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

ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

46.04.02 Документоведение и архивоведение
Код и наименование направления подготовки/специальности

Теория и практика работы с электронными документами в управлении и архивах
Наименование направленности (профиля)/ специализации

Уровень высшего образования: *магистратура*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2022

Правовые основы информационной безопасности
Рабочая программа дисциплины

Составитель(и):
к. ю. н., доцент, доцент кафедры предпринимательского права юридического факультета Белова Т.В

УТВЕРЖДЕНО
Протокол заседания кафедры
№_5___ от__30.03. 2022_____

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины: формирование у обучающихся системных представлений о современном состоянии законодательства, обеспечивающего информационную безопасность.
Задачи:
– всестороннее понимание студентами природы и сущности основных понятий, правового регулирования информационной безопасности;
– формирование умения применять нормы законодательства, закрепляющего информационную безопасность к конкретным жизненным ситуациям, анализировать и давать им правовое толкование;
– формирование разносторонней творческой личности, профессионального правосознания будущих специалистов.

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

Коды компетенции	**ПК**	**Перечень планируемых результатов обучения по дисциплине**
УК -1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 знать принципы стратегического развития и системного подхода в условиях цифровой экономики	***Знать:*** *нормативные-правовые акты, закрепляющие информационную безопасность; примерные проблемные ситуации, для разрешения которых требуется знание правовых основ информационной безопасности.* ***Уметь:*** *использовать нормативные-правовые акты, закрепляющие правовые основы информационной безопасности; осуществлять критический анализ проблемных ситуаций с применением правовых основы информационной безопасности.*
		Уметь: *применять нормативные-правовые акты, закрепляющие правовые основы информационной безопасности с целью осуществления критического анализа проблемных ситуаций с применением правовых механизмов, обеспечивающих информационную безопасность.* ***Владеть:*** *навыками применения нормативных-правовых актов, закрепляющих информационную безопасность с целью осуществления критического анализа проблемных ситуаций с применением механизмов, обеспечивающих информационную безопасность.*

ПК- 4 Способен организовывать разработку и внедрение корпоративной системы электронного документооборота	ПК-4.1 использует в работе принципы организации электронного документооборота, в то м числе на межведомственном уровне	***Знать:*** *правовые принципы организации электронного документооборота с соблюдением правовых основ информационной безопасности, в том числе на межведомственном уровне* ***Уметь:*** *использовать правовые основы информационной безопасности при организации электронного документооборота, в том числе на межведомственном уровне*
		Уметь: *применять правовые основы информационной безопасности при организации электронного документооборота, в том числе на межведомственном уровне* ***Владеть:*** *навыками использования правовых основ информационной безопасности при организации электронного документооборота, в том числе на межведомственном уровне*
	ПК-4.2 организует внедрение системы электронного документооборота	***Знать:*** *правовые основы информационной безопасности организации внедрения системы электронного документооборота* ***Уметь:*** *использовать нормативные-правовые акты в области информационной безопасности при организации электронного документооборота*
		Уметь: *применять правовые основы информационной безопасности при организации внедрения электронного документооборота* ***Владеть:*** *навыками использования правовых основы информационной безопасности при организации внедрения электронного документооборота.*

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Правовые основы информационной безопасности» относится к части, формируемой участниками образовательных отношений (Дисциплины (модули) блока дисциплин по выбору учебного плана программы магистратуры «Теория и практика работы с электронными документами в управлении и архивах» по направлению подготовки 46.04.02. Документоведение и архивоведение.

Для освоения дисциплины необходимы компетенции, сформированные в ходе изучения дисциплин: «Архивы электронных документов», «Цифровое государственное управление», «Управление документами в организации» и других дисциплин учебного плана.

В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин: «Методология электронного документооборота», «Управление кадровой документацией в цифровой экономике», а также успешного прохождения научно-исследовательской практики и выполнения научно-исследовательской работы.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 2 з.е., 72 ч. 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
	Лекции	**16**
	Семинары/лабораторные работы	**24**
	Всего:	**40**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _32_ академических часа(ов).

3. Содержание дисциплины

Тема 1. Правовые режимы информационных ресурсов

Понятие правового режима информационных ресурсов. Понятие и виды охраноспособной информации. Режимы защиты информации. Государственная тайна. Служебная и профессиональная тайна. Тайна частной жизни. Коммерческая тайна.

Тема 2. Система органов государственной власти регулирующих информационную сферу.

Государственное управление в информационной сфере. Система и полномочия органов государственной власти, обеспечивающих охрану государственной тайны. Компетенция органов государственной власти, обеспечивающих правовой режим конфиденциальной информации.

Тема 3. Информационная безопасность.

Понятие и виды информационной безопасности. Задачи, методы, средства обеспечения информационной безопасности. Информационная безопасность личности. Информационная безопасность государства. Информационная безопасность общества. Обеспечение безопасности в глобальном информационном пространстве.

Тема 4. Ответственность в информационной сфере.

Общая характеристика и виды ответственности за нарушения в информационной сфере. Дисциплинарная ответственность в информационной сфере. Административная ответственность в информационной сфере. Уголовная ответственность в информационной сфере. Материальная ответственность в информационной сфере. Особенности ответственности в области массовой информации. Особенности ответственности в сети интернет.

