МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ЭКОНОМИКИ, УПРАВЛЕНИЯ И ПРАВА

ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра предпринимательского права

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

40.04.01 Юриспруденция

Правовое обеспечение цифровой экономики и информационной безопасности

Уровень высшего образования: *магистратура*

Форма обучения: *очная, очно-заочная, заочная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2024

Правовое обеспечение информационной безопасности

Рабочая программа дисциплины

Составитель:

кандидат юридических наук, доцент,
Е.А. Редькина
Т.В. Белова

УТВЕРЖДЕНО
Протокол заседания кафедры предпринимательского права
№ «8» от 21.03.2024 г .

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – формирование у обучающихся компетенций, направленных на реализацию практических навыков в области правового обеспечения информационной безопасности.

Задачи дисциплины:

- выработка умения ориентироваться в действующем законодательстве, регламентирующим информационную безопасность;
- развитие способностей обучающихся толковать и применять нормы информационного законодательства, принимать решения и совершать иные юридические действия в соответствии с законом, анализировать законодательство и практику его применения, ориентироваться в специальной литературе;
- формирование у обучаемых навыков и умений применения законодательных норм, регламентирующих вопросы информационной безопасности.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ПК-2 Способен квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности, реализовывать нормы материального и процессуального права в профессиональной деятельности	ПК 2.1 Имеет представление об основных юридических понятиях и категориях, необходимых для реализации норм права в юридической деятельности	Знать: юридические понятия и категории, необходимые для реализации норм права в сфере информационной безопасности. Уметь: использовать теоретические разработки ученых юристов в области юридических понятий и категорий, необходимых для реализации норм права в сфере информационной безопасности. Владеть: навыками применения юридических понятий и категорий, необходимых для реализации норм права в сфере информационной безопасности.
	ПК 2.2 Применяет нормативные правовые акты в профессиональной деятельности	Знать: виды нормативно-правовых актов в сфере информационной безопасности. Уметь: использовать теоретические разработки ученых юристов в области применения нормативно - правовых актов в сфере информационной безопасности. Уметь: применять норма-

		тивные правовые акты, направленные на реализацию норм об обеспечении информационной безопасности. Владеть: навыками применения нормативных правовых актов в сфере информационной безопасности.
ПК-3 Способен выполнять должностные обязанности по обеспечению законности и правопорядка, выявлению и предупреждению угроз безопасности личности, общества и государства	ПК 3.1 Понимает компетенции уполномоченных органов и должностных лиц, ответственных за обеспечение законности и правопорядка, безопасности личности, общества и государства	Знать: компетенцию уполномоченных органов и их должностных лиц в информационной сфере; Уметь: давать квалифицированные юридические заключения и консультации по вопросам применения законодательства в информационной сфере, составлять юридические документы в данной сфере;
	ПК 3.2 Реализует меры по обеспечению законности и правопорядка с целью устранению опасности для личности, общества и государства	Уметь: применять нормативные правовые акты и реализовывать нормы материального права в сфере информационной безопасности, анализировать практику применения правовых норм в информационной сфере. Владеть: навыками составления юридической документации, способностью совершать действия, направленные на предупреждение правонарушений в информационной сфере.
ПК-4 Способен выявлять, пресекать, раскрывать, расследовать и предупреждать правонарушения и преступления	ПК 4.1 Исследует нормы материального права, подлежащие к применению при квалификации преступлений и правонарушений	Знать: понятие состава правонарушения как основания юридической ответственности в информационной сфере, его элементы и признаки; правила квалификации преступлений и иных правонарушений в зависимости от различных элементов состава с учетом особенностей конструкции правовых норм; Уметь: сопоставлять фактические обстоятельства совершенного деяния с при-

