МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
ЧЕБОКСАРСКИЙ ИНСТИТУТ (ФИЛИАЛ) МОСКОВСКОГО ПОЛИТЕХНИЧЕСКОГО УНИВЕРСИТЕТА

Кафедра Право

УТВЕРЖДАЮ
Директор филиала
А.В. Агафонов
"27" мая 2026г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Правовое обеспечение информационной безопасности»

(наименование дисциплины)

Направление подготовки	**40.04.01- Юриспруденция**
	(код и наименование направления подготовки)
Направленность (профиль) подготовки	**Частное право в эпоху цифровизации**
	(наименование профиля подготовки)
Квалификация выпускника	**магистр**
Форма обучения	**очная, заочная**
Год начала обучения	**2026**

Чебоксары, 2026

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 40.04.01 «Юриспруденция».

Рабочая программа дисциплины включает в себя оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине (п.6 Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины)

Автор Скворцов Евгений Николаевич, кандидат юридических наук, доцент кафедры Право

(указать ФИО, ученую степень, ученое звание или должность)

Программа одобрена на заседании кафедры Право (протокол № 9 от 22.05.2026).

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

1.1. **Целями освоения дисциплины «Правовое обеспечение информационной безопасности» являются:** формирование у обучающихся целостного представления о системе правового регулирования информационной безопасности, защите информации, персональных данных, цифровых прав и частноправовых интересов граждан и организаций в условиях цифровизации гражданского оборота.

Для достижения целей дисциплины необходимо решить следующие основные задачи:

- сформировать знания о правовых основах информационной безопасности, защите информации, персональных данных, охраняемой законом тайны и цифровых сервисов;
- изучить нормативные правовые акты, регулирующие отношения в сфере информации, информационных технологий и защиты данных;
- развить умение выявлять правовые риски, связанные с использованием информационных систем, цифровых платформ, электронных сделок и обработкой персональных данных;
- сформировать навыки анализа правоприменительной практики по вопросам нарушения требований информационной безопасности и защиты информации;
- выработать умение подготавливать юридические консультации, заключения и правовые рекомендации по вопросам обеспечения информационной безопасности;
- сформировать навыки защиты прав и законных интересов граждан и организаций при нарушении режима информации, персональных данных и цифровой безопасности.

1.2. Области профессиональной деятельности и (или) сферы профессиональной деятельности, в которых выпускники, освоившие программу, могут осуществлять профессиональную деятельность:

- *09 Юриспруденция*

1.3. К основным задачам изучения дисциплины относится подготовка обучающихся к выполнению трудовых функций в соответствии с анализом требований к профессиональным компетенциям, предъявляемых к выпускникам на рынке труда, обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей отрасли.

1.4. Компетенции обучающегося, формируемые в результате освоения дисциплины

Наименование категории (группы) компетенций	Код и наименование компетенций	Код и наименование индикатора достижения компетенции	Перечень планируемых результатов обучения
Разработка и реализация проектов	УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Знает этапы жизненного цикла проекта; этапы разработки и реализации проекта; методы разработки и управления проектами.	*на уровне знаний:* знать этапы жизненного цикла проекта в сфере правового обеспечения информационной безопасности. *на уровне умений:* уметь определять цель, задачи и этапы проекта по защите информации, персональных данных и цифровых сервисов. *на уровне навыков:* иметь навыки анализа проектных решений и правовых рисков в сфере информационной безопасности.
		УК-2.2. Умеет разрабатывать проект с учетом анализа альтернативных вариантов его реализации, определять с использованием инструментов планирования целевые этапы и основные направления работ; формулировать цель задачи, обосновывать актуальность, научную и практическую значимость, ожидаемые результаты и возможные сферы применения; управлять проектом на всех этапах его жизненного цикла, осуществлять мониторинг хода его реализации, вносить при необходимости изменения в план реализации проекта; представлять публично результаты проекта (его	*на уровне знаний:* знать основы планирования и реализации проектов в сфере информационной безопасности. *на уровне умений:* уметь разрабатывать проект, определять основные направления работ и ожидаемые результаты в сфере защиты информации. *на уровне навыков:* иметь навыки подготовки проектных материалов, отчетов и правовых заключений по вопросам информационной безопасности.

		этапов) в различной форме (отчеты, статьи, выступления на научно-практических конференциях, семинарах	
		УК-2.3. Владеет методиками разработки и управления проектом; методами оценки потребности в ресурсах и эффективности проекта.	*на уровне знаний:* знать методы оценки ресурсов и эффективности проектов в сфере информационной безопасности. *на уровне умений:* уметь оценивать ресурсное обеспечение и результативность проекта по защите информации и цифровых прав. *на уровне навыков:* иметь навыки управления проектом, оценки его эффективности и корректировки проектных решений.
правоприменительный	ПК-2 Способен квалифицированно применять нормативные правовые акты, реализовывать нормы материального и процессуального права в соответствующей сфере профессиональной деятельности	ПК-2.1. Знает правовые основы и правоприменительную практику; теоретические основы юридической оценки ситуаций; методику решения практических задач применения норм материального и процессуального права в сфере частного права и гражданского оборота.	*на уровне знаний:* знать правовые основы информационной безопасности, защиты информации, персональных данных и цифровых прав. *на уровне умений:* уметь определять подлежащие применению нормы права при разрешении ситуаций, связанных с нарушением требований информационной безопасности. *на уровне навыков:* иметь навыки юридической оценки фактов и обстоятельств в сфере защиты информации и персональных данных.

		ПК-2.2. Умеет собирать и анализировать правовую и фактическую информацию, имеющую значение для реализации правовых норм в ходе правоприменительной деятельности, участвовать в процессе решения споров, оценивать результативность и последствия правовых решений в сфере частного права и гражданского оборота.	*на уровне знаний:* знать порядок сбора и анализа правовой и фактической информации в сфере информационной безопасности. *на уровне умений:* уметь анализировать правовые ситуации, связанные с защитой информации, персональных данных и охраняемой законом тайны. *на уровне навыков:* иметь навыки подготовки правовой позиции по вопросам обеспечения информационной безопасности.
		ПК-2.3. Владеет навыками составления правовых документы по требованиям юридической техники в сфере частного права и гражданского оборота	*на уровне знаний:* знать требования к составлению правовых документов в сфере информационной безопасности. *на уровне умений:* уметь составлять локальные акты, согласия, уведомления, соглашения о конфиденциальности и иные документы в сфере защиты информации. *на уровне навыков:* иметь навыки подготовки юридических документов по требованиям юридической техники в сфере информационной безопасности.
консультационный	ПК-4 Способен давать юридические консультации и заключения в различных сферах юридической дея-	ПК-4.1. Знает законодательство об осуществлении консультационной работы в сфере частного права и гражданского оборота для физических и юридических лиц, органов	*на уровне знаний:* знать законодательство и формы консультирования по вопросам информационной безопасности, защиты

	тельности	государственной власти и местного самоуправления, общественных объединений; виды и формы юридических консультаций, применяемых в сфере частного права и гражданского оборота, а также особенности консультирования по вопросам правового режима цифровых прав, токенов, краудфандинга, смарт-контрактов, платформенной экономики, защиты персональных данных, применения искусственного интеллекта в частном праве.	информации, персональных данных и цифровых прав. *на уровне умений:* уметь определять содержание юридической консультации по вопросам защиты информации и безопасности цифрового гражданского оборота. *на уровне навыков:* иметь навыки подготовки консультаций по вопросам информационной безопасности и защиты персональных данных.
		ПК-4.2. Умеет составлять юридические заключения, используемые для осуществления консультационной работы в сфере частного права и гражданского оборота для физических и юридических лиц, органов государственной власти и местного самоуправления, общественных объединений, включая заключения по вопросам соблюдения законодательства об экспериментальных правовых режимах, о цифровых платформах, об обороте криптоактивов.	*на уровне знаний:* знать требования к юридическим заключениям в сфере информационной безопасности, цифровых платформ, персональных данных и цифровых активов. *на уровне умений:* уметь составлять юридические заключения по вопросам соблюдения законодательства о защите информации, персональных данных и цифровых сервисов. *на уровне навыков:* иметь навыки подготовки юридических заключений по вопросам информационной безопасности и цифровых прав.
		ПК-4.3. Владеет навыками представления юридических заключений, используемых для осуществления консультационной работы	*на уровне знаний:* знать порядок представления юридических заключений и

		в сфере частного права и гражданского оборота для физических и юридических лиц, органов государственной власти и местного самоуправления, общественных объединений, а также консультирования правоохранительных органов по квалификации преступлений в сфере цифровых активов и киберпреступности, по вопросам цифровой безопасности и защиты цифровых прав граждан	особенности консультирования по вопросам цифровой безопасности и защиты цифровых прав. *на уровне умений:* уметь представлять правовую позицию по вопросам информационной безопасности, киберрисков и защиты цифровых активов. *на уровне навыков:* иметь навыки консультирования и представления заключений по вопросам защиты информации, цифровых прав и кибербезопасности.

2. Место дисциплины в структуре ОПОП

Дисциплина Б1.Д(М).В.6 «Правовое обеспечение информационной безопасности» реализуется в рамках части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» учебного плана обучающихся по программе магистратуры очной и заочной форм обучения.

Дисциплина направлена на формирование компетенций УК-2, ПК-2, ПК-4 и обеспечивает подготовку обучающихся к решению профессиональных задач, связанных с правовым обеспечением информационной безопасности, защитой информации, персональных данных, цифровых прав, охраняемой законом тайны, электронного документооборота, цифровых платформ и информационных систем.

По очной форме обучения дисциплина изучается в 3-м и 4-м семестрах, по заочной форме обучения – на 2-м курсе.

Освоение дисциплины основывается на знаниях, умениях и навыках, полученных обучающимися при изучении дисциплин «Информационные технологии в юриспруденции», «Цифровые права человека и гражданина», «Проблемы договорного права в цифровой экономике», «Актуальные проблемы частного права», «Нормотворческий процесс в Российской Федерации», «Правовое регулирование инновационной деятельности».

Дисциплина имеет значение для последующего прохождения производственной практики: правоприменительной практики, производственной практики: преддипломной практики, а также для подготовки выпускной квалификационной работы, связанной с проблемами правового регулирования цифровой среды, защиты информации, персональных данных, цифровых сервисов и частноправовых интересов участников гражданского оборота.

Формой промежуточной аттестации по дисциплине является зачет.

3. Объем дисциплины

очная форма обучения:

Вид учебной работы по дисциплине	Всего в з.е. и часах	Семестр 3 в часах	Семестр 4 в часах
Общая трудоёмкость дисциплины	**6 з.е. – 216 ак.час**	**72 ак.час**	**144 ак.час**
Контактная работа - Аудиторные занятия	**28**	12	16
Лекции	14	6	8
Лабораторные занятия	-	-	
Семинары, практические занятия	14	6	8
Консультация	-	-	-
Самостоятельная работа	**188**	**60**	**128**
Курсовая работа (курсовой проект)	-	-	-
Вид промежуточной аттестации	Зачет	Зачет	Зачет

заочная форма обучения:

Вид учебной работы по дисциплине	Всего в з.е. и часах	2 курс (семестр 3) в часах	2 курс (семестр 4) в часах
Общая трудоёмкость дисциплины	**6 з.е. – 216 ак.час**	**72 ак.час**	**144 ак.час**
Контактная работа - Аудиторные занятия	**22**	8	14
Лекции	10	4	6
Лабораторные занятия	-	-	
Семинары, практические занятия	12	4	8
Консультация	-	-	-
Самостоятельная работа	**186**	**60**	**126**
Курсовая работа (курсовой проект)	-	-	-
Вид промежуточной аттестации	Зачет	Зачет	Зачет

4. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

4.1. Учебно-тематический план

Очная форма обучения

Наименование тем (разделов) дисциплины	Трудоемкость в часах				Код индикатора достижений компетенции
	Контактная работа – Аудиторная работа			самостоятельная работа	
	лекции	лабораторные занятия	семинары и практические занятия		
Тема 1. Теоретико-правовые основы информационной безопасности в условиях цифровизации частного права и	4	-	4	28	УК-2.1 УК-2.2 УК-2.3 ПК-2.1

гражданского оборота					ПК-2.2 ПК-2.3 ПК-4.1 ПК-4.2 ПК-4.3
Тема 2. Правовой режим информации, персональных данных и охраняемой законом тайны в цифровом гражданском обороте	2	-	2	32	УК-2.1 УК-2.2 УК-2.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-4.1 ПК-4.2 ПК-4.3
Тема 3. Правовое обеспечение безопасности цифровых платформ, электронных сделок, информационных систем и цифровых сервисов	4	-	4	64	УК-2.1 УК-2.2 УК-2.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-4.1 ПК-4.2 ПК-4.3
Тема 4. Юридическая ответственность, защита прав и консультирование в сфере информационной безопасности и цифровых рисков	4	-	4	64	УК-2.1 УК-2.2 УК-2.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-4.1 ПК-4.2 ПК-4.3
Консультации	-			-	УК-2.1 УК-2.2 УК-2.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-4.1 ПК-4.2 ПК-4.3
Контроль (зачет)	-			-	УК-2.1 УК-2.2 УК-2.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-4.1 ПК-4.2 ПК-4.3
ИТОГО	28			188	

Заочная форма обучения

Наименование тем (разделов) дисциплины	**Трудоемкость в часах**				Код индикатора достижений компетенции
	Контактная работа – Аудиторная работа			самостоятельная работа	
	лекции	лабораторные занятия	семинары и практические занятия		
Тема 1. Теоретико-правовые основы информационной безопасности в условиях цифровизации частного права и гражданского оборота	2	-	2	30	УК-2.1 УК-2.2 УК-2.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-4.1 ПК-4.2 ПК-4.3
Тема 2. Правовой режим информации, персональных данных и охраняемой законом тайны в цифровом гражданском обороте	2	-	2	30	УК-2.1 УК-2.2 УК-2.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-4.1 ПК-4.2 ПК-4.3
Тема 3. Правовое обеспечение безопасности цифровых платформ, электронных сделок, информационных систем и цифровых сервисов	2	-	4	64	УК-2.1 УК-2.2 УК-2.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-4.1 ПК-4.2 ПК-4.3
Тема 4. Юридическая ответственность, защита прав и консультирование в сфере информационной безопасности и цифровых рисков	4	-	4	62	УК-2.1 УК-2.2 УК-2.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-4.1 ПК-4.2 ПК-4.3
Консультации	-			-	УК-2.1 УК-2.2 УК-2.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-4.1 ПК-4.2

			ПК-4.3
Контроль (зачет)	-	-	УК-2.1 УК-2.2 УК-2.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-4.1 ПК-4.2 ПК-4.3
ИТОГО	22	194	

4.2. Содержание дисциплины

Тема 1. Теоретико-правовые основы информационной безопасности в условиях цифровизации частного права и гражданского оборота

Понятие, сущность и значение информационной безопасности в современной правовой системе Российской Федерации. Информационная безопасность как условие устойчивого функционирования цифровой экономики, электронного взаимодействия, цифрового гражданского оборота и защиты прав участников частноправовых отношений. Основные угрозы информационной безопасности: неправомерный доступ к информации, утечка персональных данных, нарушение конфиденциальности, распространение недостоверной информации, киберриски, использование цифровых технологий в противоправных целях. Система нормативного правового регулирования информационной безопасности. Соотношение публично-правовых и частноправовых средств обеспечения информационной безопасности. Значение правового обеспечения информационной безопасности для защиты имущественных, договорных, корпоративных и иных частноправовых интересов граждан и организаций.

Тема 2. Правовой режим информации, персональных данных и охраняемой законом тайны в цифровом гражданском обороте

нформация как объект правового регулирования. Виды информации и особенности ее правового режима. Общедоступная информация, информация ограниченного доступа, конфиденциальная информация. Правовой режим персональных данных: понятие, принципы обработки, права субъектов персональных данных, обязанности операторов, требования к согласию на обработку персональных данных. Коммерческая, банковская, служебная, профессиональная и иная охраняемая законом тайна в гражданском обороте. Правовые требования к сбору, хранению, передаче, распространению и защите информации. Договорные способы обеспечения конфиденциальности: соглашения о неразглашении, условия о защите информации, ответственность сторон за нарушение режима конфиденциальности. Особенности защиты информации в отношениях с участием цифровых платформ, операторов информационных систем, пользователей цифровых сервисов и иных участников цифровой среды.

Тема 3. Правовое обеспечение безопасности цифровых платформ, электронных сделок, информационных систем и цифровых сервисов

Правовые основы обеспечения безопасности цифровых платформ, информационных систем, электронного документооборота и цифровых сервисов. Электронные сделки и юридически значимый электронный документооборот: требования к достоверности, идентификации участников, электронной подписи, сохранности электронных документов и защите передаваемой информации. Правовые риски функционирования цифровых платформ: нарушение прав пользователей, утрата данных, несанкционированный доступ, злоупотребление цифровой инфраструктурой, нарушение договорных обязательств в цифровой среде. Обеспечение безопасности цифровых прав, цифровых активов, электронных платежей, онлайн-сервисов и автоматизированных информационных систем. Применение технологий искусственного интеллекта, алгоритмических систем и автоматизированной обработки данных: правовые требования, риски и пределы использования. Локальное регулирование информационной безопасности в организации: положения, регламенты, политики обработки данных, инструкции, договорные условия и внутренние процедуры контроля.

Тема 4. Юридическая ответственность, защита прав и консультирование в сфере информационной безопасности и цифровых рисков

Виды юридической ответственности за нарушение требований информационной безопасности, законодательства о персональных данных, защите информации, коммерческой и иной охраняемой законом тайне. Гражданско-правовая ответственность за причинение имущественного вреда, нарушение договорных обязательств, разглашение конфиденциальной информации, неправомерное использование данных и цифровых сервисов. Способы защиты прав граждан и организаций при нарушении информационной безопасности: возмещение убытков, компенсация морального вреда, пресечение противоправных действий, удаление или опровержение информации, защита деловой репутации, договорные способы защиты. Особенности доказывания нарушений в цифровой среде, значение электронных доказательств, цифровых следов, переписки, журналов событий и иных данных. Консультирование физических и юридических лиц по вопросам защиты информации, персональных данных, цифровых прав, киберрисков и безопасности электронных сделок. Подготовка юридических заключений, локальных актов, претензий, договорных условий, соглашений о конфиденциальности и иных документов в сфере правового обеспечения информационной безопасности.

Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Тема 1. Теоретико-правовые основы	УК-2: 1. Информационная безопасность как объект	Анализ теоретического

информационной безопасности в условиях цифровизации частного права и гражданского оборота	проектного правового обеспечения. 2. Этапы разработки проекта в сфере защиты информации и цифровых прав. 3. Правовые риски проекта, связанного с обеспечением информационной безопасности. 4. Планирование мероприятий по обеспечению информационной безопасности в организации. 5. Оценка эффективности проекта, направленного на снижение цифровых рисков. ПК-2: 6. Понятие и правовая природа информационной безопасности. 7. Система нормативного правового регулирования информационной безопасности в Российской Федерации. 8. Соотношение публично-правовых и частноправовых средств защиты информации. 9. Информационная безопасность как условие стабильности цифрового гражданского оборота. 10. Правовые угрозы информационной безопасности граждан и организаций в цифровой среде. ПК-4: 11. Основные вопросы юридического консультирования в сфере информационной безопасности. 12. Консультирование граждан и организаций по вопросам защиты информации в цифровой среде. 13. Подготовка правовой позиции по вопросам цифровых рисков и защиты частноправовых интересов. 14. Юридическое консультирование по вопросам безопасного использования цифровых сервисов. 15. Разъяснение правовых последствий нарушения требований информационной безопасности.	материала и правоприменительной практики, поиск проблемных аспектов и путей решения, систематизация изученного материала.
Тема 2. Правовой режим информации, персональных данных и охраняемой законом тайны в цифровом гражданском обороте	УК-2: 1. Планирование проекта по внедрению системы защиты персональных данных в организации. 2. Оценка ресурсов, необходимых для правового обеспечения режима конфиденциальной информации. 3. Этапы реализации проекта по приведению обработки персональных данных в соответствие с законодательством. 4. Разработка проекта локального регулирования обработки персональных данных. 5. Оценка эффективности мер по обеспечению	Анализ теоретического материала и правоприменительной практики, поиск проблемных аспектов и путей решения, систематизация изученного материала.

	режима коммерческой тайны. ПК-2: 6. Информация как объект правового регулирования. 7. Виды информации и особенности их правового режима. 8. Правовой режим персональных данных и обязанности оператора персональных данных. 9. Права субъекта персональных данных и способы их защиты. 10. Коммерческая, банковская, профессиональная и иная охраняемая законом тайна в гражданском обороте. ПК-4: 11. Консультирование по вопросам получения согласия на обработку персональных данных. 12. Подготовка юридического заключения о соблюдении режима коммерческой тайны. 13. Разъяснение правовых последствий нарушения режима конфиденциальной информации. 14. Подготовка рекомендаций по правовому оформлению политики обработки персональных данных. 15. Консультирование по вопросам передачи персональных данных третьим лицам.	
Тема 3. Правовое обеспечение безопасности цифровых платформ, электронных сделок, информационных систем и цифровых сервисов	УК-2: 1. Проектное сопровождение внедрения цифровой платформы с учетом требований информационной безопасности. 2. Оценка правовых рисков проекта электронного документооборота. 3. Мониторинг реализации проекта по обеспечению безопасности цифрового сервиса. 4. Планирование проекта по правовой защите данных пользователей цифровой платформы. 5. Оценка ресурсов, необходимых для внедрения безопасного электронного взаимодействия. ПК-2: 6. Правовые требования к безопасности цифровых платформ и информационных систем. 7. Информационная безопасность при совершении электронных сделок. 8. Правовое значение электронной подписи в обеспечении безопасности цифрового оборота. 9. Защита цифровых прав, цифровых активов и данных участников гражданского оборота. 10. Правовые риски использования искусственного интеллекта и автоматизированных систем в цифровой среде.	Анализ теоретического материала и правоприменительной практики, поиск проблемных аспектов и путей решения, систематизация изученного материала.

	ПК-4: 11. Консультирование по вопросам безопасности электронных сделок. 12. Подготовка заключения о правовых рисках использования цифровой платформы. 13. Юридическая оценка условий пользовательских соглашений цифровых сервисов. 14. Консультирование по вопросам защиты цифровых активов и электронных данных. 15. Подготовка рекомендаций по снижению рисков при использовании информационных систем. Анализ теоретического материала и правоприменительной практики, поиск проблемных аспектов и путей решения, систематизация изученного	
Тема 4. Юридическая ответственность, защита прав и консультирование в сфере информационной безопасности и цифровых рисков	УК-2: 1. Проектирование комплекса мер по предупреждению нарушений информационной безопасности. 2. Оценка эффективности правового проекта по снижению цифровых рисков организации. 3. Корректировка проектных решений при выявлении нарушений требований защиты информации. 4. Планирование проекта правового реагирования на утечку персональных данных. 5. Оценка результативности правовых мер по защите цифровых прав граждан и организаций. ПК-2: 6. Виды юридической ответственности за нарушение требований информационной безопасности. 7. Гражданско-правовая ответственность за утечку персональных данных. 8. Ответственность за разглашение коммерческой и иной охраняемой законом тайны. 9. Гражданско-правовые способы защиты прав при нарушении информационной безопасности. 10. Электронные доказательства при разрешении споров, связанных с нарушением информационной безопасности. ПК-4: 11. Подготовка юридической консультации по факту утечки персональных данных. 12. Составление заключения о перспективах защиты прав гражданина или организации в цифровой среде. 13. Консультирование по вопросам киберрисков, цифровых активов и защиты	Анализ теоретического материала и правоприменительной практики, поиск проблемных аспектов и путей решения, систематизация изученного материала.

	цифровых прав. 14. Подготовка правового заключения о возможности взыскания убытков, причиненных нарушением информационной безопасности. 15. Разъяснение порядка защиты деловой репутации при распространении недостоверной информации в цифровой среде.	

Шкала оценивания ответов на вопросы

Шкала оценивания	Критерии оценивания
«Отлично»	Обучающийся глубоко и содержательно раскрывает ответ на каждый теоретический вопрос, не допустив ошибок. Ответ носит развернутый и исчерпывающий характер.
«Хорошо»	Обучающийся в целом раскрывает теоретические вопросы, однако ответ хотя бы на один из них не носит развернутого и исчерпывающего характера.
«Удовлетворительно»	Обучающийся в целом раскрывает теоретические вопросы и допускает ряд неточностей, фрагментарно раскрывает содержание теоретических вопросов или их раскрывает содержательно, но допуская значительные неточности.
«Неудовлетворительно»	Обучающийся не знает ответов на поставленные теоретические вопросы.

6. Оценочные материалы (фонд оценочных средств) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

6.1. Паспорт фонда оценочных средств

№	Контролируемые разделы (темы) дисциплины	Код и наименование компетенции	Индикатор достижения компетенции	Наименование оценочного средства
1.	Тема 1. Теоретико-правовые основы информационной безопасности в условиях цифровизации частного права и гражданского оборота.	УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Знает этапы жизненного цикла проекта; этапы разработки и реализации проекта; методы разработки и управления проектами. УК-2.2. Умеет разрабатывать проект с учетом анализа альтернативных вариантов его реализации, определять с использованием инструментов планирования целевые этапы и основные направления работ; формулировать цель задачи, обосновывать актуальность, научную и практическую значимость, ожидаемые результаты и возможные сферы применения; управлять проектом на всех этапах его жизненного цикла, осуществлять мониторинг хода его реализации, вносить при необходимости	опрос, тест, реферат, решение задач

			изменения в план реализации проекта; представлять публично результаты проекта (его этапов) в различной форме (отчеты, статьи, выступления на научно-практических конференциях, семинарах	
			УК-2.3. Владеет методиками разработки и управления проектом; методами оценки потребности в ресурсах и эффективности проекта.	
		ПК-2. Способен квалифицированно применять нормативные правовые акты, реализовывать нормы материального и процессуального права в соответствующей сфере профессиональной деятельности	ПК-2.1. Знает правовые основы и правоприменительную практику; теоретические основы юридической оценки ситуаций; методику решения практических задач применения норм материального и процессуального права в сфере частного права и гражданского оборота, включая особенности применения норм к отношениям с использованием цифровых технологий.	опрос, тест, реферат, решение задач
			ПК-2.2. Умеет собирать и анализировать правовую и фактическую информацию, имеющую значение для реализации правовых норм в ходе правоприменительной деятельности, участвовать в процессе решения споров, оценивать результативность и последствия правовых решений в сфере частного права и гражданского оборота, в том числе споров, связанных с оборотом цифровых активов, электронными сделками, защитой персональных данных, ответственностью операторов платформ.	
			ПК-2.3. Владеет навыками составления правовых документов по требованиям юридической техники в сфере частного права и гражданского оборота, а также подготовки и использования электронных доказательств в гражданском, арбитражном и административном процессе.	
		ПК-4 Способен давать юридические консультации и	ПК-4.1. Знает законодательство об осуществлении консультационной работы в сфере частного права и гражданского оборота для	опрос, тест, реферат, решение задач

		заключения в различных сферах юридической деятельности	физических и юридических лиц, органов государственной власти и местного самоуправления, общественных объединений; виды и формы юридических консультаций, применяемых в сфере частного права и гражданского оборота, а также особенности консультирования по вопросам правового режима цифровых прав, токенов, краудфандинга, смарт-контрактов, платформенной экономики, защиты персональных данных, применения искусственного интеллекта в частном праве.	
			ПК-4.2. Умеет составлять юридические заключения, используемые для осуществления консультационной работы в сфере частного права и гражданского оборота для физических и юридических лиц, органов государственной власти и местного самоуправления, общественных объединений, включая заключения по вопросам соблюдения законодательства об экспериментальных правовых режимах, о цифровых платформах, об обороте криптоактивов.	
			ПК-4.3. Владеет навыками представления юридических заключений, используемых для осуществления консультационной работы в сфере частного права и гражданского оборота для физических и юридических лиц, органов государственной власти и местного самоуправления, общественных объединений, а также консультирования правоохранительных органов по квалификации преступлений в сфере цифровых активов и киберпреступности, по вопросам цифровой безопасности и защиты цифровых прав граждан.	
2.	Тема 2. Правовой режим информации, персональных данных и	УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Знает этапы жизненного цикла проекта; этапы разработки и реализации проекта; методы разработки и управления проектами.	опрос, тест, реферат, решение задач
			УК-2.2. Умеет разрабатывать проект	

