Лебедева Екатерина Александровна
Подписано цифровой подписью: Лебедева Екатерина Александровна
Дата: 2026.06.25 14:42:36 +03'00'

Приложение 4

к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.04 Основы кибербезопасности в информационных и цифровых системах
(индекс, наименование дисциплины в соответствии с учебным планом)

40.04.01 Юриспруденция
(код, наименование направления подготовки/специальности)

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:

Чайка Юлия Валерьевна, старший преподаватель кафедры гражданского и международного права

Заведующий кафедрой:

Калинина Евгения Валерьевна, д-р. юрид. наук., доцент, заведующий кафедрой гражданского и международного права

Рабочая программа дисциплины Б1.В.04 Основы кибербезопасности в информационных и цифровых системах одобрена на заседании кафедры гражданского и международного права

протокол № 6 от «4» марта 2026 г.

3. СОДЕРЖАНИЕ

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

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

Дисциплина Б1.В.04 Основы кибербезопасности в информационных и цифровых системах обеспечивает формирование у обучающихся следующих универсальных, общепрофессиональных и профессиональных компетенций*:

ОТФ/ТФ и реквизиты ПС *(при наличии)* **	**Код компетенции** **	**Наименование Компетенции** **	**Код индикатора достижения компетенций** **	**Наименование индикатора достижения компетенций** **	**Образовательный результат** **
	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИУК-1.1	Определяет стратегию действий на основе критического анализа и системного подхода	**Знать:** правовые и технологические принципы обеспечения приватности данных (PETs), включая дифференциальную приватность, гомоморфное шифрование, безопасные многосторонние вычисления, нулевое разглашение, синтетические данные. **Уметь:** критическ и оценивать правовые риски обработки персональных данных и выбирать адекватную стратегию их минимизации с использованием PETs. **Владеть:** навыка ми системного

					анализа правовых проблем и выработки стратегии внедрения PETs для соблюдения требований законодательства о персональных данных.
	ПКс-ИИ-1	Способен анализировать правовые риски и разрабатывать юридические модели внедрения и эксплуатации систем искусственного интеллекта (АИ) в бизнес-процессы организации, включая оценку соответствия законодательству о персональных данных, интеллектуальной собственности и конкуренции	ИПКс-ИИ-1.1	Разрабатывает юридические модели и рекомендации по внедрению и эксплуатации систем АИ в бизнес-процессы, обеспечивающие минимизацию правовых рисков и соответствие требованиям законодательства о персональных данных, интеллектуальной собственности и конкуренции. Проводит комплексный правовой аудит (due diligence) АИ-проекта на всех этапах его жизненного цикла (данные, обучение, эксплуатация) и формирует карту рисков	**Знать:** требования Федерального закона «О персональных данных» (152-ФЗ), GDPR, принципы data minimization, purpose limitation, accountability, а также правовые последствия использования PETs для соблюдения этих требований. **Уметь:** проводить правовой аудит АИ-проектов на предмет соответствия требованиям приватности и разрабатывать рекомендации по применению PETs (дифференциальной приватности, синтетических данных, SMPC и др.). **Владеть:** методами юридической оценки PETs и навыками интеграции PETs в политики обработки данных

					организации, включая документацию DPIA.
	ПКс-ИИ-3	Способен представлять интересы клиентов в спорах, связанных с причинением вреда решениями АИ, защитой интеллектуальных прав на AI-модели и данные, а также в административных процедурах, связанных с регулированием инновационных технологий	ИПКс-ИИ-3.1	Разрабатывает правовые позиции и процессуальные документы (исковые заявления, отзывы, ходатайства, жалобы) для защиты интересов клиентов в спорах, связанных с причинением вреда решениями АИ и нарушением интеллектуальных прав на AI-модели и данные. Представляет интересы клиентов во взаимодействии с регуляторами (Роскомнадзор, ФАС, ФСТЭК и др.) в рамках административных процедур, связанных с расследованием инцидентов и регулированием инновационных технологий	**Знать:** практику привлечения к ответственности за утечки данных (ст. 13.11 КоАП РФ), основания для проведения проверок Роскомнадзора, порядок расследования инцидентов и роль PETs как доказательства принятия достаточных мер. **Уметь:** формировать правовую позицию по спорам, связанным с недостаточной защитой данных, и обосновывать применение PETs в качестве надлежащей меры защиты (надлежащей технологии приватности). **Владеть:** навыками подготовки процессуальных документов, ходатайств о назначении компьютерной экспертизы и взаимодействия с регуляторами по вопросам применения PETs.

** Дисциплина может формировать компетенцию полностью или частично.*

***Должно соответствовать Приложению 1 к образовательной программе*

2. Объем и место дисциплины в структуре образовательной программы

Общая трудоемкость дисциплины составляет 108 а.ч. (3 з.е.)

Количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся составляет 47 часов, в том числе:

- очная форма обучения:

4 сем. - лекции – 12 а.ч., лабораторные занятия – 2 а.ч., практические занятия – 22 а.ч., самостоятельная работа – 43 а.ч., контактная работа на аттестацию в период экзаменационных сессий – 9 часов, самостоятельная работа на подготовку к экзамену – 18 часов, консультации – 2 часа.

Дисциплина *«Б1.В.04 Технологии приватности (Privacy-Enhancing Technologies – PETs) и их правовая оценка»* относится к элективной части, формируемой участниками самостоятельно. Изучается в 4 семестре 2 курса магистерской программы.

Для освоения дисциплины «*Б1.В.04 Технологии приватности (Privacy-Enhancing Technologies – PETs) и их правовая оценка»* обучающиеся используют знания, умения, навыки, способы деятельности и установки, сформированные в ходе изучения дисциплин: *«Информационные технологии в юридической деятельности», «Информационное право», «Правовые режимы данных «Data Law)»*.

