



Федеральное государственное образовательное бюджетное учреждение высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)

Кафедра международного и публичного права
Юридический факультет

Документ подписан усиленной неквалифицированной электронной подписью.

Организация: «ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ»

Сертификат: DCJO0hEGUmELue5t+GwbVs1biVGZLnhN

Утверждено: Проректор по учебной и методической работе, Е.А. Каменева
Дата: 02.10.2025 г.

И.Ш. Исмаилов

Правовое обеспечение кибербезопасности

Рабочая программа дисциплины

для студентов, обучающихся по направлению подготовки

40.03.01 - Юриспруденция,

Образовательная программа «Юриспруденция»

Профиль:

«Экономическое право»

Рекомендовано

Юридический факультет

(протокол № 07 от 22.04.2026 г.)

Одобрено

Кафедра международного и публичного права

(протокол № 8 от 26.03.2026 г.)



Содержание

1. Наименование дисциплины	3
2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине	3
3. Место дисциплины в структуре образовательной программы	
4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся	4
5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий	5
5.1. Содержание дисциплины	5
5.2. Учебно – тематический план	6
5.3. Содержание семинаров, практических занятий	7
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	9
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	9
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю	10
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	12
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	10
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	10
10. Методические указания для обучающихся по освоению дисциплины	17
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)	18
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	18



1. Наименование дисциплины

Правовое обеспечение кибербезопасности

2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
ПКП-1	Способность использовать фундаментальные знания в области частного права и публичного права в современных условиях и оказывать помощь в реализации правовых норм субъектами гражданского оборота	1. Демонстрирует знания нормативных правовых актов, а также прогнозирует результат экономической деятельности для решения практических задач	Знать: Основные нормативные акты, регулирующие отношения в сфере кибербезопасности, способы и методы толкования права и прогнозирования экономических процессов Уметь: Готовить акты толкования нормативных правовых актов и правоприменительные акты, корректно применять нормы законодательства по отношению к конкретным правоотношениям и прогнозировать последствия их применения
		2. Использует фундаментальные знания в области частного и публичного права в современных условиях	Знать: Основы правового обеспечения информационной безопасности, нормы публичного и частного права, регулирующие общественные отношения в сфере цифровизации Уметь: Пользоваться современными инструментами урегулирования и анализа юридических кейсов на основе полученных знаний
		3. Оказывает помощь в реализации правовых норм субъектами гражданского оборота	Знать: Основные пробелы и коллизии в сфере правового обеспечения кибербезопасности, правила составления юридически значимых документов Уметь: Выявлять пробелы и противоречия в регулировании процессов создания и использования финансовых технологий, осуществлять юридическое консультирование
ПКП-2	Способность действовать с учетом кризисных ситуаций в экономике, вызываемых рисками правового и экономического характера, анализировать проблемные ситуации на рынке товаров, работ, услуг, а также выявлять правонарушения при осуществлении предпринимательской деятельности и давать юридически обоснованные предложения по их преодолению и устранению	1. Действует с учетом кризисных ситуаций в экономике, вызываемых рисками правового и экономического характера	Знать: Ключевые правовые, экономические и технические риски в сфере кибербезопасности Уметь: Корректно применять нормы права и оказывать юридические консультации с учетом рисков правового и экономического характера
		2. Выявляет правонарушения при осуществлении предпринимательской деятельности	Знать: Способы и методы толкования права и анализа конкретных юридических кейсов для выявления возможных нарушений Уметь: Формировать обоснованную юридическую позицию по вопросам кибербезопасности на основе действующего законодательства и сложившейся правоприменительной практики
		3. Дает юридически обоснованные предложения по преодолению и устранению правонарушений при осуществлении предпринимательской деятельности	Знать: Основные виды правонарушений в сфере кибербезопасности и меры ответственности за их совершение Уметь: Выявлять и предотвращать возможные нарушения в сфере обеспечения кибербезопасности при осуществлении предпринимательской деятельности



3. Место дисциплины в структуре образовательной программы

Дисциплина «Правовое обеспечение кибербезопасности» относится к «Модулю "Право цифровой экономики"».

4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

очно-заочная форма обучения

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Семестр 8 (в часах)
Общая трудоемкость дисциплины	3/108	108
Контактная работа – Аудиторные занятия	16	16
<i>Лекции</i>	<i>8</i>	<i>8</i>
<i>Семинары, практические занятия</i>	<i>8</i>	<i>8</i>
<i>Самостоятельная работа</i>	<i>92</i>	<i>92</i>
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	Зачет	Зачет



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

5.1. Содержание дисциплины

Тема 1. Теоретико-правовые основы кибербезопасности: правовое регулирование и роль в обеспечении технологического суверенитета

Предмет, цели и задачи дисциплины «Правовое обеспечение кибербезопасности», её взаимосвязь с другими дисциплинами. Роль и место дисциплины «Правовое обеспечение кибербезопасности» в формировании специалистов по специальности «Юриспруденция». Роль информации в жизни личности, общества и государства. Понятие и место кибербезопасности в системе национальной безопасности России. Соотношение понятий: "кибербезопасность", "информационная безопасность", "защита информации". Понятие киберпространства как источника социальных опасностей и безопасности. Цели, задачи, функции кибербезопасности. Оценка предпосылок, условий и гарантий обеспечения кибербезопасности. Основные законодательные и нормативные акты, регулирующие общественные отношения в сфере информационной и кибербезопасности. Международно-правовое регулирование обеспечения информационной безопасности при использовании систем интернет-технологий и интернет-среды. Доктрина информационной безопасности Российской Федерации. Соотношение и взаимовлияние кибербезопасности и иных видов безопасности в системе общественных отношений. Виды рисков в сфере кибербезопасности. Правовые тенденции в области цифровизации и обеспечения кибербезопасности. Полномочия Федеральной службы безопасности, Федеральной службы по техническому и экспортному контролю, Минцифры, Роскомнадзора и других органов в сфере обеспечения кибербезопасности. Технологический суверенитет и роль кибербезопасности в его обеспечении. Цифровой суверенитет.

