Лебедева Екатерина Александровна
Подписано цифровой подписью: Лебедева Екатерина Александровна
Дата: 2026.06.25 14:34:00 +03'00'

Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.02 Правовая диагностика (Due Diligence) ИИ-проектов и цифровых активов

(индекс, наименование дисциплины в соответствии с учебным планом)

40.04.01 "Юриспруденция"
(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.О.02 Правовая диагностика (Due Diligence) ИИ-проектов и цифровых активов» 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.О.02 Правовая диагностика (Due Diligence) ИИ-проектов и цифровых активов» 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**
	ОПК-1	Способен анализировать нестандартные ситуации правоприменительной практики и предлагать оптимальные варианты их решения	ИОПК-1.2	Квалифицирует юридическую природу новых цифровых активов (токены, модели ИИ, датасеты) и отношений, возникающих при их использовании	Знает: современные дискуссии в доктрине о правовой природе объектов, созданных с помощью ИИ, криптоактивов, цифровых прав; существующие и предлагаемые подходы к их регулированию. Умеет: анализировать фактические обстоятельства, связанные с использованием новых цифровых объектов, и подбирать к ним наиболее подходящие правовые конструкции; формулировать правовую квалификацию для целей Due Diligence.
	ОПК-7	Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности	ИОПК-7.1	Использует стратегии цифровой трансформации, информационные технологии и правовые базы данных, методы и инструменты управления процессами, проектами, продуктами цифровой трансформации для принятия правовых решений на основе стандартов правомерного поведения в информационной и цифровой среде	Знает: основы информационной безопасности, функционал правовых систем (Консультант+, Гарант), инструменты цифровой трансформации в юридической практике, включая Legal Tech. Умеет: использовать правовые базы данных для поиска информации, применять цифровые инструменты в профессиональной деятельности при проведении Due Diligence, обеспечивать защиту данных при работе с виртуальными комнатами данных (Data Room).

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

Общая трудоемкость дисциплины составляет 180 а.ч. (5 з.е.)
Количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся: лекции – 14 а.ч., практические занятия – 42 а.ч., самостоятельная работа – 95 а.ч., контактная работа на аттестацию в период экзаменационных сессий – 9 часов, самостоятельная работа на подготовку к экзамену – 18 часов.

Дисциплина *«Б1.О.02 Правовая диагностика (Due Diligence) ИИ-проектов и цифровых активов»* относится к дисциплинам обязательной части. Изучается на очной форме обучения - на 2 курсе в 3 семестре.

Для освоения дисциплины «*Б1.О.02 Правовая диагностика (Due Diligence) ИИ-проектов и цифровых активов»* обучающиеся используют знания, умения, навыки, способы деятельности и установки, сформированные в ходе изучения дисциплин *«Информационное право» и «Информационные технологии в юридической деятельности»*.

Форма промежуточной аттестации в соответствии с учебным планом – экзамен.

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.	Понятие и цели Due Diligence в сфере ИИ и цифровых активов	10	1	0	0	2	0	0	0	0		0	1	6	Устный опрос, Ситуационная задача
Тема 2.	Объекты правовой диагностики: классификация и особенности	11	1	0	0	3	0	0	0	0		0	1	6	Устный опрос, Ситуационная задача
Тема 3.	Процесс и стадии проведения DD	11	1	0	0	3	0	0	0	0		0	1	6	Устный опрос, Ситуационная задача

Тема 4.	Юрисдикционные аспекты проверки	11	1	0	0	3	0	0	0	0	0	1	6	Устный опрос, Ситуационная задача
Тема 5.	Проверка прав на программный код и архитектуру	10	0	0	0	3	0	0	0	0	0	1	6	Устный опрос, Ситуационная задача
Тема 6.	Правовая экспертиза обучающих данных (датасетов)	11	1	0	0	3	0	0	0	0	0	1	6	Устный опрос, Ситуационная задача
Тема 7.	Средства индивидуализации и доменные имена	10	0	0	0	3	0	0	0	0	0	1	6	Устный опрос, Ситуационная задача
Тема 8.	Коммерческая тайна и ноу-хау (секреты производства)	11	1	0	0	3	0	0	0	0	0	1	6	Устный опрос, Ситуационная задача
Тема 9.	Соответствие законодательству о персональных данных (152-ФЗ)	11	1	0	0	3	0	0	0	0	0	1	6	Устный опрос, Ситуационная задача
Тема 10.	Регулирование в сфере ИИ (ФЗ об ЭПР, стандартизация, этика)	11	1	0	0	3	0	0	0	0	0	1	6	Устный опрос, Ситуационная задача
Тема 11.	Ответственность за контент, сгенерированный ИИ	12	1	0	0	3	0	0	0	0	0	1	7	
Тема 12.	Проверка договорной базы и корпоративной структуры	12	1	0	0	3	0	0	0	0	0	1	7	
Тема 13.	Налоговые риски структурирования сделки и активов	13	1	0	0	3	0	0	0	0	0	2	7	
Тема 14.	Оценка активов и механизмы защиты цены	13	1	0	0	3	0	0	0	0	0	2	7	

Тема 15.	Комплексный анализ ИИ-стартапа	14	2	0	0	3	0	0	0	0	0	2	7	
Промежуточная аттестация		29							2	9		18		Экзамен
Итого		180	14	0	0	42	0	0	2	9	0	18	95	

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

Модуль 1. Введение в правовую диагностику объектов новых технологий

Тема 1. Понятие и цели Due Diligence в сфере ИИ и цифровых активов. ОПК-1

1. В чем принципиальное отличие DD ИИ-проекта от классической юридической проверки "традиционного" бизнеса (акцент на нематериальные активы и регуляторные риски)?
2. Какие цели преследуют стороны сделки (инвестор, стратегический покупатель, стартап) при проведении правовой диагностики технологической компании?
3. Кто является основными участниками процесса и какие роли они выполняют (технические специалисты, юристы, аудиторы)?
4. На каких этапах жизненного цикла ИИ-проекта (посевная, венчурная стадия, exit) требуется проведение Due Diligence?

Тема 2. Объекты правовой диагностики: классификация и особенности. ОПК-7

1. Что входит в понятие "цифровые активы" в контексте DD (криптовалюта, токены, доменные имена, базы данных)?
2. В чем специфика проверки ИИ-продукта как объекта: проверка кода, обученной модели, датасетов, архитектуры?
3. Как различаются подходы к проверке "коробочного" ПО, облачного сервиса (SaaS) и открытого кода (Open Source)?
4. Почему стартап на стадии MVP (Minimum Viable Product) требует иной глубины проверки, чем зрелая ИИ-платформа?

Тема 3. Процесс и стадии проведения DD. ОПК-1

1. Какова стандартная процедура сделки: от подписания соглашения о конфиденциальности (NDA) до закрытия сделки?
2. Что такое "виртуальная комната данных" (Data Room) и какие требования предъявляются к организации документооборота?
3. Как формируется запрос на предоставление документов (чек-лист) с учетом специфики ИИ-активов?
4. Какова структура итогового отчета (Legal Report) и что такое "disclosure letter" (письмо о раскрытии информации)?

Тема 4. Юрисдикционные аспекты проверки. ОПК-7

1. Как выбрать применимое право при трансграничных сделках с цифровыми активами?
2. Каковы особенности проверки компаний, зарегистрированных в иностранных юрисдикциях (offshore), но ведущих бизнес в РФ?
3. Как координация работы юристов в нескольких юрисдикциях влияет на полноту и достоверность выводов DD?
4. В каких случаях требуется получение согласия антимонопольных органов (ФАС) и как это влияет на структурирование сделки?

Модуль 2. Юридическая проверка интеллектуальной собственности и кода

Тема 5. Проверка прав на программный код и архитектуру. ОПК-1

1. Как проверить титул прав на код, созданный разработчиками (по договору подряда/ГПХ) и установить отсутствие притязаний со стороны бывших работников?

2. Какие риски несет использование открытых библиотек с "вирусными" лицензиями (GPL, AGPL) в коммерческом продукте?
3. Как проверить действительность отчуждения исключительного права и отсутствие обременений (залог, спор о праве)?
4. Что делать, если код не депонирован или документация (техническая документация) отсутствует?

Тема 6. Правовая экспертиза обучающих данных (датасетов). ОПК-7

Как проверить законность сбора данных для обучения модели: было ли получено согласие субъектов персональных данных?

1. Какие риски связаны с использованием "публично доступных" данных (например, из соцсетей) и существуют ли исключения для text and data mining (TDM)?
2. Как проверить права на контент внутри датасета (объекты авторского права, базы данных) и не нарушают ли они права третьих лиц?
3. Что такое анонимизация и обезличивание данных, и достаточно ли этого для минимизации рисков?

Тема 7. Средства индивидуализации и доменные имена. ОПК-7

1. Как проверить, не нарушает ли название продукта или компании (товарный знак) права третьих лиц (проведение патентно-информационного поиска)?
2. В чем особенности проверки прав на доменное имя, соответствующее товарному знаку?
3. Как оценить риски блокировки сайта или мобильного приложения как актива?
4. Кто является надлежащим правообладателем и не истек ли срок охраны?

Тема 8. Коммерческая тайна и ноу-хау (секреты производства). ОПК-1

1. Введен ли в компании режим коммерческой тайны? Как проверить наличие локальных актов, журналов ознакомления и допуска?
2. Какие риски утечки данных существуют при использовании облачных нейросетей сотрудниками (например, внесение кода в ChatGPT)?
3. Как защищены алгоритмы и архитектура нейросети, если они не патентуются?
4. Что делать с конфиденциальной информацией, которая раскрывается потенциальному инвестору в ходе DD?

Модуль 3. Регуляторный комплаенс и риски ИИ-проектов

Тема 9. Соответствие законодательству о персональных данных (152-ФЗ). ОПК-7

1. Есть ли у компании правовое основание для обработки персональных данных? Получено ли согласие и соответствует ли оно принципам конкретности и информированности?
2. Соблюдается ли требование о локализации баз данных на территории РФ?
3. Не является ли использование иностранной нейросети (например, OpenAI) трансграничной передачей данных и получено ли на это разрешение (РКН)?
4. Какие штрафы и риски блокировки деятельности (ст. 13.11 КоАП, ст. 272.1 УК РФ) существуют за выявленные нарушения?

Тема 10. Регулирование в сфере ИИ (ФЗ об ЭПР, стандартизация, этика). ОПК-1

1. Подпадает ли ИИ-продукт под экспериментальный правовой режим (ЭПР) и какие обязательства это налагает?

2. Как проверить соблюдение требований к системам ИИ (например, ГОСТы или рекомендации в области безопасности)?
3. Разработан ли в компании кодекс этики ИИ и соблюдаются ли Национальный кодекс этики ИИ?
4. Существуют ли риски, связанные с дискриминацией (bias) в работе модели, и как они могут быть оспорены пользователями?

Тема 11. Ответственность за контент, сгенерированный ИИ. ОПК-1

1. Кто несет ответственность за "галлюцинации" нейросети, если они причинили вред (администратор, разработчик, пользователь)?
2. Как квалифицируется дипфейк с точки зрения законодательства об информации и персональных данных?
3. Должна ли компания маркировать контент, созданный ИИ (принцип прозрачности)?
4. Можно ли использовать сгенерированные тексты в качестве доказательств в суде? Какова доказательственная сила таких материалов?