4. Образовательные технологии

№ п/п	**Наименование раздела**	**Виды учебной работы**	**Информационные и образовательные технологии**
1	***2***	***3***	***4***
1	Правовые режимы информационных ресурсов	Лекция № 1	Лекция-визуализация с применением слайд-проектора

		Практическое занятие	Семинар в диалоговом режиме, обсуждение поставленных проблем Решение практических задач Обсуждение докладов Решение тестов
		Самостоятельная работа	Консультирование и проверка домашних заданий посредством электронной почты
2	Система органов государственной власти регулирующих информационную сферу	Лекция № 2	Лекция-визуализация с применением слайд-проектора
		Практическое занятие	Семинар в диалоговом режиме, обсуждение поставленных проблем Решение практических задач Обсуждение докладов Решение тестов
		Самостоятельная работа	Консультирование и проверка домашних заданий посредством электронной почты
3	Информационная безопасность	Лекция № 3	Лекция-визуализация с применением слайд-проектора
		Практическое занятие	Семинар в диалоговом режиме, обсуждение поставленных проблем Решение практических задач Доклад по проблемному вопросу с использованием компьютерной презентации
		Самостоятельная работа	Изучение рекомендованной литературы и Интернет-ресурсов; Подготовка докладов Выполнение письменных заданий.
4	Ответственность в информационной сфере	Лекция № 4	Лекция-визуализация с применением слайд-проектора
		Практическое занятие	Семинар в диалоговом режиме, обсуждение поставленных проблем Тестирование по темам курса Доклад по проблемному вопросу с использованием компьютерной презентации Решение ситуационных задач Деловая игра Решение тестов
		Самостоятельная работа	Изучение рекомендованной литературы и Интернет-ресурсов; Подготовка докладов Выполнение письменных

			заданий.

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль: - обсуждение вопросов на семинаре - обсуждение практических вопросов / решение задач - доклад - тестирование по теме	 2 балла 5 баллов 20 баллов 5 баллов	 10 баллов 20 баллов 20 баллов 10 баллов
Промежуточная аттестация (итоговая контрольная работа / зачет с оценкой)	40 баллов	40 баллов
Итого за дисциплину		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	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
		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 профессиональной 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	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	удовлетво-рительно/ 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	неудовлет-ворительно/ 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 направленности стандартного уровня

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		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

Примерные тесты

Вариант 1.

Тест №1. Термином «право» обозначается:

а) обоснованная, оправданная свобода или возможность поведения человека в его взаимоотношениях с другими людьми, которая признана и поддерживается обществом;

б) отрасль науки, которая изучает уголовный кодекс;

в) отрасль науки, которая изучает уголовный кодекс;

г) нет верного ответа.

Тест № 2.В зависимости от формы проявления общественного признания этой свободы и способа ее поддержки со стороны общества различают следующие виды права:

а) обычное право, моральное право, корпоративное право;

б) обычное право, моральное право, корпоративное право, естественное право, юридическое право;

в) естественное право, юридическое право;

г) корпоративное право, естественное право.

Тест №3. Юридическое право представляет собой:

а) систему общеобязательных норм, выраженных в только в уставах организаций;

б) свободу, или возможность поведения, основанную на принципах добра, справедливости (заботливое отношение детей к родителям, уважение к женщине);

в) свободу, или возможность поведения, основанную на уставных и иных положениях, которые действуют внутри общественных, негосударственных объединений, организаций, партий (право избирать и быть избранным в руководящие органы, право руководящих органов налагать взыскания);

г) систему общеобязательных норм, выраженных в законах, иных признаваемых государством источниках права и являющихся общеобязательным основанием для определения правомерно-дозволенного, запрещенного и предписанного поведения.

Тест№ 4. Наиболее известными в настоящее время правовыми системами являются:

а) религиозная, базирующаяся на священной для мусульман книге — Коране (мусульманское право характерно, например, для Ирана);
б) романо-германская, основанная на праве законодателя (континентальная Европа);
в) прецедентная, основанная на праве судей (Великобритания и США);
г) верны все варианты.

Тест № 5. Предмет правового обеспечения информационной безопасности представляет собой:

а) совокупность общественных отношений, на которые направлено правовое воздействие в целях недопущения, выявления и пресечения проявлений угроз объектам национальных интересов в информационной сфере, а также минимизации негативных последствий проявления этих угроз;
б) совокупность общественных отношений, на которые направлено правовое воздействие только в целях недопущения проявлений угроз объектам национальных интересов в информационной сфере;
в) нет верного ответа.

Тест№ 6. Правовое обеспечение безопасности информации в форме сведений образуется:

а) совокупностью норм и институтов, регулирующих отношения по поводу только объекта - сведений, обладателем которых является субъект права;
б) совокупностью норм и институтов, регулирующих отношения по поводу следующих объектов: сведения, обладателем которых является субъект права; свобода мысли; субъективная значимость национальных культурных ценностей;
в) совокупностью норм и институтов, регулирующих отношения по поводу только объекта - свобода мысли.

Тест №7. Правовое обеспечение безопасности информации в форме сообщений определяется:

а) совокупностью норм и институтов, регулирующих отношения по поводу следующих объектов: сведения, обладателем которых является субъект права; свобода мысли; субъективная значимость национальных культурных ценностей;
б) совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются сообщения, передаваемые по каналам связи, данные, накапливаемые и обрабатываемые в информационных системах, автоматизированных системах управления, а также документы как входящие, так и не входящие в информационные системы;
в) совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются средства связи, автоматизации обработки информации, информационно-телекоммуникационные системы и средства массовой информации;
г) совокупностью правовых норм и институтов.

Тест №8. Содержание и структура законодательства в области информационной безопасности включает:

а) Конституция Российской Федерации - Нормативно-правовые акты (Указы) Президента Российской Федерации - Подзаконные акты Правительства Российской Федерации - Федеральные законы - Кодексы;
б) