Лебедева Екатерина Александровна
Подписано цифровой подписью: Лебедева Екатерина Александровна
Дата: 2026.06.25 14:37:05 +03'00'

Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.07 Правовые режимы данных (Data Law) для консультанта
(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.07 «Правовые режимы данных (Data Law) для консультанта» одобрена на заседании кафедры гражданского и международного права

протокол № 6 от «04» 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.07 «Правовые режимы данных (Data Law) для консультанта» 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-1.1**	В точном соответствии с законом осуществляет квалификацию юридических фактов и определяет стратегию действий в конкретных правовых ситуациях.	**ИОПК-1.1 З-1 (Data Law).** ***Знает:*** российское и зарубежное законодательство, определяющее правовой режим различных категорий данных (персональные данные, коммерческая тайна, Big Data, открытые данные); судебную практику по спорам, связанным с оборотом данных и защитой прав субъектов. **ИОПК-1.1 У-1 (Data Law).** ***Умеет:*** квалифицировать фактические обстоятельства обработки данных в нестандартных ситуациях (использование публично доступных данных, обезличивание, профилирование); определять применимый правовой режим и формулировать стратегию действий для минимизации рисков.
	ОПК-3	Способен квалифицированно толковать правовые акты, в том числе в ситуациях наличия пробелов и коллизий норм прав	**ИОПК-3.1**	Демонстрирует навыки использования приемов и способов толкования норм права, устранения и восполнения пробелов правового регулирования, устранения и преодоления коллизий норм права, формулирует заключение по результатам толкования.	**ИОПК-3.1 З-1 (Data Law).** ***Знает:*** иерархию и системные связи нормативных актов, регулирующих отношения в сфере данных (ФЗ «О персональных данных», ФЗ «Об информации...», ГК РФ, отраслевое законодательство); типичные коллизии и пробелы в правовом регулировании оборота данных. **ИОПК-3.1 У-1 (Data Law).** ***Умеет:*** применять различные способы толкования для разрешения правовой неопределенности в вопросах сбора, хранения и использования данных; выявлять коллизии между требованиями законодательства о данных и иными отраслевыми нормами (банковская тайна, врачебная тайна) и предлагать способы их преодоления; формулировать обоснованные

					выводы по результатам толкования в форме консультаций и заключений.
	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	ИОПК-7.1 З-1 (Data Law). Знает: современные информационные технологии и системы, используемые для обработки и защиты данных; функциональные возможности справочно-правовых систем для поиска и анализа нормативных актов и судебной практики в сфере Data Law; основные угрозы информационной безопасности и правовые требования к их нейтрализации. ИОПК-7.1 У-1 (Data Law). Умеет: использовать правовые базы данных и специализированное ПО для анализа соответствия систем обработки данных требованиям законодательства; оценивать достаточность организационных и технических мер защиты данных с точки зрения соответствия правовым стандартам; применять цифровые инструменты для подготовки документов, связанных с оборотом данных.

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

Общая трудоемкость дисциплины составляет 216 а.ч. (6 з.е.)

Количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся (очная форма обучения):

2 сем. - лекции – 16 а.ч., практические занятия – 16 а.ч., самостоятельная работа – 72 а.ч., зачет.

3 сем. - лекции – 14 а.ч., практические занятия – 28 а.ч., самостоятельная работа – 37 а. ч., экзамен

Контактная работа на аттестацию в период экзаменационных сессий – 13 часов, самостоятельная работа на подготовку к экзамену – 18 часов, консультации – 2 часа.

Дисциплина *«Правовые режимы данных (Data Law) для консультанта»* относится к дисциплинам обязательной части. Изучается на очной форме обучения - на 1 и 2 курсах.

Для освоения дисциплины «*Правовые режимы данных (Data Law) для консультанта»* обучающиеся используют знания, умения, навыки, способы деятельности и установки, сформированные в ходе изучения дисциплин *«Информационное право», «Информационные технологии в юридической деятельности», «Гражданское право», «Международное право»*.

Форма промежуточной аттестации в соответствии с учебным планом:

Очная форма обучения – экзамен, зачет

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Очная форма обучения

№ п/п	Наименование тем и (или) разделов	ВСЕГО	Объем дисциплины, ак.час											Форма текущего контроля успеваемости, промежуточной аттестации
			Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа		
			Период теоретического обучения						Период промежуточной аттестации (сессия)					
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Кат тэк	Контроль	СРкр	СРэк	СР
			Л	ВЛ	ЛР	ПЗ								
СЕМЕСТР 2 (Зачет) Раздел 1. Базовые концепции и персональные данные														
Тема 1.	Понятие, экономическая природа и правовая квалификация данных (Data as an Asset).	18	2	0	0	2	0	0	0	0		0	0	14	Устный опрос, Ситуационная задача
Тема 2.	Конфиденциальна	20	2	0	0	4	0	0	0	0		0	0	14	Устный опрос,

	я информация: коммерческая, служебная, профессиональная тайна.													Ситуационная задача
Тема 3.	Правовой режим персональных данных (GDPR vs. Российский подход).	23	4	0	0	4	0	0	0	0	0	0	15	Устный опрос, Ситуационная задача
Тема 4.	Трансграничная передача данных и локализация баз данных.	22	4	0	0	4	0	0	0	0	0	0	14	Устный опрос, Ситуационная задача
Тема 5.	Согласие субъекта и законный интерес как правовые основания обработки.	21	4	0	0	2	0	0	0	0	0	0	15	Устный опрос, Ситуационная задача
		108	16	0	0	16	0	0	0	4	0	0	72	Зачет
СЕМЕСТР 3 (Экзамен) Раздел 2. Данные в цифровой экономике и ответственность														
Тема 6.	Правовой режим открытых данных и общедоступной информации.	13	2	0	0	5	0	0	0	0	0	0	6	Устный опрос, Ситуационная задача
Тема 7.	Правовое регулирование Big Data и анализа данных (Data Analytics).	13	2	0	0	5	0	0	0	0	0	0	6	Устный опрос, Ситуационная задача
Тема 8.	Данные как объект интеллектуальной собственности (базы данных, датасеты).	13	2	0	0	5	0	0	0	0	0	0	6	Устный опрос, Ситуационная задача
Тема 9.	Ответственность за нарушение законодательства	12	2	0	0	4	0	0	0	0	0	0	6	Устный опрос, Ситуационная задача

	о данных.													
Тема 10.	Правовые аспекты оборота данных в ИИ-проектах: датасеты для обучения и валидации.	14	3	0	0	5	0	0	0	0	0	0	6	Устный опрос, Ситуационная задача
Тема 11.	Инцидент-менеджмент и реагирование на утечки данных (Data Breach Response).	14	3	0	0	4	0	0	0	0	0	0	7	Устный опрос, Ситуационная задача
		29	14			28			2	9		18	37	Экзамен
Промежуточная аттестация		33							2	13		18		
Итого		216	30	0	0	44	0	0	2	13	0	18	109	

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

СЕМЕСТР 2 (Зачет)

Раздел 1. Базовые концепции и персональные данные (ОПК-1.1, ОПК-3.1, ОПК-7.1)

Тема 1. Понятие, экономическая природа и правовая квалификация данных (Data as an Asset). ОПК-1.1, ОПК-3.1

Формирование понятийного аппарата: данные, информация, цифровой актив. Изучение экономической сущности данных как актива современной компании. Анализ подходов к правовой квалификации данных в российском и зарубежном праве (вещные права, обязательственные права, интеллектуальная собственность, иное имущество). Дискуссия о «праве собственности» на данные и правовом режиме data as an asset для целей консультирования бизнеса.

Тема 2. Конфиденциальная информация: коммерческая, служебная, профессиональная тайна. ОПК-3.1, ОПК-7.1

Обзор режимов конфиденциальной информации по российскому законодательству. Коммерческая тайна: понятие, признаки (режим, гриф «КТ»), меры охраны. Служебная и профессиональная тайна (врачебная, адвокатская, банковская тайна и др.). Разграничение смежных понятий. Особенности консультирования клиентов по внедрению режима коммерческой тайны и защите конфиденциальной информации.

Тема 3. Правовой режим персональных данных (GDPR vs. Российский подход). ОПК-1.1, ОПК-3.1

Основы законодательства о персональных данных (ПДн). Сравнительный анализ принципов обработки ПДн в российском ФЗ-152 и Общем регламенте защиты данных (GDPR) ЕС. Понятие субъекта, оператора и обработчика. Категории ПДн (специальные, биометрические, общедоступные). Особенности применения этих режимов в консультационной практике для российских и международных компаний.

Тема 4. Трансграничная передача данных и локализация баз данных. ОПК-1.1, ОПК-3.1, ОПК-7.1

Правила трансграничной передачи персональных данных. Перечень стран, обеспечивающих адекватную защиту. Требования Роскомнадзора к уведомлениям. Изучение требования о локализации баз данных ПДн на территории РФ. Риски и правовые механизмы для бизнеса при передаче данных через границу. Роль консультанта в аудите трансграничных потоков.

Тема 5. Согласие субъекта и законный интерес как правовые основания обработки. ОПК-1.1, ОПК-7.1

Анализ правовых оснований для обработки персональных данных. Детальный разбор требований к форме и содержанию согласия субъекта (когда оно обязательно). Изучение альтернативного основания — «законный интерес оператора». Практика применения баланса интересов (legitimate interest assessment). Формирование навыков консультирования по выбору надлежащего правового основания.

СЕМЕСТР 3 (Экзамен)

Раздел 2. Данные в цифровой экономике и ответственность (ОПК-1.1, ОПК-3.1, ОПК-7.1)

Тема 6. Правовой режим открытых данных и общедоступной информации. ОПК-1.1, ОПК-3.1

Понятие и виды общедоступной информации. Правовой режим открытых данных (open data) государства и муниципалитетов. Условия использования общедоступных данных, размещенных в интернете. Пределы использования такой информации, защита авторских прав и ПДн в открытых источниках. Консультирование по легальному сбору (парсингу) общедоступных данных.

Тема 7. Правовое регулирование Big Data и анализа данных (Data Analytics). ОПК-1.1, ОПК-3.1

Вызовы регулирования больших данных (Big Data). Проблема обезличивания данных как способа снятия регуляторных ограничений (ПДн, тайна). Правовые риски анализа данных (профилирования, дискриминация, принятие автоматизированных решений). Подходы к саморегулированию и этические кодексы в сфере Big Data. Консультант по внедрению Compliance by Design в проекты анализа данных.

Тема 8. Данные как объект интеллектуальной собственности (базы данных, датасеты). ОПК-3.1, ОПК-7.1

Анализ баз данных и датасетов как объектов авторского права и смежных прав (прав изготовителя базы данных). Условия охраноспособности. Правовой режим программ для ЭВМ и данных как их части. Особенности распоряжения исключительными правами на базы данных. Консультирование по вопросам лицензирования и передачи прав на структурированные наборы данных.

Тема 9. Ответственность за нарушение законодательства о данных. ОПК-1.1, ОПК-3.1, ОПК-7.1

Систематизация видов юридической ответственности за нарушения в сфере оборота данных: административная (штрафы по КоАП РФ, оборотные штрафы за утечки), уголовная, гражданско-правовая (компенсация морального вреда, убытков). Анализ судебной практики и размеров санкций. Оценка рисков для бизнеса-клиента и меры по их минимизации.