	охраняемой законом тайны в цифровом гражданском обороте		с учетом анализа альтернативных вариантов его реализации, определять с использованием инструментов планирования целевые этапы и основные направления работ; формулировать цель задачи, обосновывать актуальность, научную и практическую значимость, ожидаемые результаты и возможные сферы применения; управлять проектом на всех этапах его жизненного цикла, осуществлять мониторинг хода его реализации, вносить при необходимости изменения в план реализации проекта; представлять публично результаты проекта (его этапов) в различной форме (отчеты, статьи, выступления на научно-практических конференциях, семинарах	
			УК-2.3. Владеет методиками разработки и управления проектом; методами оценки потребности в ресурсах и эффективности проекта.	
		ПК-2. Способен квалифицированно применять нормативные правовые акты, реализовывать нормы материального и процессуального права в соответствующей сфере профессиональной деятельности	ПК-2.1. Знает правовые основы и правоприменительную практику; теоретические основы юридической оценки ситуаций; методику решения практических задач применения норм материального и процессуального права в сфере частного права и гражданского оборота, включая особенности применения норм к отношениям с использованием цифровых технологий.	опрос, тест, реферат, решение задач
			ПК-2.2. Умеет собирать и анализировать правовую и фактическую информацию, имеющую значение для реализации правовых норм в ходе правоприменительной деятельности, участвовать в процессе решения споров, оценивать результативность и последствия правовых решений в сфере частного права и гражданского оборота, в том числе споров, связанных с оборотом цифровых активов, электронными сделками, защитой персональных	

			данных, ответственностью операторов платформ.	
			ПК-2.3. Владеет навыками составления правовых документов по требованиям юридической техники в сфере частного права и гражданского оборота, а также подготовки и использования электронных доказательств в гражданском, арбитражном и административном процессе.	
		ПК-4 Способен давать юридические консультации и заключения в различных сферах юридической деятельности	ПК-4.1. Знает законодательство об осуществлении консультационной работы в сфере частного права и гражданского оборота для физических и юридических лиц, органов государственной власти и местного самоуправления, общественных объединений; виды и формы юридических консультаций, применяемых в сфере частного права и гражданского оборота, а также особенности консультирования по вопросам правового режима цифровых прав, токенов, краудфандинга, смарт-контрактов, платформенной экономики, защиты персональных данных, применения искусственного интеллекта в частном праве.	опрос, тест, реферат, решение задач
			ПК-4.2. Умеет составлять юридические заключения, используемые для осуществления консультационной работы в сфере частного права и гражданского оборота для физических и юридических лиц, органов государственной власти и местного самоуправления, общественных объединений, включая заключения по вопросам соблюдения законодательства об экспериментальных правовых режимах, о цифровых платформах, об обороте криптоактивов.	
			ПК-4.3. Владеет навыками представления юридических заключений, используемых для осуществления консультационной работы в сфере частного права и гражданского оборота для физических и юридических лиц,	

			органов государственной власти и местного самоуправления, общественных объединений, а также консультирования правоохранительных органов по квалификации преступлений в сфере цифровых активов и киберпреступности, по вопросам цифровой безопасности и защиты цифровых прав граждан.	
3.	Тема 3. Правовое обеспечение безопасности цифровых платформ, электронных сделок, информационных систем и цифровых сервисов	УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Знает этапы жизненного цикла проекта; этапы разработки и реализации проекта; методы разработки и управления проектами.	опрос, тест, реферат, решение задач
			УК-2.2. Умеет разрабатывать проект с учетом анализа альтернативных вариантов его реализации, определять с использованием инструментов планирования целевые этапы и основные направления работ; формулировать цель задачи, обосновывать актуальность, научную и практическую значимость, ожидаемые результаты и возможные сферы применения; управлять проектом на всех этапах его жизненного цикла, осуществлять мониторинг хода его реализации, вносить при необходимости изменения в план реализации проекта; представлять публично результаты проекта (его этапов) в различной форме (отчеты, статьи, выступления на научно-практических конференциях, семинарах	
			УК-2.3. Владеет методиками разработки и управления проектом; методами оценки потребности в ресурсах и эффективности проекта.	
		ПК-2. Способен квалифицированно применять нормативные правовые акты, реализовывать нормы материального и процессуального права в соответствующей	ПК-2.1. Знает правовые основы и правоприменительную практику; теоретические основы юридической оценки ситуаций; методику решения практических задач применения норм материального и процессуального права в сфере частного права и гражданского оборота, включая особенности применения норм к отношениям с использованием цифровых	опрос, тест, реферат, решение задач

		сфере профессиональной деятельности	технологий.	
			ПК-2.2. Умеет собирать и анализировать правовую и фактическую информацию, имеющую значение для реализации правовых норм в ходе правоприменительной деятельности, участвовать в процессе решения споров, оценивать результативность и последствия правовых решений в сфере частного права и гражданского оборота, в том числе споров, связанных с оборотом цифровых активов, электронными сделками, защитой персональных данных, ответственностью операторов платформ.	
			ПК-2.3. Владеет навыками составления правовых документов по требованиям юридической техники в сфере частного права и гражданского оборота, а также подготовки и использования электронных доказательств в гражданском, арбитражном и административном процессе.	
		ПК-4 Способен давать юридические консультации и заключения в различных сферах юридической деятельности	ПК-4.1. Знает законодательство об осуществлении консультационной работы в сфере частного права и гражданского оборота для физических и юридических лиц, органов государственной власти и местного самоуправления, общественных объединений; виды и формы юридических консультаций, применяемых в сфере частного права и гражданского оборота, а также особенности консультирования по вопросам правового режима цифровых прав, токенов, краудфандинга, смарт-контрактов, платформенной экономики, защиты персональных данных, применения искусственного интеллекта в частном праве.	опрос, тест, реферат, решение задач
			ПК-4.2. Умеет составлять юридические заключения, используемые для осуществления консультационной работы в сфере частного права и гражданского оборота для физических и	

			юридических лиц, органов государственной власти и местного самоуправления, общественных объединений, включая заключения по вопросам соблюдения законодательства об экспериментальных правовых режимах, о цифровых платформах, об обороте криптоактивов.	
			ПК-4.3. Владеет навыками представления юридических заключений, используемых для осуществления консультационной работы в сфере частного права и гражданского оборота для физических и юридических лиц, органов государственной власти и местного самоуправления, общественных объединений, а также консультирования правоохранительных органов по квалификации преступлений в сфере цифровых активов и киберпреступности, по вопросам цифровой безопасности и защиты цифровых прав граждан.	
4	Тема 4. Юридическая ответственность, защита прав и консультирование в сфере информационной безопасности и цифровых рисков	УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Знает этапы жизненного цикла проекта; этапы разработки и реализации проекта; методы разработки и управления проектами.	опрос, тест, реферат, решение задач
			УК-2.2. Умеет разрабатывать проект с учетом анализа альтернативных вариантов его реализации, определять с использованием инструментов планирования целевые этапы и основные направления работ; формулировать цель задачи, обосновывать актуальность, научную и практическую значимость, ожидаемые результаты и возможные сферы применения; управлять проектом на всех этапах его жизненного цикла, осуществлять мониторинг хода его реализации, вносить при необходимости изменения в план реализации проекта; представлять публично результаты проекта (его этапов) в различной форме (отчеты, статьи, выступления на научно-практических конференциях,	

			семинарах	
			УК-2.3. Владеет методиками разработки и управления проектом; методами оценки потребности в ресурсах и эффективности проекта.	
		ПК-2. Способен квалифицированно применять нормативные правовые акты, реализовывать нормы материального и процессуального права в соответствующей сфере профессиональной деятельности	ПК-2.1. Знает правовые основы и правоприменительную практику; теоретические основы юридической оценки ситуаций; методику решения практических задач применения норм материального и процессуального права в сфере частного права и гражданского оборота, включая особенности применения норм к отношениям с использованием цифровых технологий.	опрос, тест, реферат, решение задач
			ПК-2.2. Умеет собирать и анализировать правовую и фактическую информацию, имеющую значение для реализации правовых норм в ходе правоприменительной деятельности, участвовать в процессе решения споров, оценивать результативность и последствия правовых решений в сфере частного права и гражданского оборота, в том числе споров, связанных с оборотом цифровых активов, электронными сделками, защитой персональных данных, ответственностью операторов платформ.	
			ПК-2.3. Владеет навыками составления правовых документов по требованиям юридической техники в сфере частного права и гражданского оборота, а также подготовки и использования электронных доказательств в гражданском, арбитражном и административном процессе.	
		ПК-4 Способен давать юридические консультации и заключения в различных сферах юридической деятельности	ПК-4.1. Знает законодательство об осуществлении консультационной работы в сфере частного права и гражданского оборота для физических и юридических лиц, органов государственной власти и местного самоуправления, общественных объединений; виды и формы юридических консультаций, применяемых в сфере частного	опрос, тест, реферат, решение задач

			права и гражданского оборота, а также особенности консультирования по вопросам правового режима цифровых прав, токенов, краудфандинга, смарт-контрактов, платформенной экономики, защиты персональных данных, применения искусственного интеллекта в частном праве.	
			ПК-4.2. Умеет составлять юридические заключения, используемые для осуществления консультационной работы в сфере частного права и гражданского оборота для физических и юридических лиц, органов государственной власти и местного самоуправления, общественных объединений, включая заключения по вопросам соблюдения законодательства об экспериментальных правовых режимах, о цифровых платформах, об обороте криптоактивов.	
			ПК-4.3. Владеет навыками представления юридических заключений, используемых для осуществления консультационной работы в сфере частного права и гражданского оборота для физических и юридических лиц, органов государственной власти и местного самоуправления, общественных объединений, а также консультирования правоохранительных органов по квалификации преступлений в сфере цифровых активов и киберпреступности, по вопросам цифровой безопасности и защиты цифровых прав граждан.	

Дисциплина изучается по очной форме обучения в 3-м и 4-м семестрах, по заочной форме обучения – на 2-м курсе и является промежуточным этапом формирования компетенций УК-2, ПК-2 и ПК-4.

По очной форме обучения формирование компетенции УК-2 начинается при изучении дисциплины «Профессиональная этика юриста» в 1-м семестре. Дисциплина «Правовое обеспечение информационной безопасности», изучаемая в 3-м и 4-м семестрах, обеспечивает дальнейшее формирование данной компетенции применительно к разработке и сопровождению правовых проектов в сфере защиты

информации, персональных данных, цифровых сервисов, информационных систем и цифровых прав. После освоения дисциплины формирование компетенции УК-2 продолжается в ходе производственной практики: преддипломной практики. Итоговая оценка сформированности компетенции УК-2 осуществляется в период государственной итоговой аттестации: подготовка к процедуре защиты и защита выпускной квалификационной работы.

По заочной форме обучения формирование компетенции УК-2 начинается при изучении дисциплины «Профессиональная этика юриста» на 1-м курсе в зимнюю сессию. Дисциплина «Правовое обеспечение информационной безопасности», изучаемая на 2-м курсе в зимнюю и летнюю сессии, выступает следующим этапом формирования компетенции УК-2 в части проектного сопровождения правовых решений в сфере информационной безопасности. Дальнейшее закрепление компетенции осуществляется при прохождении производственной практики: преддипломной практики, а итоговая оценка – в период государственной итоговой аттестации.

По очной форме обучения формирование компетенции ПК-2 начинается при изучении дисциплин «Цифровые права человека и гражданина», «Актуальные проблемы семейного права», а также при прохождении учебной практики: ознакомительной практики во 2-м семестре. Дисциплина «Правовое обеспечение информационной безопасности» продолжает формирование компетенции ПК-2 в 3-м и 4-м семестрах применительно к квалифицированному применению законодательства об информации, информационных технологиях, защите информации, персональных данных, охраняемой законом тайне, цифровых правах и электронном взаимодействии. На этом же этапе компетенция ПК-2 закрепляется при прохождении производственной практики: правоприменительной практики. В дальнейшем формирование компетенции продолжается при изучении элективных дисциплин «Корпоративное право в цифровой трансформации бизнеса» / «Актуальные проблемы коммерческого права». Итоговая оценка сформированности компетенции ПК-2 осуществляется в период государственной итоговой аттестации.

По заочной форме обучения формирование компетенции ПК-2 начинается при изучении дисциплин «Цифровые права человека и гражданина», «Актуальные проблемы семейного права» и прохождении учебной практики: ознакомительной практики на 1-м курсе в летнюю сессию. Дисциплина «Правовое обеспечение информационной безопасности», изучаемая на 2-м курсе в зимнюю и летнюю сессии, является последующим этапом формирования компетенции ПК-2. Одновременно компетенция закрепляется при прохождении производственной практики: правоприменительной практики. Дальнейшее формирование компетенции осуществляется при изучении элективных дисциплин «Корпоративное право в цифровой трансформации бизнеса» / «Актуальные проблемы коммерческого права», а итоговая оценка – в период государственной итоговой аттестации.

По очной форме обучения формирование компетенции ПК-4 начинается при изучении дисциплины «Актуальные проблемы семейного права» во 2-м семестре. Дисциплина «Правовое обеспечение информационной безопасности» в 3-м и 4-м семестрах обеспечивает дальнейшее формирование компетенции ПК-4 в части подготовки юридических консультаций и заключений по вопросам защиты

информации, персональных данных, цифровых прав, охраняемой законом тайны, цифровых платформ, электронных сделок и киберрисков. На данном этапе компетенция также формируется при изучении дисциплины «Правовое регулирование инновационной деятельности» и прохождении производственной практики: правоприменительной практики. В дальнейшем формирование компетенции ПК-4 продолжается при изучении элективных дисциплин «Правовая политика развития цифровой экономики» / «Права граждан в информационной сфере», «Корпоративное право в цифровой трансформации бизнеса» / «Актуальные проблемы коммерческого права», а также при прохождении производственной практики: преддипломной практики. Итоговая оценка сформированности компетенции ПК-4 осуществляется в период государственной итоговой аттестации.

По заочной форме обучения формирование компетенции ПК-4 начинается при изучении дисциплины «Актуальные проблемы семейного права» на 1-м курсе в летнюю сессию. Дисциплина «Правовое обеспечение информационной безопасности», изучаемая на 2-м курсе в зимнюю и летнюю сессии, продолжает формирование компетенции ПК-4 применительно к консультационной деятельности в сфере информационной безопасности и цифрового гражданского оборота. На этом же этапе компетенция развивается при изучении дисциплины «Правовое регулирование инновационной деятельности», элективных дисциплин «Правовая политика развития цифровой экономики» / «Права граждан в информационной сфере», а также при прохождении производственной практики: правоприменительной практики. Дальнейшее формирование компетенции ПК-4 осуществляется при изучении элективных дисциплин «Корпоративное право в цифровой трансформации бизнеса» / «Актуальные проблемы коммерческого права» и при прохождении производственной практики: преддипломной практики. Итоговая оценка сформированности компетенции ПК-4 осуществляется в период государственной итоговой аттестации: подготовка к процедуре защиты и защита выпускной квалификационной работы. В процессе изучения дисциплины, компетенции также формируются поэтапно.

Основными этапами формирования УК-2 при изучении дисциплины Б1.Д(М).В.6 «Правовое обеспечение информационной безопасности» является последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение студентами необходимыми дескрипторами (составляющими) компетенций. Для оценки уровня сформированности компетенций в процессе изучения дисциплины предусмотрено проведение текущего контроля успеваемости по темам (разделам) дисциплины и промежуточной аттестации по дисциплине – зачет.

6.2. Контрольные задания и материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

6.2.1. Контрольные вопросы по темам (разделам) для опроса на занятиях

Тема (раздел)	Вопросы
Тема 1. Теоретико-правовые основы	УК-2 Какие этапы следует предусмотреть при разработке

информационной безопасности в условиях цифровизации частного права и гражданского оборота	правового проекта, направленного на повышение уровня информационной безопасности организации? Какие показатели могут использоваться для оценки эффективности проекта по снижению цифровых рисков? Как соотносятся правовые, организационные и технические мероприятия в проекте обеспечения информационной безопасности? ПК-2 В чем выражается значение информационной безопасности для устойчивости гражданского оборота в цифровой среде? Какие правовые последствия может повлечь отсутствие надлежащей системы защиты информации у участника цифрового оборота? Как разграничиваются публично-правовые и частноправовые механизмы обеспечения информационной безопасности? Какие юридически значимые обстоятельства необходимо установить при оценке нарушения требований информационной безопасности? ПК-4 Какие вопросы должен выяснить юрист перед подготовкой консультации по факту нарушения информационной безопасности? Как разъяснить клиенту различие между правовыми и техническими мерами защиты информации? Какие рекомендации могут быть включены в консультацию по предупреждению цифровых рисков в деятельности организации?
Тема 2. Правовой режим информации, персональных данных и охраняемой законом тайны в цифровом гражданском обороте	УК-2 Какие этапы должен включать проект по приведению деятельности организации в соответствие с требованиями законодательства о персональных данных? Как определить необходимые ресурсы для внедрения режима коммерческой тайны в организации? Какие риски следует учитывать при планировании проекта по защите конфиденциальной информации? ПК-2 Какие критерии позволяют отнести информацию к информации ограниченного доступа? Какие обязанности возникают у оператора при обработке персональных данных в цифровой среде? В каких случаях обработка персональных данных может быть признана неправомерной? Какие правовые последствия наступают при разглашении коммерческой, банковской или иной охраняемой законом

	тайны? ПК-4 Какие положения необходимо проверить юристу при анализе согласия на обработку персональных данных? Какие рекомендации следует дать организации при введении режима коммерческой тайны? Как сформулировать вывод в юридическом заключении о правомерности передачи персональных данных третьим лицам?
Тема 3. Правовое обеспечение безопасности цифровых платформ, электронных сделок, информационных систем и цифровых сервисов	УК-2 Какие правовые задачи должны быть включены в проект запуска цифровой платформы? Как организовать мониторинг правовых рисков при эксплуатации цифрового сервиса? Какие изменения могут потребоваться в проекте электронного документооборота при выявлении угроз информационной безопасности? ПК-2 Какие требования должны соблюдаться при использовании электронной подписи в цифровом гражданском обороте? Какие правовые риски возникают при заключении договоров через цифровые платформы? Как оценить правомерность условий пользовательского соглашения цифрового сервиса? Какие нормы права подлежат применению при нарушении безопасности информационной системы, используемой для совершения электронных сделок? ПК-4 Какие вопросы следует отразить в консультации по безопасному заключению электронных сделок? Как подготовить правовое заключение о рисках использования цифровой платформы в предпринимательской деятельности? Какие рекомендации могут быть даны пользователю цифрового сервиса при нарушении доступа к его данным или цифровым активам?
Тема 4. Юридическая ответственность, защита прав и консультирование в сфере информационной безопасности и цифровых рисков	УК-2 Какие этапы должен включать проект правового реагирования на утечку персональных данных? Как оценить результативность мер, принятых организацией после нарушения информационной безопасности? Какие корректирующие действия необходимо предусмотреть в проекте при повторном выявлении цифровых рисков? ПК-2

	Какие виды юридической ответственности могут наступать за нарушение требований информационной безопасности? Какие обстоятельства имеют значение для взыскания убытков, причиненных утечкой данных или разглашением тайны? Какие способы гражданско-правовой защиты могут применяться при распространении недостоверной информации в цифровой среде? Какова роль электронных доказательств при рассмотрении споров, связанных с нарушением информационной безопасности? ПК-4 Как построить юридическую консультацию для гражданина, чьи персональные данные были незаконно распространены? Какие выводы должно содержать заключение о перспективах защиты деловой репутации в цифровой среде? Какие рекомендации следует дать организации для минимизации ответственности после выявления нарушения режима защиты информации?

Шкала оценивания ответов на вопросы

Шкала оценивания	Критерии оценивания
«Отлично»	Обучающийся глубоко и содержательно раскрывает ответ на каждый теоретический вопрос, не допустив ошибок. Ответ носит развернутый и исчерпывающий характер, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные;
«Хорошо»	Обучающийся в целом раскрывает теоретические вопросы, однако ответ хотя бы на один из них не носит развернутого и исчерпывающего характера.
«Удовлетворительно»	Обучающийся в целом раскрывает теоретические вопросы и допускает ряд неточностей, фрагментарно раскрывает содержание теоретических вопросов или их раскрывает содержательно, но допуская значительные неточности.
«Неудовлетворительно»	Обучающийся не знает ответов на поставленные теоретические вопросы.

6.2.2. Темы для докладов

Тема (раздел)	Вопросы
Тема 1. Теоретико-правовые основы информационной безопасности в условиях	УК-2 1. Проектный подход к правовому обеспечению информационной безопасности организации. 2. Этапы разработки проекта по снижению цифровых рисков в гражданском обороте. 3. Управление проектом внедрения правовых мер защиты

цифровизации частного права и гражданского оборота	информации. 4. Оценка эффективности проекта по обеспечению информационной безопасности. 5. Правовые риски проекта цифровизации деятельности юридического лица. ПК-2 6. Понятие и правовая природа информационной безопасности. 7. Информационная безопасность как условие устойчивости цифрового гражданского оборота. 8. Система нормативного правового регулирования информационной безопасности в Российской Федерации. 9. Частноправовые и публично-правовые средства обеспечения информационной безопасности. 10. Основные угрозы информационной безопасности граждан и организаций в цифровой среде. ПК-4 11. Юридическое консультирование по вопросам информационной безопасности: предмет и пределы. 12. Консультирование организаций по вопросам предупреждения цифровых рисков. 13. Подготовка юридического заключения о правовых последствиях нарушения информационной безопасности. 14. Правовое сопровождение защиты цифровых прав граждан и организаций. 15. Роль юриста в обеспечении информационной безопасности участников гражданского оборота.
Тема 2. Правовой режим информации, персональных данных и охраняемой законом тайны в цифровом гражданском обороте	УК-2 1. Проект внедрения системы защиты персональных данных в организации. 2. Управление проектом по обеспечению режима коммерческой тайны. 3. Планирование правовых мероприятий по защите конфиденциальной информации. 4. Оценка ресурсов проекта по приведению обработки персональных данных в соответствие с законодательством. 5. Мониторинг реализации проекта по защите информации ограниченного доступа. ПК-2 6. Информация как объект правового регулирования в цифровом гражданском обороте. 7. Правовой режим персональных данных и обязанности оператора. 8. Права субъекта персональных данных и способы их защиты. 9. Коммерческая тайна как объект правовой охраны в предпринимательской деятельности. 10. Банковская, профессиональная и иная охраняемая законом тайна в частноправовых отношениях. ПК-4 11. Консультирование по вопросам получения согласия на обработку персональных данных. 12. Подготовка юридического заключения о правомерности обработки персональных данных. 13. Консультирование по вопросам введения режима коммерческой

	тайны. 14. Юридическая оценка соглашений о конфиденциальности. 15. Подготовка рекомендаций по защите информации ограниченного доступа.
Тема 3. Правовое обеспечение безопасности цифровых платформ, электронных сделок, информационных систем и цифровых сервисов	УК-2 1. Проектное сопровождение запуска цифровой платформы с учетом требований информационной безопасности. 2. Планирование проекта безопасного электронного документооборота. 3. Управление проектом защиты данных пользователей цифрового сервиса. 4. Оценка правовых рисков проекта внедрения электронной подписи. 5. Мониторинг правовых рисков функционирования цифровой платформы. ПК-2 6. Правовые требования к безопасности цифровых платформ. 7. Информационная безопасность при совершении электронных сделок. 8. Электронная подпись как средство обеспечения достоверности цифрового взаимодействия. 9. Защита цифровых прав и цифровых активов участников гражданского оборота. 10. Правовые риски применения искусственного интеллекта и автоматизированных систем в цифровой среде. ПК-4 11. Консультирование по вопросам безопасного заключения электронных сделок. 12. Подготовка заключения о рисках использования цифровой платформы. 13. Юридическая оценка пользовательского соглашения цифрового сервиса. 14. Консультирование по вопросам защиты цифровых активов. 15. Подготовка рекомендаций по снижению правовых рисков при использовании информационных систем.
Тема 4. Юридическая ответственность, защита прав и консультирование в сфере информационной безопасности и цифровых рисков	УК-2 1. Проект правового реагирования на утечку персональных данных. 2. Управление проектом восстановления нарушенных цифровых прав организации. 3. Планирование мероприятий по минимизации ответственности при нарушении информационной безопасности. 4. Оценка эффективности правового проекта по снижению киберрисков. 5. Корректировка проектных решений при выявлении повторных нарушений защиты информации. ПК-2 6. Виды юридической ответственности за нарушение требований информационной безопасности. 7. Гражданско-правовая ответственность за утечку персональных данных. 8. Ответственность за разглашение коммерческой и иной охраняемой законом тайны.

	9. Способы гражданско-правовой защиты при нарушении информационной безопасности. 10. Электронные доказательства в спорах о нарушении цифровых прав и защите информации. ПК-4 11. Консультирование гражданина при незаконном распространении его персональных данных. 12. Подготовка юридического заключения о перспективах взыскания убытков при утечке информации. 13. Консультирование организации по вопросам минимизации ответственности за нарушение режима защиты информации. 14. Подготовка правовой позиции по спору о защите деловой репутации в цифровой среде. 15. Юридическое консультирование по вопросам киберрисков, цифровых активов и защиты цифровых прав.

Шкала оценивания

Шкала оценивания	Критерии оценивания
«Отлично»	Обучающийся глубоко и содержательно раскрывает тему доклада, не допустив ошибок. Ответ носит развернутый и исчерпывающий характер.
«Хорошо»	Обучающийся в целом раскрывает тему доклада, однако ответ хотя бы на один из них не носит развернутого и исчерпывающего характера.
«Удовлетворительно»	Обучающийся в целом раскрывает тему доклада и допускает ряд неточностей, фрагментарно раскрывает содержание теоретических вопросов или их раскрывает содержательно, но допуская значительные неточности.
«Неудовлетворительно»	Обучающийся не владеет выбранной темой

6.2.3. Оценочные средства остаточных знаний (тест)

УК-2

1. Проект в сфере правового обеспечения информационной безопасности должен начинаться с:

а) определения целей, задач, рисков и ожидаемых результатов;

б) немедленного привлечения к ответственности работников;

в) отказа от анализа действующего законодательства;

г) исключения локального регулирования.

2. К этапам проекта по защите персональных данных в организации относится:

а) выявление обрабатываемых персональных данных и правовых оснований их обработки;

б) удаление всех документов организации;

в) отказ от получения согласий субъектов персональных данных;

г) передача всех данных третьим лицам без проверки оснований.

3. При управлении проектом информационной безопасности необходимо учитывать:

а) правовые, организационные, технические и кадровые ресурсы;

б) только количество компьютеров;

в) исключительно мнение оператора информационной системы;

г) только стоимость программного обеспечения.

4. Мониторинг проекта по обеспечению информационной безопасности направлен на:

а) оценку хода реализации мероприятий и своевременное устранение выявленных рисков;

б) прекращение всех договорных отношений;

в) замену законодательства внутренними правилами организации;

г) исключение ответственности за нарушения.

5. Эффективность проекта по защите информации оценивается с учетом:

а) достижения целей проекта, снижения правовых рисков и соблюдения требований законодательства;

б) только количества подготовленных приказов;

в) только устных распоряжений руководителя;

г) отсутствия анализа результатов.

6. Корректировка проекта информационной безопасности требуется, если:

а) выявлены новые правовые риски или нарушения режима защиты информации;

б) проект уже утвержден и не может изменяться;

в) отсутствуют цифровые сервисы;

г) не проводится обработка текстовых документов.

ПК-2

7. Информационная безопасность в правовом смысле связана с:

а) защитой информации, прав субъектов, цифровых сервисов и информационных систем от угроз;

б) исключительно установкой программного обеспечения;

в) отказом от электронного документооборота;

г) ограничением всех гражданских прав.

8. Персональные данные – это:

а) любая информация, относящаяся к прямо или косвенно определенному физическому лицу;

б) только сведения о юридическом лице;

в) только коммерческая тайна;

г) только сведения, размещенные в открытых источниках.

9. Оператор персональных данных обязан:

а) обеспечивать законность обработки персональных данных и принимать меры по их защите;

б) передавать данные любым лицам без согласия;

в) не уведомлять субъектов персональных данных о целях обработки;

г) хранить данные бессрочно без правового основания.

10. Коммерческая тайна охраняется при условии:

а) введения обладателем информации режима коммерческой тайны;

б) устного заявления о конфиденциальности без оформления режима;

в) отсутствия ценности информации;

г) передачи сведений всем контрагентам без ограничений.

11. Электронная подпись в цифровом гражданском обороте используется для:

а) подтверждения волеизъявления и идентификации участника электронного взаимодействия;

б) замены всех норм гражданского права;

в) отмены договорных обязательств;

г) исключения необходимости хранения документов.

12. Нарушение требований информационной безопасности может повлечь:

а) гражданско-правовую, административную, дисциплинарную или уголовную ответственность;

б) только устное предупреждение;

в) автоматическое прекращение всех договоров;

г) освобождение от обязанности возместить вред.

13. Электронные доказательства в спорах об информационной безопасности могут включать:

а) электронную переписку, журналы событий, сведения информационных систем, электронные документы;

б) только бумажные объяснения сторон;

в) только устные показания без фиксации;

г) сведения, не относящиеся к спору.

14. При утечке персональных данных важное значение имеет установление:

а) факта нарушения, объема раскрытых данных, причин утечки и последствий для субъекта данных;

б) только даты создания организации;

в) только наименования информационной системы;

г) исключительно размера уставного капитала.

ПК-4

15. Юридическая консультация по вопросам информационной безопасности должна содержать:

а) правовую оценку ситуации, применимые нормы, риски и рекомендации по защите прав;

б) только техническое описание программного обеспечения;

в) исключительно общие советы без правового анализа;

г) сведения, не связанные с вопросом клиента.

16. Юридическое заключение по вопросу обработки персональных данных должно включать:

а) анализ правовых оснований обработки, обязанностей оператора и возможных рисков;

б) только перечень сотрудников организации;

в) только сведения о количестве компьютеров;

г) отказ от оценки документов.

17. При консультировании по вопросам коммерческой тайны юрист должен проверить:

а) наличие локальных актов, перечня конфиденциальной информации, договорных условий и мер защиты;

б) только название организации;

в) только устные объяснения руководителя;

г) исключительно бухгалтерскую отчетность.

18. Консультация по безопасному заключению электронной сделки должна учитывать:

а) идентификацию сторон, электронную подпись, сохранность документов и защиту передаваемой информации;

б) только цену договора;

в) только дату регистрации сайта;

г) только форму логотипа цифровой платформы.

19. Заключение о рисках использования цифровой платформы должно содержать:

а) оценку пользовательского соглашения, режима данных, ответственности сторон и защиты цифровых прав;

б) только описание интерфейса платформы;

в) только маркетинговые преимущества сервиса;

г) сведения, не имеющие юридического значения.

20. При консультировании по факту незаконного распространения персональных данных необходимо разъяснить:

а) возможные способы защиты права, порядок обращения к оператору, в суд и уполномоченные органы;

б) невозможность защиты персональных данных;

в) обязанность гражданина самостоятельно удалить все сведения из сети;

г) отсутствие правовых последствий для нарушителя.

Открытые тестовые задания

УК-2

21. Проект в сфере правового обеспечения информационной безопасности – это _____.

22. Основными этапами проекта по защите персональных данных являются _____.

23. Оценка эффективности проекта информационной безопасности предполагает _____.

ПК-2

24. Информационная безопасность в цифровом гражданском обороте означает _____.

25. Правовой режим персональных данных включает _____.

26. Коммерческая тайна охраняется при условии _____.

27. Электронные доказательства по спорам в сфере информационной безопасности могут включать _____.

ПК-4

28. Юридическая консультация по вопросам информационной безопасности должна содержать _____.

29. Юридическое заключение о правомерности обработки персональных данных включает _____.

30. Консультирование по вопросам цифровых рисков направлено на _____.

Ключ: 1 – а; 2 – а; 3 – а; 4 – а; 5 – а; 6 – а; 7 – а; 8 – а; 9 – а; 10 – а; 11 – а; 12 – а; 13 – а; 14 – а; 15 – а; 16 – а; 17 – а; 18 – а; 19 – а; 20 – а.

21. Проект в сфере правового обеспечения информационной безопасности – это комплекс взаимосвязанных правовых, организационных и иных мероприятий, направленных на защиту информации, персональных данных, цифровых прав, информационных систем и цифровых сервисов.

22. Основными этапами проекта по защите персональных данных являются анализ обрабатываемых данных, определение правовых оснований обработки, подготовка локальных актов, получение согласий, внедрение мер защиты, контроль и корректировка правовых решений.

23. Оценка эффективности проекта информационной безопасности предполагает проверку достижения целей проекта, снижения правовых рисков, соблюдения требований законодательства и результативности принятых мер защиты информации.

24. Информационная безопасность в цифровом гражданском обороте означает состояние защищенности информации, цифровых прав, электронных сделок, цифровых сервисов и интересов участников гражданского оборота от неправомерного доступа, утечки, искажения или незаконного использования данных.

25. Правовой режим персональных данных включает принципы обработки, права субъекта персональных данных, обязанности оператора, правовые основания обработки, требования к согласию, хранению, передаче и защите данных.

26. Коммерческая тайна охраняется при условии введения обладателем информации режима коммерческой тайны, определения перечня охраняемых сведений, ограничения доступа к ним и принятия мер по сохранению их конфиденциальности.

27. Электронные доказательства по спорам в сфере информационной безопасности могут включать электронные документы, переписку, журналы событий информационных систем, сведения об авторизации, цифровые следы, скриншоты, файлы и иные данные в электронной форме.

28. Юридическая консультация по вопросам информационной безопасности должна содержать правовую оценку ситуации, указание применимых норм законодательства, анализ рисков, возможных способов защиты права и рекомендации по дальнейшим действиям.

29. Юридическое заключение о правомерности обработки персональных данных включает анализ целей и оснований обработки, объема данных, порядка получения согласия, обязанностей оператора, мер защиты и возможной ответственности за нарушение законодательства.

30. Консультирование по вопросам цифровых рисков направлено на выявление правовых угроз, предупреждение нарушений информационной

безопасности, защиту цифровых прав, персональных данных, электронных сделок и частноправовых интересов граждан и организаций.

Шкала оценивания результатов тестирования

% верных решений (ответов)	Шкала оценивания
85 - 100	отлично
70 - 84	хорошо
50- 69	удовлетворительно
0 - 49	неудовлетворительно

6.2.4. Примеры задач при разборе конкретных ситуаций

Тема 1. Теоретико-правовые основы информационной безопасности в условиях цифровизации частного права и гражданского оборота

УК-2

Задача 1.

Общество с ограниченной ответственностью планирует запуск цифрового сервиса, через который клиенты смогут заключать договоры, направлять заявки, получать электронные документы и передавать персональные данные. Руководитель поручил юридическому отделу подготовить правовое сопровождение проекта. При этом на момент начала работы не определены этапы реализации проекта, ответственные лица, правовые риски, порядок обработки данных пользователей и меры защиты информации.

1. Какие этапы жизненного цикла проекта необходимо выделить в данной ситуации?
2. Какие правовые риски следует учитывать при запуске цифрового сервиса?
3. Какие правовые документы и организационные меры необходимо подготовить до начала работы сервиса?

Задача 2.Организация реализует проект по снижению цифровых рисков при использовании внутренней информационной системы. В ходе мониторинга выявлено, что часть работников имеет избыточный доступ к сведениям о клиентах и договорах, а утвержденный план проекта не предусматривает регулярной проверки прав доступа.

1. Какие недостатки имеются в управлении проектом информационной безопасности?
2. Какие изменения следует внести в план реализации проекта?
3. По каким критериям можно оценить эффективность скорректированного проекта?

ПК-2

Задача 1.

Юридическое лицо использует информационную систему для хранения договоров, актов, переписки с клиентами и сведений о контрагентах. Локальный акт о

порядке доступа к информации не принят, перечень лиц, имеющих право работать с данными, не определен. Один из работников получил доступ к договору, не связанному с его должностными обязанностями, и использовал сведения из него при переговорах с третьим лицом.

1. Какие нормы законодательства подлежат применению при правовой оценке ситуации?
2. Какие требования информационной безопасности могли быть нарушены?
3. Какие правовые последствия могут наступить для организации и работника?

Задача 2.

В результате технического сбоя на сайте компании часть сведений о клиентах, включая фамилии, номера телефонов, адреса электронной почты и сведения о заказах, стала доступна другим пользователям сайта. Компания не уведомила клиентов о произошедшем, полагая, что сбой был кратковременным и не повлек существенных последствий.

1. Как квалифицировать данную ситуацию с точки зрения законодательства о персональных данных и защите информации?
2. Какие обязанности возникают у оператора персональных данных при выявлении подобного нарушения?
3. Какие способы защиты могут использовать клиенты, чьи данные стали доступны третьим лицам?

ПК-4

Задача 1.

Индивидуальный предприниматель планирует перевести взаимодействие с клиентами в электронную форму: заключать договоры через сайт, хранить документы в облачном сервисе, использовать электронную подпись и обрабатывать персональные данные покупателей. Предприниматель обратился за юридической консультацией о том, какие правовые меры необходимо принять для безопасной работы.

1. Какие вопросы необходимо выяснить юристу перед подготовкой консультации?
2. Какие основные рекомендации должны быть включены в юридическую консультацию?
3. Какие документы следует предложить подготовить предпринимателю?

Задача 2.

Коммерческая организация намерена использовать облачный сервис для хранения договоров, счетов, актов, персональных данных клиентов и внутренней переписки. Руководитель просит юриста подготовить заключение о правовых рисках такого решения.

1. Какие обстоятельства должен проанализировать юрист при подготовке заключения?
2. Какие риски связаны с использованием облачного сервиса для хранения юридически значимой информации?
3. Какие выводы и рекомендации должны быть отражены в юридическом заключении?

Тема 2. Правовой режим информации, персональных данных и охраняемой законом тайны в цифровом гражданском обороте

УК-2

Задача 1.

Компания оказывает услуги через сайт и мобильное приложение, собирая персональные данные клиентов. После внутренней проверки установлено, что согласия на обработку персональных данных оформлены по-разному, часть документов отсутствует, а сроки хранения данных не определены. Руководство решило запустить проект по приведению обработки персональных данных в соответствие с законодательством.

1. Какие этапы должен включать данный проект?
2. Какие ресурсы необходимы для его реализации?
3. Какие результаты должны быть достигнуты по итогам проекта?

Задача 2.

Организация планирует ввести режим коммерческой тайны в отношении клиентской базы, условий договоров, ценовой политики и бизнес-планов. При этом ранее такие сведения свободно направлялись контрагентам по электронной почте без специальных оговорок о конфиденциальности.

1. Какие мероприятия должны быть включены в проект введения режима коммерческой тайны?
2. Какие документы необходимо разработать и утвердить?
3. Как оценить эффективность реализации данного проекта?

ПК-2

Задача 1.

На сайте интернет-магазина размещена форма согласия на обработку персональных данных, содержащая только фразу: «Пользователь дает согласие на обработку своих данных». В документе не указаны цели обработки, перечень обрабатываемых данных, срок обработки, сведения о передаче данных третьим лицам и порядок отзыва согласия.

1. Какие недостатки имеются в оформлении согласия на обработку персональных данных?
2. Какие правовые последствия могут наступить для оператора персональных данных?
3. Какие положения необходимо включить в новую редакцию согласия?

Задача 2.

Работник организации после увольнения передал конкуренту сведения о клиентах, ценах и условиях договоров. Организация считает, что эти сведения составляют коммерческую тайну, однако перечень конфиденциальной информации не утверждался, режим коммерческой тайны не вводился, а соглашение о неразглашении с работником не заключалось.

1. Можно ли в данной ситуации квалифицировать переданные сведения как коммерческую тайну?
2. Какие ошибки допустила организация при защите конфиденциальной информации?

3. Какие меры необходимо принять для надлежащего оформления режима коммерческой тайны?

ПК-4

Задача 1.

В юридическую консультацию обратился владелец интернет-сервиса, который собирает имена, телефоны, адреса электронной почты и платежные сведения пользователей. Клиент просит разъяснить, какие документы необходимы для законной обработки персональных данных.

1. Какие документы должен рекомендовать подготовить юрист?
2. Какие положения необходимо включить в политику обработки персональных данных?
3. Какие риски следует разъяснить клиенту при отсутствии надлежащего документального оформления обработки данных?

Задача 2.

Организация планирует передать подрядчику доступ к персональным данным клиентов для оказания услуг технической поддержки. Договор с подрядчиком уже подготовлен, однако в нем отсутствуют условия о целях обработки данных, обязанностях подрядчика, мерах защиты информации и ответственности за нарушение конфиденциальности.

1. Какие положения договора должен проверить и дополнить юрист?
2. Какие условия необходимо включить для законной передачи персональных данных подрядчику?
3. Какой вывод должен быть сделан в юридическом заключении о правомерности такой передачи?

Тема 3. Правовое обеспечение безопасности цифровых платформ, электронных сделок, информационных систем и цифровых сервисов

УК-2

Задача 1.

Акционерное общество разрабатывает цифровую платформу для заключения договоров между пользователями. Платформа должна обеспечивать регистрацию пользователей, обмен документами, оплату услуг и хранение истории сделок. На этапе проектирования не определены правовые требования к идентификации пользователей, защите данных и хранению электронных документов.

1. Какие этапы правового сопровождения проекта необходимо предусмотреть?
2. Какие правовые риски возникают при запуске цифровой платформы?
3. Какие ожидаемые результаты должны быть определены в проекте?

Задача 2.

Организация внедряет систему электронного документооборота. В процессе реализации проекта выяснилось, что не разработан порядок использования электронной подписи, не определены сроки хранения электронных документов, не установлены правила доступа работников к системе.

1. Какие недостатки имеются в проекте внедрения электронного документооборота?
2. Какие изменения необходимо внести в проектную документацию?

3. Какие правовые результаты должны быть достигнуты после корректировки проекта?

ПК-2

Задача 1.

Пользовательское соглашение цифровой платформы предусматривает, что оператор вправе по своему усмотрению ограничивать доступ пользователя к аккаунту и удалять документы без объяснения причин. При этом соглашение не содержит порядка идентификации сторон, правил хранения электронных документов и ответственности оператора за сбои.

1. Какие правовые риски содержит данное пользовательское соглашение?
2. Какие нормы материального права могут быть применены к возникшим отношениям?
3. Какие положения необходимо включить в соглашение для защиты прав участников цифрового гражданского оборота?