		знаками составов преступлений и иных правонарушений, указанными в законе, и определять правовую норму, необходимую для квалификации деяния; Владеть: навыками осуществления процесса квалификации конкретного правонарушения в информационной сфере.
	ПК 4.2 Применяет способы выявления, пресечения, раскрытия, расследования и предупреждения преступлений и правонарушений	Знать: установленный законом порядок действий, необходимых для выявления, пресечения, раскрытия и расследования преступлений и иных правонарушений; содержание нормативных правовых актов, регулирующих осуществление предупреждения преступлений и иных правонарушений в информационной сфере; Уметь: оценивать конкретное деяние на предмет определения наличия в нем признаков преступления или иного правонарушения для осуществления процессов его выявления, пресечения, раскрытия и расследования; выявлять причины и условия, способствующие совершению преступлений и иных правонарушений; Владеть: навыками юридической оценки преступлений и иных правонарушений на основе норм права и использования правил квалификации для выявления, пресечения и расследования конкретного деяния, а также для разработки мер их предупреждения;
ПК-5 Способен защищать права и законные интересы субъектов права	ПК 5.1 Понимает механизм защиты прав и законных интересов субъектов права	Знать: теоретические основы механизма защиты прав и законных интересов субъектов права; нормативные акты, судебную практику, устанавливающие защиту в

		судебном и внесудебном порядке. Уметь: использовать теоретические основы, подходы и концепции, нормативные правовые акты, судебную практику для механизма защиты прав и законных интересов субъектов права в сфере информационной безопасности. Владеть: навыками использования механизма защиты прав и законных интересов субъектов права в сфере информационной безопасности.
	ПК 5.2 Применяет различные способы защиты прав и законных интересов субъектов права	Знать: теоретические основы способов защиты прав и законных интересов субъектов права; нормативные акты, судебную практику, устанавливающие способы защиты участников отношений в сфере информационной безопасности; Уметь: использовать теоретические основы, подходы и концепции, нормативные акты, судебную практику для защиты прав и законных интересов участников отношений в сфере информационной безопасности; применять различные способы защиты прав и законных интересов субъектов права в данной сфере. Владеть: навыками использования различных способов защиты прав и законных интересов субъектов права в сфере информационной безопасности.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Правовое обеспечение информационной безопасности» относится к части, формируемой участниками образовательных отношений блока 1 дисциплин учебного плана по направлению подготовки 40.04.01 «Юриспруденция».

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: «Гражданско-правовая защита субъектов

цифровой экономики», «Правовое регулирование защиты персональных данных в цифровой среде», «Правовой режим оборота цифровых данных»

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин «Правовое регулирование в области закупок товаров и услуг для государственных и муниципальных нужд и проведения электронных торгов», «Правовое исследование в сфере правового обеспечения цифровой экономики и информационной безопасности» и прохождения практик: ознакомительная, научно-исследовательская работа.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 академических часов.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
2	Лекции	6
2	Семинары	24
	Всего:	30

Объем дисциплины в форме самостоятельной работы обучающихся составляет 78 академических часов.

Структура дисциплины для очно-заочной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
2	Лекции	4
2	Семинары	20
	Всего:	24

Объем дисциплины в форме самостоятельной работы обучающихся составляет 84 академических часа.

Структура дисциплины для заочной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Курс	Тип учебных занятий	Количество часов
1	Лекции	4
2	Семинары	8
	Всего:	12

Объем дисциплины в форме самостоятельной работы обучающихся составляет 96 академических часов.

3. Содержание дисциплины

№	Наименование раздела (темы) дисциплины	Содержание
1.	Правовое обеспечение информационной безопасности: понятие, законодательное регулирование, система уполномоченных органов.	Понятие информации. Специфические особенности и юридические свойства информации. Понятие информационной безопасности. Виды угроз информационной безопасности и методы ее обеспечения. Основные положения государственной политики обеспечения информационной безопасности. Законодательное регулирование вопросов обеспечения информационной безопасности. Право граждан на информацию, его конституционные гарантии и механизм реализации. Доктрина информационной безопасности РФ. Иные нормативные правовые акты. Система и полномочия органов обеспечения информационной безопасности.
2.	Правовое обеспечение защиты отдельных видов информации	Понятие и виды защищаемой информации. Государственная тайна как особый вид защищаемой информации. Правовой режим защиты государственной тайны (понятие государственной тайны, допуск граждан к государственной тайне, степень секретности сведений). Правовой режим защиты информации ограниченного доступа (защита конфиденциальной информации, коммерческой тайны, государственный и муниципальных информационных систем, персональных данных).
3.	Ответственность за нарушение законодательства об информационной безопасности	Понятие юридической ответственности за нарушение законодательства об информационной безопасности. Дисциплинарная ответственность за нарушение законодательства об информационной безопасности. Материальная ответственность за нарушение законодательства об информационной безопасности. Гражданско-правовая ответственность за нарушение законодательства об информационной безопасности. Административная ответственность за нарушение законодательства об информационной безопасности. Уголовная ответственность за нарушение законодательства об информационной безопасности.