Тема 10. Правовые аспекты оборота данных в ИИ-проектах: датасеты для обучения и валидации. ОПК-1.1, ОПК-3.1, ОПК-7.1

Специфика правового режима данных, используемых для обучения систем искусственного интеллекта (ИИ). Проблемы формирования обучающих датасетов: соблюдение авторских прав, защита ПДн, работа с конфиденциальной информацией. Юридические риски на этапах сбора, очистки и валидации данных. Консультирование стартапов и корпораций по Data Governance в проектах ИИ.

Тема 11. Инцидент-менеджмент и реагирование на утечки данных (Data Breach Response). ОПК-1.1, ОПК-7.1

Понятие инцидента информационной безопасности и утечки данных. Алгоритм действий оператора при утечке ПДн по законодательству РФ (взаимодействие с Роскомнадзором и ФСБ России, уведомление субъектов). Внутреннее расследование, взаимодействие с правоохранительными органами. Роль консультанта в антикризисном управлении (crisis management), подготовка отчетности и минимизация репутационных и регуляторных последствий.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.О.07 «Правовые режимы данных (Data

Law) для консультанта» 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.07 «Правовые режимы данных (Data Law) для консультанта» используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

Устный опрос, ситуационная задача, тестирование.

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

Тема 1. Понятие, экономическая природа и правовая квалификация данных (Data as an Asset). ОПК-1.1, ОПК-3.1

Подготовка к практическому занятию:

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

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

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

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

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Являются ли данные самостоятельным объектом гражданских прав по ГК РФ?
2. Что означает концепция «Data as an Asset» (данные как актив) для бизнеса?
3. Какие правовые режимы могут быть применены к данным в зависимости от их характера?
4. Какие основные пробелы существуют в признании данных объектом права в РФ?

Ситуационные задачи.

Ситуационная задача № 1.1

IT-компания «ТехноДата» занимается сбором и обработкой данных о поведении пользователей в интернете. Компания хочет поставить собранные данные на баланс как нематериальный актив, а также заключить договор с крупным рекламным агентством о продаже доступа к этим данным. Финансовый директор спрашивает юриста: «Можем ли мы официально учесть данные как актив и продавать их как товар?»

Вопросы:

1. Являются ли данные самостоятельным объектом гражданских прав по ГК РФ?
2. В каких правовых формах возможна коммерциализация данных (передача прав)?
3. Какие рекомендации вы дадите компании для постановки данных на баланс и их оборота?

Ситуационная задача № 1.2

Стартап «SmartCity» собирает данные с датчиков умного города (трафик, погода, загруженность парковок) и планирует продавать их строительным компаниям для планирования новых объектов. Данные обезличены и не содержат персональных данных. Потенциальный покупатель требует гарантий, что данные не нарушают прав третьих лиц и что стартап вправе их продавать.

Вопросы:

1. Какие правовые риски существуют при обороте таких данных?
2. Нужно ли получать согласие муниципалитета на сбор и продажу данных с городских датчиков?
3. Как юридически оформить передачу данных покупателю?

Тема 2. Конфиденциальная информация: коммерческая, служебная, профессиональная тайна. ОПК-3.1, ОПК-7.1

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. Что относится к коммерческой тайне и каковы условия ее охраны?
2. Чем профессиональная тайна отличается от коммерческой?
3. Какие сведения не могут составлять коммерческую тайну?
4. Какие документы необходимо разработать консультанту для клиента, желающего защитить информацию как коммерческую тайну?

Ситуационные задачи.

Ситуационная задача № 2.1

ООО «Инновация» разработало уникальную технологию производства композитных материалов. Генеральный директор хочет защитить техническую документацию, чертежи, рецептуру и списки поставщиков от конкурентов. В компании работают 50 сотрудников, и регулярно привлекаются сторонние подрядчики для обслуживания оборудования.

Вопросы:

1. Какой правовой режим необходимо ввести для защиты этой информации?
2. Какие документы должен разработать юрист?
3. Какие меры необходимо принять в отношении сотрудников и подрядчиков?

Ситуационная задача № 2.2

К нотариусу обратился бывший сотрудник банка, который требует выдать ему копии кредитных договоров его клиентов для использования в суде против банка (по спору о взыскании убытков). Нотариус отказывает, ссылаясь на банковскую тайну.

Вопросы:

1. Что такое банковская тайна и к какому виду тайн она относится (коммерческая, профессиональная)?
2. Вправе ли нотариус истребовать документы, составляющие банковскую тайну?
3. Каков порядок доступа к сведениям, составляющим банковскую тайну?

Тема 3. Правовой режим персональных данных (GDPR vs. Российский подход). ОПК-1.1, ОПК-3.1

Подготовка к практическому занятию:

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

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

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

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

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Что относится к персональным данным по российскому законодательству?
2. В чем отличие российского подхода к ПД от GDPR?
3. Какие категории персональных данных являются специальными и требуют усиленной защиты?
4. Кто такой оператор персональных данных и каковы его обязанности?

Ситуационные задачи.

Ситуационная задача № 3.1

Российский интернет-магазин «Shop24» продает товары по всему миру, включая страны ЕС. При оформлении заказа магазин собирает стандартные данные: ФИО, адрес доставки, телефон, e-mail, платежные данные. Магазин хранит все данные на серверах в РФ, использует их для маркетинговых рассылок (с согласия) и передает службам доставки. К магазину поступил запрос от гражданина Германии с требованием удалить все его данные (право на забвение). В службе поддержки не знают, что делать.

Вопросы:

1. Подпадает ли российский магазин под действие GDPR?
2. Какие права имеет гражданин ЕС по GDPR?
3. Обязан ли магазин удалить данные по требованию немецкого клиента? Каков порядок действий?

Ситуационная задача № 3.2

Российский банк «Кредит-Капитал» собирает биометрические данные клиентов (изображения лица, образцы голоса) для удаленной идентификации при открытии счетов через мобильное приложение. Банк планирует использовать эти данные также для скоринга (оценки кредитоспособности) и для передачи в бюро кредитных историй.

Вопросы:

1. К какой категории персональных данных относятся биометрические данные по ФЗ-152?
2. Каковы особенности обработки биометрических данных в РФ?
3. Вправе ли банк использовать биометрию для скоринга и передавать в БКИ?

Тема 4. Трансграничная передача данных и локализация баз данных. ОПК-1.1, ОПК-3.1, ОПК-7.1

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. Что такое трансграничная передача персональных данных?
2. Каковы условия трансграничной передачи в РФ?
3. В чем суть требования о локализации баз данных (ст. 18 ФЗ-152)?
4. Какие рекомендации может дать консультант компании, работающей с данными граждан РФ и ЕС?

Ситуационные задачи.

Ситуационная задача № 4.1

Международная IT-компания «CloudCorp» (США) предоставляет облачные услуги российским клиентам. Серверы компании находятся в США и Ирландии. Российский клиент — банк «Новый стандарт» — хочет разместить в облаке базу данных с персональными данными своих клиентов (ФИО, паспортные данные, доходы). Банк обращается к юристу за консультацией.

Вопросы:

1. Соответствует ли размещение ПД граждан РФ на серверах в США и Ирландии требованиям ФЗ-152?
2. Каков порядок трансграничной передачи данных в США и Ирландию?
3. Какие варианты легального использования облачных услуг вы можете предложить банку?

Ситуационная задача № 4.2

Российский стартап «DataLab» разрабатывает мобильное приложение для изучения иностранных языков. Приложение собирает данные пользователей (имя, возраст, прогресс обучения, голосовые записи произношения). Пользователи есть в РФ, странах СНГ и ЕС. Стартап использует облачные серверы в Финляндии (для удобства европейских пользователей) и планирует привлечь инвестиции от американского фонда, который требует доступ к данным для анализа.

Вопросы:

1. Какие требования к локализации и трансграничной передаче нужно соблюсти в отношении пользователей из РФ?
2. Какие требования GDPR нужно соблюсти в отношении пользователей из ЕС?
3. Может ли стартап предоставить американскому инвестору доступ к данным пользователей? Если да, то на каких условиях?

Тема 5. Согласие субъекта и законный интерес как правовые основания обработки. ОПК-1.1, ОПК-7.1

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. Какие требования предъявляются к согласию на обработку персональных данных в РФ?
2. В каких случаях согласие не требуется для обработки персональных данных?
3. Что означает концепция «законный интерес» (legitimate interest) в GDPR?
4. Как консультанту проверить, достаточно ли оснований для обработки данных в проекте клиента?

Ситуационные задачи:

Ситуационная задача № 5.1

Интернет-магазин «Style24» при регистрации пользователя предлагает поставить галочку в чек-боксе с текстом: «Я согласен на обработку моих персональных данных». Ниже мелким шрифтом дана ссылка на Политику обработки ПД (30 страниц). При этом данные используются не только для исполнения заказа, но и для маркетинговых рассылок (включая партнерские), передачи в аналитические системы (Google Analytics, Яндекс.Метрика) и для скоринга платежеспособности. Отдельных согласий на эти цели не запрашивается.

Вопросы:

1. Соответствует ли такая форма получения согласия требованиям ФЗ-152?
2. Какие цели обработки должны быть явно указаны в согласии?
3. Какие риски возникают у магазина и как их минимизировать?

Ситуационная задача № 5.2

Банк «Финанс-Плюс» обрабатывает данные клиентов для целей предотвращения мошенничества (антифрод). Банк анализирует поведение клиентов в мобильном приложении, их транзакции, геолокацию, тип устройства, чтобы выявлять подозрительные операции. Согласие на такую обработку отдельно не запрашивается, банк ссылается на «законный интерес» (ст. 6 ФЗ-152) и на договор банковского счета.

Вопросы:

1. Возможно ли использование законного интереса для антифрод-мониторинга?
2. Какие условия должны быть соблюдены для правомерности обработки на основе законного интереса?
3. Какие риски существуют у банка и как их снизить?

СЕМЕСТР 3 (Экзамен)

Раздел 2. Данные в цифровой экономике и ответственность (ОПК-1.1, ОПК-3.1, ОПК-7.1)

Тема 6. Правовой режим открытых данных и общедоступной информации. ОПК-1.1, ОПК-3.1

Подготовка к практическому занятию:

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

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

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

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

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Что понимается под общедоступными персональными данными?
2. Каковы риски обработки данных из открытых источников?
3. Какие данные являются открытыми данными государства?
4. Каков правовой режим использования открытых государственных данных в коммерческих целях?

Ситуационные задачи.

Ситуационная задача № 6.1

Маркетинговое агентство «SmartTarget» собирает данные из открытых профилей пользователей в социальных сетях (ВКонтакте, Instagram*) для таргетированной рекламы. Агентство собирает: имя, возраст, город, интересы (по подпискам), фотографии профиля, список друзей. Эти данные используются для сегментации аудитории и продажи рекламодателям. Агентство считает, что раз данные открытые, то согласие не требуется.

Вопросы:

1. Относятся ли данные из открытых профилей к общедоступным персональным данным (ст. 8 ФЗ-152)?
2. Каковы риски такого сбора и использования?
3. Какие рекомендации вы дадите агентству?

Ситуационная задача № 6.2

Аналитический центр «Городские решения» использует открытые данные портала data.gov.ru для прогнозирования транспортных потоков. Центр скачал датасеты о ДТП, ремонтах дорог и работе светофоров. На основе этих данных разрабатывается мобильное приложение для водителей с платной подпиской.

Вопросы:

1. Вправе ли центр использовать открытые государственные данные в коммерческих целях?
2. Есть ли ограничения на такое использование?
3. Нужно ли указывать источник данных?

Тема 7. Правовое регулирование Big Data и анализа данных (Data Analytics). ОПК-1.1, ОПК-3.1

Подготовка к практическому занятию:

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

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

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

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

Вопросы к практическому занятию для проведения опроса:

Вопросы для устного опроса:

1. Что такое Big Data с правовой точки зрения?
2. Что такое обезличивание персональных данных и какие существуют методы?
3. Какие правовые риски возникают при аналитике Big Data?
4. Как консультанту обеспечить правовую чистоту проекта по аналитике данных?

Ситуационные задачи.

Ситуационная задача № 7.1

Ритейлер «СуперМаркет» собирает данные о покупках своих клиентов по картам лояльности (ФИО, телефон, состав покупок, сумма, время). Компания хочет использовать эти данные для аналитики: выявлять тренды, прогнозировать спрос, сегментировать аудиторию для рассылок. Маркетологи также хотят передавать обезличенные агрегированные данные производителям товаров за плату.

Вопросы:

1. Какие правовые основания нужны для сбора и аналитики данных?
2. Что такое обезличивание и достаточно ли его для передачи данных производителям?
3. Какие риски возникают при передаче агрегированных данных третьим лицам?

Ситуационная задача № 7.2

Страховая компания «Защита» внедряет систему анализа телематических данных с автомобилей клиентов (датчики скорости, стиля вождения, пробега). На основе этих данных компания хочет рассчитывать индивидуальные тарифы ОСАГО: аккуратным водителям — скидки, агрессивным — повышающие коэффициенты. Клиенты дают согласие на установку датчиков и сбор данных при заключении договора.

Вопросы:

1. Какие правовые риски возникают при использовании телематических данных для тарификации?
2. Может ли компания использовать данные для повышения тарифа (ухудшения положения клиента)?
3. Требуется ли дополнительное согласие на такую обработку?

Тема 8. Данные как объект интеллектуальной собственности (базы данных, датасеты). ОПК-3.1, ОПК-7.1

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. Что признается базой данных как объектом авторского права?
2. Какие права существуют на базы данных?
3. Что такое датасет и как его защитить?
4. Какие условия необходимо включить в договор на создание датасета?

Ситуационные задачи.

Ситуационная задача № 8.1

Научно-исследовательский институт (НИИ) создал уникальную базу данных генетических последовательностей редких растений. Сотрудники института собирали образцы в экспедициях, проводили секвенирование, систематизировали данные, написали программное обеспечение для поиска. Институт хочет зарегистрировать права на базу данных и продавать доступ фармацевтическим компаниям.

Вопросы:

1. Какие права возникают на базу данных?
2. Что такое смежное право изготовителя базы данных (ст. 1333-1336 ГК РФ)?
3. Как институту защитить свои права и оформить передачу прав фармкомпаниям?

Ситуационная задача № 8.2

Стартап «DataMine» нанял фрилансера для сбора и структурирования датасета изображений животных для обучения нейросети. Фрилансер скачал изображения из открытых источников (Google Images, Flickr, соцсети), подписал их и передал заказчику. Через полгода стартап получил претензию от фотографа, чье изображение использовано в датасете, с требованием компенсации за нарушение авторских прав.

Вопросы:

1. Кто несет ответственность за нарушение авторских прав — стартап или фрилансер?
2. Какие риски возникают при использовании изображений из интернета для датасетов?
3. Как стартапу обезопасить себя при создании датасетов?

Тема 9. Ответственность за нарушение законодательства о данных. ОПК-1.1, ОПК-3.1, ОПК-7.1

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. Какие виды ответственности предусмотрены за нарушение законодательства о персональных данных?
2. Каков размер штрафов за утечку персональных данных по новым правилам (2024)?
3. Что такое моральный вред и как он компенсируется при утечке данных?
4. Какие рекомендации дать клиенту для минимизации рисков ответственности?

Ситуационные задачи.

Ситуационная задача № 9.1

Интернет-магазин «МодныйШоп» допустил утечку базы данных клиентов: хакеры получили доступ к ФИО, адресам, телефонам, e-mail и хешированным паролям. Утечка затронула 150 000 человек. Роскомнадзор начал проверку. Выяснилось, что магазин хранил данные без шифрования, не уведомил РКН о начале обработки (как оператор) и не имел политики обработки ПД.

Вопросы:

1. Какие составы административных правонарушений усматриваются?
2. Каков размер возможных штрафов?
3. Какие действия необходимо предпринять магазину для минимизации ответственности?

Ситуационная задача № 9.2

Бывший сотрудник банка передал коллекторскому агентству базу данных должников, с которыми банк уже не работал. Коллекторы начали звонить этим людям, требуя погасить долги (уступленные банком коллекторам ранее). Один из должников обратился в суд, узнав, что его данные были переданы без его согласия.

Вопросы:

1. Кто является надлежащим ответчиком по иску должника?
2. Какие нормы права нарушены?
3. Какова возможная ответственность бывшего сотрудника и коллекторского агентства?

Тема 10. Правовые аспекты оборота данных в ИИ-проектах: датасеты для обучения и валидации. ОПК-1.1, ОПК-3.1, ОПК-7.1

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. Какие требования предъявляются к обучающим выборкам для ИИ?
2. Что такое TDM (text and data mining) и как оно регулируется в РФ?
3. Какие риски возникают при использовании датасетов, скачанных из интернета?
4. Как консультанту провести legal due diligence датасета?

Ситуационные задачи.

Ситуационная задача № 10.1

IT-компания «AI-Solutions» разрабатывает систему распознавания лиц для офисных пропусков. Для обучения нейросети компания использовала датасет, скачанный с GitHub (открытый датасет лиц людей из разных стран, собранный университетом для научных целей). Лицензия на датасет — MIT (разрешает коммерческое использование с указанием авторства). При этом в датасете есть фотографии, которые могут быть персональными данными (лица). Компания планирует продавать систему корпоративным клиентам.

Вопросы:

1. Достаточно ли лицензии MIT для коммерческого использования датасета?
2. Какие риски, связанные с персональными данными, возникают при использовании такого датасета?
3. Какие меры должна принять компания для легального использования датасета и обучения модели?

Ситуационная задача № 10.2

Банк «Кредит-Про» разрабатывает модель ИИ для кредитного скоринга на основе данных своих клиентов за 10 лет: анкетные данные, доходы, кредитная история, транзакции по счетам. Банк хочет передать обезличенный датасет (без ФИО, паспортных данных, но с полными транзакциями и доходами) дочерней IT-компании для обучения модели. IT-компания затем вернет обученную модель банку.

Вопросы:

1. Являются ли данные о транзакциях и доходах персональными данными после удаления ФИО?
2. Какое правовое основание необходимо для передачи датасета IT-компании?
3. Какие меры безопасности и договорные условия должны быть предусмотрены?

Тема 11. Инцидент-менеджмент и реагирование на утечки данных (Data Breach Response). ОПК-1.1, ОПК-7.1

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. Что такое инцидент безопасности персональных данных?
2. Каков порядок уведомления Роскомнадзора об утечке персональных данных?
3. Какие действия должен предпринять оператор при обнаружении утечки?
4. Что должен включать план реагирования на инциденты (Incident Response Plan)?

Ситуационные задачи.

Ситуационная задача № 11.1

В пятницу вечером системный администратор ООО «Логистика-Сервис» обнаружил, что база данных клиентов (ФИО, паспортные данные, адреса, история заказов) была скопирована неизвестными. Следы взлома ведут к одному из сотрудников, который уволился на прошлой неделе. База содержит данные 50 000 клиентов. Администратор сообщил генеральному директору.

Вопросы:

1. Каковы первые действия компании в первые часы после обнаружения утечки?
2. Каковы сроки уведомления Роскомнадзора по новым правилам (с 2024 г.)?
3. Нужно ли уведомлять самих клиентов?

Ситуационная задача № 11.2

Медицинская клиника «Здоровье+» обнаружила, что из-за ошибки в настройках доступа к электронной медицинской системе данные пациентов (диагнозы, результаты анализов, паспортные данные) в течение двух недель были доступны в интернете без пароля. Клиника устранила проблему, но точно неизвестно, скачивал ли кто-то данные. Юрист клиники спрашивает, нужно ли сообщать об инциденте в Роскомнадзор и пациентам.

Вопросы:

1. Является ли данная ситуация утечкой, требующей уведомления РКН?
2. Какие факторы влияют на решение об уведомлении пациентов?
3. Каковы возможные последствия, если клиника не сообщит об инциденте, а позже выяснится, что данные были скачаны?

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

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

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

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

Формула расчета результата контрольной точки:

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

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

КТ – 1.
Тема 1-11.
Доклад.
Тематика докладов:

Раздел 1. Базовые концепции и персональные данные

Тема 1. Понятие, экономическая природа и правовая квалификация данных (Data as an Asset)

1. Информация, данные, сведения: соотношение понятий в праве и экономике.
2. Данные как нематериальный актив (Data as an Asset): балансовая стоимость, капитализация, оборот.
3. Правовой режим информации по 149-ФЗ: виды информации по доступу (общедоступная, ограниченного доступа) и по роли (массовая, рекламная, документированная).
4. Информация как объект гражданских прав (ст. 128 ГК РФ): дискуссия об оборотоспособности.
5. Субъекты информационных правоотношений: обладатель информации, оператор информационной системы, пользователь.

Тема 2. Конфиденциальная информация: коммерческая, служебная, профессиональная тайна

1. Понятие и признаки конфиденциальности информации. Перечень сведений конфиденциального характера (Указ Президента № 188).
2. Коммерческая тайна (ФЗ-98): условия охраноспособности, режим коммерческой тайны, гриф «Коммерческая тайна».
3. Ответственность за разглашение коммерческой тайны (ст. 183 УК РФ, ст. 14.33 КоАП РФ).
4. Служебная тайна: понятие и отграничение от коммерческой и государственной тайны.
5. Профессиональная тайна (банковская, врачебная, нотариальная, адвокатская, аудиторская тайна): особенности режима и субъектный состав.

Тема 3. Правовой режим персональных данных (GDPR vs. Российский подход)

1. Понятие персональных данных (ПДн) по ФЗ-152 и GDPR: сходства и различия.
2. Принципы обработки ПДн законность, справедливость, минимизация, точность, ограничение хранения).

3. Категории субъектов ПДн (потребители, сотрудники, кандидаты, родственники).
4. Правовой статус оператора и обработчика.
5. Специальные категории ПДн (расовая, национальная принадлежность, политические взгляды, здоровье).
6. Биометрические ПДн: понятие, правовой режим, информированное согласие.
7. Трансграничная передача данных: адекватность защиты, типовые договоры, BCRs.
8. Требование о локализации баз данных (ст. 18 ФЗ-152): практика применения.