Тема 2. Правовой режим защиты персональных, биометрических и иных видов данных в контексте обеспечения кибербезопасности в приоритетных отраслях отечественной экономики

Персональные данные: понятие, состав и роль в современной системе кибербезопасности. Правовые основы защиты персональных и биометрических данных. Биометрические системы и биометрические персональные данные: новое регулирование. Конфиденциальная информация и режим работы с ней. Правовые основы хранения и обработки биометрических данных. Ответственность за нарушения режима хранения, сбора и обработки персональных данных. Биометрическая идентификация в системе государственных услуг и в финансовой сфере. Биоэквайринг: правовые основы, технологические решения и риски. Роль Единой системы идентификации и аутентификации (ЕСИА) в современной архитектуре кибербезопасности. Виды информации с ограниченным доступом. Государственная, служебная, профессиональная и коммерческая тайна. Банковская тайна. Правовой режим использования инсайдерской информации. Система сбора и распространения коммерческой информации. Приоритетные отрасли экономики: состав и особенности обеспечения защиты информации. Концепция технологического развития Российской Федерации на период до 2030 года. Вызовы в сфере кибербезопасности для развития приоритетных отраслей экономики. Квалификационные требования к специалисту в сфере защиты информации. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) и ее роль в системе отечественной кибербезопасности.

Тема 3. Кибербезопасность в финансовой сфере и при использовании критической информационной инфраструктуры: правовые основы обеспечения

Инструментарий обеспечения кибербезопасности в финансовой сфере. Требования к финансовым организациям и их цифровым ресурсам: доступность, открытость, безопасность. Информационная безопасность кредитных организаций: защита информации, требования к информационным системам и квалификации. Правовые основы применения технологии искусственного интеллекта в финансовой сфере: влияние на информационную и кибербезопасность финансовых организаций. Федеральный закон «О безопасности критической информационной инфраструктуры» (№ 187-ФЗ) и его роль в обеспечении кибербезопасности. Принципы обеспечения безопасности критической информационной инфраструктуры. Объекты критической информационной инфраструктуры и значимые объекты критической информационной инфраструктуры. Государственные информационные системы: понятие, функционирование и риски кибербезопасности. Роль Банка России в системе кибербезопасности в финансовой сфере. Использование мобильных приложений и интерфейсов API: правовые вопросы и риски кибербезопасности. Концепция открытого банкинга и мультибанкинга в контексте обеспечения кибербезопасности. Риски кибербезопасности в финансовой сфере: особенности и возможные последствия кибератак.

Тема 4. Киберпреступность: виды правонарушений и практика применения законодательства в сфере кибербезопасности

Понятие, правовые признаки, виды и формы угроз кибербезопасности. Основные угрозы в киберпространстве: компьютерные атаки, кибершпионаж, кибертерроризм. Киберпреступность как угроза кибербезопасности. Правоохранительные органы в системе обеспечения кибербезопасности. Цифровые и иные информационно-технологические источники угроз кибербезопасности. Понятие и виды киберпреступлений, их уголовно-правовая оценка и квалификация. Киберпространство, киберпреступность, ее причины, условия, киберпреступники, потенциальные и реальные потерпевшие от киберпреступлений как объекты кибербезопасности. Кибермошенничество и ключевые аспекты противодействия мошенническим практикам в сети Интернет. Иные виды правонарушений в цифровой среде. Предупреждение киберпреступлений. Государственная информационная система противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий (ГИС "Антифрод") и ее роль в противодействии незаконным практикам. Платформа "Знай своего клиента" и ее роль в обеспечении идентификации и безопасности. Кибербуллинг и киберсталкинг: ответственность за нарушения по отечественному и зарубежному законодательству. Искусственный интеллект как источник угроз безопасности.



5.2. Учебно – тематический план

Очно-заочная форма обучения

п/ п	Наименование тем (разделов) дисциплины	Трудоемкость в часах				
		Всего	Контактная работа - Аудиторная работа			Самостоятельная работа
			Общая, в т.ч.:	Лекции	Семинары, практические занятия	
1	Теоретико-правовые основы кибербезопасности: правовое регулирование и роль в обеспечении технологического суверенитета	27	4	2	2	23
2	Правовой режим защиты персональных, биометрических и иных видов данных в контексте обеспечения кибербезопасности в приоритетных отраслях отечественной экономики	27	4	2	2	23
3	Кибербезопасность в финансовой сфере и при использовании критической информационной инфраструктуры: правовые основы обеспечения	27	4	2	2	23
4	Киберпреступность: виды правонарушений и практика применения законодательства в сфере кибербезопасности	27	4	2	2	23
В целом по дисциплине		108	16	8	8	92