4. Образовательные технологии

Для проведения учебных занятий по дисциплине используются различные образовательные технологии. Для организации учебного процесса может быть использовано электронное обучение и (или) дистанционные образовательные технологии.

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		60 баллов
участие в обсуждении вопросов темы	5 баллов	20 баллов
доклады по проблемным вопросам	10 баллов	20 баллов
выполнение практического задания	10 баллов	20 баллов
Промежуточная аттестация (зачет с оценкой)		40 баллов
Итого за семестр *(дисциплину)* *зачет с оценкой*		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессио-

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		нальной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Оценочные материалы для текущего контроля успеваемости по дисциплине

Вопросы для подготовки к участию в обсуждении вопросов темы (ПК-2, ПК-3, ПК-4, ПК-5)

№ п/п	*Наименование разделов*	*Контрольные вопросы*
1.	Правовое обеспечение информационной безопасности: понятие, законодательное регулирование, система уполномоченных органов.	Специфические особенности и юридические свойства информации. Понятие информационной безопасности. Виды угроз информационной безопасности и методы ее обеспечения. Основные положения государственной политики обеспечения информационной безопасности. Законодательное регулирование вопросов обеспечения информационной безопасности. Право граждан на информацию, его конституционные гарантии и механизм реализации. Система и полномочия органов обеспечения информационной безопасности.
2.	Правовое обеспечение защиты отдельных видов информации	Государственная тайна как особый вид защищаемой информации Защита коммерческой тайны Защита государственных и муниципальных информационных систем. Защита персональных данных.
3.	Ответственность за нарушение законодательства об информационной безопасности	Дисциплинарная ответственность за нарушение законодательства об информационной безопасности. Материальная ответственность за нарушение законодательства об информационной безопасности. Гражданско-правовая ответственность за нарушение законодательства об информационной безопасности. Административная ответственность за нарушение законодательства об информационной безопасности. Уголовная ответственность за нарушение законодательства об

		информационной безопасности.

Примерные практические задания (ПК-2, ПК-3, ПК-4, ПК-5)

1. Осуществление сравнительного анализа отдельных положений Доктрины информационной безопасности Российской Федерации 2000 года и Доктрины информационной безопасности Российской Федерации 2016 года.

Параметр	**Доктрина информационной безопасности (2000)**	**Доктрина информационной безопасности (2016)**
Понятие информационной безопасности		
Национальные интересы РФ в информационной сфере		
Угрозы информационной безопасности РФ		
Методы обеспечения информационной безопасности		
Государственная политика в обеспечения информационной безопасности (2000) / Стратегическая цель и основные направления обеспечения информационной безопасности (2016)		
Организационные основы обеспечения информационной безопасности		

2. Исследуйте нормы Кодекса РФ об административных правонарушениях и Уголовного кодекса РФ и выделите статьи, устанавливающие ответственность за нарушение законодательства об информационной безопасности. Проанализируйте и классифицируйте данные нормы.

Тематика докладов по проблемным вопросам (ПК-2, ПК-3, ПК-4, ПК-5)

№ п/п	*Наименование разделов*	*Содержание*
1.	Правовое обеспечение информационной безопасности: понятие, законодательное регулирование, система уполномоченных органов.	• Информация как объект правового регулирования • Основные направления государственной политики обеспечения информационной безопасности. • Полномочия органов обеспечения информационной безопасности. • Проблемы правового обеспечения информационной безопасности в сети «Интернет». • Роль судебных актов в правовом обеспечении информационной безопасности.
2.	Правовое обеспечение защиты отдельных видов ин-	• Проблемы защиты конфиденциальной информации

	формации	• Правовое регулирование защиты коммерческой тайны • Правовые проблемы защиты государственных и муниципальных информационных систем. • Проблемы защиты персональных данных

Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

Теоретические вопросы: (ПК-2, ПК-3, ПК-4, ПК-5)

1. Административная ответственность за нарушение законодательства об информационной безопасности.
2. Государственная тайна как особый вид защищаемой информации.
3. Гражданско-правовая ответственность за нарушение законодательства об информационной безопасности.
4. Дисциплинарная ответственность за нарушение законодательства об информационной безопасности.
5. Доктрина информационной безопасности РФ.
6. Законодательное регулирование вопросов обеспечения информационной безопасности.
7. Защита персональных данных.
8. Материальная ответственность за нарушение законодательства об информационной безопасности.
9. Основные положения государственной политики обеспечения информационной безопасности.
10. Понятие и виды защищаемой информации.
11. Понятие и виды юридической ответственности за нарушение законодательства об информационной безопасности.
12. Понятие информации. Специфические особенности и юридические свойства информации.
13. Понятие информационной безопасности. Виды угроз информационной безопасности и методы ее обеспечения.
14. Право граждан на информацию, его конституционные гарантии и механизм реализации.
15. Правовой режим защиты государственной тайны (понятие государственной тайны, допуск граждан к государственной тайне, степень секретности сведений).
16. Правовой режим защиты информации ограниченного доступа: защита государственных и муниципальных информационных систем
17. Правовой режим защиты информации ограниченного доступа: защита конфиденциальной информации
18. Правовой режим защиты информации ограниченного доступа: защита коммерческой тайны
19. Система и полномочия органов обеспечения информационной безопасности.
20. Уголовная ответственность за нарушение законодательства об информационной безопасности.

Примеры ситуационных задач (ПК-2, ПК-3, ПК-4, ПК-5)

1. А. обратился в суд с иском к ответчику – юридическому лицу о прекращении обработки персональных данных и взыскании компенсации морального вреда. А. указал, что что 1 сентября 2019 г. между сторонами был заключен договор об оказании услуг. При за-

ключении договора А. выразил согласие на обработку его персональных данных. 10 сентября 2021 года договор расторгнут. При расторжении договора А. отозвал согласие на обработку персональных данных и заявил требование об удалении всей имеющейся личной информации. В дальнейшем ответчиком в адрес А. было направлено несколько смс-сообщений рекламного характера с предложением услуг. А. полагает данные действия ответчика незаконными и нарушающими требования Федерального закона от 27.07.2006 г. N 152-ФЗ «О персональных данных». На основании изложенного А. просил обязать ответчика прекратить обработку персональных данных истца. Подлежат ли требования А. удовлетворению?

2. Интернет-магазин осуществлял продажу товаров, не имеющих возрастного ограничения. При этом, при заполнении формы заказа было необходимо указать Ф.И.О., дату рождения, пол и местожительство покупателя, а также номер его телефона. Также на сайте отсутствовал документ, содержащих политику конфиденциальности. Будет ли в данной ситуации нарушение законодательства о персональных данных?

3. Сотрудник Банка получил доступ к базе данных на основании трудового договора в ходе выполнения им трудовых обязанностей. Сотрудник выгрузил базы данных клиентов Банка (скопировал ее на съемный носитель) и разместил предложение о продаже данной базы в сети «Интернет». Нарушено ли законодательство о персональных данных?

4. Гражданка И. с 2006 года являлась штатным сотрудником закрытого НИИ с допуском к государственной тайне. В 2015 году она вышла на пенсию по возрасту. В 2021 году И. обратилась с заявлением на оформление заграничного паспорта и разрешением на выезд из Российской Федерации на постоянное место жительства к своему сыну в Италию. В выдаче заграничного паспорта и разрешения на выезд было отказано, т.к. сведения, к которым И. была допущена в 2006 году, сохраняют секретность. И. не согласилась с отказом и обратилась за юридической помощью. Правомерно ли гражданке И. отказали в выдаче загранпаспорта и разрешения на выезд из России на постоянное место жительства к своему сыну?

5. На заводе с химическим опасным производством произошла авария, погиб человек. Один из работников выложил видео аварии на своей странице в социальной сети «Вконтакте». Служба безопасности предприятия вычислила этого человека. Его увольняют за разглашение коммерческой тайны. Является ли данный факт коммерческой тайной? Правомерно ли увольнение?