Тема 12. Проверка договорной базы и корпоративной структуры. ОПК-7

1. Соответствуют ли лицензионные договоры (EULA) с пользователями законодательству и специфике продукта?
2. Есть ли действующие договоры с контрагентами (хостинг, облачные провайдеры, подрядчики)?
3. Как проверяется корпоративная структура стартапа: есть ли корпоративные договоры, опционные программы для сотрудников, "чистая" доля основателя?
4. Существуют ли риски, связанные с "грязным" финансированием или непрозрачной структурой владения?

Модуль 4. Финансово-правовые аспекты и налогообложение

Тема 13. Налоговые риски структурирования сделки и активов. ОПК-1

1. Как форма сделки (покупка доли, покупка активов, реорганизация) влияет на налоговые последствия?
2. Какие существуют риски доначисления налогов при использовании "упрощенки" (УСН) IT-компанией?
3. Как учитываются для налогообложения операции с криптовалютой и токенами?
4. Какие льготы для IT-компаний (страховые взносы, налог на прибыль) применяются и не потеряет ли их покупатель после сделки?

Тема 14. Оценка активов и механизмы защиты цены. ОПК-7

1. Как коррелируют выводы юридической проверки с оценкой стоимости бизнеса?
2. Что такое механизмы "earn-out" (отложенное вознаграждение) и "escrow" (счет эскроу) и как они защищают покупателя?
3. Какие заверения и гарантии (representations and warranties) продавца должны быть включены в договор для покрытия юридических рисков?
4. Что такое "существенное изменение обстоятельств" (Material Adverse Change) и как оно применяется в IT-сделках?

Модуль 5. Итоговый практикум (кейс-стади)

Тема 15. Комплексный анализ ИИ-стартапа. ОПК-1

1. Провести экспресс-анализ предоставленного пакета документов условного стартапа (устав, договоры с разработчиками, политика обработки ПД, ссылки на GitHub).
2. Какие "красные флаги" (риски) выявлены в части IP и персональных данных?
3. Как структурировать сделку (покупка доли или активов), чтобы минимизировать эти риски?
4. Какие пункты договора купли-продажи (заверения, indemnity) необходимы для защиты покупателя?

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине «Б1.О.02 Правовая диагностика (Due Diligence) ИИ-проектов и цифровых активов» 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.О.02 Правовая диагностика (Due Diligence) ИИ-проектов и цифровых активов» 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):

Раздел 1. Теоретико-правовые основы реагирования на инциденты

Модуль 1. Введение в правовую диагностику объектов новых технологий

Тема 1. Понятие и цели Due Diligence в сфере ИИ и цифровых активов. ОПК-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. В чем принципиальное отличие DD ИИ-проекта от классической юридической проверки "традиционного" бизнеса (акцент на нематериальные активы и регуляторные риски)?
2. Какие цели преследуют стороны сделки (инвестор, стратегический покупатель, стартап) при проведении правовой диагностики технологической компании?
3. Кто является основными участниками процесса и какие роли они выполняют (технические специалисты, юристы, аудиторы)?
4. На каких этапах жизненного цикла ИИ-проекта (посевная, венчурная стадия, exit) требуется проведение Due Diligence?

Ситуационные задачи.

Задание 1

Инвестор проверяет ИИ-стартап, который разрабатывает нейросеть для анализа медицинских снимков. В ходе DD выяснено, что компания не имеет патентов, но код обученной модели хранится в закрытом репозитории. Классический юрист настаивает на отсутствии «осязаемых активов».

Вопрос: в чем принципиальное отличие DD ИИ-проекта от классического DD с точки зрения оценки нематериальных активов?

Задание 2

Стартап на стадии Seed ищет инвестиции. Основатели предлагают провести полный DD, аналогичный сделке по покупке зрелой платформы.

Вопрос: на каком этапе жизненного цикла ИИ-проекта целесообразно проводить углубленный DD, а где достаточно экспресс-проверки?

Тема 2. Объекты правовой диагностики: классификация и особенности. ОПК-7

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. Что входит в понятие "цифровые активы" в контексте DD (криптовалюта, токены, доменные имена, базы данных)?

2. В чем специфика проверки ИИ-продукта как объекта: проверка кода, обученной модели, датасетов, архитектуры?

3. Как различаются подходы к проверке "коробочного" ПО, облачного сервиса (SaaS) и открытого кода (Open Source)?

4. Почему стартап на стадии MVP (Minimum Viable Product) требует иной глубины проверки, чем зрелая ИИ-платформа?

Ситуационные задачи.

Задание 1

Стартап использует датасет, собранный из открытых соцсетей, и обученную модель, работающую в облаке AWS.

Вопрос: какие три типа цифровых активов подлежат проверке в рамках DD?

Задание 2

Продукт — коробочное ПО с использованием библиотеки Open Source под лицензией AGPL.

Вопрос: почему для «коробочного» ПО риски и глубина проверки иные, чем для SaaS?

Тема 3. Процесс и стадии проведения DD. ОПК-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. Какова стандартная процедура сделки: от подписания соглашения о конфиденциальности (NDA) до закрытия сделки?
2. Что такое "виртуальная комната данных" (Data Room) и какие требования предъявляются к организации документооборота?

3. Как формируется запрос на предоставление документов (чек-лист) с учетом специфики ИИ-активов?
4. Какова структура итогового отчета (Legal Report) и что такое "disclosure letter" (письмо о раскрытии информации)?

Ситуационные задачи.

Задание 1
Виртуальная комната данных (Data Room) содержит только финансовую отчетность. Юрист запрашивает договоры с разработчиками и политику обработки ПД.
Вопрос: какие требования к организации документооборота нарушены?

Задание 2
После закрытия сделки покупатель обнаружил, что стартап использовал данные с нарушением 152-ФЗ. В disclosure letter это указано не было.
Вопрос: каково правовое значение disclosure letter?

Тема 4. Юрисдикционные аспекты проверки. ОПК-7

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. Как выбрать применимое право при трансграничных сделках с цифровыми активами?
2. Каковы особенности проверки компаний, зарегистрированных в иностранных юрисдикциях (offshore), но ведущих бизнес в РФ?
3. Как координация работы юристов в нескольких юрисдикциях влияет на полноту и достоверность выводов DD?
4. В каких случаях требуется получение согласия антимонопольных органов (ФАС) и как это влияет на структурирование сделки?

Ситуационные задачи.

Задание 1
Стартап зарегистрирован на Кипре, команда в РФ, сервера в Нидерландах, пользователи из РФ.
Вопрос: как выбрать применимое право к договору купли-продажи доли?

Задание 2
Покупка ИИ-сервиса, который занимает более 30% рынка в РФ. Сделка структурирована как покупка активов.
Вопрос: требуется ли согласие ФАС и как это влияет на структурирование?

Модуль 2. Юридическая проверка интеллектуальной собственности и кода

Тема 5. Проверка прав на программный код и архитектуру. ОПК-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. Как проверить титул прав на код, созданный разработчиками (по договору подряда/ГПХ) и установить отсутствие притязаний со стороны бывших работников?
2. Какие риски несет использование открытых библиотек с «вирусными» лицензиями (GPL, AGPL) в коммерческом продукте?
3. Как проверить действительность отчуждения исключительного права и отсутствие обременений (залог, спор о праве)?
4. Что делать, если код не депонирован или документация (техническая документация) отсутствует?

Ситуационные задачи:

Задание 1
Код писал фрилансер по договору ГПХ, в котором указано: «результат интеллектуальной деятельности принадлежит заказчику».
Вопрос: достаточен ли этот пункт для перехода исключительного права?

Задание 2
В продукте используется библиотека с лицензией GPL. Код продукта не открыт.
Вопрос: какие риски и как их минимизировать?

Тема 6. Правовая экспертиза обучающих данных (датасетов). ОПК-7

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. Как проверить законность сбора данных для обучения модели: было ли получено согласие субъектов персональных данных?
2. Какие риски связаны с использованием "публично доступных" данных (например, из соцсетей) и существуют ли исключения для text and data mining (TDM)?
3. Как проверить права на контент внутри датасета (объекты авторского права, базы данных) и не нарушают ли они права третьих лиц?
4. Что такое анонимизация и обезличивание данных, и достаточно ли этого для минимизации рисков?

Ситуационные задачи.

Задание 1

Для обучения ИИ использовались фото из Instagram без согласия пользователей. *Вопрос: законен ли сбор?*

Задание 2

Стартап утверждает, что обезличил данные перед обучением.
Вопрос: достаточно ли этого для минимизации рисков?

Тема 7. Средства индивидуализации и доменные имена. ОПК-7

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. Как проверить, не нарушает ли название продукта или компании (товарный знак) права третьих лиц (проведение патентно-информационного поиска)?

2. В чем особенности проверки прав на доменное имя, соответствующее товарному знаку?
3. Как оценить риски блокировки сайта или мобильного приложения как актива?
4. Кто является надлежащим правообладателем и не истек ли срок охраны?

Ситуационные задачи.

Задание 1
Название ИИ-продукта — «NeuroDoc». Проверка по базе ФИПС показала, что товарный знак «NeuroDoc» зарегистрирован на третье лицо в 10 классе МКТУ.
Вопрос: какие риски и действия?

Задание 2
Домен neurodoc.ru зарегистрирован на физлицо, которое не является разработчиком, но готов его продать.
Вопрос: как проверить права на домен и риски его блокировки?

Тема 8. Коммерческая тайна и ноу-хау (секреты производства). ОПК-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. Введен ли в компании режим коммерческой тайны? Как проверить наличие локальных актов, журналов ознакомления и допуска?
2. Какие риски утечки данных существуют при использовании облачных нейросетей сотрудниками (например, внесение кода в ChatGPT)?
3. Как защищены алгоритмы и архитектура нейросети, если они не патентуются?
4. Что делать с конфиденциальной информацией, которая раскрывается потенциальному инвестору в ходе DD?

Ситуационные задачи.

Задание 1
Сотрудник загрузил код нейросети в ChatGPT для отладки.
Вопрос: нарушен ли режим коммерческой тайны?

Задание 2
В компании нет локальных актов о коммерческой тайне, но алгоритм нигде не раскрыт.
Вопрос: можно ли защитить алгоритм как ноу-хау?

Модуль 3. Регуляторный комплаенс и риски ИИ-проектов

Тема 9. Соответствие законодательству о персональных данных (152-ФЗ). ОПК-7

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. Есть ли у компании правовое основание для обработки персональных данных? Получено ли согласие и соответствует ли оно принципам конкретности и информированности?
2. Соблюдается ли требование о локализации баз данных на территории РФ?
3. Не является ли использование иностранной нейросети (например, OpenAI) трансграничной передачей данных и получено ли на это разрешение (РКН)?
4. Какие штрафы и риски блокировки деятельности (ст. 13.11 КоАП, ст. 272.1 УК РФ) существуют за выявленные нарушения?

Ситуационные задачи.

Задание 1

Сервер с ПД пользователей из РФ расположен в Германии. Согласия на трансграничную передачу нет.

Вопрос: нарушена ли локализация и что грозит?

Задание 2

Пользователь подписал согласие на обработку ПД, но через год отозвал его. Модель уже обучена.

Вопрос: обязан ли стартап удалить данные из датасета?

Тема 10. Регулирование в сфере ИИ (ФЗ об ЭПР, стандартизация, этика). ОПК-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. Подпадает ли ИИ-продукт под экспериментальный правовой режим (ЭПР) и какие обязательства это налагает?
2. Как проверить соблюдение требований к системам ИИ (например, ГОСТы или рекомендации в области безопасности)?
3. Разработан ли в компании кодекс этики ИИ и соблюдаются ли Национальный кодекс этики ИИ?
4. Существуют ли риски, связанные с дискриминацией (bias) в работе модели, и как они могут быть оспорены пользователями?

Ситуационные задачи.
Задание 1
ИИ-продукт диагностирует сердечные заболевания без участия врача. *Вопрос: нужен ли ЭПР и какие обязательства?*

Задание 2
Модель отказывает женщинам в выдаче кредита чаще, чем мужчинам. *Вопрос: какой риск и как проверяется?*

Тема 11. Ответственность за контент, сгенерированный ИИ. ОПК-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. Кто несет ответственность за "галлюцинации" нейросети, если они причинили вред (администратор, разработчик, пользователь)?
2. Как квалифицируется дипфейк с точки зрения законодательства об информации и персональных данных?
3. Должна ли компания маркировать контент, созданный ИИ (принцип прозрачности)?
4. Можно ли использовать сгенерированные тексты в качестве доказательств в суде? Какова доказательственная сила таких материалов?

Ситуационные задачи.
Задание 1
Нейросеть сгенерировала дипфейк-видео с лицом известного политика без его согласия. *Вопрос: кто отвечает — разработчик или пользователь?*

Задание 2
Сгенерированный текст содержит клевету на третье лицо. Суд требует предоставить исходные данные.

Вопрос: можно ли использовать сгенерированный текст как доказательство?

Тема 12. Проверка договорной базы и корпоративной структуры. ОПК-7

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. Соответствуют ли лицензионные договоры (EULA) с пользователями законодательству и специфике продукта?
2. Есть ли действующие договоры с контрагентами (хостинг, облачные провайдеры, подрядчики)?
3. Как проверяется корпоративная структура стартапа: есть ли корпоративные договоры, опционные программы для сотрудников, "чистая" доля основателя?
4. Существуют ли риски, связанные с "грязным" финансированием или непрозрачной структурой владения?

Ситуационные задачи.

Задание 1

EULA запрещает пользователю использовать ИИ для медицинских консультаций, но пользователь нарушил запрет.

Вопрос: как проверяется EULA на соответствие рискам?

Задание 2

Основатель обещал разработчикам 10% доли в стартапе устно. В уставе это не отражено.

Вопрос: как проверяется опционная программа?

Модуль 4. Финансово-правовые аспекты и налогообложение

Тема 13. Налоговые риски структурирования сделки и активов. ОПК-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. Как форма сделки (покупка доли, покупка активов, реорганизация) влияет на налоговые последствия?
2. Какие существуют риски доначисления налогов при использовании "упрощенки" (УСН) IT-компанией?
3. Как учитываются для налогообложения операции с криптовалютой и токенами?
4. Какие льготы для IT-компаний (страховые взносы, налог на прибыль) применяются и не потеряет ли их покупатель после сделки?

Ситуационные задачи.
Задание 1
Покупатель хочет приобрести только обученную модель и датасет, не принимая долги стартапа.
Вопрос: покупка доли или активов — что выгоднее с точки зрения налоговых рисков?

Задание 2
Стартап на УСН «доходы минус расходы» продал токены за криптовалюту.
Вопрос: признается ли это доходом и какие риски?

Тема 14. Оценка активов и механизмы защиты цены. ОПК-7

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. Как коррелируют выводы юридической проверки с оценкой стоимости бизнеса?
2. Что такое механизмы «earn-out» (отложенное вознаграждение) и «escrow» (счет эскроу) и как они защищают покупателя?
3. Какие заверения и гарантии (representations and warranties) продавца должны быть включены в договор для покрытия юридических рисков?
4. Что такое «существенное изменение обстоятельств» (Material Adverse Change) и как оно применяется в IT-сделках?

Ситуационные задачи.
Задание 1
Покупатель опасается, что после сделки выяснится нарушение авторских прав в коде.
Вопрос: какие заверения и гарантии должны быть в договоре?

Задание 2

После подписания договора, но до closing, у модели обнаружилась системная ошибка, снижающая точность с 95% до 60%.
Вопрос: применяется ли MAC (Material Adverse Change)?

Модуль 5. Итоговый практикум (кейс-стади)

Тема 15. Комплексный анализ ИИ-стартапа. ОПК-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. Провести экспресс-анализ предоставленного пакета документов условного стартапа (устав, договоры с разработчиками, политика обработки ПД, ссылки на GitHub).
2. Какие «красные флаги» (риски) выявлены в части IP и персональных данных?
3. Как структурировать сделку (покупка доли или активов), чтобы минимизировать эти риски?
4. Какие пункты договора купли-продажи (заверения, indemnity) необходимы для защиты покупателя?

Ситуационные задачи.
Задание 1
Выявлено:
- код написан фрилансером (договор ГПХ без отчуждения прав);
- датасет — фото из Instagram;
- сервер в AWS, согласий на ТПД нет;
-товарный знак не проверялся.
Вопрос: какие «красные флаги» и как структурировать сделку?

Задание 2
Покупатель хочет защититься от риска утечки кода после сделки.
Вопрос: какие пункты договора купли-продажи необходимы?

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	0,3	30
КТ 2	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 1-15.

Доклад.

Тематика докладов:

1. Отличие DD ИИ-проекта от классической юридической проверки «традиционного» бизнеса (акцент на нематериальные активы и регуляторные риски).
2. Цели сторон сделки (инвестор, стратегический покупатель, стартап) при проведении правовой диагностики технологической компании.
3. Основные участники процесса и их роли (технические специалисты, юристы, аудиторы).
4. Этапы жизненного цикла ИИ-проекта (посевная, венчурная стадия, exit), на которых требуется проведение Due Diligence.
5. Содержание понятия «цифровые активы» в контексте DD (криптовалюта, токены, доменные имена, базы данных.
6. Специфика проверки ИИ-продукта как объекта: проверка кода, обученной модели, датасетов, архитектуры.
7. Различия подходов к проверке «коробочного» ПО, облачного сервиса (SaaS) и открытого кода (Open Source).
8. Почему стартап на стадии MVP (Minimum Viable Product) требует иной глубины проверки, чем зрелая ИИ-платформа?
9. Стандартная процедура сделки: от подписания соглашения о конфиденциальности (NDA) до закрытия сделки.
10. «Виртуальная комната данных» (Data Room) и требования, предъявляемые к организации документооборота.
11. Формирование запроса на предоставление документов (чек-лист) с учетом специфики ИИ-активов.
12. Структура итогового отчета (Legal Report) и суть "disclosure letter" (письмо о раскрытии информации).
13. Выбор применимого права при трансграничных сделках с цифровыми активами.

14. Особенности проверки компаний, зарегистрированных в иностранных юрисдикциях (offshore), но ведущих бизнес в РФ.
15. Влияние координации работы юристов в нескольких юрисдикциях на полноту и достоверность выводов DD.
16. Случаи, когда требуется получение согласия антимонопольных органов (ФАС) и как это влияет на структурирование сделки.
17. Проверка титула прав на код, созданный разработчиками (по договору подряда/ГПХ) и установление отсутствия притязаний со стороны бывших работников.
18. Риски использования открытых библиотек с «вирусными» лицензиями (GPL, AGPL) в коммерческом продукте.
19. Проверка действительности отчуждения исключительного права и отсутствия обременений (залог, спор о праве).
20. Порядок действий в случае, если код не депонирован или документация (техническая документация) отсутствует.
21. Проверка законности сбора данных для обучения модели: было ли получено согласие субъектов персональных данных.
22. Риски, связанные с использованием «публично доступных» данных (например, из соцсетей) и допустимость исключения для text and data mining (TDM).
23. Проверка права на контент внутри датасета (объекты авторского права, базы данных) и не нарушают ли они права третьих лиц.
24. Понятия «анонимизации» и «обезличивания» данных, и их достаточность для минимизации рисков.
25. Порядок проверки того, не нарушает ли название продукта или компании (товарный знак) права третьих лиц, включая проведение патентно-информационного поиска.
26. Особенности проверки прав на доменное имя, соответствующее товарному знаку.
27. Оценка рисков блокировки сайта или мобильного приложения как актива.
28. Определение надлежащего правообладателя и проверка срока действия охраны.
29. Наличие в компании режима коммерческой тайны и порядок проверки локальных актов, журналов ознакомления и допуска.
30. Риски утечки данных при использовании облачных нейросетей сотрудниками (на примере внесения кода в ChatGPT).
31. Способы защиты алгоритмов и архитектуры нейросети в случае, если они не патентуются.
32. Порядок работы с конфиденциальной информацией, раскрываемой потенциальному инвестору в ходе Due Diligence.
33. Правовые основания для обработки персональных данных: требования к согласию, его конкретности и информированности.
34. Соблюдение требования о локализации баз данных на территории РФ.
35. Квалификация использования иностранной нейросети (например, OpenAI) как трансграничной передачи данных и необходимость разрешения РКН.
36. Штрафы и риски блокировки деятельности (ст. 13.11 КоАП, ст. 272.1 УК РФ) за выявленные нарушения.
37. Подпадание ИИ-продукта под экспериментальный правовой режим (ЭПР) и обязательства, которые это налагает.
38. Порядок проверки соблюдения требований к системам ИИ (ГОСТы, рекомендации в области безопасности).
39. Наличие в компании кодекса этики ИИ и соблюдение Национального кодекса этики ИИ.
40. Риски, связанные с дискриминацией (bias) в работе модели, и возможности их оспаривания пользователями.

41. Ответственность за «галлюцинации» нейросети, причинившие вред (администратор, разработчик, пользователь).
42. Квалификация дипфейка с точки зрения законодательства об информации и персональных данных.
43. Обязанность компании маркировать контент, созданный ИИ (принцип прозрачности).
44. Возможность использования сгенерированных текстов в качестве доказательств в суде и их доказательственная сила.
45. Соответствие лицензионных договоров (EULA) с пользователями законодательству и специфике продукта.
46. Наличие действующих договоров с контрагентами (хостинг, облачные провайдеры, подрядчики).
47. Порядок проверки корпоративной структуры стартапа: корпоративные договоры, опционные программы для сотрудников, «чистая» доля основателя.
48. Риски, связанные с «грязным» финансированием или непрозрачной структурой владения.
49. Влияние формы сделки (покупка доли, покупка активов, реорганизация) на налоговые последствия.
50. Риски доначисления налогов при использовании «упрощенки» (УСН) IT-компанией.
51. Порядок учета для налогообложения операций с криптовалютой и токенами.
52. Льготы для IT-компаний (страховые взносы, налог на прибыль) и риски их утраты покупателем после сделки.
53. Корреляция выводов юридической проверки с оценкой стоимости бизнеса.
54. Механизмы «earn-out» (отложенное вознаграждение) и «escrow» (счет эскроу) как способы защиты покупателя.
55. Заверения и гарантии (representations and warranties) продавца, которые должны быть включены в договор для покрытия юридических рисков.
56. Понятие «существенное изменение обстоятельств» (Material Adverse Change) и порядок его применения в IT-сделках.
57. Экспресс-анализ предоставленного пакета документов условного стартапа (устав, договоры с разработчиками, политика обработки ПД, ссылки на GitHub).
58. «Красные флаги» (риски) в части интеллектуальной собственности и персональных данных.
59. Способы структурирования сделки (покупка доли или активов) для минимизации выявленных рисков.
60. Пункты договора купли-продажи (заверения, indemnity), необходимые для защиты покупателя.

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 1-15

Устный опрос:

Вопросы для опроса:

№ п.п.	Содержание вопроса
1.	Отличие DD ИИ-проекта от классической юридической проверки «традиционного» бизнеса (акцент на нематериальные активы и регуляторные риски).
2.	Цели сторон сделки (инвестор, стратегический покупатель, стартап) при проведении правовой диагностики технологической компании.

3.	Основные участники процесса и их роли (технические специалисты, юристы, аудиторы).
4.	Этапы жизненного цикла ИИ-проекта (посевная, венчурная стадия, exit), на которых требуется проведение Due Diligence.
5.	Содержание понятия «цифровые активы» в контексте DD (криптовалюта, токены, доменные имена, базы данных.
6.	Специфика проверки ИИ-продукта как объекта: проверка кода, обученной модели, датасетов, архитектуры.
7.	Различия подходов к проверке «коробочного» ПО, облачного сервиса (SaaS) и открытого кода (Open Source).
8.	Почему стартап на стадии MVP (Minimum Viable Product) требует иной глубины проверки, чем зрелая ИИ-платформа?
9.	Стандартная процедура сделки: от подписания соглашения о конфиденциальности (NDA) до закрытия сделки.
10.	«Виртуальная комната данных» (Data Room) и требования, предъявляемые к организации документооборота.
11.	Формирование запроса на предоставление документов (чек-лист) с учетом специфики ИИ-активов.
12.	Структура итогового отчета (Legal Report) и суть "disclosure letter" (письмо о раскрытии информации).
13.	Выбор применимого права при трансграничных сделках с цифровыми активами.
14.	Особенности проверки компаний, зарегистрированных в иностранных юрисдикциях (offshore), но ведущих бизнес в РФ.
15.	Влияние координации работы юристов в нескольких юрисдикциях на полноту и достоверность выводов DD.
16.	Случаи, когда требуется получение согласия антимонопольных органов (ФАС) и как это влияет на структурирование сделки.
17.	Проверка титула прав на код, созданный разработчиками (по договору подряда/ГПХ) и установление отсутствия притязаний со стороны бывших работников.
18.	Риски использования открытых библиотек с «вирусными» лицензиями (GPL, AGPL) в коммерческом продукте.
19.	Проверка действительности отчуждения исключительного права и отсутствия обременений (залог, спор о праве).
20.	Порядок действий в случае, если код не депонирован или документация (техническая документация) отсутствует.
21.	Проверка законности сбора данных для обучения модели: было ли получено согласие субъектов персональных данных.
22.	Риски, связанные с использованием «публично доступных» данных (например, из соцсетей) и допустимость исключения для text and data mining (TDM).
23.	Проверка права на контент внутри датасета (объекты авторского права, базы данных) и не нарушают ли они права третьих лиц.
24.	Понятия «анонимизации» и «обезличивания» данных, и их достаточность для минимизации рисков.
25.	Порядок проверки того, не нарушает ли название продукта или компании (товарный знак) права третьих лиц, включая проведение патентно-информационного поиска.
26.	Особенности проверки прав на доменное имя, соответствующее товарному знаку.
27.	Оценка рисков блокировки сайта или мобильного приложения как актива.
28.	Определение надлежащего правообладателя и проверка срока действия охраны.
29.	Наличие в компании режима коммерческой тайны и порядок проверки

	локальных актов, журналов ознакомления и допуска.
30.	Риски утечки данных при использовании облачных нейросетей сотрудниками (на примере внесения кода в ChatGPT).
31.	Способы защиты алгоритмов и архитектуры нейросети в случае, если они не патентуются.
32.	Порядок работы с конфиденциальной информацией, раскрываемой потенциальному инвестору в ходе Due Diligence.
33.	Правовые основания для обработки персональных данных: требования к согласию, его конкретности и информированности.
34.	Соблюдение требования о локализации баз данных на территории РФ.
35.	Квалификация использования иностранной нейросети (например, OpenAI) как трансграничной передачи данных и необходимость разрешения РКН.
36.	Штрафы и риски блокировки деятельности (ст. 13.11 КоАП, ст. 272.1 УК РФ) за выявленные нарушения.
37.	Подпадание ИИ-продукта под экспериментальный правовой режим (ЭПР) и обязательства, которые это налагает.
38.	Порядок проверки соблюдения требований к системам ИИ (ГОСТы, рекомендации в области безопасности).
39.	Наличие в компании кодекса этики ИИ и соблюдение Национального кодекса этики ИИ.
40.	Риски, связанные с дискриминацией (bias) в работе модели, и возможности их оспаривания пользователями.
41.	Ответственность за «галлюцинации» нейросети, причинившие вред (администратор, разработчик, пользователь).
42.	Квалификация дипфейка с точки зрения законодательства об информации и персональных данных.
43.	Обязанность компании маркировать контент, созданный ИИ (принцип прозрачности).
44.	Возможность использования сгенерированных текстов в качестве доказательств в суде и их доказательственная сила.
45.	Соответствие лицензионных договоров (EULA) с пользователями законодательству и специфике продукта.
46.	Наличие действующих договоров с контрагентами (хостинг, облачные провайдеры, подрядчики).
47.	Порядок проверки корпоративной структуры стартапа: корпоративные договоры, опционные программы для сотрудников, «чистая» доля основателя.
48.	Риски, связанные с «грязным» финансированием или непрозрачной структурой владения.
49.	Влияние формы сделки (покупка доли, покупка активов, реорганизация) на налоговые последствия.
50.	Риски доначисления налогов при использовании «упрощенки» (УСН) IT-компанией.
51.	Порядок учета для налогообложения операций с криптовалютой и токенами.
52.	Льготы для IT-компаний (страховые взносы, налог на прибыль) и риски их утраты покупателем после сделки.
53.	Корреляция выводов юридической проверки с оценкой стоимости бизнеса.
54.	Механизмы «earn-out» (отложенное вознаграждение) и «escrow» (счет эскроу) как способы защиты покупателя.
55.	Заверения и гарантии (representations and warranties) продавца, которые должны быть включены в договор для покрытия юридических рисков.
56.	Понятие «существенное изменение обстоятельств» (Material Adverse Change) и

	порядок его применения в IT-сделках.
57.	Экспресс-анализ предоставленного пакета документов условного стартапа (устав, договоры с разработчиками, политика обработки ПД, ссылки на GitHub).
58.	«Красные флаги» (риски) в части интеллектуальной собственности и персональных данных.
59.	Способы структурирования сделки (покупка доли или активов) для минимизации выявленных рисков.
60.	Пункты договора купли-продажи (заверения, indemnity), необходимые для защиты покупателя.

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.

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:

Модуль 1. Введение в правовую диагностику объектов новых технологий

Тема 1. Понятие и цели Due Diligence в сфере ИИ и цифровых активов. ОПК-1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	В чем принципиальное отличие DD ИИ-проекта от классической юридической проверки «традиционного» бизнеса (акцент на нематериальные активы и регуляторные риски)?
2.	Какие цели преследуют стороны сделки (инвестор, стратегический покупатель, стартап) при проведении правовой диагностики технологической компании?
3.	Кто является основными участниками процесса и какие роли они выполняют (технические специалисты, юристы, аудиторы)?
4.	На каких этапах жизненного цикла ИИ-проекта (посевная, венчурная стадия, exit) требуется проведение Due Diligence?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Какое из перечисленных обстоятельств является **ключевым отличием** Due Diligence ИИ-проекта от классического DD «традиционного» бизнеса? а) Необходимость проверки материальных активов (склады, оборудование) б) Отсутствие регуляторных рисков в) Акцент на проверку нематериальных активов (код, датасеты, ноу-хау) и специфических регуляторных рисков (ПД, этика ИИ) г) Проведение DD только на стадии exit		
2.	Какую **основную цель** преследует венчурный инвестор, проводя правовую диагностику ИИ-стартапа		

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
	на стадии seed? а) Получить полный доступ к исходному коду для его копирования б) Минимизировать риски обесценивания инвестиций путём проверки прав на IP и чистоты данных в) Ускорить регистрацию товарного знака г) Проверить бухгалтерскую отчётность за 5 лет		

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 цифру выбранного варианта ответа.

1. **В чём ключевое отличие Due Diligence ИИ-проекта от классического DD «традиционного» бизнеса?**
   а) В отсутствии необходимости проверять бухгалтерскую отчётность
   б) В акценте на нематериальные активы и регуляторные риски, связанные с данными и алгоритмами
   в) В меньшей глубине проверки из-за отсутствия материальных активов
   г) В невозможности проверки кода из-за коммерческой тайны.

2. **Какую цель преследует инвестор при проведении правовой диагностики ИИ-стартапа?**
   а) Уменьшить налоговую базу стартапа
   б) Выявить юридические риски, которые могут обесценить инвестиции
   в) Получить доступ к исходному коду без согласия основателей
   г) Ускорить регистрацию товарного знака

3. **Кто из перечисленных участников НЕ является обязательным для DD ИИ-проекта?**
   а) Технические специалисты (анализ кода, архитектуры)
   б) Юристы по IP и персональным данным
   в) Финансовые аудиторы
   г) Сотрудники ФСБ для согласования сделки

4. **На каком этапе жизненного цикла ИИ-проекта проведение DD наименее формализовано, но наиболее рискованно для инвестора?**

а) На стадии «посевной» (seed)
б) На стадии выхода (exit) через IPO
в) При продаже зрелой платформы стратегическому покупателю
г) На стадии пост-венчурного роста

Тема 2. Объекты правовой диагностики: классификация и особенности. ОПК-7

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Что входит в понятие «цифровые активы» в контексте DD (криптовалюта, токены, доменные имена, базы данных)?
2.	В чем специфика проверки ИИ-продукта как объекта: проверка кода, обученной модели, датасетов, архитектуры?
3.	Как различаются подходы к проверке «коробочного» ПО, облачного сервиса (SaaS) и открытого кода (Open Source)?
4.	Почему стартап на стадии MVP (Minimum Viable Product) требует иной глубины проверки, чем зрелая ИИ-платформа?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Что из перечисленного **не относится** к «цифровым активам» в контексте DD ИИ-проекта? а) Криптовалюта и токены б) Доменные имена в) Производственное оборудование (станки, серверы в офисе) г) Базы данных, используемые для обучения		
2.	Почему стартап на стадии **MVP (Minimum Viable Product)** требует иной глубины проверки, чем зрелая ИИ-платформа? а) Проверка MVP не проводится вообще из-за отсутствия юридических рисков б) Глубина проверки всегда одинакова независимо от стадии в) На стадии MVP акцент делается на проверку прав на код и данные, а		

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
	не на полный регуляторный комплаенс г) Проверка MVP требует обязательного участия налоговых органов		

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 цифру выбранного варианта ответа.

1. **Что из перечисленного НЕ относится к «цифровым активам» в контексте DD?**
   а) Криптовалюта и токены
   б) Доменные имена
   в) Производственное оборудование
   г) Базы данных

2. **В чём особенность проверки ИИ-продукта по сравнению с проверкой обычного ПО?**
   а) Проверке подлежат не только код, но и обученные модели, датасеты и архитектура
   б) Проверка ИИ-продукта не требует анализа лицензий
   в) ИИ-продукт невозможно проверить из-за отсутствия нормативной базы
   г) Проверка ограничивается только пользовательским соглашением

3. **Какой подход к проверке требуется при использовании открытого кода (Open Source) в коммерческом ИИ-продукте?**
   а) Проверка не требуется, так как открытый код всегда бесплатен
   б) Необходимо проверить совместимость лицензий (например, отсутствие «вирусных» условий)
   в) Достаточно убедиться, что код опубликован на GitHub
   г) Открытый код запрещён в любом коммерческом продукте

4. **Почему стартап на стадии MVP требует иной глубины проверки, чем зрелая ИИ-платформа?**
   а) Проверка MVP не проводится вообще
   б) У MVP нет юридических рисков
   в) Акцент делается на проверку прав на код и данные, а не на полный комплаенс
   г) Глубина проверки всегда одинакова независимо от стадии

Тема 3. Процесс и стадии проведения DD. ОПК-1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Какова стандартная процедура сделки: от подписания соглашения о конфиденциальности (NDA) до закрытия сделки?
2.	Что такое «виртуальная комната данных» (Data Room) и какие требования предъявляются к организации документооборота?
3.	Как формируется запрос на предоставление документов (чек-лист) с учетом специфики ИИ-активов?
4.	Какова структура итогового отчета (Legal Report) и что такое «disclosure letter» (письмо о раскрытии информации)?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Какой документ **подписывается первым** при стандартной процедуре DD перед открытием доступа к документам? а) Договор купли-продажи долей (SPA) б) Соглашение о конфиденциальности (NDA) в) Акт приёма-передачи исходного кода г) Исковое заявление в арбитраж	б)	NDA подписывается до передачи любой конфиденциальной информации, чтобы защитить продавца от разглашения. Без NDA продавец не открывает Data Room. Ответ а) — финальный этап. Ответ в) — после сделки. Ответ г) — судебный процесс, не связанный с DD.
2.	Что такое **«виртуальная комната данных» (Data Room)** в контексте DD? а) Физическое помещение с серверами, куда приглашают проверяющих б) Защищённое онлайн-хранилище с разграничением доступа, аудитом действий и запретом на скачивание в) Электронная почта для обмена файлами г) Реестр судебных решений	б)	Data Room — это технологическое решение для безопасного удалённого доступа к документам. Он позволяет продавцу контролировать, кто, что и когда смотрел, часто с водяными знаками и запретом скачивания. Ответ а) — анахронизм. Ответ в) — небезопасно. Ответ г) — не относится к процессу DD.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
	по ИИ-спорам		

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 цифру выбранного варианта ответа.

1. **Какой документ обычно подписывается первым при начале процедуры DD?**
   а) Договор купли-продажи акций
   б) Соглашение о конфиденциальности (NDA)
   в) Акт приёма-передачи кода
   г) Исковое заявление

2. **Что такое «виртуальная комната данных» (Data Room) в контексте DD?**
   а) Физическое помещение с серверами
   б) Защищённое онлайн-хранилище документов для доступа проверяющих
   в) Комната для допроса сотрудников
   г) Реестр судебных решений

3. **Что из перечисленного должно быть включено в чек-лист запроса документов для DD ИИ-активов?**
   а) Только бухгалтерская отчётность
   б) Лицензии на датасеты, согласия на обработку ПД, договоры с разработчиками
   в) Паспорта всех сотрудников
   г) Схема электропитания офиса

4. **Какова основная функция письма о раскрытии информации (disclosure letter)?**
   а) Замена договора купли-продажи
   б) Раскрытие покупателю известных продавцу рисков, которые не являются нарушением заверений
   в) Уведомление налоговой инспекции
   г) Регистрация товарного знака

Тема 4. Юрисдикционные аспекты проверки. ОПК-7

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Как выбрать применимое право при трансграничных сделках с цифровыми

	активами?
2.	Каковы особенности проверки компаний, зарегистрированных в иностранных юрисдикциях (offshore), но ведущих бизнес в РФ?
3.	Как координация работы юристов в нескольких юрисдикциях влияет на полноту и достоверность выводов DD?
4.	В каких случаях требуется получение согласия антимонопольных органов (ФАС) и как это влияет на структурирование сделки?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Какой фактор является **приоритетным** при выборе применимого права в трансграничной сделке с ИИ-активами, если пользователи находятся в РФ? а) Место регистрации сервера б) Гражданство основателей в) Место нахождения покупателя и требования регуляторов РФ (152-ФЗ, локализация БД) г) Валюта расчётов		
2.	В каком случае **требуется получение согласия ФАС России** при покупке ИИ-компании? а) Всегда, если в сделке участвует ИИ-компания б) Если стоимость активов по балансу превышает порог, установленный ст. 28 Закона о защите конкуренции (например, >7 млрд руб.) в) Только при банкротстве продавца г) Согласие ФАС никогда не требуется, так как ИИ-активы нематериальны		

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 цифру выбранного варианта ответа.

1. **Какой критерий является приоритетным при выборе применимого права в трансграничной сделке с цифровыми активами?**
   а) Место регистрации сервера
   б) Гражданство основателей
   в) Место нахождения покупателя и регуляторные требования к обработке данных
   г) Валюта расчётов

2. **В чём особенность проверки компании, зарегистрированной в офшоре, но ведущей бизнес в РФ?**
   а) Такая компания не подлежит проверке
   б) Необходимо анализировать как офшорное право, так и фактическое российское регулирование (риск «контролируемой иностранной компании»)
   в) Достаточно проверить только российские налоги
   г) Офшорная регистрация полностью освобождает от российского права

3. **Почему координация юристов в нескольких юрисдикциях критична для полноты DD?**
   а) Чтобы увеличить стоимость сделки
   б) Чтобы избежать противоречивых выводов и пробелов в проверке (например, по ПД и IP)
   в) Чтобы скрыть нарушения от регулятора
   г) Координация не требуется

4. **В каком случае требуется получение согласия антимонопольного органа (ФАС России)?**
   а) При покупке любой доли в ООО
   б) Если стоимость активов превышает порог, установленный законом о защите конкуренции
   в) Всегда, если в сделке участвует ИИ-компания
   г) Только при банкротстве

Модуль 2. Юридическая проверка интеллектуальной собственности и кода

Тема 5. Проверка прав на программный код и архитектуру. ОПК-1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Как проверить титул прав на код, созданный разработчиками (по договору подряда/ГПХ) и установить отсутствие притязаний со стороны бывших работников?
2.	Какие риски несет использование открытых библиотек с «вирусными» лицензиями (GPL, AGPL) в коммерческом продукте?
3.	Как проверить действительность отчуждения исключительного права и отсутствие обременений (залог, спор о праве)?
4.	Что делать, если код не депонирован или документация (техническая документация) отсутствует?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	При проверке договоров с разработчиками (ГПХ) обнаружено отсутствие условия об отчуждении исключительного права на код. **Какой риск это создаёт?** а) Налоговый риск б) Код может принадлежать разработчику, а не компании (отсутствие титула) в) Риск отсутствует, так как код всегда принадлежит заказчику г) Автоматический переход прав в силу закона		
2.	Каков **основной риск** использования библиотеки с лицензией **GPL v3** в коммерческом ИИ-продукте, распространяемом как SaaS? а) Необходимость платить роялти правообладателю б) Обязанность раскрыть исходный код всего продукта («вирусный» эффект) в) Риск отсутствует, так как GPL разрешает коммерческое использование г) Запрет на использование любых открытых библиотек		

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 цифру выбранного варианта ответа.

1. **Как проверить титул прав на код, созданный внешним разработчиком по договору ГПХ?**
   а) Достаточно устного подтверждения разработчика

б) Проверить наличие в договоре условия об отчуждении исключительного права или лицензии в пользу компании
в) Код, созданный по ГПХ, всегда принадлежит заказчику без договора
г) Такой код нельзя проверить

2. **Какой риск создаёт использование библиотеки с лицензией GPL в коммерческом ИИ-продукте?**
а) Риск отсутствия обновлений
б) «Вирусный» эффект — обязанность открыть исходный код всего продукта
в) Риск утечки персональных данных
г) Отсутствие рисков

3. **Что означает отсутствие депонирования исходного кода?**
а) Код не охраняется авторским правом
б) Затруднено доказывание авторства и содержания кода на определённую дату
в) Код автоматически переходит в общественное достояние
г) Это не имеет правового значения

4. **Какое обременение может быть выявлено при проверке исключительного права на код?**
а) Залог (например, в пользу банка)
б) Высокая зарплата разработчика
в) Устаревший язык программирования
г) Отсутствие комментариев в коде

Тема 6. Правовая экспертиза обучающих данных (датасетов). ОПК-7

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Как проверить законность сбора данных для обучения модели: было ли получено согласие субъектов персональных данных?
2.	Какие риски связаны с использованием «публично доступных» данных (например, из соцсетей) и существуют ли исключения для text and data mining (TDM)?
3.	Как проверить права на контент внутри датасета (объекты авторского права, базы данных) и не нарушают ли они права третьих лиц?
4.	Что такое анонимизация и обезличивание данных, и достаточно ли этого для минимизации рисков?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Компания собрала датасет из публичных постов в социальной сети (ВКонтакте) для обучения ИИ-модели без согласия пользователей. **Это нарушает:** а) Ничего, так как данные публично доступны б) Только авторские права на текст постов в) Законодательство о персональных данных (152-ФЗ) — отсутствие согласия на обработку г) Только этические нормы		
2.	Что такое **анонимизация персональных данных** и достаточно ли её для полного снятия рисков по 152-ФЗ при обучении ИИ? а) Удаление всех прямых идентификаторов (ФИО, адрес) — достаточно б) Необратимое преобразование, исключающее возможность идентификации субъекта любым способом — риск снижается, но требуется экспертная оценка необратимости в) Шифрование данных — полностью снимает риски г) Анонимизация запрещена законом		

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 цифру выбранного варианта ответа.

1. **Какое правовое основание чаще всего требуется для законного сбора персональных данных для обучения ИИ?**
   а) Публичный договор
   б) Согласие субъекта персональных данных

в) Распоряжение руководителя компании
г) Отсутствие согласия допустимо всегда

2. **В чём основной риск использования данных из открытых источников (например, соцсетей) для обучения ИИ?**
а) Низкое качество данных
б) Нарушение авторских прав и законодательства о персональных данных (отсутствие явного согласия)
в) Высокая стоимость хранения
г) Риск отсутствует

3. **Что такое анонимизация данных и достаточно ли её для минимизации рисков по 152-ФЗ?**
а) Полное удаление всех данных; достаточно
б) Обезличивание, при котором невозможно определить субъекта без дополнительных данных; обычно достаточно, но требуется экспертная оценка необратимости
в) Шифрование данных; не требуется
г) Согласие на обработку; всегда необходимо

4. **Что проверяется в отношении контента внутри датасета (фото, текст, видео)?**
а) Только объём данных
б) Наличие авторских прав третьих лиц и законность их использования (лицензия, исключение для TDM)
в) Формат файлов
г) Ничего, контент не охраняется

Тема 7. Средства индивидуализации и доменные имена. ОПК-7

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Как проверить, не нарушает ли название продукта или компании (товарный знак) права третьих лиц (проведение патентно-информационного поиска)?
2.	В чем особенности проверки прав на доменное имя, соответствующее товарному знаку?
3.	Как оценить риски блокировки сайта или мобильного приложения как актива?
4.	Кто является надлежащим правообладателем и не истек ли срок охраны?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	При проверке товарного знака ИИ-		

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
	продукта обнаружено, что сходное обозначение уже зарегистрировано другим лицом в классе МКТУ 9 (программы для ЭВМ). **Какой риск?** а) Отсутствие риска, так как классы МКТУ не имеют значения б) Риск признания использования незаконным и требования о смене названия (нарушение исключительного права) в) Риск только налоговый г) Автоматический переход права на товарный знак к компании		
2.	Что проверяется в отношении **доменного имени**, которое полностью совпадает с товарным знаком компании? а) Только дата регистрации домена б) Кто является администратором домена, дата регистрации, нет ли спора о киберсквоттинге в) Ничего, домен не имеет правового значения г) Только стоимость домена на рынке		

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 цифру выбранного варианта ответа.