Форма промежуточной аттестации в соответствии с учебным планом:

Очная форма обучения – экзамен.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Очная форма обучения

№ п/п	Наименование тем и (или) разделов	ВСЕГО	Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
			Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа			
			Период теоретического обучения						Период промежуточной аттестации (сессия)						
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Каттэк	Контроль	СРкр	СРэк	СР	
			Л	ВЛ	ЛР	ПЗ									
Тема 1	Понятие и правовое значение Privacy-Enhancing Technologies (PETs)	14	2			5								7	Устный опрос
Тема 2	Анонимизация и псевдонимизация данных: правовые критерии и технологические	14	2			5								7	Устный опрос

	методы													
Тема 3	Дифференциальная приватность (Differential Privacy) и её правовая оценка	14	2			5							7	Устный опрос
Тема 4	Криптографические PETs: гомоморфное шифрование, безопасные многосторонние вычисления (SMPC), ZKP	14	2			5							7	Устный опрос
Тема 5	Синтетические данные как инструмент приватности: правовые риски и возможности	14	2			5							7	Устный опрос
Тема 6	PETs в корпоративном комплаенсе: внедрение, аудит и документация	15	2		2	5	2						8	Устный опрос
Промежуточная аттестация		29							2	9		18		Экзамен
Итого		108	12		2	30			2	9		18	43	

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

Контроль - контактная работа на аттестацию в период экзаменационных сессий для заочной формы обучения

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

СРэк – самостоятельная работа на подготовку к экзамену.

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

3.2. Содержание дисциплины

Тема 1. Понятие и правовое значение Privacy-Enhancing Technologies (PETs). Определение PETs. Место PETs в системе технических и организационных мер защиты персональных данных. Принципы privacy by design и privacy by default. Обзор международных подходов (GDPR, OECD Guidelines). PETs как инструмент реализации требований 152-ФЗ. УК-1.

Тема 2. Анонимизация и псевдонимизация данных: правовые критерии и технологические методы. Юридическое определение анонимных и псевдонимных данных. Критерии необратимости анонимизации. Методы: suppression, generalization, noise addition. Практика Роскомнадзора и судов по признанию данных анонимными. Риски реидентификации. УК-1.

Тема 3. Дифференциальная приватность (Differential Privacy) и её правовая оценка. Понятие дифференциальной приватности (ε-дельта гарантии). Применение в официальной статистике и корпоративных аналитических системах. Правовое значение параметра ε. Соответствие дифференциальной приватности требованиям 152-ФЗ и GDPR. ПКс-АИ-1.

Тема 4. Криптографические PETs: гомоморфное шифрование, безопасные многосторонние вычисления (SMPC), ZKP. Гомоморфное шифрование (полное и частичное). Безопасные многосторонние вычисления (Secure Multi-Party Computation). Протоколы с нулевым разглашением (Zero-Knowledge Proofs). Правовые аспекты использования: возможность верификации без раскрытия данных, распределенная обработка данных. ПКс-АИ-1.

Тема 5. Синтетические данные как инструмент приватности: правовые риски и возможности. Понятие синтетических данных (полностью искусственные, частично синтетические). Генерация с использованием GAN и вариационных автоэнкодеров. Правовой статус синтетических данных: являются ли они персональными? Риски мемоизации и атрибуции. Применение в тестировании и обучении моделей ИИ. ПКс-АИ-3.

Тема 6. PETs в корпоративном комплаенсе: внедрение, аудит и документация. Оценка влияния на защиту данных (DPIA) для PETs. Документирование выбора технологии. Политика использования PETs в организации. Роль PETs в трансграничной передаче данных. Аудит эффективности PETs. ПКс-АИ-3.

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.В.04 Технологии приватности (Privacy-Enhancing Technologies – PETs) и их правовая оценка входят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляет 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 выбором одного правильного ответа из предложенных и	Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ.	Ответ считается верным, если правильно указана цифра или буква и приведены корректные аргументы, используемые при выборе ответа

обоснованием выбора	ответа	4. Записать только номер (или букву) выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	
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	100баллов

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

5.1. В ходе реализации дисциплины Б1.В.04 Технологии приватности (Privacy-Enhancing Technologies – PETs) и их правовая оценка используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

Устный опрос, тестирование, реферат, эссе, практическое задание (кейс).

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

Включаются типовые оценочные материалы по формам текущего контроля, перечисленным соответственно в п. 3.1 и 4.1, вне контрольных точек

Тема 1. Понятие и правовое значение Privacy-Enhancing Technologies (PETs). УК-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 для опроса:

1. Определение PETs. Место PETs в системе технических и организационных мер защиты персональных данных.
2. Принципы privacy by design и privacy by default. Обзор международных подходов (GDPR, OECD Guidelines).
3. PETs как инструмент реализации требований 152-ФЗ.

Тема 2. Анонимизация и псевдонимизация данных: правовые критерии и технологические методы. УК-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 для опроса:

1. Юридическое определение анонимных и псевдонимных данных. Критерии необратимости анонимизации.
2. Методы: suppression, generalization, noise addition.
3. Практика Роскомнадзора и судов по признанию данных анонимными. Риски реидентификации.

Тема 3. Дифференциальная приватность (Differential Privacy) и её правовая оценка. ПКс-АИ-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 для опроса:

1. Понятие дифференциальной приватности (ε-дельта гарантии).
2. Применение в официальной статистике и корпоративных аналитических системах.
3. Правовое значение параметра ε. Соответствие дифференциальной приватности требованиям 152-ФЗ и GDPR.

Тема 4. Криптографические PETs: гомоморфное шифрование, безопасные многосторонние вычисления (SMPC), ZKP. ПКс-АИ-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 для опроса:

1. Гомоморфное шифрование (полное и частичное).
2. Безопасные многосторонние вычисления (Secure Multi-Party Computation). Протоколы с нулевым разглашением (Zero-Knowledge Proofs).
3. Правовые аспекты использования: возможность верификации без раскрытия данных, распределенная обработка данных.