Задача 2.

Организация заключает договоры с клиентами в электронной форме, используя простую электронную подпись. Однако соглашение об использовании электронной подписи не оформлено, порядок подтверждения волеизъявления сторон не определен, электронные документы хранятся без установленного регламента.

1. Какие правовые проблемы могут возникнуть при доказывании факта заключения договора?
2. Какие документы необходимо оформить для надлежащего использования электронной подписи?
3. Какие правовые последствия может повлечь отсутствие регламента хранения электронных документов?

ПК-4

Задача 1.

Пользователь цифровой платформы утратил доступ к личному кабинету, где хранились электронные документы, сведения о сделках и переписка с контрагентами. Оператор платформы отказывается восстановить доступ, ссылаясь на внутренние правила сервиса, которые пользователь фактически не изучал.

1. Какие обстоятельства должен выяснить юрист при подготовке консультации?
2. Какие способы защиты прав пользователя могут быть предложены?
3. Какие доказательства следует собрать для подтверждения позиции пользователя?

Задача 2.

Компания планирует использовать систему искусственного интеллекта для автоматической обработки заявок клиентов, оценки рисков и формирования индивидуальных предложений. Руководство просит юриста подготовить заключение о правовых рисках использования такой системы.

1. Какие вопросы должны быть отражены в юридическом заключении?
2. Какие риски связаны с обработкой персональных данных и автоматизированным принятием решений?
3. Какие рекомендации следует дать компании для снижения правовых рисков?

Тема 4. Юридическая ответственность, защита прав и консультирование в сфере информационной безопасности и цифровых рисков

УК-2

Задача 1.

После утечки персональных данных клиентов организация решила разработать проект правового реагирования. Необходимо уведомить заинтересованных лиц, провести внутреннюю проверку, определить причины нарушения, подготовить изменения в локальные акты и принять меры по предупреждению повторных инцидентов.

1. Какие этапы должен включать проект правового реагирования?
2. Какие мероприятия следует предусмотреть для минимизации последствий утечки данных?
3. Как оценить результативность проекта после его реализации?

Задача 2.

Организация ранее реализовала проект по снижению киберрисков, однако через несколько месяцев вновь произошел инцидент, связанный с неправомерным доступом к конфиденциальной информации. Проверка показала, что часть мероприятий была выполнена формально, а контроль их исполнения не осуществлялся.

1. Какие ошибки были допущены при управлении проектом?
2. Какие корректирующие действия необходимо включить в обновленный проект?
3. Какие показатели следует использовать для оценки эффективности системы управления цифровыми рисками?

ПК-2

Задача 1.

В результате неправомерного доступа к информационной системе интернет-магазина были раскрыты персональные данные клиентов, сведения о заказах и адресах доставки. Один из клиентов заявил о причинении морального вреда и риске имущественных потерь, связанных с использованием его данных третьими лицами.

1. Какие виды юридической ответственности могут наступить в данной ситуации?
2. Какие способы защиты может использовать клиент?
3. Какие обстоятельства имеют значение для доказывания нарушения и его последствий?

Задача 2.

В сети Интернет распространены сведения о том, что компания якобы допустила массовую утечку данных клиентов. Компания утверждает, что эти сведения недостоверны, а после их распространения несколько контрагентов отказались от заключения договоров.

1. Какие способы защиты деловой репутации может использовать организация?
2. Какие обстоятельства необходимо доказать для взыскания убытков?
3. Какие электронные доказательства могут иметь значение для разрешения спора?

ПК-4

Задача 1.

Гражданин обнаружил, что его персональные данные, включая номер телефона, адрес электронной почты и сведения о месте работы, размещены в открытом доступе на интернет-ресурсе без его согласия. Он обратился за юридической консультацией о порядке защиты своих прав.

1. Какие правовые способы защиты необходимо разъяснить гражданину?
2. В какие органы и с какими требованиями он может обратиться?
3. Какие доказательства следует собрать для защиты его прав?

Задача 2.

Организация понесла убытки после утечки конфиденциальной информации о переговорах с контрагентами. Руководитель просит подготовить юридическое заключение о перспективах взыскания убытков с лица, допустившего разглашение сведений.

1. Какие обстоятельства должны быть установлены для взыскания убытков?
2. Какие документы и доказательства необходимо проанализировать юристу?
3. Какие выводы должны быть отражены в юридическом заключении?

Шкала оценивания

Шкала оценивания	Критерии оценивания
«Отлично»	обучающийся ясно изложил условие задачи, решение обосновал
«Хорошо»	обучающийся ясно изложил условие задачи, но в обосновании решения имеются сомнения;
«Удовлетворительно»	обучающийся изложил решение задачи, но обосновал его формулировками обыденного мышления;
«Неудовлетворительно»	обучающийся не уяснил условие задачи, решение не обосновал либо не сдал работу на проверку (в случае проведения решения задач в письменной форме).

6.2.4. Темы для рефератов

Тема (раздел)	Вопросы
Тема 1. Теоретико-правовые основы информационной безопасности в условиях цифровизации частного права и гражданского оборота	УК-2 1. Проектный подход к формированию системы правового обеспечения информационной безопасности организации. 2. Правовое планирование мероприятий по снижению цифровых рисков в гражданском обороте. 3. Управление правовым проектом в сфере защиты информации и цифровых прав. 4. Оценка эффективности правовых мер обеспечения информационной безопасности. 5. Ресурсное обеспечение проектов в сфере информационной безопасности. ПК-2 6. Информационная безопасность как правовая категория и элемент цифрового гражданского оборота. 7. Правовые основы обеспечения информационной безопасности в Российской Федерации. 8. Соотношение публично-правовых и частноправовых механизмов

	защиты информации. 9. Информационная безопасность как условие защиты имущественных и договорных интересов участников гражданского оборота. 10. Правовые угрозы информационной безопасности граждан и организаций в условиях цифровизации. ПК-4 11. Юридическое консультирование по вопросам информационной безопасности: содержание и особенности. 12. Роль юриста в предупреждении цифровых рисков в деятельности организации. 13. Подготовка юридических заключений по вопросам защиты информации и цифровых прав. 14. Консультирование граждан и организаций по вопросам безопасного электронного взаимодействия. 15. Правовое сопровождение защиты частноправовых интересов в цифровой среде.
Тема 2. Правовой режим информации, персональных данных и охраняемой законом тайны в цифровом гражданском обороте	УК-2 1. Проект внедрения системы обработки и защиты персональных данных в организации. 2. Управление проектом по введению режима коммерческой тайны. 3. Планирование правовых мероприятий по защите конфиденциальной информации. 4. Оценка эффективности локального регулирования обработки персональных данных. 5. Правовые ресурсы, необходимые для обеспечения режима охраняемой законом тайны. ПК-2 6. Информация как объект правового регулирования в условиях цифровизации гражданского оборота. 7. Персональные данные: понятие, правовой режим и способы защиты. 8. Права субъекта персональных данных и обязанности оператора. 9. Коммерческая тайна в предпринимательской деятельности: правовой режим и способы защиты. 10. Банковская, профессиональная и иная охраняемая законом тайна в частноправовых отношениях. ПК-4 11. Юридическое консультирование по вопросам обработки персональных данных. 12. Подготовка юридического заключения о правомерности передачи персональных данных третьим лицам. 13. Консультирование по вопросам введения и соблюдения режима коммерческой тайны. 14. Правовая оценка соглашений о конфиденциальности в гражданском обороте. 15. Подготовка рекомендаций по защите информации ограниченного доступа.
Тема 3. Правовое обеспечение безопасности цифровых платформ, электронных	УК-2 1. Правовое сопровождение проекта запуска цифровой платформы. 2. Проект внедрения электронного документооборота в организации.

сделок, информационных систем и цифровых сервисов	3. Управление проектом по обеспечению безопасности цифрового сервиса. 4. Оценка правовых рисков при внедрении электронной подписи. 5. Мониторинг правовых рисков функционирования информационной системы. ПК-2 6. Правовые требования к безопасности цифровых платформ в гражданском обороте. 7. Электронная сделка: правовая природа и требования информационной безопасности. 8. Электронная подпись как средство обеспечения юридической значимости электронного взаимодействия. 9. Защита цифровых прав и цифровых активов участников гражданского оборота. 10. Правовые риски применения искусственного интеллекта и автоматизированной обработки данных. ПК-4 11. Юридическое консультирование по вопросам безопасного заключения электронных сделок. 12. Подготовка юридического заключения о рисках использования цифровой платформы. 13. Правовая оценка пользовательских соглашений цифровых сервисов. 14. Консультирование по вопросам защиты цифровых активов и электронных документов. 15. Подготовка рекомендаций по снижению правовых рисков при использовании информационных систем.
Тема 4. Юридическая ответственность, защита прав и консультирование в сфере информационной безопасности и цифровых рисков	УК-2 1. Проект правового реагирования на утечку персональных данных. 2. Управление проектом минимизации ответственности за нарушение требований информационной безопасности. 3. Планирование мероприятий по предупреждению повторных нарушений защиты информации. 4. Оценка эффективности правовых мер по снижению киберрисков. 5. Корректировка проектных решений при выявлении нарушений информационной безопасности. ПК-2 6. Юридическая ответственность за нарушение законодательства об информации и защите информации. 7. Гражданско-правовая ответственность за незаконную обработку или утечку персональных данных. 8. Ответственность за разглашение коммерческой и иной охраняемой законом тайны. 9. Гражданско-правовые способы защиты при нарушении информационной безопасности. 10. Электронные доказательства в спорах о защите информации и цифровых прав. ПК-4 11. Консультирование гражданина при незаконном распространении его персональных данных. 12. Подготовка юридического заключения о перспективах взыскания убытков при утечке информации.

	13. Консультирование организации по вопросам минимизации ответственности за нарушение режима защиты информации. 14. Подготовка правовой позиции по делу о защите деловой репутации в цифровой среде. 15. Юридическое консультирование по вопросам киберрисков, цифровых активов и защиты цифровых прав.

6.3. ОЦЕНОЧНЫЕ СРЕДСТВА ПРОМЕЖУТОЧНОГО КОНТРОЛЯ

Вопросы для подготовки к промежуточной аттестации по итогам освоения дисциплины Правовое обеспечение информационной безопасности

УК-2.

1. Проектный подход к правовому обеспечению информационной безопасности организации.
2. Этапы жизненного цикла проекта в сфере защиты информации и цифровых прав.
3. Определение целей и задач проекта по обеспечению информационной безопасности.
4. Планирование мероприятий по снижению цифровых рисков в деятельности организации.
5. Разработка проекта внедрения системы защиты персональных данных.
6. Управление проектом введения режима коммерческой тайны.
7. Проектное сопровождение внедрения электронного документооборота.
8. Правовое сопровождение проекта запуска цифровой платформы.
9. Оценка правовых рисков проекта цифровизации деятельности юридического лица.
10. Определение ресурсов, необходимых для реализации проекта в сфере информационной безопасности.
11. Мониторинг реализации проекта по защите информации и цифровых сервисов.
12. Корректировка проектных решений при выявлении нарушений информационной безопасности.
13. Оценка эффективности проекта по снижению киберрисков.
14. Правовое планирование мероприятий по защите конфиденциальной информации.
15. Проект правового реагирования на утечку персональных данных.
16. Управление проектом минимизации ответственности за нарушение режима защиты информации.
17. Оценка ожидаемых результатов проекта по обеспечению безопасности цифрового гражданского оборота.
18. Публичное представление результатов проекта в сфере информационной безопасности.
19. Подготовка отчетных и аналитических материалов по итогам реализации проекта.
20. Значение проектного управления для защиты частноправовых интересов граждан и организаций в цифровой среде.

ПК-2.

21. Понятие и правовая природа информационной безопасности.
22. Система нормативного правового регулирования информационной безопасности в Российской Федерации.
23. Информация как объект правового регулирования.
24. Виды информации и особенности их правового режима.
25. Информация ограниченного доступа: понятие и правовое значение.
26. Персональные данные: понятие, признаки и правовой режим.
27. Принципы обработки персональных данных.
28. Права субъекта персональных данных и способы их защиты.
29. Обязанности оператора персональных данных.
30. Согласие на обработку персональных данных: содержание и правовое значение.
31. Правовые условия передачи персональных данных третьим лицам.
32. Коммерческая тайна как объект правовой охраны в предпринимательской деятельности.
33. Банковская, профессиональная, служебная и иная охраняемая законом тайна.
34. Правовые требования к безопасности цифровых платформ и информационных систем.
35. Информационная безопасность при совершении электронных сделок.
36. Электронная подпись и ее значение в цифровом гражданском обороте.
37. Электронные документы и электронные доказательства в спорах об информационной безопасности.
38. Юридическая ответственность за нарушение требований информационной безопасности.
39. Гражданско-правовые способы защиты при утечке персональных данных или разглашении тайны.
40. Защита деловой репутации при распространении недостоверной информации в цифровой среде.

ПК-4.

41. Юридическое консультирование по вопросам информационной безопасности: понятие, содержание и пределы.
42. Виды юридических консультаций в сфере защиты информации и цифровых прав.
43. Подготовка юридического заключения по вопросам правового режима персональных данных.
44. Консультирование по вопросам получения согласия на обработку персональных данных.
45. Подготовка рекомендаций по оформлению политики обработки персональных данных.
46. Юридическое заключение о правомерности передачи персональных данных подрядчику или иному третьему лицу.
47. Консультирование организации по вопросам введения режима коммерческой тайны.

48. Правовая оценка соглашения о конфиденциальности.

49. Подготовка юридического заключения о рисках использования облачных сервисов.

50. Консультирование по вопросам безопасного заключения электронных сделок.

51. Подготовка заключения о правовых рисках использования цифровой платформы.

52. Юридическая оценка пользовательского соглашения цифрового сервиса.

53. Консультирование по вопросам защиты цифровых активов и электронных документов.

54. Подготовка заключения о рисках применения искусственного интеллекта при обработке данных.

55. Консультирование гражданина при незаконном распространении его персональных данных.

56. Подготовка правовой позиции по спору о нарушении информационной безопасности.

57. Юридическое заключение о перспективах взыскания убытков, причиненных утечкой информации.

58. Консультирование организации по вопросам минимизации ответственности за нарушение режима защиты информации.