5.3. Содержание семинаров, практических занятий

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
Теоретико-правовые основы кибербезопасности: правовое регулирование и роль в обеспечении технологического суверенитета	Предмет, цели и задачи дисциплины «Правовое обеспечение кибербезопасности», её взаимосвязь с другими дисциплинами. Роль и место дисциплины «Правовое обеспечение кибербезопасности» в формировании специалистов по специальности «Юриспруденция». Роль информации в жизни личности, общества и государства. Понятие и место кибербезопасности в системе национальной безопасности России. Соотношение понятий: "кибербезопасность", "информационная безопасность", "защита информации". Цели, задачи, функции кибербезопасности. Оценка предпосылок, условий и гарантий обеспечения кибербезопасности. Основные законодательные и нормативные акты, регулирующие общественные отношения в сфере информационной и кибербезопасности. Соотношение и взаимовлияние кибербезопасности и иных видов безопасности в системе общественных отношений. Виды рисков в сфере кибербезопасности. Правовые тенденции в области цифровизации и обеспечения кибербезопасности. Полномочия Федеральной службы безопасности, Федеральной службы по техническому и экспортному контролю, Минцифры, Роскомнадзора и других органов в сфере обеспечения кибербезопасности. Технологический суверенитет и роль кибербезопасности в его обеспечении. Цифровой суверенитет.	устный опрос, обсуждение дискуссионных вопросов, решение тестовых заданий
Правовой режим защиты персональных, биометрических и иных видов данных в контексте обеспечения кибербезопасности в приоритетных отраслях отечественной экономики	Персональные данные: понятие, состав и роль в современной системе кибербезопасности. Правовые основы защиты персональных и биометрических данных. Биометрические системы и биометрические персональные данные: новое регулирование. Конфиденциальная информация и режим работы с ней. Правовые основы хранения и обработки биометрических данных. Ответственность за нарушения режима хранения, сбора и обработки персональных данных. Биозквейринг: правовые основы, технологические решения и риски. Роль Единой системы идентификации и аутентификации (ЕСИА) в современной архитектуре кибербезопасности. Виды информации с ограниченным доступом. Государственная, служебная, профессиональная и коммерческая тайна. Банковская тайна. Система сбора и распространения коммерческой информации. Приоритетные отрасли экономики: состав и особенности обеспечения защиты информации. Концепция технологического развития Российской Федерации на период до 2030 года. Вызовы в сфере кибербезопасности для развития приоритетных отраслей экономики.	устный опрос, обсуждение дискуссионных вопросов, решение ситуационных задач, тренинг по командной работе с предпринимательской направленностью
Кибербезопасность в финансовой сфере и при использовании критической информационной инфраструктуры: правовые основы обеспечения	Инструментарий обеспечения кибербезопасности в финансовой сфере. Требования к финансовым организациям и их цифровым ресурсам: доступность, открытость, безопасность. Информационная безопасность кредитных организаций: защита информации, требования к информационным системам и квалификации. Федеральный закон «О безопасности критической информационной инфраструктуры» (№ 187-ФЗ) и его роль в обеспечении кибербезопасности. Принципы обеспечения безопасности критической информационной инфраструктуры. Объекты критической информационной инфраструктуры и значимые объекты критической информационной инфраструктуры. Государственные информационные системы: понятие, функционирование и риски кибербезопасности. Роль Банка России в системе кибербезопасности в финансовой сфере. Использование мобильных приложений и интерфейсов API: правовые вопросы и риски кибербезопасности. Концепция открытого банкинга и мультибанкинга в контексте обеспечения кибербезопасности. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) и ее роль в системе отечественной кибербезопасности.	устный опрос, обсуждение дискуссионных вопросов, решение ситуационных задач
Киберпреступность: виды правонарушений и практика применения законодательства в сфере кибербезопасности	Понятие, правовые признаки, виды и формы угроз кибербезопасности. Основные угрозы в киберпространстве: компьютерные атаки, кибершпионаж, кибертерроризм. Киберпреступность как угроза кибербезопасности. Правоохранительные органы в системе обеспечения кибербезопасности. Цифровые и иные информационно-технологические источники угроз кибербезопасности. Понятие и виды киберпреступлений, их уголовно-правовая оценка и квалификация. Киберпространство, киберпреступность, ее причины, условия, киберпреступники, потенциальные и	устный опрос, обсуждение дискуссионных вопросов, решение тестовых заданий



Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
	реальные потерпевшие от киберпреступлений как объекты кибербезопасности. Кибермошенничество и ключевые аспекты противодействия мошенническим практикам в сети Интернет. Иные виды правонарушений в цифровой среде. Предупреждение киберпреступлений. Государственная информационная система противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий (ГИС "Антифрод") и ее роль в противодействии незаконным практикам. Платформа "Знай своего клиента" и ее роль в обеспечении идентификации и безопасности.	



6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. 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
Теоретико-правовые основы кибербезопасности: правовое регулирование и роль в обеспечении технологического суверенитета	Международно-правовое регулирование обеспечения информационной безопасности при использовании систем интернет-технологий и интернет-среды. Доктрина информационной безопасности Российской Федерации. Понятие киберпространства как источника социальных опасностей и безопасности.	Работа с учебной литературой. Изучение нормативных правовых актов и судебной практики с использованием справочно-правовых систем. Подготовка к тестированию.
Правовой режим защиты персональных, биометрических и иных видов данных в контексте обеспечения кибербезопасности в приоритетных отраслях отечественной экономики	Правовой режим использования инсайдерской информации. Квалификационные требования к специалисту в сфере защиты информации. Биометрическая идентификация в системе государственных услуг и в финансовой сфере.	Работа с учебной литературой. Изучение нормативных правовых актов и судебной практики с использованием справочно-правовых систем. Работа с электронными ресурсами Банка России и других ведомств, поиск релевантных нормативных актов и актов стратегического планирования, анализ конкретных ситуаций.
Кибербезопасность в финансовой сфере и при использовании критической информационной инфраструктуры: правовые основы обеспечения	Правовые основы применения технологии искусственного интеллекта в финансовой сфере: влияние на информационную и кибербезопасность финансовых организаций. Риски кибербезопасности в финансовой сфере: особенности и возможные последствия кибератак	Работа с учебной литературой. Изучение нормативных правовых актов и судебной практики с использованием справочно-правовых систем. Работа с электронными ресурсами Банка России и других ведомств, поиск релевантных нормативных актов и актов стратегического планирования.
Киберпреступность: виды правонарушений и практика применения законодательства в сфере кибербезопасности	Кибербуллинг и киберсталкинг: ответственность за нарушения по отечественному и зарубежному законодательству. Искусственный интеллект как источник угроз безопасности.	Работа с учебной литературой. Изучение нормативных правовых актов и судебной практики с использованием справочно-правовых систем. Подготовка к тестированию.



6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю

Примерные темы для контрольной работы

1. Правовое обеспечение кибербезопасности в финансовой сфере в России.
2. Примеры систем кибербезопасности в отечественной и мировой практике.
3. Технологический и финансовый суверенитет государства: вызовы в сфере кибербезопасности.
4. Международно-правовые акты и международное сотрудничество в сфере кибербезопасности.
5. Что такое критическая информационная инфраструктура (КИИ) и какие объекты к ней относятся?
6. Кибермошенничество: понятие и меры по противодействию.
7. Особенности регулирования криптовалют и цифровых активов с точки зрения кибербезопасности.
8. Доктрина информационной безопасности Российской Федерации: ключевые положения и значение.
9. Биометрическая идентификация: риски и преимущества.
10. Использование мобильных приложений и интерфейсов API: правовые вопросы.
11. Значение законодательства об электронной подписи в системе информационной безопасности.
12. Правовое регулирование сбора и использования персональных данных в России и зарубежных стран.
13. Суверенный Рунет: концепция и правовые основы.
14. Государственные системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и ее роль в обеспечении национальной кибербезопасности.
15. Киберпреступность: статистика и основы противодействия.
16. Значение государственных информационных систем (ГИС) в обеспечении кибербезопасности.
17. Охраняемые законом тайны: правовые основы оборота информации.
18. Риски кибербезопасности, связанные с использованием технологии анализа больших данных и искусственного интеллекта.
19. Роль Единой системы идентификации и аутентификации (ЕСИА) в современной архитектуре кибербезопасности.
20. Кейсы создания и использования биометрических систем.
21. Риски биометрической идентификации и аутентификации в финансовой сфере.
22. Виды правонарушений и преступлений в сфере кибербезопасности.
23. Ответственность за утечки персональных данных: статистика и правоприменительная практика.
24. Национальный координационный центр по компьютерным инцидентам: правовой статус и механизм взаимодействия.
25. Объекты критической информационной инфраструктуры: понятие, критерии выделения и особенности защиты.
26. Правовые основы защиты информации и кибербезопасности: ключевые нормативные акты.
27. Обзор правоприменительной практики в сфере обеспечения кибербезопасности.
28. Вызовы в сфере кибербезопасности для развития приоритетных отраслей экономики.
29. Кибербуллинг и киберсталкинг: понятие, квалификация и ответственность.
30. Концепция открытого банкинга и мультибанкинга в контексте обеспечения кибербезопасности.

Дополнительная информация

Рабочая программа дисциплины подготовлена в рамках фундаментальной научно-исследовательской работы в рамках государственного задания Финуниверситета 2026 года на тему: «Обеспечение технологического суверенитета и развития приоритетных отраслей отечественной экономики: поиск новых правовых решений».

Примеры типовых тестовых заданий

1. Видами электронных подписей, отношения в области использования которых регулируются Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи» являются:

- a. простая электронная подпись
- b. усиленная квалифицированная электронная подпись
- c. электронная цифровая подпись (ЭЦП)
- d. верифицированная подтвержденная электронная подпись
- e. усиленная неквалифицированная электронная подпись

2. В Единой биометрической системе (ЕБС) используются три типа биометрической записи: подтверждённая, стандартная и ... (впишите верный ответ)

3. Реестр экспериментальных правовых режимов в сфере цифровых инноваций ведет:

- a. Банк России
- b. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
- c. Министерство экономического развития Российской Федерации
- d. Министерство финансов Российской Федерации
- e. такого реестра не существует

4. Ключевые отличительные признаки неквалифицированной электронной подписи:

- a. позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания
- b. ключ проверки электронной подписи указан в квалифицированном сертификате
- c. получена в результате криптографического преобразования информации с использованием ключа электронной подписи
- d. предполагает использования кодов, паролей или иных средств
- e. позволяет определить лицо, подписавшее электронный документ



5. Применение сквозных цифровых технологий в ходе хозяйственной деятельности должно обеспечивать (Постановление Правительства РФ от 03.05.2019 N 551) следующие результаты:

- a. повышение результативности, точности или иных значимых характеристик технологического процесса
- b. разнообразие и выбор различных производственных процессов
- c. повышение качества или иных значимых характеристик производимых (поставляемых) товаров, оказываемых услуг и выполняемых работ
- d. повышение издержек
- e. снижение издержек

Примерный сценарий тренинга по командной работе с предпринимательской направленностью

Мозговой штурм по теме биометрической идентификации и аутентификации в различных бизнес-процессах.

Краткий сценарий: студенты разбиваются на несколько команд (3-5 команд), за каждой темой закрепляется какое-то конкретное направление предпринимательской деятельности.

- 1 команда — банковская и микрофинансовая деятельность,
- 2 команда — недвижимость и инвестиции,
- 3 команда — страхование и другие виды финансовой деятельности,
- 4 команда — транспорт и госуслуги,
- 5 команда — медицина и безопасность.