Тема 5. Синтетические данные как инструмент приватности: правовые риски и возможности. ПКи-АИ-3.

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 для опроса:

1. Понятие синтетических данных (полностью искусственные, частично синтетические).
2. Генерация с использованием GAN и вариационных автоэнкодеров.
3. Правовой статус синтетических данных: являются ли они персональными?
4. Риски мемоизации и атрибуции. Применение в тестировании и обучении моделей ИИ.

Тема 6. PETs в корпоративном комплаенсе: внедрение, аудит и документация. ПКи-АИ-3.

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 для опроса:

1. Оценка влияния на защиту данных (DPIA) для PETs.
2. Документирование выбора технологии.
3. Политика использования PETs в организации.
4. Роль PETs в трансграничной передаче данных. Аудит эффективности PETs.

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 студент	Коэффициент веса контрольной точки	Результат контрольной точки, участвующий в формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО)
КТ 1	100	0,3	30
КТ 2	100	0,3	30
Итого:	x	0,6	60

Формула расчета результата контрольной точки:

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

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

КТ – 1.

Тема 1-3.

Доклады.

Темы докладов:

1. Синтетические данные — панацея для приватности или новый правовой пробел?
2. Может ли дифференциальная приватность служить полным аналогом анонимизации по российскому законодательству?

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.
Тема 4-6

Тестовые задания с инструкцией по выполнению:

В каждом вопросе один правильный ответ.

Вопрос: Какая технология позволяет выполнять вычисления над зашифрованными данными без их расшифровки?
а) Дифференциальная приватность
б) Гомоморфное шифрование
в) Анонимизация
г) Токенизация

Правильный ответ: б
Обоснование: Гомоморфное шифрование обеспечивает возможность выполнения арифметических операций над шифротекстом, при этом результат расшифровывается в корректный результат операций над открытым текстом, что соответствует определению.

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.

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

6.1. Промежуточная аттестация проводится в форме зачета с оценкой.
Обучающийся получает экзаменационный билет и готовится к устному ответу.

6.2. Типовые оценочные материалы промежуточной аттестации.
Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

Тема 1. Понятие и правовое значение Privacy-Enhancing Technologies (PETs). УК-1.

Вопросы открытого типа:

№ п.п.	Вопрос
1.	Определение PETs. Место PETs в системе технических и организационных мер защиты персональных данных.
2.	Принципы privacy by design и privacy by default. Обзор международных подходов (GDPR, OECD Guidelines).
3.	PETs как инструмент реализации требований 152-ФЗ.

Задания комбинированного типа:

Тестовые задания с обоснованием выбора:

Задание 1. Организация внедряет технологию **псевдонимизации** (замена прямых идентификаторов на уникальные коды, ключ соответствия хранится отдельно в защищённом хранилище). Выберите все верные утверждения о правовом значении этой меры и обоснуйте выбор.

А. Псевдонимизированные данные перестают быть персональными в соответствии с 152-ФЗ.
Б. Псевдонимизация является одной из рекомендуемых мер защиты, указанных в ст. 19 152-ФЗ (как «обезличивание» в широком смысле).
В. Применение псевдонимизации полностью освобождает оператора от необходимости получать согласие субъекта на обработку.
Г. Ключ соответствия между псевдонимом и субъектом должен защищаться так же, как и сами персональные данные.

Задание 2. Соотнесите принципы GDPR с потенциальными требованиями 152-ФЗ. Выберите верные утверждения и обоснуйте.

А. Принцип privacy by design (встроенная защита) предполагает учёт мер защиты персональных данных уже на этапе проектирования информационной системы, что коррелирует с требованием ст. 19 152-ФЗ о применении мер до начала обработки.
Б. Российский 152-ФЗ прямо закрепляет принцип privacy by default как обязанность обрабатывать только минимально необходимые данные.
В. Руководящие принципы ОЭСР (OECD Guidelines) не содержат упоминаний о встроенной защите данных.
Г. Принцип privacy by default в GDPR обязывает оператора по умолчанию устанавливать самые строгие настройки конфиденциальности для каждого субъекта.

Задания закрытого типа.

Тестовые задания.

Внимательно прочитайте вопрос и выберите один или несколько правильных, на ваш взгляд, вариантов ответа. Запишите номера выбранных ответов.

Вопрос 1. Что из перечисленного наиболее полно отражает **юридически значимое определение** Privacy-Enhancing Technologies (PETs) в контексте защиты персональных данных?

1. Любые криптографические средства, обеспечивающие конфиденциальность передачи данных.
2. Совокупность технологических и организационных решений, направленных на минимизацию обрабатываемых персональных данных, исключение или существенное затруднение их связывания с конкретным субъектом без необходимости.
3. Программные продукты, полностью автоматизирующие получение согласий субъектов персональных данных.
4. Системы контроля доступа к базам данных на основе биометрии.

Вопрос 2. Какое из следующих определений наиболее полно и юридически корректно раскрывает понятие **Privacy-Enhancing Technologies (PETs)** в контексте защиты персональных данных?

1. Совокупность исключительно криптографических средств (шифрование, электронная подпись), обеспечивающих конфиденциальность передачи данных по сети.
2. Технологические решения, позволяющие полностью автоматизировать процесс получения согласий субъектов персональных данных в электронной форме.
3. Комплекс технических и организационных мер, реализованных в виде программно-аппаратных средств, направленных на минимизацию обрабатываемых персональных данных, исключение или существенное затруднение их связывания с конкретным субъектом без необходимости, а также повышение уровня защищённости при обработке.
4. Любые системы контроля доступа к базам данных, основанные на биометрической аутентификации.

Вопрос 3. В соответствии с принципом **privacy by default** («защита по умолчанию»), закреплённым в ст. 25 GDPR, какое требование является основным?

1. Обработка персональных данных должна осуществляться в максимально возможном объёме, если субъект явно не запретил это.
2. По умолчанию должны обрабатываться только те персональные данные, которые строго необходимы для конкретной цели обработки, а срок их хранения должен быть минимальным.
3. Все меры защиты персональных данных должны быть реализованы исключительно на этапе ввода системы в эксплуатацию, без учёта этапа проектирования.
4. Оператор обязан ежегодно пересматривать настройки конфиденциальности всех информационных систем без учёта мнения пользователей.

Вопрос 4. Какие из **конкретных требований** Федерального закона № 152-ФЗ «О персональных данных» могут быть реализованы с помощью Privacy-Enhancing Technologies (PETs)?

(Выберите все верные варианты.)

1. Обеспечение точности, достаточности и актуальности персональных данных (ст. 5, ч. 5).
2. Уничтожение персональных данных при достижении целей обработки или утраты необходимости (ст. 21, ч. 4).
3. Хранение персональных данных в форме, позволяющей идентифицировать субъекта, не дольше, чем этого требуют цели обработки (ст. 17, ч. 1).
4. Получение письменного согласия на обработку биометрических данных (ст. 11, ч. 2).
5. Применение организационных и технических мер для защиты от несанкционированного доступа, включая обезличивание (ст. 19, ч. 1).

Тема 2. Анонимизация и псевдонимизация данных: правовые критерии и технологические методы. УК-1.

Вопросы открытого типа:

№ п.п.	Вопрос
1.	Юридическое определение анонимных и псевдонимных данных. Критерии необратимости анонимизации.
2.	Методы: suppression, generalization, noise addition.
3.	Методы: suppression, generalization, noise addition. Практика Роскомнадзора и судов по признанию данных анонимными. Риски реидентификации

Задания комбинированного типа:

Тестовые задания с обоснованием выбора:

Задание 1. Оператор обрабатывает данные пациентов: заменяет ФИО на уникальные коды, а таблицу соответствия хранит в защищённой базе данных. Выберите **все верные** утверждения о правовом статусе таких данных и обоснуйте.

А. Данные являются анонимными, поскольку прямые идентификаторы удалены.
Б. Данные являются псевдонимизированными и остаются персональными в смысле 152-ФЗ.
В. Оператор вправе передать такие данные третьему лицу без согласия субъекта, так как это уже не персональные данные.

Г. Ключ соответствия (таблица кодов) должен защищаться наравне с исходными персональными данными.

Задание 2. Изучите описание кейса: организация опубликовала данные о доходах граждан, удалив ФИО и адреса, но оставив поля: «пол, год рождения, профессия, город (населённый пункт до 10 тыс. жителей), доход». Исследователи смогли сопоставить эти данные с открытой базой соцсетей и идентифицировать несколько человек. Выберите верные правовые оценки и обоснуйте.

А. Поскольку прямые идентификаторы удалены, данные являются анонимными, и Роскомнадзор не вправе привлечь организацию к ответственности.
Б. Роскомнадзор может признать данные не прошедшими надлежащую анонимизацию, так как сохранены редкие комбинации квази-идентификаторов.
В. Риск реидентификации не имеет правового значения, если он не реализован на практике.
Г. Организация обязана была оценить возможность сопоставления с общедоступными источниками перед публикацией.

1. *Задания закрытого типа.*

Тестовые задания.

Внимательно прочитайте вопрос и выберите один или несколько правильных, на ваш взгляд, вариантов ответа. Запишите номера выбранных ответов.

Вопрос 1. Согласно Федеральному закону № 152-ФЗ «О персональных данных», **анонимизированными** признаются данные, которые:

1. Зашифрованы с использованием ключа, известного только оператору.
2. Заменены на псевдонимы (коды), но ключ соответствия хранится отдельно.
3. Не позволяют определить принадлежность персональных данных конкретному субъекту без использования дополнительной информации, а такая информация уничтожена или недоступна.
4. Содержат только обезличенную статистику, даже если возможна обратная идентификация при больших затратах.

Вопрос 2. Какие из перечисленных **методов анонимизации** относятся к группе **обобщения (generalization)** и **подавления (suppression)**?

(Выберите все верные варианты.)

1. Замена точного возраста (25 лет) на возрастной диапазон (20–30 лет).
2. Полное удаление столбца с ФИО из таблицы.
3. Добавление случайного шума к значению зарплаты (например, ±5%).
4. Замена конкретного адреса проживания на уровень района или города.
5. Исключение записей, содержащих редкие комбинации признаков (например, записей с уникальным диагнозом).

Вопрос 3. Что из перечисленного является **наиболее серьёзным риском реидентификации** при публикации анонимизированного набора данных?

1. Использование слабого алгоритма шифрования.

2. Наличие уникальных или редких комбинаций квази-идентификаторов (например, «пол + точная дата рождения + место работы»), которые могут быть сопоставлены с внешними базами данных.
3. Отсутствие резервного копирования данных.
4. Превышение срока хранения ключей шифрования.

Вопрос 4. Какие из следующих **позиций** соответствуют официальной практике Роскомнадзора и судов по признанию данных анонимными?

(Выберите все верные варианты.)

1. Достаточно удалить только явные идентификаторы (ФИО, СНИЛС, адрес), остальные данные можно публиковать как анонимные.
2. Анонимизация должна быть необратимой с учётом всех доступных на данный момент методов и внешних источников данных.
3. Данные считаются анонимными, если для их деанонимизации требуются несоразмерные временные и материальные затраты.
4. Псевдонимизированные данные (с сохранением ключа у оператора) автоматически признаются анонимными.
5. При решении вопроса об анонимности учитывается возможность сопоставления с общедоступными базами данных (соцсети, справочники).

Тема 3. Информационно-технологическое обеспечение юридической деятельности: основные направления. УК-6.

Вопросы открытого типа:

№ п.п.	Вопрос
1.	Понятие дифференциальной приватности (ε-дельта гарантии).
2.	Применение в официальной статистике и корпоративных аналитических системах.
3.	Правовое значение параметра ε. Соответствие дифференциальной приватности требованиям 152-ФЗ и GDPR.

Задания комбинированного типа:

Тестовые задания с обоснованием выбора:

Задание 1. Компания внедряет внутреннюю аналитическую систему, которая делает DP-защищённые запросы к базе персональных данных сотрудников (без публикации вовне). Выберите верные утверждения и обоснуйте.

А. Поскольку результаты запросов защищены DP, компания может не применять другие меры защиты доступа к исходным данным.
Б. DP не освобождает от необходимости разграничения доступа к исходным персональным данным на уровне базы.
В. Использование DP должно быть отражено в политике обработки персональных данных и в уведомлении сотрудников.
Г. Параметры ε и δ являются коммерческой тайной и не подлежат раскрытию даже регулирующим органам.

Задание 2. Эксперт утверждает: «Дифференциальная приватность математически гарантирует анонимность, поэтому данные, обработанные с её помощью, автоматически соответствуют определению анонимных данных по 152-ФЗ». Выберите верные опровержения этого утверждения и обоснуйте.

А. 152-ФЗ требует необратимой анонимизации, тогда как DP не исключает возможности извлечения информации о конкретном субъекте при наличии сильной априорной информации.
Б. DP гарантирует, что результат не зависит существенно от наличия одного субъекта, но не гарантирует, что сам субъект не может быть идентифицирован путём сопоставления нескольких запросов (композиция).
В. Если ключ случайности (seed) или параметры шума скомпрометированы, данные могут быть деанонимизированы, поэтому DP – это не анонимизация, а псевдонимизация.
Г. Российское законодательство не признаёт математических гарантий, а требует проверки практической невозможности идентификации, поэтому каждая реализация DP должна доказывать соответствие критериям РКН.

1. *Задания закрытого типа.*

Тестовые задания.

Внимательно прочитайте вопрос и выберите один или несколько правильных, на ваш взгляд, вариантов ответа. Запишите номера выбранных ответов.

Вопрос 1. В каком сценарии применение дифференциальной приватности является **наиболее обоснованным** с точки зрения баланса между приватностью и полезностью данных?

1. Хранение паролей пользователей в открытом виде.
2. Публикация агрегированных статистических отчётов (например, средняя зарплата по региону) с гарантией, что включение/исключение любого человека не изменит результат сверх допустимого предела.
3. Передача файлов с персональными данными по незащищённому каналу.
4. Аутентификация пользователя по биометрии в режиме реального времени.

Вопрос 2. Какие из перечисленных **правовых требований** 152-ФЗ и GDPR могут быть реализованы с помощью дифференциальной приватности?

(Выберите все верные варианты.)

1. Обеспечение минимизации данных (ст. 5 152-ФЗ, ст. 5 GDPR).
2. Проведение оценки воздействия на защиту данных (DPIA) при высоких рисках.
3. Получение явного согласия субъекта на каждую операцию с его данными.
4. Анонимизация данных для их дальнейшей публикации без согласия (ст. 3 152-ФЗ).
5. Обеспечение права на забвение (ст. 14 GDPR, ст. 21 152-ФЗ) путём невозможности извлечь информацию о конкретном субъекте.

Вопрос 3. Какие из следующих утверждений о **ε-дельта дифференциальной приватности**являются верными?

(Выберите все верные варианты.)

1. ε = 0 означает идеальную приватность (результат не зависит от данных).
2. Чем больше ε, тем выше гарантия приватности.

3. Параметр δ (дельта) допускает небольшую вероятность нарушения ε-гарантии и обычно выбирается меньше, чем 1/размер выборки.
4. Дифференциальная приватность гарантирует защиту от атак на основе разницы в результатах запросов.
5. Механизм дифференциальной приватности не требует добавления случайного шума.

Вопрос 4. Что означает параметр **ε (epsilon)** в определении ε-дифференциальной приватности?

1. Максимальный размер выборки, к которой может быть применён механизм приватности.
2. Верхнюю границу изменения вероятности любого исхода анализа при добавлении или удалении одного субъекта из набора данных (гарантию приватности).
3. Долю синтетических данных в общем наборе.
4. Количество раундов взаимодействия между сервером и клиентом.

Тема 4. Криптографические PETs: гомоморфное шифрование, безопасные многосторонние вычисления (SMPC), ZKP. ПКс-АИ-1.

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Гомоморфное шифрование (полное и частичное).
2.	Безопасные многосторонние вычисления (Secure Multi-Party Computation). Протоколы с нулевым разглашением (Zero-Knowledge Proofs).
3.	Правовые аспекты использования: возможность верификации без раскрытия данных, распределенная обработка данных.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

Задание 1. Три банка хотят совместно выявить общих клиентов-мошенников, не раскрывая свои базы данных друг другу, используя протокол SMPC. Выберите верные утверждения и обоснуйте.

А. SMPC позволяет реализовать принцип минимизации данных (ст. 5 GDPR, ст. 5 152-ФЗ), так как каждый банк раскрывает только зашифрованные доли, а не полные записи.
Б. Поскольку данные не раскрываются в открытом виде, согласие клиентов на такое межбанковское взаимодействие не требуется.
В. Результат SMPC (например, список ID общих клиентов) может являться персональными данными и должен защищаться соответственно.
Г. Применение SMPC полностью освобождает банки от обязанности проводить оценку воздействия на защиту данных (DPIA) перед началом обработки.

Задание 2. Сервис аренды жилья требует подтвердить, что пользователь старше 21 года, но не хочет получать его точную дату рождения или паспортные данные. Предлагается использовать ZKP. Выберите верные утверждения и обоснуйте.

А. ZKP позволяет сервису получить криптографическое доказательство того, что возраст пользователя > 21 года, не узнавая его точный возраст или другие данные.

Б. Применение ZKP означает, что сервис вообще не обрабатывает персональные данные, поэтому 152-ФЗ не применяется.
В. ZKP должен быть реализован совместно с выпуском доказательства от доверенного эмитента (например, государственного органа, подтверждающего возраст), иначе доказательство не имеет юридической силы.
Г. Использование ZKP для верификации возраста без передачи даты рождения соответствует принципу минимизации данных (ст. 5 152-ФЗ).

3. Задания закрытого типа.

Тестовые задания.

Вопрос 1. Что из перечисленного **наиболее точно** характеризует **полное гомоморфное шифрование** (Fully Homomorphic Encryption, FHE)?

1. Шифрование, при котором ключ расшифровки совпадает с ключом зашифрования (симметричное шифрование).
2. Технология, позволяющая выполнять произвольное количество операций сложения и умножения над зашифрованными данными без их расшифровки, получая зашифрованный результат, который после расшифровки совпадает с результатом операций над открытыми данными.
3. Шифрование, которое можно применять только к числовым данным, но не к текстовым.
4. Метод шифрования, при котором данные можно только складывать, но не умножать.

Вопрос 2. Какие из следующих утверждений о **безопасных многосторонних вычислениях (SMPC)** и **протоколах с нулевым разглашением (ZKP)** являются верными?

(Выберите все верные варианты.)

1. SMPC позволяет нескольким сторонам совместно вычислить функцию (например, среднюю зарплату), не раскрывая друг другу свои исходные данные.
2. ZKP позволяет одной стороне (доказывающему) доказать другой стороне (проверяющему) истинность утверждения, не раскрывая никакой дополнительной информации, кроме самого факта истинности.
3. SMPC требует, чтобы все участники полностью доверяли центральному серверу.
4. ZKP может использоваться для подтверждения возраста пользователя без передачи даты рождения.
5. И SMPC, и ZKP не требуют криптографических операций и работают только на открытых данных.

Вопрос 3. Какое правовое преимущество даёт применение **протоколов с нулевым разглашением (ZKP)** при обработке персональных данных?

1. Полное освобождение оператора от обязанности получать согласие субъекта на любую обработку.
2. Возможность подтвердить наличие у субъекта определённого свойства (например, возраст > 18 лет) без передачи самого свойства или идентификаторов третьим лицам, что минимизирует объём раскрываемых персональных данных.
3. Обязательное шифрование всех данных на диске, что заменяет необходимость в политике конфиденциальности.

4. Автоматическое уничтожение всех персональных данных через 24 часа.

Вопрос 4. Какие из перечисленных **правовых требований** могут быть реализованы с помощью гомоморфного шифрования и SMPC?

(Выберите все верные варианты.)

1. Обработка персональных данных в недоверенной облачной среде без раскрытия их провайдеру (ст. 19 152-ФЗ).
2. Обеспечение конфиденциальности при трансграничной передаче данных, если иностранный оператор не имеет доступа к открытым данным (ст. 12 152-ФЗ).
3. Полный отказ от ведения журналов аудита доступа.
4. Проведение совместного анализа данных несколькими организациями (например, банками) без раскрытия клиентских записей друг другу, что соответствует принципу минимизации.
5. Анонимизация данных без удаления идентификаторов.

Тема 5. Синтетические данные как инструмент приватности: правовые риски и возможности. ПКи-АИ-3.

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Понятие синтетических данных (полностью искусственные, частично синтетические).
2.	Генерация с использованием GAN и вариационных автоэнкодеров.
3.	Правовой статус синтетических данных: являются ли они персональными?
4.	Риски мемоизации и атрибуции. Применение в тестировании и обучении моделей ИИ.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

Задание 1. Организация создаёт два набора данных:
Набор А – **полностью синтетический**, все записи сгенерированы GAN без использования реальных записей.
Набор Б – **частично синтетический**, где реальные значения чувствительного признака (диагноз) заменены на синтетические, но идентификаторы (пол, возраст, город) остаются реальными.

Выберите верные правовые оценки и обоснуйте.

А. Набор А всегда является анонимным, поскольку не содержит реальных субъектов.
Б. Набор Б может содержать персональные данные, если по оставшимся реальным идентификаторам можно установить субъекта.
В. Для генерации набора А не требуется правового основания, если используется только статистика, а не реальные записи.
Г. Для набора Б необходимо правовое основание (согласие или иное), так как обработка реальных идентификаторов – это обработка ПДн.

Задание 2. Компания обучила GAN на базе реальных медицинских карт пациентов (ФИО, диагнозы, анализы) и сгенерировала 100 000 синтетических записей. При анализе обнаружено, что около 0.1% записей практически идентичны реальным записям (мемоизация). Выберите верные утверждения и обоснуйте.

А. Наличие мемоизации означает, что синтетические данные содержат реальные персональные данные.
Б. Компания может спокойно публиковать синтетические данные, так как 0.1% – это незначительная доля.
В. Компания обязана провести оценку рисков и, если мемоизация выявлена, удалить скопированные реальные записи или перегенерировать данные.
Г. Мемоизация не является проблемой, если реальные записи были получены на законном основании.

3. Задания закрытого типа.

Тестовые задания.

Вопрос 1. Какое определение **полностью синтетических данных** (fully synthetic data) является верным?

1. Данные, полученные путём шифрования реальных персональных данных с последующим удалением ключа.
2. Набор данных, в котором **ни одна запись не соответствует реальному субъекту**, а все значения сгенерированы на основе статистических свойств исходной выборки, без использования реальных записей.
3. Данные, в которых реальные значения чувствительных атрибутов заменены на синтетические, но идентификаторы остаются реальными.
4. Любые данные, созданные с использованием нейронных сетей независимо от исходных данных.

Вопрос 2. Какие из следующих утверждений о **генеративных моделях** (GAN, VAE) для создания синтетических данных являются верными?