59. Подготовка правовой позиции по делу о защите деловой репутации в цифровой среде.

60. Консультирование по вопросам киберрисков, цифровой безопасности и защиты частноправовых интересов граждан и организаций.

6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Основной целью проведения промежуточной аттестации является определение степени достижения целей по учебной дисциплине или ее разделам. Осуществляется это проверкой и оценкой уровня теоретической знаний, полученных обучающимися, умения применять их в решении практических задач, степени овладения обучающимися практическими навыками и умениями в объеме требований рабочей программы по дисциплине, а также их умение самостоятельно работать с учебной литературой.

Организация проведения промежуточной аттестации регламентирована «Положением об организации образовательного процесса в федеральном государственном автономном образовательном учреждении «Московский политехнический университет»

6.4.1. Показатели оценивания компетенций на различных этапах их формирования, достижение обучающимися планируемых результатов обучения по дисциплине

Код и наименование компетенции УК-2. Способен управлять проектом на всех этапах его жизненного цикла				
Этап (уровень)	**Критерии оценивания**			
	неудовлетворительно	**удовлетворительно**	**хорошо**	**отлично**
знать	Не знает этапы жизненного цикла проекта, не раскрывает особенности проектного подхода в сфере информационной безопасности.	Фрагментарно знает этапы проекта, отдельные методы планирования и управления проектами в сфере защиты информации.	В целом знает этапы разработки и реализации проекта, методы планирования и оценки рисков в сфере информационной безопасности.	Полно знает этапы жизненного цикла проекта, методы разработки, планирования, мониторинга и оценки эффективности проектов по защите информации, персональных данных и цифровых сервисов.
уметь	Не умеет формулировать цель, задачи и этапы проекта, не определяет риски и ожидаемые результаты.	Частично умеет определять отдельные задачи проекта, но затрудняется в анализе рисков и планировании мероприятий	Умеет разрабатывать проект, определять этапы, основные направления работ, правовые риски и ожидаемые результаты.	Уверенно умеет разрабатывать и корректировать проект в сфере информационной безопасности, обосновывать его актуальность, оценивать альтернативы, ресурсы, риски и результаты.
владеть	Не владеет навыками разработки и сопровождения проекта.	Владеет отдельными элементами проектной деятельности, но допускает существенные ошибки при оценке ресурсов и эффективности.	Владеет навыками планирования, сопровождения и оценки проекта по обеспечению информационной безопасности.	Свободно владеет методиками разработки, управления, мониторинга и оценки эффективности проектов в сфере защиты информации, цифровых прав и цифрового гражданского оборота.

Код и наименование компетенции ПК-2 Способен квалифицированно применять нормативные правовые акты, реализовывать нормы материального и процессуального права в соответствующей сфере профессиональной деятельности				
Этап (уровень)	**Критерии оценивания**			
	неудовлетворительно	**удовлетворительно**	**хорошо**	**отлично**

знать	Не знает правовые основы информационной безопасности, защиты информации, персональных данных и цифровых прав.	Фрагментарно знает отдельные нормы законодательства об информации, персональных данных и защите информации.	В целом знает нормативные правовые акты и правоприменительную практику в сфере информационной безопасности и цифрового гражданского оборота.	Полно знает законодательство об информации, информационных технологиях, защите информации, персональных данных, охраняемой законом тайне, цифровых правах и электронном взаимодействии.
уметь	Не умеет определять применимые нормы права и квалифицировать правовую ситуацию	Частично умеет находить применимые нормы, но допускает ошибки при их толковании и применении.	Умеет анализировать фактические обстоятельства, определять применимые нормы материального и процессуального права, оценивать правовые последствия нарушений.	Уверенно умеет квалифицированно применять нормы права к ситуациям, связанным с утечкой данных, нарушением конфиденциальности, цифровыми сервисами, электронными сделками и защитой цифровых прав.
владеть	Не владеет навыками правовой оценки ситуаций в сфере информационной безопасности.	Владеет отдельными навыками анализа, но испытывает затруднения при формировании правовой позиции.	Владеет навыками правовой оценки, применения нормативных актов и подготовки выводов по вопросам защиты информации и персональных данных.	Свободно владеет навыками квалифицированного применения законодательства, анализа правоприменительной практики, подготовки правовой позиции и выбора способов защиты прав в цифровой среде.

Код и наименование компетенции ПК-4 Способен давать юридические консультации и заключения в различных сферах юридической деятельности

Этап (уровень)	**Критерии оценивания**			
	неудовлетворительно	**удовлетворительно**	**хорошо**	**отлично**
знать	Не знает виды и формы юридических консультаций и заключений в сфере информационной безопасности.	Фрагментарно знает отдельные формы консультирования по вопросам защиты информации и персональных данных.	В целом знает порядок подготовки юридических консультаций и заключений по вопросам информационной безопасности, цифровых прав и охраняемой законом тайны.	Полно знает законодательство и методику консультирования по вопросам защиты информации, персональных данных, цифровых платформ, электронных сделок, цифровых активов и киберрисков.

уметь	Не умеет определять содержание консультации и формулировать правовые выводы.	Частично умеет составлять консультации и заключения, но выводы недостаточно аргументированы.	Умеет составлять юридические консультации и заключения по вопросам информационной безопасности, защиты данных и цифровых прав.	Уверенно умеет готовить обоснованные юридические консультации и заключения для граждан и организаций, анализировать документы, оценивать риски и предлагать способы защиты прав.
владеть	Не владеет навыками подготовки и представления юридических заключений.	Владеет отдельными навыками консультирования, но допускает неточности в правовой аргументации.	Владеет навыками подготовки правовых заключений, консультаций, рекомендаций и правовых позиций по вопросам информационной безопасности.	Свободно владеет навыками комплексного консультирования, представления юридических заключений, оценки цифровых рисков и защиты частноправовых интересов граждан и организаций в цифровой среде.

6.4.2 Методика оценивания результатов промежуточной аттестации

Показателями оценивания компетенций на этапе промежуточной аттестации по дисциплине «Правовое обеспечение информационной безопасности» являются результаты обучения по дисциплине.

Оценочный лист результатов обучения по дисциплине

Код компетенции	Знания	Умения	Навыки	Уровень сформированности компетенции на данном этапе / оценка
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	На уровне знаний: знает этапы разработки и реализации проекта в сфере правового обеспечения информационной безопасности; правовые нормы, ресурсы и ограничения, влияющие на выбор способов защиты информации, персональных данных, цифровых сервисов и информационных систем.	На уровне умений: умеет определять цель, задачи, этапы и ожидаемые результаты проекта по обеспечению информационной безопасности; выбирать оптимальные правовые и организационные способы решения задач с учетом действующего законодательства, ресурсов и цифровых рисков.	На уровне навыков: владеет навыками планирования, сопровождения и оценки проекта в сфере защиты информации, персональных данных, цифровых прав, электронного документооборота и цифрового гражданского оборота.	

ПК-2 Способен квалифицированно применять нормативные правовые акты, реализовывать нормы материального и процессуального права в соответствующей сфере профессиональной деятельности	На уровне знаний: знает законодательство об информации, информационных технологиях, защите информации, персональных данных, охраняемой законом тайне, цифровых правах, электронных сделках и правовые основы защиты участников цифрового гражданского оборота.	На уровне умений: умеет определять подлежащие применению нормы материального и процессуального права при разрешении ситуаций, связанных с нарушением требований информационной безопасности, утечкой персональных данных, разглашением тайны и защитой цифровых прав.	На уровне навыков: владеет навыками юридической оценки фактических обстоятельств, квалифицированного применения нормативных правовых актов и подготовки правовой позиции по вопросам информационной безопасности и защиты прав в цифровой среде.	
ПК-4 Способен давать юридические консультации и заключения в различных сферах юридической деятельности	На уровне знаний: знает виды и формы юридических консультаций и заключений по вопросам информационной безопасности, защиты информации, персональных данных, цифровых платформ, электронных сделок, цифровых активов и киберрисков	На уровне умений: умеет составлять юридические консультации и заключения по вопросам соблюдения законодательства о защите информации, обработке персональных данных, обеспечении конфиденциальности, безопасности цифровых сервисов и защите цифровых прав.	На уровне навыков: владеет навыками подготовки и представления юридических заключений, консультаций, рекомендаций и правовых позиций по вопросам информационной безопасности, цифровых рисков и защиты частноправовых интересов граждан и организаций.	
Оценка по дисциплине (среднее арифметическое)				

Промежуточная аттестация обучающихся в форме зачета проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по дисциплине «Правовое обеспечение информационной безопасности», при

этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине проводится преподавателем, ведущим занятия по дисциплине методом экспертной оценки. По итогам промежуточной аттестации по дисциплине выставляется оценка «зачтено», «незачтено».

Шкала оценивания	**Описание**
Зачтено	Выполнены все виды учебной работы, предусмотренные учебным планом. Магистрант демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
незачтено	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Магистрант демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, магистрант испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7. Электронная информационно-образовательная среда

Каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронной информационно-образовательной среде Чебоксарского института (филиала) Московского политехнического университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), как на территории филиала, так и вне ее.

Электронная информационно-образовательная среда – совокупность информационных и телекоммуникационных технологий, соответствующих технологических средств, обеспечивающих освоение обучающимися образовательных программ в полном объёме независимо от места нахождения обучающихся.

Электронная информационно-образовательная среда обеспечивает:

а) доступ к учебным планам, рабочим программам дисциплин (модулей), практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), практик;

б) формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы;

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих.

Функционирование электронной информационно-образовательной среды соответствует законодательству Российской Федерации.

Основными составляющими ЭИОС филиала являются:

а) официальный сайт института в сети Интернет, расположенный по адресу www.polytech21.ru , который обеспечивает:

- доступ обучающихся к учебным планам, рабочим программам дисциплин, практик, к изданиям электронных библиотечных систем, электронным информационным и образовательным ресурсам, указанных в рабочих программах (разделы сайта «Сведения об образовательной организации», «Библиотека», «Студенту», «Абитуриенту», «ДПО»);

- информирование обучающихся обо всех изменениях учебного процесса (разделы сайта «Студенту», «Кафедры», новостная лента сайта, лента анонсов);

- взаимодействие между участниками образовательного процесса (подразделы сайта «Вопрос кафедре», «Задать вопрос директору»);

б) официальные электронные адреса подразделений и сотрудников института с Яндекс-доменом @polytech21.ru (список контактных данных подразделений Филиала размещен на официальном сайте Филиала в разделе «Контакты», списки контактных официальных электронных данных преподавателей размещены в подразделах «Кафедры») обеспечивают взаимодействие между участниками образовательного процесса;

в) личный кабинет обучающегося (портфолио) (вход в личный кабинет размещен на официальном сайте Филиала в разделе «Студенту» подразделе «Электронная информационно-образовательная среда») включает в себя портфолио студента, электронные ведомости, рейтинг студентов и обеспечивает:

- фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательных программ обучающимися,

- формирование электронного портфолио обучающегося, в том числе с сохранение работ обучающегося, рецензий и оценок на эти работы,

г) электронные библиотеки, включающие электронные каталоги, полнотекстовые документы и обеспечивающие доступ к учебно-методическим материалам, выпускным квалификационным работам и т.д.:

Чебоксарского института (филиала) - «ИРБИС»

д) электронно-библиотечные системы (ЭБС), включающие электронный каталог и полнотекстовые документы:

- «ЛАНЬ» - www.e.lanbook.com

- Образовательная платформа Юрайт - https://urait.ru

е) платформа цифрового образования Политеха - https://lms.mospolytech.ru/

ж) система «Антиплагиат» - https://www.antiplagiat.ru/

з) система электронного документооборота DIRECTUM Standard – обеспечивает документооборот между Филиалом и Университетом;

и) система «1С Управление ВУЗом Электронный деканат» (Московский политехнический университет) обеспечивает фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательных программ обучающимися;

к) система «POLYTECH systems» обеспечивает информационное, документальное автоматизированное сопровождение образовательного процесса;

л) система «Абитуриент» обеспечивает документальное автоматизированное сопровождение работы приемной комиссии.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Нормативные правовые акты

1. Конституция Российской Федерации принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 14.03.2020 № 1-ФКЗ) / Российская Федерация // Российская газета. – 2020. - № 144.

Основная литература:

1. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2026. – 357 с. – (Высшее образование). – ISBN 978-5-534-19108-0. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/583236.

2. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. – 2-е изд. – Москва : Издательство Юрайт, 2026. – 252 с. – (Высшее образование). – ISBN 978-5-9916-4299-6. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/589902.

3. Жарова, А. К. Информационное право. Правовое регулирование создания и использования информационной инфраструктуры : учебник для вузов / А. К. Жарова. – Москва : Издательство Юрайт, 2026. – 300 с. – (Высшее образование). – ISBN 978-5-534-19904-8. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/588704.

Дополнительная литература:

1. Жарова, А. К. Информационное право. Правовое регулирование создания и использования информационной инфраструктуры : учебник для вузов / А. К. Жарова. – Москва : Издательство Юрайт, 2026. – 300 с. – (Высшее образование). – ISBN 978-5-534-19904-8. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/588704.

2. Жарова, А. К. Информационное право. Правовое регулирование создания и использования информационной инфраструктуры : учебник для вузов / А. К. Жарова. – Москва : Издательство Юрайт, 2026. – 300 с. – (Высшее образование). – ISBN 978-5-534-19904-8. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/588704.

3. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. – Москва : Издательство Юрайт, 2026. – 111 с. – (Высшее образование). – ISBN 978-5-534-12769-0. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/588094.