1. **Какой инструмент используется для проверки того, что название продукта не нарушает чужие права на товарный знак?**
   а) Аудит бухгалтерии
   б) Патентно-информационный поиск по реестрам Роспатента и WIPO
   в) Опрос фокус-группы
   г) Анализ SEO-оптимизации

2. **В чём особенность проверки прав на доменное имя, совпадающее с товарным знаком?**
   а) Доменное имя не требует проверки

б) Необходимо убедиться, что домен зарегистрирован на правообладателя ТЗ или есть лицензия, иначе возможен спор о киберсквоттинге
в) Домен всегда принадлежит регистратору
г) Товарный знак и домен никак не связаны

3. **Что из перечисленного может привести к блокировке сайта как актива?**
а) Наличие контактной формы
б) Неуплата налогов
в) Нарушение законодательства об информации (например, распространение дипфейков без маркировки)
г) Использование HTTPS

4. **Что проверяется в отношении срока охраны товарного знака?**
а) Дата первой публикации в соцсетях
б) Дата регистрации и оплата пошлин за продление (10-летние периоды)
в) Возраст генерального директора
г) Количество сотрудников

Тема 8. Коммерческая тайна и ноу-хау (секреты производства). ОПК-1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Введен ли в компании режим коммерческой тайны? Как проверить наличие локальных актов, журналов ознакомления и допуска?
2.	Какие риски утечки данных существуют при использовании облачных нейросетей сотрудниками (например, внесение кода в ChatGPT)?
3.	Как защищены алгоритмы и архитектура нейросети, если они не патентуются?
4.	Что делать с конфиденциальной информацией, которая раскрывается потенциальному инвестору в ходе DD?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Какие **документы необходимы** для подтверждения введения режима коммерческой тайны в компании? а) Только трудовой договор с генеральным директором б) Приказ о введении режима, Положение о коммерческой тайне, журналы ознакомления сотрудников в) Свидетельство Роспатента на ноу-		

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
	хау г) Достаточно устного распоряжения руководителя		
2.	**Какой риск** возникает при использовании сотрудниками ИИ-компании публичной нейросети (ChatGPT) для написания кода, содержащего ноу-хау? а) Риск ускорения разработки б) Риск утечки конфиденциальной информации (код может быть использован для обучения модели и стать известен третьим лицам) в) Риск отсутствует, так как ChatGPT не сохраняет данные г) Только налоговый риск		

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 цифру выбранного варианта ответа.

1. **Какой локальный акт является обязательным для введения режима коммерческой тайны?**
   а) Правила внутреннего трудового распорядка
   б) Положение о коммерческой тайне и приказ о допуске сотрудников
   в) Штатное расписание
   г) Коллективный договор

2. **Каков основной риск при использовании сотрудниками облачных нейросетей (например, ChatGPT) для работы с кодом?**
   а) Ускорение разработки
   б) Утечка конфиденциальной информации (код может использоваться для обучения модели)
   в) Снижение зарплаты
   г) Риск отсутствует

3. **Как защищены алгоритмы нейросети, если они не патентуются?**
   а) Никак
   б) Режимом коммерческой тайны (ноу-хау) при соблюдении соответствующих мер

в) Только авторским правом на код
г) Автоматически, без действий компании

4. **Что должно быть предусмотрено в соглашении с инвестором при раскрытии ему конфиденциальной информации в ходе DD?**
а) Отказ от любой ответственности
б) Положения о неразглашении (NDA) и ограничении использования информации
в) Передача всех прав на ноу-хау инвестору
г) Ничего, информация раскрывается свободно

Модуль 3. Регуляторный комплаенс и риски ИИ-проектов

Тема 9. Соответствие законодательству о персональных данных (152-ФЗ). ОПК-7

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Есть ли у компании правовое основание для обработки персональных данных? Получено ли согласие и соответствует ли оно принципам конкретности и информированности?
2.	Соблюдается ли требование о локализации баз данных на территории РФ?
3.	Не является ли использование иностранной нейросети (например, OpenAI) трансграничной передачей данных и получено ли на это разрешение (РКН)?
4.	Какие штрафы и риски блокировки деятельности (ст. 13.11 КоАП, ст. 272.1 УК РФ) существуют за выявленные нарушения?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	ИИ-компания обрабатывает персональные данные граждан РФ на серверах в Нидерландах, не уведомив РКН. **Какое требование нарушено?** а) Требование о лицензировании б) Требование о локализации баз данных (ст. 18 152-ФЗ) и о трансграничной передаче в) Никакое, так как Нидерланды — в ЕС, этого достаточно г) Требование о наличии сертификата ISO		

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
2.	**Какой максимальный штраф** по ст. 13.11 КоАП РФ может быть наложен на юридическое лицо за повторную утечку персональных данных (необеспечение сохранности)? а) 100 000 руб. б) 1 млн руб. в) До 6 млн руб. (оборотный штраф от 0,1% до 3% выручки) г) 10 млн руб.		

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 цифру выбранного варианта ответа.

1. **Какое из перечисленного является правовым основанием обработки персональных данных?**
   а) Устное согласие по телефону
   б) Письменное или в форме электронного документа согласие субъекта
   в) Отсутствие возражений
   г) Любое упоминание имени в сети

2. **Что означает требование о локализации баз данных на территории РФ?**
   а) Запрет на любое использование иностранных серверов
   б) Обязанность обеспечить первичную запись, систематизацию и хранение персональных данных россиян на серверах в РФ
   в) Запрет на передачу данных внутри компании
   г) Требование к дублированию данных на бумаге

3. **Использование иностранной нейросети OpenAI для обработки персональных данных клиентов из РФ без дополнительных мер: какой риск возникает?**
   а) Риск ускорения работы
   б) Риск незаконной трансграничной передачи данных (требуется уведомление или разрешение РКН)
   в) Риск отсутствует
   г) Риск только налоговый

4. **Какая статья КоАП РФ предусматривает штрафы за нарушение порядка обработки персональных данных?**
   а) Ст. 13.11

б) Ст. 159
в) Ст. 228
г) Ст. 272

Тема 10. Регулирование в сфере ИИ (ФЗ об ЭПР, стандартизация, этика). ОПК-1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Подпадает ли ИИ-продукт под экспериментальный правовой режим (ЭПР) и какие обязательства это налагает?
2.	Как проверить соблюдение требований к системам ИИ (например, ГОСТы или рекомендации в области безопасности)?
3.	Разработан ли в компании кодекс этики ИИ и соблюдаются ли Национальный кодекс этики ИИ?
4.	Существуют ли риски, связанные с дискриминацией (bias) в работе модели, и как они могут быть оспорены пользователями?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Что такое **экспериментальный правовой режим (ЭПР)** в сфере ИИ по ФЗ № 258-ФЗ? а) Полная отмена всех законов для ИИ-компаний б) Возможность отступления от отдельных требований законодательства на определённой территории для внедрения ИИ в) Обязательная сертификация всех ИИ-систем г) Налоговая льгота на прибыль		
2.	Является ли соблюдение **ГОСТ Р 59277-2020** (Безопасность систем ИИ) обязательным для всех ИИ-компаний в РФ? а) Да, все ГОСТы обязательны б) Нет, данный ГОСТ носит рекомендательный характер, но его соблюдение проверяется в DD как		

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
	индикатор качества в) Запрещено соблюдение любых ГОСТов г) Только для государственных ИИ-систем		

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 цифру выбранного варианта ответа.

1. **Что такое экспериментальный правовой режим (ЭПР) в сфере ИИ?**
   а) Запрет на использование ИИ
   б) Особый правовой режим, позволяющий отступление от отдельных требований закона для внедрения ИИ на ограниченной территории
   в) Обязательная сертификация всех ИИ-систем
   г) Налоговая льгота

2. **Как проверяется соблюдение этических норм в ИИ-компании?**
   а) Только через опрос сотрудников
   б) Анализ наличия кодекса этики ИИ и соответствия Национальному кодексу этики ИИ
   в) Этические нормы не проверяются
   г) Достаточно публичной оферты

3. **Что такое «bias» (смещение) в работе модели ИИ?**
   а) Высокая скорость работы
   б) Систематическая ошибка, приводящая к дискриминации или необъективным результатам
   в) Лицензионное соглашение
   г) Способ шифрования

4. **Обязательны ли ГОСТы для всех ИИ-систем в РФ?**
   а) Да, все ГОСТы обязательны
   б) Нет, большинство носит рекомендательный характер, но их соблюдение может проверяться в рамках DD как индикатор качества и безопасности
   в) ГОСТы запрещены для ИИ
   г) Только международные стандарты

Тема 11. Ответственность за контент, сгенерированный ИИ. ОПК-1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Кто несет ответственность за «галлюцинации» нейросети, если они причинили вред (администратор, разработчик, пользователь)?
2.	Как квалифицируется дипфейк с точки зрения законодательства об информации и персональных данных?
3.	Должна ли компания маркировать контент, созданный ИИ (принцип прозрачности)?
4.	Можно ли использовать сгенерированные тексты в качестве доказательств в суде? Какова доказательственная сила таких материалов?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Нейросеть сгенерировала ложную информацию (галлюцинацию) о том, что известный политик совершил уголовное преступление. **Кто может быть привлечён к ответственности по текущему законодательству РФ?** а) Сама нейросеть б) Разработчик или оператор сервиса, если не принял мер для предотвращения распространения в) Пользователь, который просто нажал «сгенерировать» г) Никто, так как ИИ не субъект права		
2.	**Обязана ли компания маркировать контент, созданный с помощью ИИ** (например, текст статьи на сайте), если она не подпадает под ЭПР и не является СМИ? а) Да, всегда под страхом уголовной ответственности б) Нет, прямой обязанности для всех нет, но рекомендуется в соответствии с Национальным кодексом этики ИИ в) Запрещено маркировать г) Только если контент касается здоровья		

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 цифру выбранного варианта ответа.

1. **Кто, по общему правилу текущего российского законодательства, несёт ответственность за вред от «галлюцинаций» нейросети?**
   а) Сама нейросеть
   б) Разработчик или оператор сервиса (лицо, контролирующее использование)
   в) Пользователь, задавший вопрос
   г) Никто

2. **Дипфейк (deepfake) с точки зрения законодательства РФ — это:**
   а) Всегда законно
   б) Синтезированное изображение или голос, которое может нарушать право на частную жизнь, авторские права и требовать маркировки
   в) Вид открытой лицензии
   г) Способ шифрования

3. **Обязана ли компания маркировать контент, созданный ИИ?**
   а) Нет, никогда
   б) Да, если это предусмотрено специальным регулированием (например, ЭПР) или из принципов прозрачности, но прямого общего закона пока нет; рекомендуется
   в) Только для видео
   г) Только для текстов

4. **Может ли текст, сгенерированный ИИ, быть доказательством в суде?**
   а) Никогда
   б) Да, на общих основаниях, но требуется проверка достоверности и источника (проблема авторства)
   в) Только если он заверен нотариусом
   г) Только если ИИ зарегистрирован как СМИ

Тема 12. Проверка договорной базы и корпоративной структуры. ОПК-7

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Соответствуют ли лицензионные договоры (EULA) с пользователями законодательству и специфике продукта?

2.	Есть ли действующие договоры с контрагентами (хостинг, облачные провайдеры, подрядчики)?
3.	Как проверяется корпоративная структура стартапа: есть ли корпоративные договоры, опционные программы для сотрудников, «чистая» доля основателя?
4.	Существуют ли риски, связанные с «грязным» финансированием или непрозрачной структурой владения?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	При проверке корпоративной структуры стартапа обнаружено, что **опционная программа для сотрудников** не утверждена решением совета директоров и не оформлена в письменном виде. **Какой риск?** а) Риск отсутствует, опционы можно выдать устно б) Опционы не имеют юридической силы, сотрудники могут оспорить их или требовать выплат на общих основаниях в) Автоматическое признание всех сотрудников соучредителями г) Только налоговый риск		
2.	Что означает риск **«грязного финансирования»** при проверке ИИ-стартапа? а) Отсутствие прибыли б) Непрозрачное происхождение средств, возможное нарушение 115-ФЗ (ПОД/ФТ) в) Высокая заработная плата основателей г) Использование кредитных средств		

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 цифру выбранного варианта ответа.

1. **Что должно быть проверено в EULA (лицензионном договоре с пользователем)?**
   а) Только цена
   б) Соответствие законодательству, порядок обработки ПД, ограничение ответственности, право на обновления
   в) Адрес офиса
   г) Цвет логотипа

2. **Какой документ подтверждает право стартапа использовать облачного провайдера (например, AWS)?**
   а) Устное соглашение
   б) Действующий договор с провайдером, проверка условий о передаче данных
   в) Счёт на оплату
   г) Достаточно скриншота

3. **Что проверяется в корпоративной структуре стартапа?**
   а) Наличие корпоративного договора (shareholders‘ agreement) и опционной программы, «чистота» долей основателей
   б) Только размер уставного капитала
   в) Количество сотрудников
   г) Дизайн сайта

4. **Что означает риск «грязного» финансирования?**
   а) Отсутствие прибыли
   б) Непрозрачное происхождение средств, возможное нарушение антиотмывочного законодательства (115-ФЗ)
   в) Использование кредита
   г) Высокая зарплата директора

Модуль 4. Финансово-правовые аспекты и налогообложение

Тема 13. Налоговые риски структурирования сделки и активов. ОПК-1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Как форма сделки (покупка доли, покупка активов, реорганизация) влияет на налоговые последствия?
2.	Какие существуют риски доначисления налогов при использовании «упрощенки» (УСН) IT-компанией?
3.	Как учитываются для налогообложения операции с криптовалютой и токенами?
4.	Какие льготы для IT-компаний (страховые взносы, налог на прибыль) применяются и не потеряет ли их покупатель после сделки?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Какая форма сделки **покупателем ИИ-активов** чаще всего позволяет **амортизировать** приобретённое программное обеспечение для целей налога на прибыль? а) Покупка доли (долей) в ООО б) Покупка активов (исключительного права на код) по отдельному договору в) Реорганизация в форме слияния г) Безвозмездная передача		
2.	IT-компания на УСН (доходы минус расходы) продаёт криптовалюту, полученную в результате майнинга. **Как учитывается доход?** а) Доход не облагается б) Доход облагается как имущество по ставке УСН (15% с разницы между ценой продажи и расходами на майнинг) по разъяснениям ФНС в) Доход облагается НДФЛ (13%), а не налогом при УСН г) Майнинг запрещён		

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 цифру выбранного варианта ответа.

1. **Какая форма сделки обычно наименее налогово-рискованна для покупателя с точки зрения получения вычета по НДС и амортизации активов?**
   а) Покупка доли (долей) в ООО
   б) Покупка активов по отдельности
   в) Безвозмездная передача
   г) Мена

2. **Какой риск возникает при покупке IT-компании на УСН?**
   а) Риск отсутствует
   б) Покупатель может потерять право на УСН после сделки, если изменится состав

участников или доля юрлиц превысит лимит
в) УСН запрещена для IT
г) Риск только для продавца

3. **Как в настоящее время облагаются налогом операции с криптовалютой в РФ (при отсутствии прямого закона о цифровой валюте)?**
а) Не облагаются вообще
б) Облагаются как имущество (НДФЛ при продаже) по разъяснениям Минфина и ФНС
в) Облагаются по ставке 0%
г) Облагаются как внешнеторговая сделка

4. **Какая льгота для IT-компаний является наиболее значимой?**
а) Освобождение от НДС
б) Пониженные тарифы страховых взносов (15% вместо 30%) и пониженная ставка налога на прибыль
в) Освобождение от НДФЛ
г) Отмена налога на имущество

Тема 14. Оценка активов и механизмы защиты цены. ОПК-7

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Как коррелируют выводы юридической проверки с оценкой стоимости бизнеса?
2.	Что такое механизмы «earn-out» (отложенное вознаграждение) и «escrow» (счет эскроу) и как они защищают покупателя?
3.	Какие заверения и гарантии (representations and warranties) продавца должны быть включены в договор для покрытия юридических рисков?
4.	Что такое «существенное изменение обстоятельств» (Material Adverse Change) и как оно применяется в IT-сделках?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Что такое механизм **escrow (счёт эскроу)** в сделке по покупке ИИ-стартапа? а) Часть цены, выплачиваемая продавцу при достижении KPI б) Сумма, блокируемая на счёте на определённый срок для покрытия		

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
	убытков от нарушения заверений и гарантий продавца в) Задаток, который теряется при отказе от сделки г) Банковский кредит		
2.	**Заверения и гарантии (R&W)** продавца в договоре купли-продажи ИИ-компании нужны для: а) Увеличения цены сделки б) Распределения риска между сторонами: если заверение окажется ложным, покупатель может требовать компенсации в) Налоговой оптимизации г) Регистрации товарного знака		

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 цифру выбранного варианта ответа.

1. **Как коррелируют выводы юридического DD с оценкой бизнеса?**
   а) Не коррелируют
   б) Выявленные юридические риски снижают справедливую стоимость (делается скидка на риски)
   в) Риски увеличивают стоимость
   г) Только налоговые риски влияют

2. **Что такое механизм earn-out?**
   а) Фиксированная цена
   б) Отложенное вознаграждение продавцу, зависящее от будущих финансовых показателей компании
   в) Штраф за нарушение
   г) Банковская гарантия

3. **Для покрытия каких рисков предназначены заверения и гарантии продавца (R&W)?**
   а) Только налоговых
   б) За достоверность юридического статуса, IP, отсутствие долгов и т.д. (покупатель

получает право на компенсацию при несоответствии)
в) Только за качество кода
г) За будущую прибыль

4. **Что такое Material Adverse Change (MAC) в IT-сделке?**
а) Смена логотипа
б) Существенное ухудшение состояния бизнеса (например, потеря ключевой лицензии, иск на крупную сумму) между подписанием и закрытием сделки, дающее право отказаться от сделки
в) Инфляция
г) Смена генерального директора

Модуль 5. Итоговый практикум (кейс-стади)

Тема 15. Комплексный анализ ИИ-стартапа. ОПК-1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Провести экспресс-анализ предоставленного пакета документов условного стартапа (устав, договоры с разработчиками, политика обработки ПД, ссылки на GitHub). Вопрос: Какие «красные флаги» (риски) выявлены в части IP и персональных данных?
2.	Какие «красные флаги» (риски) выявлены в части IP и персональных данных? (Продолжение вопроса 1)
3.	Как структурировать сделку (покупка доли или активов), чтобы минимизировать эти риски?
4.	Какие пункты договора купли-продажи (заверения, indemnity) необходимы для защиты покупателя?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	При экспресс-анализе документов ИИ-стартапа выявлено: (1) договоры с разработчиками не содержат условия об отчуждении IP; (2) на GitHub найден фрагмент кода с лицензией GPL; (3) политика обработки ПД отсутствует. **Какой из этих рисков является наиболее критичным для возможности продажи бизнеса?** а) Отсутствие политики ПД б) Отсутствие отчуждения IP от		

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
	разработчиков (компания может не владеть своим основным активом) в) Наличие GPL-кода г) Все риски равнозначны		
2.	Какая **структура сделки** наиболее предпочтительна для покупателя, если в ходе DD обнаружены неустранимые риски в IP (код написан с нарушением авторских прав третьих лиц)? а) Покупка 100% долей в уставном капитале б) Покупка отдельных активов (код, товарный знак) с созданием нового юридического лица (carve-out) в) Аренда сотрудников г) Отказ от сделки без альтернатив		

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 цифру выбранного варианта ответа.

1. **При экспресс-анализе документов стартапа обнаружено, что договоры с разработчиками не содержат условия об отчуждении исключительного права на код. Какой это «красный флаг»?**
   а) Налоговый риск
   б) Риск отсутствия прав на основной актив (код может принадлежать разработчикам)
   в) Экологический риск
   г) Риск отсутствует

2. **В политике обработки ПД отсутствует согласие на трансграничную передачу, но ИИ-модель работает на серверах в ЕС. Какой риск?**
   а) Риск блокировки деятельности и штрафы РКН
   б) Риск повышения скорости
   в) Риск только репутационный
   г) Риск отсутствует

3. **Какая структура сделки предпочтительнее для покупателя при выявлении неустранимых рисков в IP стартапа?**
   а) Покупка долей (100% акций)
   б) Покупка отдельных активов (код, товарный знак, база данных) с выделением их в новое юрлицо (carve-out)
   в) Аренда сотрудников
   г) Заключение опциона

4. **Какой пункт договора купли-продажи наиболее важен для защиты покупателя от нераскрытых судебных споров?**
   а) Цена
   б) Заверения и гарантии продавца об отсутствии споров и обязательство возмещения (indemnity) при нарушении заверений
   в) Срок подписания
   г) Форма оплаты

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 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	40
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	0-19

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.	

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. Принципиальное отличие DD ИИ-проекта от классической юридической проверки «традиционного» бизнеса (акцент на нематериальные активы и регуляторные риски).
2. Цели сторон сделки (инвестор, стратегический покупатель, стартап) при проведении правовой диагностики технологической компании.
3. Основные участники процесса и их роли (технические специалисты, юристы, аудиторы).
4. Этапы жизненного цикла ИИ-проекта (посевная, венчурная стадия, exit), на которых требуется проведение Due Diligence.
5. Содержание понятия «цифровые активы» в контексте DD (криптовалюта, токены, доменные имена, базы данных.
6. Специфика проверки ИИ-продукта как объекта: проверка кода, обученной модели, датасетов, архитектуры.
7. Различия подходов к проверке «коробочного» ПО, облачного сервиса (SaaS) и открытого кода (Open Source).
8. Почему стартап на стадии MVP (Minimum Viable Product) требует иной глубины проверки, чем зрелая ИИ-платформа?
9. Стандартная процедура сделки: от подписания соглашения о конфиденциальности (NDA) до закрытия сделки.
10. «Виртуальная комната данных» (Data Room) и требования, предъявляемые к организации документооборота.
11. Формирование запроса на предоставление документов (чек-лист) с учетом специфики ИИ-активов.
12. Структура итогового отчета (Legal Report) и суть "disclosure letter" (письмо о раскрытии информации).
13. Выбор применимого права при трансграничных сделках с цифровыми активами.
14. Особенности проверки компаний, зарегистрированных в иностранных юрисдикциях (offshore), но ведущих бизнес в РФ.
15. Влияние координации работы юристов в нескольких юрисдикциях на полноту и достоверность выводов DD.
16. Случаи, когда требуется получение согласия антимонопольных органов (ФАС) и как это влияет на структурирование сделки.
17. Проверка титула прав на код, созданный разработчиками (по договору подряда/ГПХ) и установление отсутствия притязаний со стороны бывших работников.
18. Риски использования открытых библиотек с «вирусными» лицензиями (GPL, AGPL) в коммерческом продукте.
19. Проверка действительности отчуждения исключительного права и отсутствия обременений (залог, спор о праве).
20. Порядок действий в случае, если код не депонирован или документация (техническая документация) отсутствует.
21. Проверка законности сбора данных для обучения модели: было ли получено согласие субъектов персональных данных.
22. Риски, связанные с использованием «публично доступных» данных (например, из соцсетей) и допустимость исключения для text and data mining (TDM).
23. Проверка права на контент внутри датасета (объекты авторского права, базы данных) и не нарушают ли они права третьих лиц.

24. Понятия «анонимизации» и «обезличивания» данных, и их достаточность для минимизации рисков.
25. Порядок проверки того, не нарушает ли название продукта или компании (товарный знак) права третьих лиц, включая проведение патентно-информационного поиска.
26. Особенности проверки прав на доменное имя, соответствующее товарному знаку.
27. Оценка рисков блокировки сайта или мобильного приложения как актива.
28. Определение надлежащего правообладателя и проверка срока действия охраны.
29. Наличие в компании режима коммерческой тайны и порядок проверки локальных актов, журналов ознакомления и допуска.
30. Риски утечки данных при использовании облачных нейросетей сотрудниками (на примере внесения кода в ChatGPT).
31. Способы защиты алгоритмов и архитектуры нейросети в случае, если они не патентуются.
32. Порядок работы с конфиденциальной информацией, раскрываемой потенциальному инвестору в ходе Due Diligence.
33. Правовые основания для обработки персональных данных: требования к согласию, его конкретности и информированности.
34. Соблюдение требования о локализации баз данных на территории РФ.
35. Квалификация использования иностранной нейросети (например, OpenAI) как трансграничной передачи данных и необходимость разрешения РКН.
36. Штрафы и риски блокировки деятельности (ст. 13.11 КоАП, ст. 272.1 УК РФ) за выявленные нарушения.
37. Подпадание ИИ-продукта под экспериментальный правовой режим (ЭПР) и обязательства, которые это налагает.
38. Порядок проверки соблюдения требований к системам ИИ (ГОСТы, рекомендации в области безопасности).
39. Наличие в компании кодекса этики ИИ и соблюдение Национального кодекса этики ИИ.
40. Риски, связанные с дискриминацией (bias) в работе модели, и возможности их оспаривания пользователями.
41. Ответственность за «галлюцинации» нейросети, причинившие вред (администратор, разработчик, пользователь).
42. Квалификация дипфейка с точки зрения законодательства об информации и персональных данных.
43. Обязанность компании маркировать контент, созданный ИИ (принцип прозрачности).
44. Возможность использования сгенерированных текстов в качестве доказательств в суде и их доказательственная сила.
45. Соответствие лицензионных договоров (EULA) с пользователями законодательству и специфике продукта.
46. Наличие действующих договоров с контрагентами (хостинг, облачные провайдеры, подрядчики).
47. Порядок проверки корпоративной структуры стартапа: корпоративные договоры, опционные программы для сотрудников, «чистая» доля основателя.
48. Риски, связанные с «грязным» финансированием или непрозрачной структурой владения.
49. Влияние формы сделки (покупка доли, покупка активов, реорганизация) на налоговые последствия.
50. Риски доначисления налогов при использовании «упрощенки» (УСН) IT-компанией.
51. Порядок учета для налогообложения операций с криптовалютой и токенами.
52. Льготы для IT-компаний (страховые взносы, налог на прибыль) и риски их утраты покупателем после сделки.
53. Корреляция выводов юридической проверки с оценкой стоимости бизнеса.

54. Механизмы «earn-out» (отложенное вознаграждение) и «escrow» (счет эскроу) как способы защиты покупателя.
55. Заверения и гарантии (representations and warranties) продавца, которые должны быть включены в договор для покрытия юридических рисков.
56. Понятие «существенное изменение обстоятельств» (Material Adverse Change) и порядок его применения в IT-сделках.
57. Экспресс-анализ предоставленного пакета документов условного стартапа (устав, договоры с разработчиками, политика обработки ПД, ссылки на GitHub).
58. «Красные флаги» (риски) в части интеллектуальной собственности и персональных данных.
59. Способы структурирования сделки (покупка доли или активов) для минимизации выявленных рисков.
60. Пункты договора купли-продажи (заверения, indemnity), необходимые для защиты покупателя.

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Методология и механизмы управления нематериальными ресурсами и активами в сфере электронной торговли на основе ценностно-ориентированной модели : монография / С. В. Панасенко, О. С. Каращук, Е. А. Красильникова [и др.] ; под общ. ред. С. В. Панасенко ; ФГБОУ ВО «РЭУ им. Г.В. Плеханова». - 2-е изд. - Москва : Издательско-торговая корпорация «Дашков и К°», 2024. - 284 с. - ISBN 978-5-394-05565-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2128209 (дата обращения: 07.06.2026). – Режим доступа: по подписке.

2. Линников, А.С. Цифровой правовой контроль как новая цивилистическая категория / А. С. Линников, A. S. Linnikov // Вестник Пермского университета. Юридические науки. — 2024. — № 64. — С. 289-310. — ISSN 1995-4190. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/journal/issue/364952 (дата обращения: 07.06.2026). — Режим доступа: для авториз. пользователей.

3. Полежаев, О. А. Право новых технологий, практика комплексной юридической проверки (due diligence) при подготовке сделок в сфере новых технологий : учебное пособие / О. А. Полежаев ; под общей редакцией Л. А. Новоселовой. — Москва : Проспект, 2021. — 79 с. — ISBN 978-5-392-34743-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/280541 (дата обращения: 07.06.2026). — Режим доступа: для авториз. пользователей.

4. Пучков, В. О. Правовая экспертиза инвестиционных проектов : учебное пособие / В. О. Пучков. — Екатеринбург : УрГЭУ, 2024. — 167 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/444029 (дата обращения: 07.06.2026). — Режим доступа: для авториз. пользователей.

8.2. Дополнительная литература

1. Wong, H. Cyber Security : Law and Guidance / H. Wong. — 2nd ed. — London : Bloomsbury Professional, 2025. — ISBN 9781526528131. (Практическое руководство по праву кибербезопасности, содержащее детальные чек-листы для реагирования на инциденты, анализ требований к уведомлению об инцидентах безопасности, вопросы ответственности работников и защиты организаций после утечек данных).

2. Криминологическая характеристика и предупреждение отдельных видов киберпреступлений // Вестник Московского университета МВД России имени В.Я. Кикотя. — 2025. (Научная статья, анализирующая современные тенденции

киберпреступности, категории преступлений в информационно-телекоммуникационном пространстве и проблемы совершенствования законодательства с учетом особенностей цифровой среды).

3. Калашников, И. В., Калашникова, Л. Н. Криминологическая характеристика и прогнозирование отдельных видов киберпреступлений, совершаемых в информационно-телекоммуникационном пространстве на территории Российской Федерации // Криминологический журнал. — 2024. — № 2. (Исследование, посвященное криминологической характеристике киберпреступлений и вопросам их прогнозирования).

8.3. Нормативные правовые документы и иная правовая информация

Российская Федерация

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». (Базовый закон, определяющий принципы обеспечения безопасности КИИ, права и обязанности субъектов КИИ, включая обязанность информировать ФСБ России о компьютерных инцидентах).
2. Приказ ФСБ России от 25.12.2025 № 547 «Об утверждении Порядка информирования ФСБ России о компьютерных атаках и компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации и иных информационных ресурсов Российской Федерации...» (Зарегистрирован в Минюсте России 30.12.2025 № 84871). (Ключевой нормативный акт, вступающий в силу с 30 января 2026 года. Устанавливает новый порядок информирования ФСБ России обо всех компьютерных атаках и инцидентах, реагирования на них и принятия мер по ликвидации последствий. Распространяется не только на субъекты КИИ, но и на государственные органы, унитарные предприятия, учреждения, фонды, госкорпорации. Признает утратившим силу ранее действовавший Приказ ФСБ России от 19.06.2019 № 282) .
3. Уголовный кодекс Российской Федерации (глава 28 «Преступления в сфере компьютерной информации»). (Статьи 272–274.1, устанавливающие ответственность за неправомерный доступ к компьютерной информации, создание и распространение вредоносных программ, нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и иные преступления в сфере компьютерной информации).
4. Кодекс Российской Федерации об административных правонарушениях (статьи 13.11–13.13). (Ответственность за нарушение законодательства о персональных данных, нарушение правил защиты информации и иные правонарушения в области информации).
5. Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации». (Утрачивает силу с 30.01.2026 в связи с изданием Приказа № 547, однако может использоваться для сравнительного анализа изменений в регулировании) .
6. Указание Банка России от 25.11.2022 № 6315-У «О порядке информирования Банка России о компьютерных атаках и компьютерных инцидентах, реагирования на них и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении объектов информационной инфраструктуры Банка России». (Ведомственный акт, регулирующий порядок реагирования на инциденты в финансовой сфере).
7. Приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении Порядка взаимодействия Федеральной службы по техническому и экспортному контролю, территориальных органов Федеральной службы по техническому и экспортному контролю, федеральных органов исполнительной власти, уполномоченных в области обеспечения функционирования государственной системы обнаружения, предупреждения и

ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и субъектов критической информационной инфраструктуры Российской Федерации по вопросам обмена информацией о компьютерных инцидентах». (Регулирует взаимодействие с ФСТЭК России по вопросам компьютерных инцидентов).

Международное и зарубежное регулирование

1. Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR). (Содержит требования к уведомлению о нарушениях безопасности персональных данных — breach notification).
2. Directive (EU) 2022/2555 (NIS 2 Directive). (Обновленная директива ЕС о безопасности сетевых и информационных систем, устанавливающая расширенные требования к реагированию на инциденты и отчетности для широкого круга организаций).

8.4. Интернет-ресурсы

1. Официальный интернет-портал правовой информации (www.pravo.gov.ru). (Гарантированный источник опубликования федеральных законов и ведомственных актов, включая Приказ ФСБ России № 547).
2. СПС «КонсультантПлюс» (www.consultant.ru). (Профессиональная справочная система, содержащая актуальные редакции документов, включая новейший Приказ ФСБ России № 547 от 25.12.2025, судебную практику по делам о киберпреступлениях, комментарии и аналитические обзоры) .
3. СПС «Гарант» (www.garant.ru). (Альтернативная справочная система с широким набором документов по информационной безопасности и реагированию на инциденты).
4. Официальный сайт ФСБ России (www.fsb.ru). (Информация о деятельности Национального координационного центра по компьютерным инцидентам (НКЦКИ), методические материалы по реагированию на компьютерные атаки).
5. Портал государственных услуг Российской Федерации (www.gosuslugi.ru/cybersecurity). (Раздел по кибербезопасности, содержащий информационно-разъяснительные материалы для граждан и организаций).
6. Официальный сайт МВД России (мвд.рф/mvd/structure1/Upravlenija/ubk). (Информация о деятельности Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий, статистика и профилактические материалы).
7. Официальный сайт ФСТЭК России (fstec.ru). (Нормативные и методические документы по технической защите информации и противодействию техническим разведкам).
8. Сайт Альянса в сфере искусственного интеллекта (a-ai.ru) и РОЦИТ (rocit.ru). (Информационно-разъяснительные материалы по кибербезопасности, аналитика инцидентов, рекомендации по защите).
9. Национальный институт стандартов и технологий США (NIST) — Cybersecurity Framework (www.nist.gov/cyberframework). (Международно признанный стандарт по управлению киберрисками и реагированию на инциденты).

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 используются 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. 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. 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-правовая система «Консультант».
9. http://www.garant.ru/ Справочно-правовая система «Гарант».