(Выберите все верные варианты.)

1. GAN (генеративно-состязательная сеть) состоит из генератора и дискриминатора, которые обучаются в состязательном режиме.
2. VAE (вариационный автоэнкодер) учится сжимать данные в скрытое пространство и затем восстанавливать их, позволяя генерировать новые образцы.
3. GAN и VAE гарантируют, что сгенерированные данные никогда не будут содержать фрагментов реальных персональных данных.
4. Обе модели могут использоваться для создания синтетических наборов данных, имитирующих структуру и распределение реальных ПДн.
5. GAN и VAE не требуют для обучения доступа к реальным персональным данным.

Вопрос 3. Согласно позиции большинства регуляторов (включая разъяснения ЕС и проекты рекомендаций Роскомнадзора), **синтетические данные, сгенерированные на основе реальных персональных данных:**

1. Всегда считаются анонимными и не подпадают под действие 152-ФЗ, так как не содержат реальных записей.

2. Могут быть признаны персональными, если существует возможность атрибуции (связывания) с конкретным субъектом, например, из-за мемоизации или уникальных комбинаций признаков.
3. Являются персональными в любом случае, поскольку созданы на основе ПДн.
4. Требуют отдельного согласия субъекта на генерацию, даже если используются только для внутреннего тестирования.

Вопрос 4. Какие из перечисленных **рисков** характерны для использования синтетических данных, сгенерированных на основе реальных персональных данных?

(Выберите все верные варианты.)

1. **Риск мемоизации** – генеративная модель может запомнить и воспроизвести точные реальные записи из обучающей выборки.
2. **Риск атрибуции** – даже при отсутствии точных копий, уникальные комбинации признаков в синтетических данных могут позволить идентифицировать конкретного субъекта.
3. **Риск отсутствия полезности** – синтетические данные могут быть полностью нереалистичными и бесполезными для обучения ИИ.
4. **Риск утечки модели** – злоумышленник может извлечь реальные данные из обученной генеративной модели через атаки на неё (например, атака на членство в выборке).
5. **Риск несовместимости с лицензией** – синтетические данные всегда защищены авторским правом генератора.

Тема 6. PETs в корпоративном комплаенсе: внедрение, аудит и документация. ПКи-АИ-3.

1. Задания открытого типа.

№ п.п.	Вопрос
1.	Оценка влияния на защиту данных (DPIA) для PETs.
2.	Документирование выбора технологии.
3.	Политика использования PETs в организации.
4.	Роль PETs в трансграничной передаче данных. Аудит эффективности PETs.

2. Задания комбинированного типа:

Тестовые задания с обоснованием выбора.

Задание 1. Организация внедряет технологию дифференциальной приватности для публикации статистических отчётов. Выберите **все верные** утверждения о требованиях к DPIA и документации и обоснуйте.

А. Проведение DPIA обязательно, если обработка создаёт высокие риски для субъектов (например, публикация медицинской статистики с возможностью атрибуции редких заболеваний).
Б. В DPIA достаточно указать факт использования DP без указания параметра ε.
В. Организация должна задокументировать, почему выбранное значение ε признано достаточным для предотвращения реидентификации.
Г. DPIA не требуется, если PETs внедряется для внутренних целей без передачи данных третьим лицам.

Задание 2. Российский оператор передаёт персональные данные европейскому партнёру, используя протокол безопасных многосторонних вычислений (SMPC), при котором каждая сторона не раскрывает свои данные в открытом виде. Выберите верные утверждения и обоснуйте.

А. Политика использования PETs должна содержать порядок применения SMPC в трансграничных операциях, включая оценку юрисдикции партнёра.
Б. Поскольку SMPC не раскрывает данные, такая передача не считается трансграничной передачей персональных данных.
В. Оператор обязан уведомить Роскомнадзор о трансграничной передаче, если иностранная сторона в процессе SMPC получает зашифрованные доли, которые могут быть сопоставлены с субъектами при наличии дополнительной информации.
Г. В политике использования PETs достаточно указать, что «применяются современные криптографические методы», без детализации протоколов.

3. Задания закрытого типа.

Тестовые задания.

Вопрос 1. Что из перечисленного **наиболее точно** характеризует цель проведения оценки влияния на защиту данных (DPIA) при внедрении Privacy-Enhancing Technologies (PETs)?

1. Получение разрешения от Роскомнадзора на использование любой PET-технологии.
2. Выявление и минимизация рисков для прав и свобод субъектов персональных данных, которые могут возникнуть в результате использования PETs, включая риски неправильной настройки или недостаточной эффективности технологии.
3. Замена политики конфиденциальности организации технической документацией на PETs.
4. Освобождение оператора от обязанности уведомлять субъектов об обработке их данных.

Вопрос 2. Какие из перечисленных **элементов** должны быть обязательно задокументированы оператором при выборе и внедрении PETs согласно требованиям 152-ФЗ и рекомендациям Роскомнадзора?

(Выберите все верные варианты.)

1. Обоснование выбора конкретной PET-технологии по сравнению с альтернативными решениями.
2. Параметры конфигурации PETs (например, значение ε для дифференциальной приватности, уровень шума, размер групп для k-анонимности).
3. Список сотрудников, имеющих доступ к ключам шифрования или параметрам PETs.
4. Мнение маркетингового отдела о привлекательности технологии для клиентов.
5. Результаты тестирования эффективности PETs (например, проверка на устойчивость к атакам реидентификации).

Вопрос 3. Какой документ в организации **должен** содержать положения о применении PETs согласно корпоративному комплаенсу?

1. Только трудовой договор каждого сотрудника.

2. Политика в отношении обработки персональных данных (или отдельная политика использования PETs), утверждённая руководителем организации.
3. Коммерческое предложение для клиентов.
4. Техническое задание на разработку мобильного приложения.

Вопрос 4. Какие из следующих утверждений о роли PETs при **трансграничной передаче персональных данных** и **аудите эффективности** являются верными?

(Выберите все верные варианты.)

1. Применение PETs (например, гомоморфного шифрования) может снизить объём раскрываемых данных, но не освобождает от обязанности уведомлять Роскомнадзор о трансграничной передаче, если иностранное лицо имеет возможность расшифровать данные.
2. Если данные передаются за рубеж в анонимизированном виде (необратимо), трансграничная передача не требует уведомления, так как это уже не персональные данные.
3. Аудит эффективности PETs должен проводиться только перед первым внедрением, повторный аудит не требуется.
4. При аудите эффективности PETs проверяется, действительно ли технология обеспечивает заявленный уровень защиты (например, невозможность реидентификации, устойчивость к атакам).

6.3. Критерии и шкала оценивания на основе БРС.

Критерии и балльная шкала определяются преподавателем

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	30-39
студент 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.	

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. студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.	0-19

7. Методические материалы по освоению дисциплины (модуля)

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:

Понятие и классификация Privacy-Enhancing Technologies (PETs). Место PETs в системе мер защиты персональных данных.

Принципы privacy by design и privacy by default: правовое закрепление в 152-ФЗ и GDPR, взаимосвязь с PETs.

Анонимизация персональных данных: правовые критерии (необратимость, невозможность идентификации), методы и риски реидентификации.

Псевдонимизация данных: отличие от анонимизации, правовые последствия, требования к ключам псевдонимизации.

Дифференциальная приватность (Differential Privacy): технологическая сущность, параметр ε (эпсилон) и его правовое значение.

Правовая оценка дифференциальной приватности: соответствует ли она требованиям 152-ФЗ к обезличиванию? Анализ разъяснений Роскомнадзора.

Гомоморфное шифрование: понятие, виды (частичное, полное), правовые возможности обработки данных без расшифровки.

Безопасные многосторонние вычисления (SMPC / MPC): применение для совместного анализа данных без раскрытия исходных данных третьим сторонам.

Протоколы с нулевым разглашением (Zero-Knowledge Proofs, ZKP): правовая природа, сценарии использования (верификация без раскрытия данных).

Синтетические данные: понятие, методы генерации (GAN, вариационные автоэнкодеры), правовой статус: являются ли персональными данными?

Правовые риски использования синтетических данных: мемоизация, атрибуция, возможность восстановления исходных данных.

Оценка влияния на защиту данных (DPIA) для PETs: структура, особенности оценки рисков при внедрении PETs, документация.

PETs как инструмент трансграничной передачи данных: анализ возможности замены стандартных гарантий (SCCs, BCR) на технологические меры.

Административная ответственность за утечку персональных данных (ст. 13.11 КоАП РФ): какие PETs помогают доказать принятие достаточных мер?

Судебная практика по искам о компенсации морального вреда за утечку данных: роль заключения экспертизы о применении PETs.

Взаимодействие с Роскомнадзором и ФСТЭК при расследовании инцидентов: порядок предоставления сведений о применяемых PETs.

PETs и принцип минимизации данных (data minimization): как технологии позволяют обрабатывать только необходимые данные (например, через ZKP).

Документирование выбора PETs в организации: политика обработки данных, приложение к DPIA, регламенты выбора технологий.

Сравнительный анализ PETs для различных сценариев обработки: внутренняя аналитика, публикация статистики, обучение ИИ-моделей, трансграничная передача.

Перспективы правового регулирования PETs в России и мире: проекты нормативных актов, международные стандарты (ISO/IEC 27555, NIST), тренды развития.

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — ISBN 978-5-16-016583-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1191479 (дата обращения: 07.06.2026)

2. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. - Йошкар-Ола : Поволжский государственный технологический университет, 2020. - 154 с. - ISBN 978-5-8158-2165-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1894130 (дата обращения: 07.06.2026). – Режим доступа: по подписке

3. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2024. — 602 с. — DOI 10.12737/1942679. - ISBN 978-5-16-018253-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1942679 (дата обращения: 07.06.2026). – Режим доступа: по подписке.

4. Родичев, Ю. А. Безопасность инфокоммуникаций: стандартизация, измерения соответствия и подготовка кадров : учебное пособие для вузов / Ю. А. Родичев, П. И. Симонов, Ю. А. Кубанков. - Москва : Горячая линия-Телеком, 2020. - 160 с. - ISBN 978-5-9912-0706-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1911622 (дата обращения: 07.06.2026). – Режим доступа: по подписке.

8.2. Дополнительная литература

1. OECD (2020). "Privacy-Enhancing Technologies: A Policy Primer". OECD Digital Economy Papers. (Режим доступа: www.oecd.org).
2. EDPB (2022). "Guidelines 05/2022 on the use of synthetic data". (Режим доступа: edpb.europa.eu).
3. Документы Роскомнадзора по разъяснению анонимизации и псевдонимизации (раздел «Разъяснения» на портале pd.rkn.gov.ru).8.3 Интернет-ресурсы

8.3. Нормативные правовые документы и иная правовая информация

В рамках данной дисциплины не предусмотрено изучение нормативных правовых актов в качестве обязательной литературы. При изучении модуля 5 (регулирование и этика) рекомендуется обращаться к актуальным документам:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

- Федеральный закон от 28.06.2021 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве»
- Этические принципы и рекомендации ЮНЕСКО по искусственному интеллекту (2021)

Указанные документы могут быть найдены в справочно-правовых системах «КонсультантПлюс» или «Гарант» (доступ через университетскую сеть).

8.4. Интернет-ресурсы

1. Официальный интернет-портал правовой информации (www.pravo.gov.ru).
2. СПС «КонсультантПлюс» (www.consultant.ru).
3. СПС «Гарант» (www.garant.ru).
4. Официальный сайт Роскомнадзора (rkn.gov.ru).
5. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций РФ (digital.gov.ru).
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».