Периодика

Юридические исследования: научный журнал - URL: https://nbpublish.com/e_contents.php?mag=lr - Текст : электронный

9. Профессиональные базы данных и информационно-справочные системы

Профессиональная база данных и информационно-справочные системы	Информация о праве собственности (реквизиты договора)
Юридическая Россия – образовательный правовой портал http://window.edu.ru	На страницах портала представлена обширная нормативная, учебная, научная и др. информация в области юриспруденции: книги, статьи, документы, организации, персоны, ссылки на интернет-ресурсы, нормативные акты, судебная практика, реестр диссертаций. Электронные каталоги юридических библиотек. Анонсы конференций, конкурсов, семинаров. Учебно-методическое объединение по юридическому образованию. Список вузов, имеющих государственную аккредитацию; сохранивших военную кафедру; проводящих интерактивные консультации для поступающих. Новинки юридической литературы. Сведения о тематических центрах по отраслям права. Работает сервис поиска Z39.50 по российским и международным библиотекам. Новости и информеры портала. Работают интерактивные сервисы: обсуждения, форму, гостиная, web-блоги. свободный доступ
Официальное опубликование правовых актов http://www.pravo.gov.ru	Статус Портала как источника официального опубликования правовых актов определен Федеральным законом от 14 июня 1994 г. № 5-ФЗ «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания» (в редакции Федеральных законов от 21 октября 2011 г. № 289-ФЗ «О внесении изменений в Федеральный закон «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания», от 25 декабря 2012 г. № 254-ФЗ «О внесении изменений в статью 30 Федерального закона «О международных договорах Российской Федерации» и статью 9-1 Федерального закона «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания», от 1 июля 2017 г. № 148-ФЗ «О внесении изменений в Федеральный закон «О государственной охране и отдельные законодательные акты Российской Федерации-*, от 1 мая 2019 г. № 83-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»), Указом Президента Российской Федерации от 23 мая 1996 г. № 763 «О порядке опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти», Указом Президента Российской Федерации от 2 апреля 2014 г. № 198 «О порядке опубликования законов и иных правовых актов на «Официальном интернет-портале правовой информации» (www.pravo.gov.ru)», Указом Президента Российской Федерации от 14 октября 2014 г. № 668 «О совершенствовании порядка опубликования нормативных правовых актов федеральных органов исполнительной власти».
Гарант (справочно-правовая система)	Универсальная справочная правовая система, предлагающая исчерпывающую базу нормативных актов, кодексов, законов и

https://www.garant.ru/	тд.
Университетская информационная система РОССИЯ https://uisrussia.msu.ru/	Тематическая электронная библиотека и база для прикладных исследований в области экономики, управления, социологии, лингвистики, философии, филологии, международных отношений, права. свободный доступ
научная электронная библиотека Elibrary http://elibrary.ru/	Научная электронная библиотека eLIBRARY.RU - это крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 26 млн научных статей и публикаций, в том числе электронные версии более 5600 российских научно-технических журналов, из которых более 4800 журналов в открытом доступе свободный доступ
Государственная автоматизированная система Российской Федерации «Правосудие» https://sudrf.ru	Государственная автоматизированная система РФ «Правосудие» - это территориально распределенная автоматизированная информационная система, предназначенная для формирования единого информационного пространства судов общей юрисдикции и системы Судебного департамента при Верховном Суде Российской Федерации (СД), обеспечивающая информационную и технологическую поддержку судопроизводства на принципах поддержания требуемого баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации. свободный доступ
Право.РУ https://pravo.ru/	российская компания, владелец одноимённого тематического интернет-издания, разработчик одноимённой справочно-правовой системы и специализированного программного обеспечения для работы с материалами судебной практики.
сайт Института научной информации по общественным наукам РАН. http://www.inion.ru	Библиографические базы данных ИНИОН РАН по социальным и гуманитарным наукам ведутся с начала 1980-х годов. Общий объём массивов составляет более 3 млн. 500 тыс. записей (данные на 1 января 2012 г.). Ежегодный прирост – около 100 тыс. записей. В базы данных включаются аннотированные описания книг и статей из журналов и сборников на 140 языках, поступивших в Фундаментальную библиотеку ИНИОН РАН. Описания статей и книг в базах данных снабжены шифром хранения и ссылками на полные тексты источников из Научной электронной библиотеки.
Федеральный портал «Российское образование» [Электронный ресурс] – http://www.edu.ru	Федеральный портал «Российское образование» – уникальный интернет-ресурс в сфере образования и науки. Ежедневно публикует самые актуальные новости, анонсы событий, информационные материалы для широкого круга читателей. Еженедельно на портале размещаются эксклюзивные материалы, интервью с ведущими специалистами – педагогами, психологами, учеными, репортажи и аналитические статьи. Читатели получают доступ к нормативно-правовой базе сферы образования, они могут пользоваться самыми различными полезными сервисами – такими, как онлайн-тестирование, опросы по актуальным темам и т.д.

Название организации	Сокращённое название	Организационно-правовая форма	Отрасль (область деятельности)	Официальный сайт
Ассоциация юристов Росс	АЮР	Российская общественная организация	Юриспруденция	www.alrf.ru
Федеральная палата адвокатов Российской Федерации	ФПА РФ	Общероссийская негосударственная некоммерческая организация	Юриспруденция	www.fparf.ru
Федеральная нотариальная палата	ФНП	Общероссийская негосударственная некоммерческая организация	Юриспруденция	www.notariat.ru
Совет судей Российской Федерации	Совет судей РФ	Орган судейского сообщества	Юриспруденция	www.ssrf.ru
Ассоциация некоммерческих организаций – адвокатских образований «Гильдия российских адвокатов»	Гильдия российских адвокатов	Ассоциация некоммерческих организаций	Юриспруденция	www.qra.ru

10. Программное обеспечение (лицензионное и свободно распространяемое), используемое при осуществлении образовательного процесса

Аудитория	Программное обеспечение	Информация о праве собственности (реквизиты договора, номер лицензии и т.д.)
№ **201** Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей) Кабинет общепрофессиональных дисциплин Учебный зал судебных заседаний	Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 150-249 Node 2 year Educational Renewal License	Сублицензионный договор №977_1049.ЕП/25 от 10.12.2025
	Windows 7 OLPNLAcdmc	договор №Д03 от 30.05.2012) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)
	AdobeReader	свободно распространяемое программное обеспечение (бессрочная лицензия)
	Гарант- справочно-правовая система	Договор №С-002-2025 от 09.01.2025
	Yandex браузер	свободно распространяемое программное обеспечение (бессрочная лицензия)
	Microsoft Office Standard 2007(Microsoft DreamSpark Premium Electronic Software Delivery Academic (Microsoft Open License	номер лицензии-42661846 от 30.08.2007) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)
	МТС Линк	Договор №2/2026 (091_168.ЕП/26) от 27.03.2026
	AIMP	отечественное свободно

		распространяемое программное обеспечение (бессрочная лицензия)
№104 Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой среднего профессионального образования/бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей) Криминалистическая лаборатория	Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 150-249 Node 2 year Educational Renewal License	Сублицензионный договор №977_1049.ЕП/25 от 10.12.2025
	Windows 7 OLPNLAcdmc	договор №Д03 от 30.05.2012) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)
	AdobeReader	свободно распространяемое программное обеспечение (бессрочная лицензия)
	Гарант- справочно-правовая система	Договор №С-002-2025 от 09.01.2025
	Yandex браузер	свободно распространяемое программное обеспечение (бессрочная лицензия)
	Microsoft Office Standard 2007(Microsoft DreamSpark Premium Electronic Software Delivery Academic (Microsoft Open License	номер лицензии-42661846 от 30.08.2007) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)
	МТС Линк	Договор №2/2026 (091_168.ЕП/26) от 27.03.2026
	AIMP	отечественное свободно распространяемое программное обеспечение (бессрочная лицензия)
№ 103а Помещение для самостоятельной работы обучающихся	Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 150-249 Node 2 year Educational Renewal License	Сублицензионный договор №977_1049.ЕП/25 от 10.12.2025
	MS Windows 10 Pro	договор № 392_469.223.ЗК/19 от 17.12.19 (бессрочная лицензия)
	AdobeReader	свободно распространяемое программное обеспечение (бессрочная лицензия)
	Гарант- справочно-правовая система	Договор №С-002-2025 от 09.01.2025
	Yandex браузер	свободно распространяемое программное обеспечение (бессрочная лицензия)
	Microsoft Office Standard 2007(Microsoft DreamSpark Premium Electronic Software Delivery Academic (Microsoft Open License	номер лицензии-42661846 от 30.08.2007) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)
	AIMP	отечественное свободно распространяемое программное обеспечение (бессрочная лицензия)

11. Материально-техническое обеспечение дисциплины

Тип и номер помещения	Перечень основного оборудования и технических средств обучения
Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей) Кабинет общепрофессиональных дисциплин Учебный зал судебных заседаний **№ 201 (**г. Чебоксары, ул. К.Маркса. 54)	Оборудование: комплект мебели для учебного процесса; скамья подсудимых, места, отведенные для других участников процесса (судья, секретарь, адвокат, государственный обвинитель и т.д.); атрибуты, отражающие судебную символику (государственный флаг, судебная мантия, молоток судьи, и т.д.) Технические средства обучения: компьютерная техника; мультимедийное оборудование (проектор, экран)
Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой среднего профессионального образования/бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей) Криминалистическая лаборатория **№ 104 (**г. Чебоксары, ул. К.Маркса. 54)	Оборудование: комплект мебели для учебного процесса; унифицированный чемодан криминалиста № 1, №2; лазерные дальномеры, 3D-сканеры, дактилоскопические наборы наглядное учебное пособие, манекен, оружие, ультрафиолетовые и инфракрасные излучатели, взрывные устройства, предметы, используемые в качестве оружия, и комплектующие к ним, натуральные коллекции, Технические средства обучения: компьютерная техника; телевизор
Помещение для самостоятельной работы обучающихся **№ 103а** (г. Чебоксары, ул. К.Маркса. 54)	Оборудование: комплект мебели для учебного процесса; Технические средства обучения: компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Филиала

12. Методические указания для обучающегося по освоению дисциплины

Методические указания для занятий лекционного типа

В ходе лекционных занятий обучающемуся необходимо вести конспектирование учебного материала, обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации.

Необходимо задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Целесообразно дорабатывать свой конспект лекции, делая в нем соответствующие записи из основной и дополнительной литературы, рекомендованной преподавателем и предусмотренной учебной программой дисциплины.

Методические указания для занятий семинарского (практического) типа.

Практические занятия позволяют развивать у обучающегося творческое теоретическое мышление, умение самостоятельно изучать литературу, анализировать практику; учат четко формулировать мысль, вести дискуссию, то есть имеют исключительно важное значение в развитии самостоятельного мышления.

Подготовка к практическому занятию включает два этапа. На первом этапе обучающийся планирует свою самостоятельную работу, которая включает: уяснение задания на самостоятельную работу; подбор основной и дополнительной литературы; составление плана работы, в котором определяются основные пункты предстоящей подготовки. Составление плана дисциплинирует и повышает организованность в работе.

Второй этап включает непосредственную подготовку к занятию, которая начинается с изучения основной и дополнительной литературы. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. Далее следует подготовить тезисы для выступлений по всем учебным вопросам, выносимым на практическое занятие или по теме, вынесенной на дискуссию (круглый стол), продумать примеры с целью обеспечения тесной связи изучаемой темы с реальной жизнью.

Готовясь к докладу или выступлению в рамках интерактивной формы (дискуссия, круглый стол), при необходимости следует обратиться за помощью к преподавателю.

Методические указания к самостоятельной работе.

Самостоятельная работа обучающегося является основным средством овладения учебным материалом во время, свободное от обязательных учебных занятий. Самостоятельная работа обучающегося над усвоением учебного материала по учебной дисциплине может выполняться в библиотеке университета, учебных кабинетах, компьютерных классах, а также в домашних условиях. Содержание и количество самостоятельной работы обучающегося определяется учебной программой дисциплины, методическими материалами, практическими заданиями и указаниями преподавателя.

Самостоятельная работа в аудиторное время может включать*:*

1) конспектирование (составление тезисов) лекций;
2) выполнение контрольных работ;
3) решение задач;
4) работу со справочной и методической литературой;
5) работу с нормативными правовыми актами;
6) выступления с докладами, сообщениями на семинарских занятиях;
7) защиту выполненных работ;
8) участие в оперативном (текущем) опросе по отдельным темам изучаемой дисциплины;
9) участие в собеседованиях, деловых (ролевых) играх, дискуссиях, круглых столах, конференциях;
10) участие в тестировании и др.

Самостоятельная работа во внеаудиторное время может состоять из:

1) повторения лекционного материала;

2) подготовки к практическим занятиям;
3) изучения учебной и научной литературы;
4) изучения нормативных правовых актов (в т.ч. в электронных базах данных);
5) решения задач, и иных практических заданий
6) подготовки к тестированию и т.д.;
7) подготовки к практическим занятиям устных докладов (сообщений);
8) подготовки рефератов по заданию преподавателя;
9) выполнения курсовых работ, предусмотренных учебным планом;
10) выделения наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями на консультациях.
11) проведения самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в данной программе задач, тестов, написания рефератов по отдельным вопросам изучаемой темы.

Текущий контроль осуществляется в форме устных, тестовых опросов, докладов.

В случае пропусков занятий, наличия индивидуального графика обучения и для закрепления практических навыков студентам могут быть выданы типовые индивидуальные задания, которые должны быть сданы в установленный преподавателем срок.

13. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение по данной дисциплине инвалидов и лиц с ограниченными возможностями здоровья (далее ОВЗ) осуществляется преподавателем с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Для студентов с нарушениями опорно-двигательной функции и с ОВЗ по слуху предусматривается сопровождение лекций и практических занятий мультимедийными средствами, раздаточным материалом.

Для студентов с ОВЗ по зрению предусматривается применение технических средств усиления остаточного зрения, а также предусмотрена возможность разработки аудиоматериалов.

По данной дисциплине обучение инвалидов и лиц с ограниченными возможностями здоровья может осуществляться как в аудитории, так и с использованием электронной информационно-образовательной среды, образовательного портала и электронной почты.

ЛИСТ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ

рабочей программы дисциплины

Рабочая программа дисциплины рассмотрена, обсуждена и одобрена для исполнения в 202__-202__ учебном году на заседании кафедры, протокол № от « » 202 г.

Внесены дополнения и изменения ____
____
____
____

Рабочая программа дисциплины рассмотрена, обсуждена и одобрена для исполнения в 202__-202__ учебном году на заседании кафедры, протокол № от « » 202 г.

Внесены дополнения и изменения ____
____
____
____

Рабочая программа дисциплины рассмотрена, обсуждена и одобрена для исполнения в 202__-202__ учебном году на заседании кафедры, протокол № от « » 202 г.

Внесены дополнения и изменения ____
____
____
____

Рабочая программа дисциплины рассмотрена, обсуждена и одобрена для исполнения в 202__-202__ учебном году на заседании кафедры, протокол № от « » 202 г.

Внесены дополнения и изменения ____
____
____
____