Тема 4. Трансграничная передача данных и локализация баз данных

1. Понятие трансграничной передачи данных (ТГПД) в РФ и ЕС.
2. Перечень стран — членов Совета Европы и иных стран, не являющихся членами Совета Европы, но обеспечивающих адекватную защиту прав субъектов ПДн (Приказ Роскомнадзора).
3. Иные правовые основания для ТГПД: согласие, исполнение договора, госинтересы.
4. Механизмы обеспечения защиты при ТГПД в страны, не обеспечивающие адекватной защиты.
5. Требование о локализации (ст. 18 ФЗ-152): систематизация, запись, хранение. Ответственность за неисполнение.

Тема 5. Согласие субъекта и законный интерес как правовые основания обработки

1. Согласие на обработку ПДн: конклюдентное действие, письменная форма, "галочка" на сайте.
2. Содержание согласия: перечень данных, цели обработки, срок действия, способ отзыва.
3. Иные правовые основания обработки (ч. 1 ст. 6 ФЗ-152, ст. 6 GDPR):
   - исполнение договора;
   - выполнение функций госоргана;
   - защита жизни и здоровья;
   - законный интерес оператора.
4. Тест баланса интересов (Legitimate Interest Assessment) при обработке на основании законного интереса.
5. Принцип минимизации данных (Data Minimization).

Раздел 2. Данные в цифровой экономике и ответственность

Тема 6. Правовой режим открытых данных и общедоступной информации

1. Понятие открытых данных (Open Data). Портал открытых данных РФ.
2. Общедоступные персональные данные (ст. 8 ФЗ-152): источники, порядок использования, право на исключение.
3. Информация, обязательная к размещению (данные госорганов, АО, профессиональных участников рынка).
4. Право на забвение (ст. 10.3 ФЗ-149): субъекты, порядок реализации, отказ.

Тема 7. Правовое регулирование Big Data и анализа данных (Data Analytics)

1. Понятие и признаки больших данных (Volume, Velocity, Variety).
2. Правовые риски Big Data:
   - обезличивание и риск деанонимизации;
   - профилирование и дискриминация;
   - Data power и антимонопольное регулирование (злоупотребление доминирующим положением на рынке данных).
3. Правовые режимы обезличенных данных: понятие, порядок обезличивания, использование обезличенных данных.

Тема 8. Данные как объект интеллектуальной собственности (базы данных, датасеты)

1. База данных как объект авторского права (ст. 1260 ГК РФ): творческий характер подбора и расположения материалов.

2. Право изготовителя базы данных (sui generis право, ст. 1333-1336 ГК РФ): субъекты, условия возникновения, срок действия, исключительное право.
3. Соотношение авторского права на структуру и смежного права на содержание.
4. Датасет (Dataset) для машинного обучения: понятие, состав, правовая природа. Отличие от базы данных.

Тема 9. Ответственность за нарушение законодательства о данных

1. Административная ответственность (КоАП РФ):
   - ст. 13.11 — нарушение законодательства о ПДн (оборотные штрафы за утечки);
   - ст. 13.14 — разглашение информации с ограниченным доступом.
2. Уголовная ответственность (УК РФ):
   - ст. 137 — нарушение неприкосновенности частной жизни;
   - ст. 183 — незаконные получение и разглашение коммерческой, налоговой или банковской тайны;
   - ст. 272 — неправомерный доступ к компьютерной информации.
3. Гражданско-правовая ответственность: возмещение убытков, компенсация морального вреда.

Тема 10. Правовые аспекты оборота данных в ИИ-проектах: датасеты для обучения и валидации

1. Жизненный цикл данных в ИИ-проекте: сбор, очистка, аннотирование (разметка), обучение, валидация, эксплуатация.
2. Источники данных: собственные данные, краулинг (веб-скрейпинг), открытые датасеты, покупка данных.
3. Правовые риски краулинга: нарушение авторских прав (если контент охраняется), нарушение условий использования сайта (Terms of Service), несанкционированный доступ (Computer Fraud and Abuse Act в США).
4. «Грязные данные» (biased data) и ответственность за дискриминационные решения ИИ.

Тема 11. Инцидент-менеджмент и реагирование на утечки данных (Data Breach Response)

1. Инцидент информационной безопасности: понятие, виды (утечка, потеря целостности, недоступность).
2. Обязанности оператора при утечке ПДн по 152-ФЗ (ст. 21.1):
   - уведомление Роскомнадзора (в течение 24 часов);
   - уведомление субъектов ПДн.
3. Внутренние процедуры: порядок локализации инцидента, расследования, оценки ущерба.
4. Взаимодействие с правоохранительными органами и регулятором в период расследования.
5. Кризисная коммуникация (PR-сопровождение).

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 1-11

Устный опрос:

Вопросы для опроса:

№ п.п.	Содержание вопроса
1.	Информация, данные, сведения: соотношение понятий в праве и экономике.
2.	Данные как нематериальный актив (Data as an Asset): балансовая стоимость, капитализация, оборот.
3.	Правовой режим информации по 149-ФЗ: виды информации по доступу (общедоступная, ограниченного доступа) и по роли (массовая, рекламная, документированная).
4.	Информация как объект гражданских прав (ст. 128 ГК РФ): дискуссия об оборотоспособности.

5.	Понятие и признаки конфиденциальности информации. Перечень сведений конфиденциального характера (Указ Президента № 188).
6.	Коммерческая тайна (ФЗ-98): условия охраноспособности, режим коммерческой тайны, гриф «Коммерческая тайна».
7.	Ответственность за разглашение коммерческой тайны (ст. 183 УК РФ, ст. 14.33 КоАП РФ).
8.	Служебная тайна: понятие и отграничение от коммерческой и государственной тайны.
9.	Понятие персональных данных (ПДн) по ФЗ-152 и GDPR: сходства и различия.
10.	Принципы обработки ПДн законность, справедливость, минимизация, точность, ограничение хранения).
11.	Категории субъектов ПДн (потребители, сотрудники, кандидаты, родственники).
12.	Правовой статус оператора и обработчика.
13.	Понятие трансграничной передачи данных (ТГПД) в РФ и ЕС.
14.	Перечень стран — членов Совета Европы и иных стран, не являющихся членами Совета Европы, но обеспечивающих адекватную защиту прав субъектов ПДн (Приказ Роскомнадзора).
15.	Иные правовые основания для ТГПД: согласие, исполнение договора, госинтересы.
16.	Механизмы обеспечения защиты при ТГПД в страны, не обеспечивающие адекватной защиты.
17.	Согласие на обработку ПДн: конклюдентное действие, письменная форма, "галочка" на сайте.
18.	Содержание согласия: перечень данных, цели обработки, срок действия, способ отзыва.
19.	Тест баланса интересов (Legitimate Interest Assessment) при обработке на основании законного интереса.
20.	Принцип минимизации данных (Data Minimization).
21.	Понятие открытых данных (Open Data). Портал открытых данных РФ.
22.	Общедоступные персональные данные (ст. 8 ФЗ-152): источники, порядок использования, право на исключение.
23.	Информация, обязательная к размещению (данные госорганов, АО, профессиональных участников рынка).
24.	Право на забвение (ст. 10.3 ФЗ-149): субъекты, порядок реализации, отказ.
25.	Понятие и признаки больших данных (Volume, Velocity, Variety).
26.	Правовые риски Big Data (обезличивание и риск деанонимизации; профилирование и дискриминация; Data power и антимонопольное регулирование (злоупотребление доминирующим положением на рынке данных)).
27.	Правовые режимы обезличенных данных: понятие, порядок обезличивания, использование обезличенных данных.
28.	База данных как объект авторского права (ст. 1260 ГК РФ): творческий характер подбора и расположения материалов.
29.	Право изготовителя базы данных (sui generis право, ст. 1333-1336 ГК РФ): субъекты, условия возникновения, срок действия, исключительное право.
30.	Соотношение авторского права на структуру и смежного права на содержание.
31.	Датасет (Dataset) для машинного обучения: понятие, состав, правовая природа. Отличие от базы данных.
32.	Административная ответственность (КоАП РФ) за нарушение законодательства о ПДн (оборотные штрафы за утечки) и за разглашение информации с ограниченным доступом.

33.	Уголовная ответственность (УК РФ) за нарушение неприкосновенности частной жизни; за незаконные получение и разглашение коммерческой, налоговой или банковской тайны; за неправомерный доступ к компьютерной информации.
34.	Гражданско-правовая ответственность: возмещение убытков, компенсация морального вреда.
35.	Жизненный цикл данных в ИИ-проекте: сбор, очистка, аннотирование (разметка), обучение, валидация, эксплуатация.
36.	Источники данных: собственные данные, краулинг (веб-скрейпинг), открытые датасеты, покупка данных.
37.	Правовые риски краулинга: нарушение авторских прав (если контент охраняется), нарушение условий использования сайта (Terms of Service), несанкционированный доступ (Computer Fraud and Abuse Act в США).
38.	«Грязные данные» (biased data) и ответственность за дискриминационные решения ИИ.
39.	Инцидент информационной безопасности: понятие, виды (утечка, потеря целостности, недоступность).
40.	Обязанности оператора при утечке ПДн по 152-ФЗ (ст. 21.1)
41.	Внутренние процедуры: порядок локализации инцидента, расследования, оценки ущерба.
42.	Взаимодействие с правоохранительными органами и регулятором в период расследования.
43.	Кризисная коммуникация (PR-сопровождение).

Критерии оценивания опроса:

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

КТ – 3.
Темы 1-1

Тестирование

1. Что из перечисленного НЕ является объектом гражданских прав согласно ст. 128 ГК РФ?
A. Информация
B. Вещи
C. Нематериальные блага
D. Результаты интеллектуальной деятельности

2. Какой признак характеризует понятие «данные» в отличие от «информации»?
A. Данные всегда являются конфиденциальными
B. Данные — это информация, представленная в формализованном виде, пригодном для обработки
C. Данные — это синоним понятия «сведения»
D. Данные всегда охраняются авторским правом

3. Что является обязательным условием для признания информации коммерческой тайной?
A. Государственная регистрация информации
B. Введение режима коммерческой тайны обладателем информации
C. Наличие грифа «Секретно»
D. Публикация в официальных источниках

4. Какая информация НЕ может составлять коммерческую тайну?
A. Сведения о численности и составе работников
B. Результаты интеллектуальной деятельности
C. Технологическая информация
D. Сведения об используемых сырье и материалах

5. Какое определение персональных данных дано в ФЗ-152?
A. Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу
B. Только паспортные данные
C. Информация о юридическом лице
D. Только биометрические данные

6. Что из перечисленного относится к специальным категориям персональных данных?
A. Фамилия и имя
B. Данные о расовой принадлежности
C. Адрес проживания
D. Номер телефона

7. Что понимается под трансграничной передачей персональных данных?
A. Передача данных внутри одной организации
B. Передача данных на территорию иностранного государства
C. Передача данных в другой город
D. Передача данных по Wi-Fi

8. Какие страны считаются обеспечивающими адекватную защиту прав субъектов ПДн?
A. Все страны мира
B. Только страны-члены ЕС

C. Страны-члены Совета Европы и иные страны, утвержденные Роскомнадзором
D. Только США

9. Какие обязательные элементы должно содержать согласие на обработку ПДн?
A. Только ФИО субъекта
B. ФИО, адрес субъекта, цель обработки, перечень данных, срок действия, порядок отзыва
C. Только цель обработки
D. Только подпись

10. Что означает "конклюдентное действие" как форма согласия?
A. Письменное заявление
B. Действия субъекта, явно свидетельствующие о его согласии (например, проставление отметки на сайте)
C. Молчание субъекта
D. Нотариально заверенное согласие

11. Что понимается под открытыми данными?
A. Секретные данные
B. Информация, размещаемая в сети "Интернет" в формате, обеспечивающем ее автоматическую обработку без предварительных изменений
C. Только новостные ленты
D. Персональные данные без ограничений

12. Что относится к общедоступным персональным данным?
A. Данные, доступ к которым предоставлен субъектом или которые опубликованы в открытых источниках (например, справочники, СМИ)
B. Любые данные из социальных сетей
C. Паспортные данные
D. Биометрические данные

13. Какие характеристики (VVV) определяют понятие "Big Data"?
A. Variety, Value, Victory
B. Volume (объем), Velocity (скорость), Variety (многообразие)
C. Vision, Voice, Video
D. Virtual, Visual, Vocal

14. Что такое обезличивание персональных данных?
A. Уничтожение данных
B. Действия, в результате которых становится невозможным определить принадлежность ПДн конкретному субъекту без использования дополнительной информации
C. Шифрование данных
D. Копирование данных

15. Что является объектом авторского права в базе данных?
A. Содержание базы (все данные)
B. Подбор и расположение материалов (структура), являющиеся результатом творческого труда
C. Аппаратное обеспечение сервера
D. Название базы данных

16. Кто обладает смежным правом изготовителя базы данных (sui generis право)?

A. Автор программы для ЭВМ
B. Лицо, организовавшее создание базы данных и понесшее существенные финансовые затраты
C. Пользователь базы данных
D. Государство

17. Какая статья КоАП РФ устанавливает ответственность за нарушение законодательства о персональных данных?
A. Ст. 13.11
B. Ст. 6.13
C. Ст. 5.35
D. Ст. 20.25

18. Что такое "оборотный штраф" за утечку данных?
A. Штраф, рассчитываемый как процент от выручки компании
B. Штраф за невыполнение оборота товаров
C. Штраф за торговлю без лицензии
D. Фиксированный штраф

19. Что такое «веб-скрейпинг» (web scraping)?
A. Создание веб-сайтов
B. Автоматизированный сбор данных с веб-страниц
C. Удаление веб-страниц
D. Дизайн веб-сайтов

20. Что такое «Terms of Service» (ToS) и как они связаны со сбором данных?
A. Это условия использования сервиса, которые могут запрещать автоматизированный сбор данных (скрейпинг)
B. Это техническая документация
C. Это гарантийный талон
D. Это лицензия на ПО

21. В течение какого времени оператор обязан уведомить Роскомнадзор о факте утечки персональных данных?
A. 7 дней
B. 24 часа
C. 3 дня
D. 1 месяц

22. Что должно содержать уведомление в Роскомнадзор об инциденте?
A. Только название компании
B. Дату обнаружения, причины, категории и объем утечки, принятые меры
C. Только количество пострадавших
D. Только ФИО директора

Критерии оценивания тестовых заданий:

Диапазон баллов	Описание критерия	
85-100	Свыше 80% правильных ответов.	Обучающийся демонстрирует глубокое познание в освоенном материале.

65-84	Свыше 70% правильных ответов.	Обучающимся материал освоен полностью, без существенных ошибок.
55-64	Свыше 50% правильных ответов.	Обучающимся материал освоен не полностью, имеются значительные пробелы в знаниях.
0-54	Менее 50% правильных ответов.	Обучающимся материал не освоен, знания обучающегося ниже базового уровня.

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

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

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

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

6.2. Типовые оценочные материалы промежуточной аттестации

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

СЕМЕСТР 2 (Зачет)

Раздел 1. Базовые концепции и персональные данные (ОПК-1.1, ОПК-3.1, ОПК-7.1)

Тема 1. Понятие, экономическая природа и правовая квалификация данных (Data as an Asset). ОПК-1.1, ОПК-3.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Являются ли данные самостоятельным объектом гражданских прав по ГК РФ?
2.	Что означает концепция «Data as an Asset» (данные как актив) для бизнеса?
3.	Какие правовые режимы могут быть применены к данным в зависимости от их характера?
4.	Какие основные пробелы существуют в признании данных объектом права в РФ?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	С точки зрения современного		

	права, данные (Big Data) как экономический актив характеризуются тем, что: а) являются традиционным объектом вещных прав (имуществом); б) имеют неоднородную структуру, включают различные виды информации (персональные данные, объекты интеллектуальной собственности, иную информацию) и могут представлять имущественный интерес для участников оборота; в) не могут быть предметом гражданско-правовых договоров; г) всегда являются общедоступной информацией и не имеют коммерческой ценности.		
2.	В чем заключается ключевая особенность данных как объекта прав по сравнению с традиционными материальными активами? а) Данные могут одновременно принадлежать множеству лиц и использоваться ими без утраты содержания (неконкурентность в потреблении); б) Данные всегда имеют строго одного собственника; в) Данные нельзя копировать; г) Данные не могут быть объектом кражи.		

3. Задания закрытого типа.

Тестовые задания.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Тест 1.1: Что из перечисленного НЕ является объектом гражданских прав согласно ст. 128 ГК РФ?
A. Информация
B. Вещи
C. Нематериальные блага
D. Результаты интеллектуальной деятельности

Тест 1.2: Какой признак характеризует понятие «данные» в отличие от «информации»?
A. Данные всегда являются конфиденциальными
B. Данные — это информация, представленная в формализованном виде, пригодном для обработки
C. Данные — это синоним понятия «сведения»
D. Данные всегда охраняются авторским правом

Тест 1.3: Кто является обладателем информации согласно ФЗ-149 «Об информации...»?
A. Только собственник материального носителя
B. Лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации
C. Любой пользователь информационной системы
D. Только государственные органы

Тест 1.4: Что понимается под термином «Data as an Asset»?
A. Данные как объект бухгалтерского учета с обязательной амортизацией
B. Признание данных в качестве экономического ресурса, имеющего стоимость и способного приносить доход
C. Данные как неотчуждаемое нематериальное благо
D. Только те данные, которые запатентованы

Тема 2. Конфиденциальная информация: коммерческая, служебная, профессиональная тайна. ОПК-3.1, ОПК-7.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Что относится к коммерческой тайне и каковы условия ее охраны?
2.	Чем профессиональная тайна отличается от коммерческой?
3.	Какие сведения не могут составлять коммерческую тайну?
4.	Какие документы необходимо разработать консультанту для клиента, желающего защитить информацию как коммерческую тайну?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Принятый в ЕС Регламент о данных (Data Act) устанавливает новый подход к		

	данным, которые одновременно являются коммерческой тайной (trade secrets) производителя, и на которые пользователь имеет право доступа. Согласно этому подходу: а) наличие статуса коммерческой тайны является безусловным основанием для отказа в предоставлении доступа к данным; б) производитель обязан предоставить доступ к данным, даже если они содержат коммерческую тайну, но при этом может принять разумные меры конфиденциальности (соглашения о неразглашении, технические меры) и в исключительных случаях отказать при угрозе серьезного экономического ущерба; в) данные, являющиеся коммерческой тайной, полностью исключены из сферы действия Регламента; г) вопрос о коммерческой тайне полностью передан на усмотрение пользователя.		
2.	Для того чтобы информация о клиентах, алгоритмах или структуре датасета могла быть защищена в режиме коммерческой тайны (ст. 1465 ГК РФ), необходимо выполнение совокупности условий, одним из которых является: а) регистрация информации в Федеральной службе по интеллектуальной собственности; б) введение обладателем режима коммерческой тайны, то есть принятие разумных мер для сохранения ее конфиденциальности (гриф "КТ", локальные акты, договоры с контрагентами); в) наличие у информации		

	физического носителя (бумажного или электронного), который нельзя скопировать; г) распространение информации в средствах массовой информации.		

3. Задания закрытого типа.

Тестовые задания.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Тест 2.1: Что является обязательным условием для признания информации коммерческой тайной?
A. Государственная регистрация информации
B. Введение режима коммерческой тайны обладателем информации
C. Наличие грифа «Секретно»
D. Публикация в официальных источниках

Тест 2.2: Какая информация НЕ может составлять коммерческую тайну?
A. Сведения о численности и составе работников
B. Результаты интеллектуальной деятельности
C. Технологическая информация
D. Сведения об используемых сырье и материалах

Тест 2.3: Какая ответственность предусмотрена за разглашение коммерческой тайны?
A. Только дисциплинарная
B. Только гражданско-правовая
C. Дисциплинарная, гражданско-правовая, административная и уголовная
D. Только административная

Тест 2.4: Что относится к профессиональной тайне?
A. Государственная тайна
B. Банковская тайна
C. Военная тайна
D. Данные космической съемки

Тема 3. Правовой режим персональных данных (GDPR vs. Российский подход). ОПК-1.1, ОПК-3.1

1. Задания открытого типа.

№ п.п.	Вопрос

1.	Что относится к персональным данным по российскому законодательству?
2.	В чем отличие российского подхода к ПД от GDPR?
3.	Какие категории персональных данных являются специальными и требуют усиленной защиты?
4.	Кто такой оператор персональных данных и каковы его обязанности?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	В 2025 году российское законодательство о персональных данных претерпело существенные изменения. Какое из следующих положений характеризует новое требование к получению согласия на обработку персональных данных, действующее с 1 сентября 2025 года? а) Согласие на обработку персональных данных может быть включено в текст пользовательского соглашения или договора в виде отдельного пункта; б) Согласие на обработку персональных данных должно быть полностью отделено от других документов и согласий, которые подписывает или подтверждает субъект (запрет на "связанные" согласия); в) Согласие на обработку персональных данных больше не требуется, если данные обрабатываются в коммерческих целях; г) Согласие должно быть заверено нотариально во всех случаях.		
2.	Ключевое различие в подходах к основанию обработки данных между GDPR и российским 152-ФЗ до недавнего времени заключалось в том, что:		

	а) GDPR полностью запрещает обработку персональных данных, а 152-ФЗ разрешает; б) 152-ФЗ позволяет оператору выбирать любое основание (согласие, договор, законный интерес) по своему усмотрению, часто допуская их "стекование" (наложение), в то время как проект реформы в РФ предлагает ограничить использование согласия, смещая приоритет на иные основания, что сближает системы; в) российское законодательство не содержит понятия "обработка данных"; г) оба закона идентичны.		

3. Задания закрытого типа.

Тестовые задания.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Тест 3.1: Какое определение персональных данных дано в ФЗ-152?
A. Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу
B. Только паспортные данные
C. Информация о юридическом лице
D. Только биометрические данные

Тест 3.2: Что из перечисленного относится к специальным категориям персональных данных?
A. Фамилия и имя
B. Данные о расовой принадлежности
C. Адрес проживания
D. Номер телефона

Тест 3.3: Какой принцип НЕ является принципом обработки персональных данных?
A. Законность и справедливость
B. Минимизация обрабатываемых данных
C. Максимизация собираемых данных на всякий случай
D. Точность и достаточность данных

Тест 3.4: Что такое GDPR?

A. Российский закон о данных
B. Общий регламент по защите данных Европейского Союза
C. Американский акт о конфиденциальности
D. Международный стандарт шифрования

Тема 4. Трансграничная передача данных и локализация баз данных. ОПК-1.1, ОПК-3.1, ОПК-7.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Что такое трансграничная передача персональных данных?
2.	Каковы условия трансграничной передачи в РФ?
3.	В чем суть требования о локализации баз данных (ст. 18 ФЗ-152)?
4.	Какие рекомендации может дать консультант компании, работающей с данными граждан РФ и ЕС?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	С 1 июля 2025 года в России вступила в силу новая редакция ч. 5 ст. 18 Федерального закона «О персональных данных» о локализации. Как изменилось требование к обработке персональных данных граждан РФ? а) Требование локализации полностью отменено для иностранных IT-компаний; б) Закон теперь прямо запрещает запись, систематизацию, накопление, хранение, уточнение, извлечение персональных данных граждан РФ с использованием баз данных, находящихся за пределами России (при сборе); в) Требование осталось прежним, но штрафы снижены; г) Локализация требуется только для биометрических		

	данных.		
2.	При осуществлении трансграничной передачи персональных данных из ЕС в третью страну, не имеющую решения Еврокомиссии об адекватном уровне защиты, оператор может использовать механизм дерогаций (частичных отступлений). В каком случае передача данных допустима без специальных гарантий (SCC, BCR)? а) Всегда, если компания зарегистрирована в России; б) Если субъект данных дал прямое согласие на передачу, будучи проинформированным о возможных рисках из-за отсутствия адекватной защиты; в) Ни при каких обстоятельствах; г) Только если данные передаются внутри одной корпоративной группы.		

3. Задания закрытого типа.

Тестовые задания.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Тест 4.1: Что понимается под трансграничной передачей персональных данных?
A. Передача данных внутри одной организации
B. Передача данных на территорию иностранного государства
C. Передача данных в другой город
D. Передача данных по Wi-Fi

Тест 4.2: Какие страны считаются обеспечивающими адекватную защиту прав субъектов ПДн?
A. Все страны мира
B. Только страны-члены ЕС
C. Страны-члены Совета Европы и иные страны, утвержденные Роскомнадзором
D. Только США

Тест 4.3: Что должно быть сделано до начала трансграничной передачи данных в страну, не обеспечивающую адекватной защиты?

A. Ничего, передача свободна
B. Получение согласия субъекта в письменной форме
C. Уведомление ФСБ
D. Получение разрешения Президента

Тест 4.4: Куда оператор должен направить уведомление о намерении осуществлять трансграничную передачу данных?
A. В прокуратуру
B. В Роскомнадзор
C. В ФСБ
D. Никуда, уведомление не требуется

Тема 5. Согласие субъекта и законный интерес как правовые основания обработки. ОПК-1.1, ОПК-7.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Какие требования предъявляются к согласию на обработку персональных данных в РФ?
2.	В каких случаях согласие не требуется для обработки персональных данных?
3.	Что означает концепция «законный интерес» (legitimate interest) в GDPR?
4.	Как консультанту проверить, достаточно ли оснований для обработки данных в проекте клиента?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Российская практика обработки персональных данных долгое время допускала использование "связанных" согласий (например, пункт в договоре или в пользовательском соглашении). Новое регулирование 2025 года направлено на борьбу с этим явлением, устанавливая правило о том, что: а) согласие должно быть "активным" и явно выделенным, а не просто предполагаемым из факта заключения договора; б) согласие больше не нужно; в) согласие может быть только		

	устным; г) согласие должно храниться у нотариуса.		
2.	В законодательстве ЕС (GDPR) и в проектах реформы российского законодательства обработка персональных данных на основе "законного интереса" (legitimate interest) контролера возможна при условии, что: а) контролер просто заявил о своем интересе, и этого достаточно; б) проведен балансирующий тест (balancing test), доказывающий, что законные интересы контролера не превалируют над фундаментальными правами и свободами субъекта данных; в) субъект данных не возражает против обработки; г) данные являются общедоступными.		

3. Задания закрытого типа.

Тестовые задания.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Тест 5.1: Какие обязательные элементы должно содержать согласие на обработку ПДн?
A. Только ФИО субъекта
B. ФИО, адрес субъекта, цель обработки, перечень данных, срок действия, порядок отзыва
C. Только цель обработки
D. Только подпись

Тест 5.2: Что означает "конклюдентное действие" как форма согласия?
A. Письменное заявление
B. Действия субъекта, явно свидетельствующие о его согласии (например, проставление отметки на сайте)
C. Молчание субъекта
D. Нотариально заверенное согласие

Тест 5.3: В каком случае обработка ПДн возможна на основании "законного интереса"?
A. Всегда, если это выгодно оператору

B. Если обработка необходима для реализации прав и законных интересов оператора или третьих лиц, при условии, что они не нарушают права субъекта
C. Никогда
D. Только для государственных органов

Тест 5.4: Что такое Legitimate Interest Assessment (LIA)?
A. Оценка законного интереса — тест баланса интересов оператора и прав субъекта
B. Финансовый аудит
C. Проверка бухгалтерской отчетности
D. Оценка стоимости бизнеса

СЕМЕСТР 3 (Экзамен)
Раздел 2. Данные в цифровой экономике и ответственность
(ОПК-1.1, ОПК-3.1, ОПК-7.1)

Тема 6. Правовой режим открытых данных и общедоступной информации. ОПК-1.1, ОПК-3.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Что понимается под общедоступными персональными данными?
2.	Каковы риски обработки данных из открытых источников?
3.	Какие данные являются открытыми данными государства?
4.	Каков правовой режим использования открытых государственных данных в коммерческих целях?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	В чем принципиальное отличие "открытых данных" (open data), публикуемых государственными органами, от просто "общедоступной информации" по смыслу ст. 7 Закона «Об информации»? а) Открытые данные публикуются в формате, обеспечивающем их автоматизированную обработку в целях повторного использования (машиночитаемый формат); б) Открытые данные могут использоваться только государственными		

	служащими; в) Открытые данные — это всегда персональные данные; г) Открытые данные не имеют юридической силы.		
2.	Международный опыт (например, Нью-Йорк) показывает, что эффективное функционирование порталов открытых данных требует законодательного закрепления не только обязанности публиковать данные, но и: а) требования о публикации словарей данных (data dictionaries) и обеспечении своевременного обновления информации; б) запрета на использование открытых данных в коммерческих целях; в) требования хранить все данные только в бумажном виде; г) ограничения доступа к данным для иностранцев.		

3. Задания закрытого типа.

Тестовые задания.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Тест 6.1: Что понимается под открытыми данными?
A. Секретные данные
B. Информация, размещаемая в сети "Интернет" в формате, обеспечивающем ее автоматическую обработку без предварительных изменений
C. Только новостные ленты
D. Персональные данные без ограничений

Тест 6.2: Что относится к общедоступным персональным данным?
A. Данные, доступ к которым предоставлен субъектом или которые опубликованы в открытых источниках (например, справочники, СМИ)
B. Любые данные из социальных сетей
C. Паспортные данные
D. Биометрические данные

Тест 6.3: Что такое «право на забвение» (ст. 10.3 ФЗ-149)?

A. Право не помнить плохое
B. Право гражданина требовать удаления ссылок на информацию о себе, распространяемую с нарушением закона или недостоверную
C. Право забыть пароль
D. Право на удаление аккаунта

Тест 6.4: Кто обязан рассматривать запросы о "праве на забвение"?
A. Любой гражданин
B. Оператор поисковой системы
C. Суд
D. Прокурор

Тема 7. Правовое регулирование Big Data и анализа данных (Data Analytics). ОПК-1.1, ОПК-3.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Что такое Big Data с правовой точки зрения?
2.	Что такое обезличивание персональных данных и какие существуют методы?
3.	Какие правовые риски возникают при аналитике Big Data?
4.	Как консультанту обеспечить правовую чистоту проекта по аналитике данных?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Согласно российским стратегическим документам (Национальная стратегия развития ИИ) и экспертным оценкам, основным правовым барьером для развития технологий анализа больших данных (Big Data) является: а) полное отсутствие интернета на территории РФ; б) конфликт между потребностями бизнеса в анализе массивов данных и жесткими рамками законодательства о персональных данных, не всегда учитывающего технологии обезличивания; в) запрет на использование любых баз данных;		

	г) отсутствие компьютеров.		
2.	Ключевой характеристикой, отличающей Big Data от обычных массивов информации, является совокупность признаков "4V". Что из перечисленного НЕ входит в стандартный набор этих признаков? а) Volume (большой объем); б) Variety (разнообразие); в) Velocity (высокая скорость изменения); г) Vulnerability (уязвимость).		

3. Задания закрытого типа.

Тестовые задания.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Тест 7.1: Какие характеристики (VVV) определяют понятие "Big Data"?
A. Variety, Value, Victory
B. Volume (объем), Velocity (скорость), Variety (многообразие)
C. Vision, Voice, Video
D. Virtual, Visual, Vocal

Тест 7.2: Что такое обезличивание персональных данных?
A. Уничтожение данных
B. Действия, в результате которых становится невозможным определить принадлежность ПДн конкретному субъекту без использования дополнительной информации
C. Шифрование данных
D. Копирование данных

Тест 7.3: Какой риск связан с деанонимизацией данных?
A. Риск потери пароля
B. Возможность восстановления связи обезличенных данных с конкретным субъектом
C. Риск поломки сервера
D. Риск вирусной атаки

Тест 7.4: Что такое «профилирование» в контексте обработки данных?
A. Создание профиля в социальных сетях
B. Автоматизированная обработка данных для оценки определенных аспектов личности, поведения, интересов
C. Фотографирование
D. Составление психологического портрета вручную

Тема 8. Данные как объект интеллектуальной собственности (базы данных, датасеты). ОПК-3.1, ОПК-7.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Что признается базой данных как объектом авторского права?
2.	Какие права существуют на базы данных?
3.	Что такое датасет и как его защитить?
4.	Какие условия необходимо включить в договор на создание датасета?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Сбор и подготовка датасета (набора данных) для машинного обучения часто осуществляется методами веб-скрапинга (автоматического сбора данных из открытых источников). С правовой точки зрения, такой датасет может: а) никогда не охраняться как объект интеллектуальной собственности; б) охраняться смежным правом изготовителя базы данных (sui generis right) как результат существенных инвестиций в создание базы данных, если соблюдены условия закона (существенность затрат); в) автоматически становиться объектом авторского права, так как в нем много цифр; г) принадлежать каждому пользователю интернета.		
2.	Датасеты, используемые для обучения нейросетей, часто включают объекты авторского права (изображения, тексты), принадлежащие третьим лицам. Это создает проблему "входных данных" (input). При каком условии использование		

	таких объектов для создания коммерческого датасета будет правомерным в РФ? а) Использование любых объектов из интернета разрешено законом; б) Необходимо получить разрешение правообладателя (лицензию) или убедиться, что использование подпадает под случай свободного использования (например, в информационных, научных или образовательных целях), что для коммерческого ML-обучения является спорным; в) Достаточно сослаться на источник заимствования; г) Можно использовать все, что найдено в открытом доступе.		