Каждая команда разрабатывает по 2 сценария использования биометрических данных для идентификации сторон при заключении сделок или осуществления других юридически значимых действий в своих сферах предпринимательской деятельности, а также фиксирует, какие требуются изменения в действующем законодательстве, инфраструктурные модернизации или другие шаги для внедрения предложенных инновационных практик по использованию биометрии.

В конце выбираются наиболее интересные инициативы (путем голосования самих студентов) для оформления их в качестве проектов и дальнейшей проработки.

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях Кафедры международного и публичного права.



7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Перечень компетенций с указанием индикаторов их достижения в процессе освоения образовательной программы содержится в разделе 2. «Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине».

Типовые контрольные задания или иные материалы, необходимые для оценки индикаторов достижения компетенций, умений и знаний

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
ПКП-1. Способность использовать фундаментальные знания в области частного права и публичного права в современных условиях и оказывать помощь в реализации правовых норм субъектами гражданского оборота	1. Демонстрирует знания нормативных правовых актов, а также прогнозирует результат экономической деятельности для решения практических задач	Знать: Основные нормативные акты, регулирующие отношения в сфере кибербезопасности, способы и методы толкования права и прогнозирования экономических процессов Уметь: Готовить акты толкования нормативных правовых актов и правоприменительные акты, корректно применять нормы законодательства по отношению к конкретным правоотношениям и прогнозировать последствия их применения	ООО «Вкусный Сок» (интернет-магазин продуктов) собирало персональные данные покупателей: ФИО, адрес доставки, номер телефона, e-mail, а также данные банковских карт (для автоматической оплаты). В феврале 2026 года в результате спланированной кибератаки произошла утечка: хакеры опубликовали в открытом доступе базу данных с информацией о 10 000 клиентах, включая платёжные данные. Выяснилось, что магазин хранил данные банковских карт покупателей на своих серверах в нарушение требований PCI DSS и не уведомил Роскомнадзор о начале обработки персональных данных. - Какие нарушения законодательства о персональных данных допустило ООО «Вкусный Сок»? Ответ обоснуйте ссылками на нормы ФЗ-152 «О персональных данных» и подзаконные акты. - Какой орган власти уполномочен рассматривать данное правонарушение и привлекать к ответственности? Какие санкции (штрафы, приостановка деятельности и т.п.) грозят обществу? - Имеют ли право пострадавшие клиенты требовать компенсации морального вреда? Если да, то в каком порядке и на основании каких статей ГК РФ?
	2. Использует фундаментальные знания в области частного и публичного права в современных условиях	Знать: Основы правового обеспечения информационной безопасности, нормы публичного и частного права, регулирующие общественные отношения в сфере цифровизации Уметь: Пользоваться современными инструментами урегулирования и анализа юридических кейсов на основе полученных знаний	Интернет-магазин «ПроДАЕМ» допустил утечку базы данных, содержащую персональные данные клиентов: в открытый доступ попали ФИО, адреса, электронные почты, телефоны и история заказов 100 000 пользователей, а также полная история их обращений. Расследование показало, что причиной стала уязвимость в системе безопасности, которую компания не устранила, несмотря на предупреждения IT-специалистов после проведения аудита систем безопасности в 2024 году. - Какие нормы российского законодательства были нарушены? Укажите конкретные законы и статьи. - Какие меры ответственности (административной, гражданской, уголовной) могут быть применены к компании и её руководству? Приведите ссылки на соответствующие статьи КоАП РФ, УК РФ и ГК РФ. - Какие действия обязана предпринять компания в соответствии с ФЗ № 152 после обнаружения утечки? Составьте краткий план реагирования.
	3. Оказывает помощь в реализации правовых норм субъектами гражданского оборота	Знать: Основные пробелы и коллизии в сфере правового обеспечения кибербезопасности, правила составления юридически значимых документов	Кредитная организация «Техно-Банк» в качестве одного из ключевых направлений своей деятельности выделяет развитие собственных биометрических систем идентификации и аутентификации клиентов, а также подтверждения платежей. В частности, для своих клиентов, согласившихся предоставить банку доступ к своим биометрическим данным, банк предлагает льготные условия по некоторым продуктам: повышенные кэшбеки на покупки в магазинах-партнерах, беспроцентный период по кредитным банковским картам, а также преференции по банковским вкладам (повышенные проценты и расширенную сумму гарантирования вклада). Помимо этого, банк предлагает таким клиентам возможность оформить вклад в форме NFT-документа, существующего только в цифровой форме. Оцените правомерность представленных действий банка. Ответ аргументируйте.



Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции	Типовые контрольные задания
		Уметь: Выявлять пробелы и противоречия в регулировании процессов создания и использования финансовых технологий, осуществлять юридическое консультирование	Опишите механизм подачи и обработки биометрических данных в соответствии с законодательством Российской Федерации.
ПКП-2. Способность действовать с учетом кризисных ситуаций в экономике, вызываемых рисками правового и экономического характера, анализировать проблемные ситуации на рынке товаров, работ, услуг, а также выявлять правонарушения при осуществлении предпринимательской деятельности и давать юридически обоснованные предложения по их преодолению и устранению	1. Действует с учетом кризисных ситуаций в экономике, вызываемых рисками правового и экономического характера	Знать: Ключевые правовые, экономические и технические риски в сфере кибербезопасности Уметь: Корректно применять нормы права и оказывать юридические консультации с учетом рисков правового и экономического характера	Банк «Финансовый Посредник» в своей деятельности использовал иностранное программное обеспечение для защиты клиентских данных, в том числе персональных. При проверке Банка России выяснилось, что используемое ПО не имеет сертификата соответствия требованиям ФСТЭК и ФСБ, а его алгоритмы шифрования не одобрены регуляторами. Банк аргументировал выбор ПО высокой скоростью обработки транзакций, а также имеющимися действующими долгосрочными контрактами с разработчиком, а переход на отечественные решения будет накладным с финансовой точки зрения. - Какие нормативные акты регулируют использование криптографических средств и сертифицированного ПО в финансовых организациях? - Какие санкции грозят банку за нарушение требований? - Каковы возможные шаги банка для устранения нарушений?
	2. Выявляет правонарушения при осуществлении предпринимательской деятельности	Знать: Способы и методы толкования права и анализа конкретных юридических кейсов для выявления возможных нарушений Уметь: Формировать обоснованную юридическую позицию по вопросам кибербезопасности на основе действующего законодательства и сложившейся правоприменительной практики	Гражданин Баранов О.А., работающий системным администратором в ООО «Зверь-Т», используя служебное положение, узнал пароль от личной электронной почты своей коллеги Сидоровой С.С. путем сбора соответствующих логов информации с рабочих серверов компании, так как Сидорова несколько раз входила в свою почту с рабочего компьютера. Он периодически входил в её почтовый ящик и читал письма, в том числе личную переписку. Полученную информацию о проблемах в семье и личной жизни коллеги он рассказал другим сотрудникам, чем причинил Сидоровой С.С. моральные страдания. Сидорова написала заявление в полицию. - Квалифицируйте действия Баранова О.А. по Уголовному кодексу РФ. Есть ли в его действиях состав преступления? - Будут ли действия Баранова О.А. являться нарушением тайны переписки (ст. 138 УК РФ)? В чём особенность этого состава преступления? - Какие доказательства необходимо собрать Сидоровой С.С. для привлечения Баранова О.А. к ответственности? Обязательно ли требовать проведения компьютерной экспертизы?
	3. Дает юридически обоснованные предложения по преодолению и устранению правонарушений при осуществлении предпринимательской деятельности	Знать: Основные виды правонарушений в сфере кибербезопасности и меры ответственности за их совершение Уметь: Выявлять и предотвращать возможные нарушения в сфере обеспечения кибербезопасности при осуществлении предпринимательской деятельности	Сеть фитнес-клубов «Фит-НессИ» внедрила биометрическую систему доступа в помещение и прохода по лицу. При оформлении абонемента администратор фотографировал клиента и заносил «биометрический шаблон» в свою локальную базу данных. Клиент Абрамов Д.А., подписывая договор, поставил галочку в поле «Согласие на обработку биометрических персональных данных» в стандартной оферте. Через месяц Абрамов Д.А. узнал, что по закону биометрия должна передаваться в Единую биометрическую систему (ЕБС), а хранить её локально запрещено. Он обратился с претензией к фитнес-клубу и потребовал компенсации. - Имеет ли право фитнес-клуб хранить биометрию клиентов в своей локальной базе данных и соответствует ли такая обработка требованиям законодательства? - Является ли «галочка» в оферте надлежащей формой согласия на сбор, хранение и обработку биометрии? - Какие меры ответственности грозят фитнес-клубу за нарушение порядка обработки биометрических данных?



Примеры практико-ориентированных заданий

Задача №1

АО «Водоканал-Сибирь», обслуживающее системы водоснабжения крупного города, подверглось целенаправленной хакерской атаке с целью похищения и уничтожения значимых данных и нарушения процессов управления системами водоснабжения. В результате атаки была нарушена работа автоматизированной системы управления технологическим процессом (АСУ ТП), что привело к временному отключению подачи воды в несколько жилых кварталов. Расследование показало, что АО «Водоканал-Сибирь» не исполнил обязанность по созданию системы безопасности значимого объекта КИИ и не подключился к ГосСОПКА.

- Подпадает ли АО «Водоканал-Сибирь» под действие ФЗ-187 «О безопасности критической информационной инфраструктуры РФ»? Аргументируйте ответ со ссылкой на критерии отнесения к объектам КИИ.
- Какие обязанности в области защиты КИИ нарушило общество?
- Какая ответственность (административная или уголовная) предусмотрена за нарушение требований к обеспечению безопасности значимых объектов КИИ?

Задача №2

Гражданин Баранов О.А., работающий системным администратором в ООО «Зверь-Т», используя служебное положение, узнал пароль от личной электронной почты своей коллеги Сидоровой С.С. путем сбора соответствующих логов информации с рабочих серверов компании, так как Сидорова несколько раз входила в свою почту с рабочего компьютера. Он периодически входил в её почтовый ящик и читал письма, в том числе личную переписку. Полученную информацию о проблемах в семье и личной жизни коллеги он рассказал другим сотрудникам, чем причинил Сидоровой С.С. моральные страдания. Сидорова написала заявление в полицию.

- Квалифицируйте действия Баранова О.А. по Уголовному кодексу РФ. Есть ли в его действиях состав преступления?
- Будут ли действия Баранова О.А. являться нарушением тайны переписки (ст. 138 УК РФ)? В чём особенность этого состава преступления?
- Какие доказательства необходимо собрать Сидоровой С.С. для привлечения Баранова О.А. к ответственности? Обязательно ли требовать проведения компьютерной экспертизы?