6. В ООО « Фотон» введён режим коммерческой тайны. Следователь на основании судебного решения хотел произвести выемку документов, имеющих значение для уголовного дела, в ООО. Следователю было отказано в проведении выемки, ООО ссылалось на режим коммерческой тайны. Разрешите ситуацию.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники:

Основные:

1. Конституция Российской Федерации. Принята всенародным голосованием 12.12.1993 г. // СПС «Консультант Плюс».
2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 г. № 195-ФЗ// СПС «Консультант Плюс».
3. Трудовой кодекс Российской Федерации от 30.12.2001 г. № 197-ФЗ // СПС «Консультант Плюс».
4. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ // СПС «Консультант Плюс».
5. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 г. № 51-ФЗ // СПС «Консультант Плюс».
6. Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «Консультант Плюс».
7. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» // СПС «Консультант Плюс».
8. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СПС «Консультант Плюс».
9. Закон РФ от 21.07.1993 г. № 5485-1 «О государственной тайне» // СПС «Консультант Плюс».
10. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «Консультант Плюс».

Дополнительные:

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // СПС «Консультант Плюс».
2. Указ Президента РФ от 30.11.1995 № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне» // СПС «Консультант Плюс».
3. Постановление Правительства РФ от 06.02.2010 № 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне».

Литература:

Основная:

- *Бачило, И. Л.* Информационное право : учебник для вузов / И. Л. Бачило. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 419 с. — (Высшее образование). — ISBN 978-5-534-00608-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/510460
- Информационное право : учебник для вузов / Н. Н. Ковалева [и др.] ; под редакцией Н. Н. Ковалевой. — Москва : Издательство Юрайт, 2023. — 353 с. — (Высшее образование). — ISBN 978-5-534-13786-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519753
- Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2023. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511239

Дополнительная:

- Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002
- Информационное право : учебник для вузов / М. А. Федотов [и др.] ; под редакцией М. А. Федотова. — Москва : Издательство Юрайт, 2022. — 497 с. — (Высшее образование). — ISBN 978-5-534-10593-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489946
- Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 415 с. — (Высшее образование). — ISBN 978-5-534-14327-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/510644

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Официальный интернет-портал правовой информации [Электронный ресурс]. - Режим доступа: http://www.pravo.gov.ru
2. Сайт Верховного Суда Российской Федерации // Режим доступа: http://www.vsrf.ru/
3. Национальная электронная библиотека (НЭБ) // Режим доступа: www.rusneb.ru
4. ELibrary.ru Научная электронная библиотека // Режим доступа: www.elibrary.ru

6.3. Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для проведения аудиторных занятий по дисциплине необходима аудитория, оснащенная ПК и мультимедиа-проектором.

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

- для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
  - устройством для сканирования и чтения с камерой SARA CE;
  - дисплеем Брайля PAC Mate 20;
  - принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
  - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
  - акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
  - передвижными, регулируемыми эргономическими партами СИ-1;
  - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

№ п/п	Наименование разделов (тем)	Вопросы для обсуждения
1.	Правовое обеспечение информационной безопасности: понятие, законодательное регулирование, система уполномоченных органов.	• Специфические особенности и юридические свойства информации. • Понятие информационной безопасности. • Виды угроз информационной безопасности и методы ее обеспечения. • Основные положения государственной политики обеспечения информационной безопасности. • Законодательное регулирование вопросов обеспечения информационной безопасности. • Право граждан на информацию, его конституционные гарантии и механизм реализации. • Система и полномочия органов обеспечения информационной безопасности.
2.	Правовое обеспечение защиты отдельных видов информации	• Государственная тайна как особый вид защищаемой информации • Защита коммерческой тайны • Защита государственных и муниципальных информационных систем. • Защита персональных данных.
3.	Ответственность за нарушение законодательства об информационной безопасности	• Дисциплинарная ответственность за нарушение законодательства об информационной безопасности. • Материальная ответственность за нарушение законодательства об информационной безопасности. • Гражданско-правовая ответственность за нарушение законодательства об информационной безопасности. • Административная ответственность за нарушение законодательства об информационной безопасности. • Уголовная ответственность за нарушение законодательства об информационной безопасности.