3. Задания закрытого типа.

Тестовые задания.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Тест 8.1: Что является объектом авторского права в базе данных?
A. Содержание базы (все данные)
B. Подбор и расположение материалов (структура), являющиеся результатом творческого труда
C. Аппаратное обеспечение сервера
D. Название базы данных

Тест 8.2: Кто обладает смежным правом изготовителя базы данных (sui generis право)?
A. Автор программы для ЭВМ
B. Лицо, организовавшее создание базы данных и понесшее существенные финансовые затраты
C. Пользователь базы данных
D. Государство

Тест 8.3: Сколько лет действует исключительное право изготовителя базы данных?
A. 5 лет
B. 15 лет
C. 25 лет
D. 70 лет

Тест 8.4: Что такое датасет (dataset) в контексте машинного обучения?
A. Любая база данных
B. Структурированная совокупность данных, размеченная для обучения модели ИИ
C. Компьютерная программа
D. Алгоритм шифрования

Тема 9. Ответственность за нарушение законодательства о данных. ОПК-1.1, ОПК-3.1, ОПК-7.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Какие виды ответственности предусмотрены за нарушение законодательства о персональных данных?
2.	Каков размер штрафов за утечку персональных данных по новым правилам (2024)?
3.	Что такое моральный вред и как он компенсируется при утечке данных?
4.	Какие рекомендации дать клиенту для минимизации рисков ответственности?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	С 30 мая 2025 года в России существенно выросли штрафы за утечки персональных данных. Какая новая мера ответственности была введена для компаний за повторную утечку данных, затронувшую большое количество субъектов? а) Пожизненное лишение свободы для генерального директора; б) Оборотный штраф в размере от 1% до 3% совокупной выручки компании, но не менее 20 млн рублей; в) Запрет на осуществление деятельности навсегда; г) Принудительная ликвидация компании.		
2.	Какая категория утечек персональных данных влечет		

	максимальный фиксированный штраф (до 20 млн рублей) согласно новым нормам КоАП РФ (ст. 13.11), введенным в 2025 году? а) Утечка фамилий и адресов; б) Утечка биометрических персональных данных; в) Утечка общедоступных данных; г) Утечка данных о любимом цвете сотрудников.		

3. Задания закрытого типа.

Тестовые задания.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Тест 9.1: Какая статья КоАП РФ устанавливает ответственность за нарушение законодательства о персональных данных?
A. Ст. 13.11
B. Ст. 6.13
C. Ст. 5.35
D. Ст. 20.25

Тест 9.2: Что такое "оборотный штраф" за утечку данных?
A. Штраф, рассчитываемый как процент от выручки компании
B. Штраф за невыполнение оборота товаров
C. Штраф за торговлю без лицензии
D. Фиксированный штраф

Тест 9.3: Какая статья УК РФ предусматривает ответственность за нарушение неприкосновенности частной жизни?
A. Ст. 137
B. Ст. 158
C. Ст. 105
D. Ст. 161

Тест 9.4: Что является объектом преступления по ст. 272 УК РФ?
A. Персональные данные
B. Компьютерная информация
C. Денежные средства
D. Недвижимость

Тема 10. Правовые аспекты оборота данных в ИИ-проектах: датасеты для обучения и валидации. ОПК-1.1, ОПК-3.1, ОПК-7.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Какие требования предъявляются к обучающим выборкам для ИИ?
2.	Что такое TDM (text and data mining) и как оно регулируется в РФ?
3.	Какие риски возникают при использовании датасетов, скачанных из интернета?
4.	Как консультанту провести legal due diligence датасета?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	Проблема "выходных данных" (output) в машинном обучении заключается в неопределенности правового статуса результатов, созданных нейросетью. Согласно доминирующему подходу в российском праве, результат, полностью сгенерированный ИИ без творческого вклада человека: а) является объектом авторского права, принадлежащим разработчику нейросети; б) не признается объектом авторского права, так как не создан творческим трудом человека, и его правовой режим нуждается в специальном урегулировании; в) является общественным достоянием с момента создания; г) принадлежит тому, кто первый его сохранил.		
2.	При формировании датасета для обучения модели ИИ разработчик сталкивается с проблемой "входных данных" (input). Использование данных из открытых источников (например, по лицензии Creative Commons) допустимо, но юрист должен проверить:		

	а) только то, что файл был скачан бесплатно; б) условия конкретной лицензии (например, требует ли она указания авторства — BY, запрещает ли коммерческое использование — NC, требует ли распространения производных на тех же условиях — SA), так как эти условия обязательны при создании производного датасета или использовании его в коммерческом продукте; в) что данные не защищены авторским правом; г) наличие у файла зеленого цвета.		

3. Задания закрытого типа.

Тестовые задания.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Тест 10.1: Что такое «веб-скрейпинг» (web scraping)?
A. Создание веб-сайтов
B. Автоматизированный сбор данных с веб-страниц
C. Удаление веб-страниц
D. Дизайн веб-сайтов

Тест 10.2: Что такое «Terms of Service» (ToS) и как они связаны со сбором данных?
A. Это условия использования сервиса, которые могут запрещать автоматизированный сбор данных (скрейпинг)
B. Это техническая документация
C. Это гарантийный талон
D. Это лицензия на ПО

Тест 10.3: Что относится к этапам жизненного цикла данных в ИИ-проекте?
A. Только обучение модели
B. Сбор, очистка, аннотирование, обучение, валидация, эксплуатация
C. Только удаление данных
D. Только хранение

Тест 10.4: Что такое "разметка данных" (аннотирование)?
A. Проставление водяных знаков
B. Процесс присвоения меток данным для обучения модели с учителем
C. Удаление лишних данных

D. Шифрование данных

Тема 11. Инцидент-менеджмент и реагирование на утечки данных (Data Breach Response). ОПК-1.1, ОПК-7.1

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Что такое инцидент безопасности персональных данных?
2.	Каков порядок уведомления Роскомнадзора об утечке персональных данных?
3.	Какие действия должен предпринять оператор при обнаружении утечки?
4.	Что должен включать план реагирования на инциденты (Incident Response Plan)?

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

№ п.п.	Содержание задания	Правильный ответ	Аргументы, обосновывающие выбор ответа
1.	С 30 мая 2025 года в России введена обязанность операторов уведомлять Роскомнадзор об утечках персональных данных. Каков срок и последствия нарушения этой обязанности? а) Уведомлять не нужно, если утечка небольшая; нарушение не наказывается; б) Необходимо уведомить Роскомнадзор об утечке; за неисполнение этой обязанности (или несвоевременное уведомление) предусмотрен штраф до 3 млн рублей; в) Уведомлять нужно только прокуратуру, но не Роскомнадзор; г) Уведомление должно быть направлено в течение 1 минуты после обнаружения утечки.		
2.	Помимо штрафов за саму утечку и за неуведомление, новое российское законодательство предусматривает возможность привлечения к		

	ответственности за "действия (бездействие) оператора, повлекшие утечку". По какому принципу дифференцируется размер штрафа в этом случае? а) В зависимости от погоды в день утечки; б) В зависимости от количества пострадавших субъектов (носителей ID) и объема утекших данных (специальные, биометрические, иные); в) Штраф всегда фиксирован и не зависит от объема; г) Размер штрафа определяет сам оператор.		

3. Задания закрытого типа.

Тестовые задания.

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

Внимательно прочитать предложенные варианты ответа.

Выбрать один верный ответ.

Записать только букву выбранного варианта ответа.

Тест 11.1: В течение какого времени оператор обязан уведомить Роскомнадзор о факте утечки персональных данных?
A. 7 дней
B. 24 часа
C. 3 дня
D. 1 месяц

Тест 11.2: Что должно содержать уведомление в Роскомнадзор об инциденте?
A. Только название компании
B. Дату обнаружения, причины, категории и объем утечки, принятые меры
C. Только количество пострадавших
D. Только ФИО директора

Тест 11.3: В каком случае оператор обязан уведомить субъектов персональных данных об утечке?
A. Всегда
B. Если Роскомнадзор признает, что это необходимо для защиты прав субъектов
C. Никогда
D. Только по решению суда

Тест 11.4: Что такое «инцидент информационной безопасности»?
A. Любое событие в IT-системе
B. Событие, нарушающее конфиденциальность, целостность или доступность информации

C. Плановое отключение сервера
D. Установка обновлений

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 навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено, т.е. обучающийся не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.	0-19

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

7. Методические материалы по освоению дисциплины

Подготовка к лекциям.

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы. В основу его нужно положить рабочие программы изучаемых в семестре дисциплин. Каждому обучающемуся следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Самостоятельная работа на лекции.

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

Подготовка к практическим занятиям.

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

работ.

Структура практического занятия:

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

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

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

Работа с литературными источниками.

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

Вопросы для самостоятельной подготовки к лекционным и практическим занятиям:

Часть 1. Базовые концепции и персональные данные

1. Информация, данные, сведения: соотношение понятий в праве и экономике.
2. Данные как нематериальный актив (Data as an Asset): балансовая стоимость, капитализация, оборот.

3. Правовой режим информации по 149-ФЗ: виды информации по доступу (общедоступная, ограниченного доступа) и по роли (массовая, рекламная, документированная).
4. Информация как объект гражданских прав (ст. 128 ГК РФ): дискуссия об оборотоспособности.
5. Субъекты информационных правоотношений: обладатель информации, оператор информационной системы, пользователь.
6. Понятие и признаки конфиденциальности информации. Перечень сведений конфиденциального характера (Указ Президента № 188).
7. Коммерческая тайна (ФЗ-98): условия охраноспособности, режим коммерческой тайны, гриф «Коммерческая тайна».
8. Ответственность за разглашение коммерческой тайны (ст. 183 УК РФ, ст. 14.33 КоАП РФ).
9. Служебная тайна: понятие и отграничение от коммерческой и государственной тайны.
10. Профессиональная тайна (банковская, врачебная, нотариальная, адвокатская, аудиторская тайна): особенности режима и субъектный состав.
11. Понятие персональных данных (ПДн) по ФЗ-152 и GDPR: сходства и различия.
12. Принципы обработки ПДн законность, справедливость, минимизация, точность, ограничение хранения).
13. Категории субъектов ПДн (потребители, сотрудники, кандидаты, родственники).
14. Правовой статус оператора и обработчика.
15. Специальные категории ПДн (расовая, национальная принадлежность, политические взгляды, здоровье).
6. Биометрические ПДн: понятие, правовой режим, информированное согласие.
17. Трансграничная передача данных: адекватность защиты, типовые договоры, BCRs.
18. Требование о локализации баз данных (ст. 18 ФЗ-152): практика применения.
19. Понятие трансграничной передачи данных (ТГПД) в РФ и ЕС.
20. Перечень стран — членов Совета Европы и иных стран, не являющихся членами Совета Европы, но обеспечивающих адекватную защиту прав субъектов ПДн (Приказ Роскомнадзора).
21. Иные правовые основания для ТГПД: согласие, исполнение договора, госинтересы.
22. Механизмы обеспечения защиты при ТГПД в страны, не обеспечивающие адекватной защиты.
23. Требование о локализации (ст. 18 ФЗ-152): систематизация, запись, хранение. Ответственность за неисполнение.
24. Согласие на обработку ПДн: конклюдентное действие, письменная форма, "галочка" на сайте.
25. Содержание согласия: перечень данных, цели обработки, срок действия, способ отзыва.
26. Иные правовые основания обработки данных (ч. 1 ст. 6 ФЗ-152, ст. 6 GDPR) (исполнение договора; выполнение функций госоргана; защита жизни и здоровья; законный интерес оператора).
27. Тест баланса интересов (Legitimate Interest Assessment) при обработке на основании законного интереса.
28. Принцип минимизации данных (Data Minimization).

Часть 2. Данные в цифровой экономике и ответственность
1. Понятие открытых данных (Open Data). Портал открытых данных РФ.
2. Общедоступные персональные данные (ст. 8 ФЗ-152): источники, порядок использования, право на исключение.
3. Информация, обязательная к размещению (данные госорганов, АО, профессиональных участников рынка).

4. Право на забвение (ст. 10.3 ФЗ-149): субъекты, порядок реализации, отказ.
5. Понятие и признаки больших данных (Volume, Velocity, Variety).
6. Правовые риски Big Data (обезличивание и риск деанонимизации; профилирование и дискриминация; Data power и антимонопольное регулирование (злоупотребление доминирующим положением на рынке данных)).
7. Правовые режимы обезличенных данных: понятие, порядок обезличивания, использование обезличенных данных.
8. База данных как объект авторского права (ст. 1260 ГК РФ): творческий характер подбора и расположения материалов.
9. Право изготовителя базы данных (sui generis право, ст. 1333-1336 ГК РФ): субъекты, условия возникновения, срок действия, исключительное право.
10. Соотношение авторского права на структуру и смежного права на содержание.
11. Датасет (Dataset) для машинного обучения: понятие, состав, правовая природа. Отличие от базы данных.
12. Административная ответственность (КоАП РФ) (ст. 13.11 — нарушение законодательства о ПДн (оборотные штрафы за утечки); ст. 13.14 — разглашение информации с ограниченным доступом).
13. Уголовная ответственность (УК РФ) (ст. 137 — нарушение неприкосновенности частной жизни; ст. 183 — незаконные получение и разглашение коммерческой, налоговой или банковской тайны; ст. 272 — неправомерный доступ к компьютерной информации).
14. Гражданско-правовая ответственность: возмещение убытков, компенсация морального вреда.
15. Жизненный цикл данных в ИИ-проекте: сбор, очистка, аннотирование (разметка), обучение, валидация, эксплуатация.
16. Источники данных: собственные данные, краулинг (веб-скрейпинг), открытые датасеты, покупка данных.
17. Правовые риски краулинга: нарушение авторских прав (если контент охраняется), нарушение условий использования сайта (Terms of Service), несанкционированный доступ (Computer Fraud and Abuse Act в США).
18. «Грязные данные» (biased data) и ответственность за дискриминационные решения ИИ.
19. Инцидент информационной безопасности: понятие, виды (утечка, потеря целостности, недоступность).
20. Обязанности оператора при утечке ПДн по 152-ФЗ (ст. 21.1) (уведомление Роскомнадзора (в течение 24 часов); уведомление субъектов ПДн).
21. Внутренние процедуры: порядок локализации инцидента, расследования, оценки ущерба.
22. Взаимодействие с правоохранительными органами и регулятором в период расследования.
23. Кризисная коммуникация (PR-сопровождение).

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 4-е изд. — Москва : РИОР : ИНФРА-М, 2026. — 398 с. — (Высшее образование). — DOI: https://doi.org/10.29039/ 03014-1. - ISBN 978-5-369-03014-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2242341 (дата обращения: 10.06.2026). – Режим доступа: по подписке.

2. Цифровое право : учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. — 2-е изд. — Москва : Проспект, 2025. — 882 с. — ISBN 978-5-392-44782-4.

3. Антонова, Е. Е. Правовой режим информации ограниченного доступа : практикум / Е. Е. Антонова, О. А. Бояринцева, А. Н. Гулемин. — Екатеринбург : Изд-во УМЦ УПИ, 2025. — 69 с. — ISBN 978-5-8295-0940-8.

4. Щепеткина, И. В. Правовое регулирование в информационной сфере : учебное пособие / И. В. Щепеткина, А. В. Андреев, Е. Н. Щепеткин ; Министерство науки и высшего образования Российской Федерации, Уральский государственный лесотехнический университет. — Екатеринбург : УГЛТУ, 2025. — 174 с. — ISBN 978-5-94984-948-4.

5. Братановский, С. Н. Специальные правовые режимы информации [Электронный ресурс] / С. Н. Братановский. - Саратов: «Научная книга», 2010. - 172 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/416111 (дата обращения: 08.06.2026). – Режим доступа: по подписке.

6.Smart Law for Smart Industry / под редакцией Е. В. Титовой, Т. П. Подшивалова. — Москва : Проспект, 2020. — 320 с. — ISBN 978-5-9988-1181-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/227225 (дата обращения: 08.06.2026). — Режим доступа: для авториз. пользователей.

7. Савельев, А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» / А. И. Савельев. — Москва : СТАТУТ, 2017. — 320 с. — ISBN 978-5-8354-1365-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/107544 (дата обращения: 08.06.2026). — Режим доступа: для авториз. пользователей.

8. Лескина, Э.И. Характеристика отдельных правовых режимов больших данных (Big Data) / Э. И. Лескина // Теоретическая и прикладная юриспруденция. — 2025. — № 1. — С. 102-116. — ISSN 2686-7834. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/journal/issue/369743 (дата обращения: 08.06.2026). — Режим доступа: для авториз. пользователей.

9. Макоха, А. Н. Базы данных и экспертные системы : учебное пособие (курс лекций) / А. Н. Макоха, И. А. Журавлева. - Ставрополь : Изд-во СКФУ, 2020. - 336 с. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2133600 (дата обращения: 07.06.2026). – Режим доступа: по подписке.

8.2. Дополнительная литература

1. Разъяснения Роскомнадзора по вопросам применения законодательства о персональных данных (2025). (Позиции регулятора, озвученные на Дне открытых дверей Роскомнадзора 27 августа 2025 года и иных публичных мероприятиях, касающиеся новых требований к согласию, локализации баз данных, трансграничной передаче и иным аспектам обработки данных).

2. Правовые позиции Роскомнадзора о мультиоператорском согласии и трансграничной передаче данных. (Разъяснения регулятора о допустимости единого согласия на обработку несколькими операторами при совпадении целей и сроков обработки, а также о критериях отнесения передачи данных к трансграничной).

3. Аналитические материалы по применению Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (с изм. от 24.06.2025). (Обзоры и комментарии к последним изменениям законодательства о персональных данных, включая новые требования к локализации баз данных и форме согласия).

4. Международные исследования в области Data Law. (Научные статьи и доклады, посвященные сравнительному анализу подходов к регулированию данных в различных юрисдикциях, включая вопросы регуляторной конкуренции и гармонизации права данных).

8.3. Нормативные правовые документы и иная правовая информация

Российская Федерация

1. Конституция Российской Федерации (ст. 23, 24 о праве на неприкосновенность частной жизни, недопустимости сбора информации о частной жизни лица без его согласия).
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 24.06.2025, с изм. и доп., вступ. в силу с 01.09.2025). (Базовый закон, определяющий основные понятия: информация, конфиденциальность информации, обладатель информации, оператор информационной системы, а также правовые режимы общедоступной информации и информации ограниченного доступа. Содержит принципы правового регулирования отношений в сфере информации).
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 24.06.2025, с изм., вступ. в силу с 01.09.2025). (Основополагающий акт, регулирующий обработку персональных данных, устанавливающий требования к согласию, трансграничной передаче, локализации баз данных, права субъектов персональных данных и обязанности операторов. Последние изменения касаются усиления требований к локализации и форме согласия).
4. Федеральный закон от 02.10.2023 № 408-ФЗ (о внесении изменений в законодательство об информации и информационных технологиях, регулирующий применение рекомендательных технологий и обработку данных в соответствующих системах).
5. Федеральный закон от 28.12.2024 № 519-ФЗ (о внесении изменений в Федеральный закон «О персональных данных», уточняющий порядок обработки персональных данных, разрешенных субъектом для распространения).
6. Приказ Роскомнадзора от 24.02.2021 № 18 (об утверждении требований к подтверждению уничтожения персональных данных).
7. Приказ Роскомнадзора от 28.10.2022 № 179 (об утверждении требований к подтверждению уничтожения персональных данных — действующая редакция).
8. Кодекс Российской Федерации об административных правонарушениях (ст. 13.11 — ответственность за нарушение законодательства о персональных данных, включая новые составы правонарушений).

Международное и зарубежное регулирование

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR). (Основополагающий акт ЕС в сфере защиты персональных данных, задающий стандарты для многих юрисдикций).
2. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+) — Council of Europe Treaty Series No. 108, as modernized by Protocol CETS No. 223. (Международный договор, устанавливающий стандарты защиты данных).
3. Актуальные редакции законодательства о персональных данных стран — торговых партнеров (включая изменения в Федеральный закон РФ № 152-ФЗ, влияющие на трансграничную передачу).

8.4. Интернет-ресурсы

1. Официальный интернет-портал правовой информации (www.pravo.gov.ru). (Гарантированный источник опубликования федеральных законов и указов Президента РФ).
2. СПС «КонсультантПлюс» (www.consultant.ru). (Профессиональная справочная система, содержащая актуальные редакции документов, включая 149-ФЗ и 152-ФЗ с последними изменениями от 2025 года, судебную практику, комментарии и аналитические статьи. Содержит тематические подборки по информационному праву и защите персональных данных).
3. СПС «Гарант» (www.garant.ru). (Альтернативная справочная система с широким набором документов по правовым режимам информации).

4. Официальный сайт Роскомнадзора (rkn.gov.ru). (Сайт регулятора в сфере персональных данных. Содержит разъяснения по применению законодательства, реестры операторов, информацию о проверках, позиции по вопросам трансграничной передачи и локализации данных, материалы публичных мероприятий).
5. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций РФ (digital.gov.ru). (Информация о государственной политике в сфере обработки данных, проектах нормативных актов).
6. ГАС «Правосудие» (sudrf.ru) и Картотека арбитражных дел (kad.arbitr.ru). (Ресурсы для мониторинга судебной практики по спорам, связанным с обработкой данных и защитой информации, включая новые дела по ч. 10 ст. 13.11 КоАП РФ о неуведомлении Роскомнадзора).
7. Портал Европейского Союза EUR-Lex (eur-lex.europa.eu). (Официальный источник для изучения GDPR и иных актов европейского законодательства в сфере данных).
8. Научная электронная библиотека eLIBRARY.RU (elibrary.ru). (Доступ к полным текстам статей из российских научных журналов по информационному праву и правовым режимам данных).
9. Профессиональные ресурсы по комплаенсу в сфере данных (comply.ru и аналогичные). (Площадки для отслеживания актуальных позиций регуляторов, разъяснений и практики применения законодательства, включая обзоры мероприятий Роскомнадзора).

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

9.1. Материально-техническая база

Перечень материально-технического обеспечения:

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

9.2. Информационные технологии, программное обеспечение:

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

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

9.3. Информационные справочные системы:

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