Примеры вопросов для подготовки к промежуточной аттестации

1. Дайте определение понятия «кибербезопасность» и сопоставьте его с понятием «информационная безопасность».
2. Назовите основные виды угроз кибербезопасности и приведите примеры каждой категории.
3. Перечислите ключевые принципы правового регулирования кибербезопасности в соответствии с законодательством Российской Федерации.
4. Какова роль международного сотрудничества в сфере кибербезопасности и какие международные организации устанавливают нормы в сфере кибербезопасности?
5. Что такое критическая информационная инфраструктура (КИИ) и какие объекты к ней относятся?
6. Охарактеризуйте уровни правового и организационного обеспечения кибербезопасности: международный, национальный, корпоративный, персональный.
7. Какие стратегические документы РФ определяют политику в области кибербезопасности?
8. Что понимается под цифровым суверенитетом государства и как он связан с кибербезопасностью?
9. Какие основные угрозы в киберпространстве выделяет Доктрина информационной безопасности РФ?
10. Перечислите основные федеральные законы, составляющие правовую основу кибербезопасности в России.
11. Каковы полномочия ФСТЭК России, ФСБ России и Роскомнадзора в области обеспечения кибербезопасности?
12. Какие конституционные права граждан ограничиваются при обеспечении кибербезопасности и на каком основании?
13. Какова роль Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)?
14. В чем заключается принцип «суверенного Рунета».
15. Какие виды административных правонарушений в области персональных данных предусмотрены КоАП РФ?
16. Опишите особенности работы с персональными данными: сбор, хранения, обработка, передача.
17. Раскройте состав преступления, предусмотренного ст. 272 УК РФ (Неправомерный доступ к компьютерной информации).
18. Что понимается под «утечкой персональных данных» и какова ответственность за неё?
19. Какие требования предъявляются к хранению и сбору биометрических персональных данных?
20. Перечислите и охарактеризуйте составы преступлений, предусмотренные главой 28 УК РФ «Преступления в сфере компьютерной информации».
21. В чем разница между понятиями «государственная тайна», «коммерческая тайна» и «конфиденциальная информация»?
22. Дайте характеристику понятию «персональные данные» и укажите какие категории персональных данных существуют.
23. Какая ответственность предусмотрена за нарушение требований к защите информации.
24. Каковы особенности привлечения к ответственности за киберпреступления несовершеннолетних?
25. Что такое «значимый объект критической информационной инфраструктуры» и каков порядок ведения их реестра?
26. Какие кибер-риски связаны с использованием ИИ и как они могут быть урегулированы законодательно?
27. Каков порядок хранения и обработки биометрических данных в Единой биометрической системе (ЕБС)?
28. Роль законодательства об электронной подписи в обеспечении кибербезопасности.
29. Какие организационно-правовые меры защиты информации предусмотрены законодательством РФ?
30. Какие нормы ФЗ № 98-ФЗ «О коммерческой тайне» применяются в контексте кибербезопасности?
31. Какие требования предъявляются к защите государственных информационных систем (ГИС)?
32. Как осуществляется лицензирование и сертификация в сфере защиты информации
33. Как квалифицируется мошенничество в сфере компьютерной информации и каковы особенности состава этого преступления.
34. Как осуществляется взаимодействие организаций с НКЦКИ (Национальным координационным центром по компьютерным
35. Какова роль Банка России в системе кибербезопасности в финансовой сфере.
36. Разъясните особенности обеспечения информационной безопасности в кредитных организациях.
37. Опишите вызовы в сфере кибербезопасности для развития приоритетных отраслей экономики.
38. Опишите виды информации с ограниченным доступом: банковская тайна, коммерческая тайна, государственная тайна и т.д.
39. Технологический суверенитет и роль кибербезопасности в его обеспечении.
40. Роль Единой системы идентификации и аутентификации (ЕСИА) в современной архитектуре кибербезопасности.



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

Основная литература:

1. Внуков, Андрей Анатольевич Защита информации : учебник для вузов / А. А. Внуков. 3-е изд., пер. и доп. Электрон. дан. Москва : Юрайт, 2026 161 с (Высшее образование) URL: <https://urait.ru/bcode/584050> (дата обращения: 27.02.2026). Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей <https://urait.ru/bcode/584050> ISBN 978-5-534-07248-8 : 979.00. [БИК ID: RU2fURAIT2f584050]
2. Макаренко, Елена Николаевна Финансовая кибербезопасность : Учебное пособие / Ростовский государственный экономический университет (РИНХ) ; Ростовский государственный экономический университет (РИНХ) 1 Ростов-на-Дону : Ростовский Государственный Экономический Университет (РГЭУ, бывший РИНХ), 2023 265 с. ВО - Специалитет <https://znanium.ru/catalog/document?id=465648> ISBN 978-5-7972-3155-4. [БИК ID: RU\infra-m\znanium\bibl\2213573]
3. Баланов, А. Н. Кибербезопасность [Электронный ресурс] : учебное пособие для вузов / Баланов А. Н. 2-е изд., стер. Санкт-Петербург : Лань, 2025 680 с. Книга из коллекции Лань - Информатика <https://e.lanbook.com/book/457463> ISBN 978-5-507-52709-0. [БИК ID: RU-LAN-BOOK-457463]

Дополнительная литература:

1. Кибербезопасность в условиях электронного банкинга : практическое пособие / А. А. Бердюгин, А. Б. Дудка, С. В. Конявская, В. А. Конявский, И. Г. Назаров ; под ред. П. В. Ревенков Москва : Прометей, 2020 522 с. : ил. Библиогр. в кн Режим доступа: электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация <https://biblioclub.ru/index.php?page=book&id=610688> ISBN 978-5-907244-61-0. [БИК ID: 28]
2. Ларионова, С. Л. Информационная безопасность дистанционного банковского обслуживания [Электронный ресурс] : учебное пособие / Ларионова С. Л. Москва : Прометей, 2022 296 с. Книга из коллекции Прометей - Экономика и менеджмент <https://e.lanbook.com/book/290516> ISBN 978-5-00172-343-1. [БИК ID: RU-LAN-BOOK-290516]
3. Ванина, А. Г. Персональная кибербезопасность: курс лекций [Электронный ресурс] : учебное пособие / Ванина А. Г., Орёл Д. В., Аникиев С. В. Ставрополь : СКФУ, 2022 137 с. Книга из коллекции СКФУ - Информатика <https://e.lanbook.com/book/386636>. [БИК ID: RU-LAN-BOOK-386636]

Нормативные правовые акты:

1. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
2. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"
3. Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне"
4. Постановление Правительства РФ от 08.02.2018 N 127 "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений"
5. Указ Президента РФ от 30.03.2022 N 166 (ред. от 07.04.2025) "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации"
6. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"
7. Приказ ФСБ России от 18.03.2025 N 117 "Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств" (Зарегистрировано в Минюсте России 26.03.2025 N 81647)
8. Приказ ФСТЭК России от 11.04.2025 N 117 "Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений"
9. "ПНСТ 1009-2025. Предварительный национальный стандарт Российской Федерации. Критическая информационная инфраструктура. Программное обеспечение для доверенных программно-аппаратных комплексов. Общие положения" (утв. и введен в действие Приказом Росстандарта от 24.06.2025 N 20-пнст)

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/> (<http://library.fa.ru/files/elibfa.pdf>)
2. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
3. www.cbr.ru - Официальный сайт Банка России



4. Официальный сайт Росфинмониторинга <https://fedsfm.ru/>
5. • Справочная правовая система «Консультант Плюс» <https://www.consultant.ru/>
6. 4. Официальный сайт Федеральной службы государственной статистики. URL: <http://www.gks.ru> (Росстат)
7. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации <https://digital.gov.ru/ru/>
8. Министерство внутренних дел Российской Федерации <http://www.mvd.ru>



10. Методические указания для обучающихся по освоению дисциплины

Рекомендации по подготовке к практическим (семинарским) занятиям

Подготовка к практическому, семинарскому занятию включает несколько этапов, в том числе организационный, когда обучающийся планирует свою самостоятельную работу, включающую уяснение задания на самостоятельную работу; подбор рекомендованной литературы; составление плана работы, в котором определяются основные пункты предстоящей подготовки и пр. На следующем этапе обучающиеся закрепляют и углубляют полученные теоретические знания, учатся применять их на практике.

Данный этап включает непосредственную подготовку студента к занятию. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического применения рассматриваемых теоретических вопросов. В процессе этой работы обучающийся должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его.

При необходимости следует обращаться за консультацией к преподавателю. Студенты под руководством преподавателя более глубоко осмысливают теоретические положения по теме занятия, раскрывают и объясняют основные явления и факты, учатся применять на практике полученные теоретические знания, в том числе при помощи решения практико-ориентированных заданий, кейсов, составления документов и пр. В процессе обсуждения и дискуссий вырабатываются умения и навыки использовать приобретенные знания для решения практических задач.

Обучающимся, пропустившим занятия (независимо от причин), рекомендуется не позже, чем в 2-недельный срок явиться на консультацию к преподавателю и отчитаться по теме, изучавшийся на занятии, в ином случае обучающийся утрачивает возможность получить положенные баллы за работу в соответствующем семестре.

Методические указания по решению практических задач

Практическая задача представляет собой проблемное задание, в котором обучающемуся предлагают осмыслить реальную ситуацию, необходимую для решения данной проблемы. Виды практических задач могут включать в себя поиск решения юридического казуса или поисково-аналитическую работу, оценку высказанного мнения. Изучение нормативного акта или составление подборки нормативных актов – также представляют собой практические задачи. Задачи решаются письменно и в большинстве случаев требуют тщательной аргументации.

Методические указания по выполнению контрольной работы

Цель контрольной работы – отразить степень освоения студентами учебного материала по данной дисциплине.

Подготовка контрольной работы способствует развитию аналитических способностей у студентов, а также выработке навыков проведения качественного юридического анализа материала по избранной проблематике. Также написание контрольной работы по заданной тематике, определенной теме создает предпосылки для дальнейших научных исследований, помогает сформировать у студентов более полное восприятие дисциплины. Также это позволяет в дальнейшем использовать материал контрольной работы для участия в конференциях, выступлениях на научных мероприятиях, дискуссиях, круглых столах, расширяет кругозор и мировоззрение студентов.

Требования к контрольной работе:

1. четкость и последовательность изложения материала;
2. наличие обобщений и выводов, сделанных на основе изучения информационных источников по данной теме (в случае необходимости);
3. правильность и в полном объеме решение имеющихся в задании практических задач;
4. использование современных способов поиска, обработки и анализа информации;
5. самостоятельность выполнения.

Объем контрольной работы – не более 7 страниц, кроме выполнения заданий по формам установленного кафедрой образца (таблицы, графики и т.д.) при необходимости



11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем

Комплект лицензионного программного обеспечения:

1. Microsoft Office (Windows)
2. Kaspersky

Современные профессиональные базы данных и информационные справочные системы

1. Информационно-правовая система «Гарант»
2. Информационно-правовая система «Консультант Плюс»
3. Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>

Сертифицированные программные и аппаратные средства защиты информации

1. не предусмотрены

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

1. **Учебная аудитория** для проведения учебных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная оборудованием и техническими средствами обучения: мебель аудиторная (столы, стулья, доска аудиторная), набор демонстрационного оборудования (проектор, экран)
2. **Помещение для самостоятельной работы** обучающихся оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде Университета.
3. **Компьютерный класс** для проведения учебных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенный оборудованием и техническими средствами обучения: мебель аудиторная (столы, стулья, доска аудиторная), персональные компьютеры, набор демонстрационного оборудования (проектор, экран)
4. Библиотека, читальный зал