 2022. — 223 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/textbook_5a16de4b7a64c4.04606576. - ISBN 978-5-16-013125-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1859601 (дата обращения: 08.06.2026). – Режим доступа: по подписке.

Братко, А. Г. Искусственный разум, правовая система и функции государства : монография / А.Г. Братко. — Москва : ИНФРА-М, 2026. — 282 с. — (Научная мысль). — DOI 10.12737/1064996. - ISBN 978-5-16-015890-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2261236 (дата обращения: 08.06.2026). – Режим доступа: по подписке.

4. Экспериментальные правовые режимы: зарубежный опыт и российский старт : доклад / А. А. Ефремов, Е. И. Добролюбова, Э. В. Талапина, В. Н. Южаков ; науч. ред. В. Н. Южаков.— Москва : Издательский дом «Дело» РАНХиГС, 2020. - 126 с. - (Научные доклады: государственное управление). - ISBN 978-5-850006-195-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1405757 (дата обращения: 08.06.2026). – Режим доступа: по подписке.

8.2. Дополнительная литература

1. Mökander, J., Floridi, L. (Eds.). The AI Act and The Risk-Based Approach to AI Regulation / J. Mökander, L. Floridi (eds.). — Cham: Springer, 2024. — (Philosophical Studies Series). (Коллективная монография, посвященная риск-ориентированному подходу к регулированию ИИ в рамках EU AI Act. Анализируются критерии отнесения систем к высокорисковым, процедуры оценки соответствия, требования к системам и механизмы обеспечения комплаенса).

2. Кузнецов, П. У. Риск-ориентированный подход в правовом регулировании искусственного интеллекта // Российское право: образование, практика, наука. — 2025. — № 1. — С. 45–53. (Научная статья, анализирующая внедрение риск-ориентированного подхода в российское законодательство об искусственном интеллекте, критерии классификации рисков и механизмы правового воздействия в зависимости от уровня риска).

3. Разъяснения Евразийской экономической комиссии по вопросам регулирования обращения систем искусственного интеллекта на территории ЕАЭС (2025). (Позиции наднационального регулятора относительно гармонизации подходов к регулированию ИИ

в рамках Евразийского экономического союза, включая вопросы классификации рисков и взаимного признания оценок соответствия).

4. Доклады Центра регулирования ИИ Альянса в сфере искусственного интеллекта «Практика комплаенса высокорисковых ИИ-систем в России и за рубежом» (2025–2026). (Аналитические материалы, подготовленные на основе опыта российских компаний-разработчиков и международной практики, содержащие практические рекомендации по организации комплаенс-процедур, проведению оценки рисков и подготовке к регуляторным проверкам).

8.3. Нормативные правовые документы и иная правовая информация

Российская Федерация

1. Федеральный закон от 26.03.2025 № 57-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования отношений, связанных с использованием систем искусственного интеллекта, отнесенных к категории высокого риска». (Вступил в силу с 01.01.2026). (Базовый закон, вводящий категорию высокорисковых систем ИИ в российское законодательство. Устанавливает критерии отнесения систем ИИ к высокому риску, обязанности разработчиков и операторов таких систем, требования к документированию, тестированию и мониторингу, а также ответственность за нарушение установленных требований).
2. Постановление Правительства РФ от 15.10.2025 № 1789 «Об утверждении Правил классификации систем искусственного интеллекта по уровням риска и перечня высокорисковых систем искусственного интеллекта». (Подзаконный акт, конкретизирующий критерии отнесения систем ИИ к категории высокого риска, а также утверждающий исчерпывающий перечень областей применения и типов систем, признаваемых высокорисковыми).
3. Постановление Правительства РФ от 28.11.2025 № 2156 «Об утверждении требований к системам управления рисками при разработке и эксплуатации высокорисковых систем искусственного интеллекта и порядка проведения оценки соответствия таких систем». (Ключевой документ, устанавливающий детальные требования к организации системы управления рисками, включая идентификацию, анализ, оценку и минимизацию рисков, а также процедуры оценки соответствия (сертификации) высокорисковых ИИ-систем перед вводом в эксплуатацию).
4. Приказ Минцифры России от 20.12.2025 № 987 «Об утверждении форм документов, необходимых для регистрации высокорисковых систем искусственного интеллекта, и порядка ведения реестра высокорисковых систем искусственного интеллекта». (Ведомственный акт, устанавливающий процедуру регистрации высокорисковых ИИ-систем в специальном реестре, формы заявлений и перечень предоставляемых документов).
5. Приказ Росстандарта от 25.12.2025 № 1542-ст «Об утверждении национального стандарта Российской Федерации ГОСТ Р 71026-2025 «Системы искусственного интеллекта. Высокорисковые системы. Требования к управлению рисками». (Национальный стандарт, детализирующий технические и организационные требования к управлению рисками высокорисковых ИИ-систем, гармонизированный с международными подходами) .
6. Кодекс этики в сфере искусственного интеллекта (в ред. 2025 г.). (Обновленная версия документа, содержащая специальные положения о повышенных этических требованиях к разработке и применению высокорисковых систем ИИ, включая прозрачность, объяснимость и справедливость принимаемых решений) .
7. Проект федерального закона «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (в части установления ответственности за нарушение требований к разработке и эксплуатации высокорисковых систем искусственного интеллекта). (Законопроект, предусматривающий введение

административной ответственности для должностных и юридических лиц за нарушение требований, установленных Федеральным законом № 57-ФЗ и подзаконными актами).

Международное и зарубежное регулирование

1. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act, AI Act). (Первый в мире всеобъемлющий закон об ИИ, устанавливающий риск-ориентированный подход к регулированию на территории ЕС. Содержит детальную классификацию систем ИИ по уровням риска, специальные требования к высокорисковым системам, процедуры оценки соответствия, требования к прозрачности и системе управления рисками. С 2 февраля 2025 года вступили в силу запреты на отдельные виды практик; с 2 августа 2025 года начали применяться правила для моделей ИИ общего назначения; с 2 августа 2026 года начнут применяться основные требования к высокорисковым системам ИИ).
2. Commission Implementing Regulation (EU) 2025/728 of 12 March 2025 laying down detailed arrangements for the conformity assessment of high-risk AI systems pursuant to Regulation (EU) 2024/1689. (Имплементационный регламент ЕС, устанавливающий детальные процедуры оценки соответствия высокорисковых систем ИИ, включая требования к технической документации, процедурам тестирования и участию нотифицированных органов).
3. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). (Международный договор, устанавливающий общие принципы регулирования ИИ, включая требования к высокорисковым системам в части защиты прав человека, демократии и верховенства права).
4. ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system. (Международный стандарт, устанавливающий требования к системе менеджмента искусственного интеллекта, включая управление рисками, процессы оценки воздействия и комплаенс-процедуры. Может использоваться в качестве основы для построения системы управления рисками высокорисковых ИИ-систем).

8.4. Интернет-ресурсы

1. Официальный интернет-портал правовой информации (www.pravo.gov.ru).
2. СПС «КонсультантПлюс» (www.consultant.ru).
3. СПС «Гарант» (www.garant.ru).
4. Официальный сайт Министерства экономического развития РФ (www.economy.gov.ru). (Информация о реализации федерального проекта «Нормативное регулирование цифровой среды», включая разработку и внедрение механизмов регулирования высокорисковых систем ИИ).
5. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций РФ (digital.gov.ru). (Информация о государственной политике в сфере искусственного интеллекта, реестре высокорисковых систем ИИ, разъяснения по применению законодательства, проекты нормативных актов).
6. Сайт Альянса в сфере искусственного интеллекта (a-ai.ru). (Публикация актуальной редакции Кодекса этики в сфере ИИ, методические материалы по комплаенсу, аналитические доклады о практике применения законодательства, информация о саморегулировании отрасли).
7. Официальный портал Европейского Союза EUR-Lex (eur-lex.europa.eu). (Официальный источник для изучения полного текста EU AI Act и имплементационных регламентов на всех официальных языках ЕС).
8. Сайт Европейского совета по искусственному интеллекту (European Artificial Intelligence Board) (ai-board.europa.eu). (Официальный сайт наднационального органа, координирующего применение EU AI Act, публикующего руководства, разъяснения и рекомендации по применению законодательства, включая вопросы классификации высокорисковых систем).

9. Научная электронная библиотека eLIBRARY.RU (elibrary.ru). (Доступ к полным текстам статей из российских научных журналов по правовому регулированию искусственного интеллекта, комплаенсу и управлению рисками).
10. Профессиональные ресурсы по комплаенсу и регуляторике (comply.ru, regulation.gov.ru и аналогичные). (Площадки для отслеживания актуальных позиций регуляторов, разъяснений и практики применения законодательства о высокорисковых системах ИИ).

9. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

9.1. Материально-техническая база

Перечень материально-технического обеспечения:

1. Учебные аудитории, оборудованные для проведения учебных занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, коллоквиумов, мероприятий текущего контроля и промежуточной аттестации, в том числе мультимедийным оборудованием для демонстрации электронных презентаций и аудио- и видеоматериалов;
2. Компьютерные классы для выполнения групповых тестовых и иных заданий, а также для самостоятельной работы обучающихся оснащенные компьютерной техникой и обеспечением доступа к сети «Интернет» и доступа в электронную информационно- образовательную среду организации;
3. Специализированные аудитории и лаборатории;
4. Библиотека с обеспечением печатными изданиями или электронно-библиотечная система обеспечивающая доступ к электронным изданиям (электронная библиотека);
5. Читальный зал;
6. Технические средства обучения: персональные компьютеры; компьютерные проекторы; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV и др.

9.2. Информационные технологии, программное обеспечение:

При осуществлении образовательного процесса по дисциплине используется информационные технологии и программное обеспечение:

1. Современная операционная система.
2. Kaspersky Endpoint Security (или аналог).
3. Средство просмотра файлов формата pdf.
4. Современные офисные средства (текстовые и табличные редакторы, средстваработы с презентационными материалами и т.д.).
5. Архиватор 7-Zip.
6. Система дистанционного обучения.
7. Автоматизированная библиотечная система.

9.3. Информационные справочные системы:

1. https://www.iprbookshop.ru – Электронно-библиотечная система [ЭБС]«IPRSMART»(ранее–IPRBooks)
2. https://e.lanbook.com -Электронно-библиотечная система [ЭБС] «Лань».

3. https://znanium.ru - Электронно-библиотечная система [ЭБС] «Znanium.com».
4. https://www.book.ru - Электронно-библиотечная система[ЭБС]«Book.ru».
5. https://ibooks.ru-Электронно-библиотечная система [ЭБС]«ibooks.ru».
6. https://ranepalib.miflib.ru - Электронная библиотека издательства «МИФ».
7. https://eivis.ru–Ивис (EastView). Полные тексты российских научных и практических журналов, а также газет центральной прессы России. Доступ с ip-адресов локальной сети Института.
8. http://www.consultant.ru/-Справочно-правоваясистема «Консультант».
9. http://www.garant.ru/Справочно-правоваясистема «Гарант».