Приложение 1. Аннотация дисциплины

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Юридическая ответственность в информационной сфере» реализуется на юридическом факультете кафедрой предпринимательского права.

Цель дисциплины – формирование у обучающихся компетенций, направленных на реализацию практических навыков в области правового обеспечения информационной безопасности.

Задачи дисциплины:

- выработка умения ориентироваться в действующем законодательстве, регламентирующим информационную безопасность;
- развитие способностей обучающихся толковать и применять нормы информационного законодательства, принимать решения и совершать иные юридические действия в соответствии с законом, анализировать законодательство и практику его применения, ориентироваться в специальной литературе;
- формирование у обучаемых навыков и умений применения законодательных норм, регламентирующих вопросы информационной безопасности.

В результате освоения дисциплины обучающийся должен:

Знать: юридические понятия и категории, необходимые для реализации норм права в сфере информационной безопасности; виды нормативно-правовых актов в сфере информационной безопасности; компетенцию уполномоченных органов и их должностных лиц в информационной сфере; понятие состава правонарушения как основания юридической ответственности в информационной сфере, его элементы и признаки; правила квалификации преступлений и иных правонарушений в зависимости от различных элементов состава с учетом особенностей конструкции правовых норм; установленный законом порядок действий, необходимых для выявления, пресечения, раскрытия и расследования преступлений и иных правонарушений; содержание нормативных правовых актов, регулирующих осуществление предупреждения преступлений и иных правонарушений в информационной сфере; теоретические основы механизма защиты прав и законных интересов субъектов права; нормативные акты, судебную практику, устанавливающие защиту в судебном и внесудебном порядке; теоретические основы способов защиты прав и законных интересов субъектов права; нормативные акты, судебную практику, устанавливающие способы защиты участников отношений в сфере информационной безопасности;

Уметь: использовать теоретические разработки ученых юристов в области юридических понятий и категорий, необходимых для реализации норм права в сфере информационной безопасности; использовать теоретические разработки ученых юристов в области применения нормативно - правовых актов в сфере информационной безопасности; применять нормативные правовые акты, направленные на реализацию норм об обеспечении информационной безопасности; давать квалифицированные юридические заключения и консультации по вопросам применения законодательства в информационной сфере, составлять юридические документы в данной сфере; применять нормативные правовые акты и реализовывать нормы материального права в сфере информационной безопасности, анализировать практику применения правовых норм в информационной сфере; сопоставлять фактические обстоятельства совершенного деяния с признаками составов преступлений и иных правонарушений, указанными в законе, и определять правовую норму, необходимую для квалификации деяния; оценивать конкретное деяние на предмет определения наличия в нем признаков преступления или иного правонарушения для осуществления процессов его выявления, пресечения, раскрытия и расследования; выявлять причины и условия, способствующие совершению преступлений и иных правонарушений; использовать теоретические основы, подходы и концепции, нормативные правовые акты, судебную практику для механизма защиты прав и законных интересов субъектов права в сфере ин-

формационной безопасности; использовать теоретические основы, подходы и концепции, нормативные акты, судебную практику для защиты прав и законных интересов участников отношений в сфере информационной безопасности; применять различные способы защиты прав и законных интересов субъектов права в данной сфере.

Владеть: навыками применения юридических понятий и категорий, необходимых для реализации норм права в сфере информационной безопасности; навыками применения нормативных правовых актов в сфере информационной безопасности; навыками составления юридической документации, способностью совершать действия, направленные на предупреждение правонарушений в информационной сфере; навыками осуществления процесса квалификации конкретного правонарушения в информационной сфере; навыками юридической оценки преступлений и иных правонарушений на основе норм права и использования правил квалификации для выявления, пресечения и расследования конкретного деяния, а также для разработки мер их предупреждения; навыками использования механизма защиты прав и законных интересов субъектов права в сфере информационной безопасности; навыками использования различных способов защиты прав и законных интересов субъектов права в сфере информационной безопасности.

По дисциплине предусмотрена промежуточная аттестация в форме зачета с оценкой.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы.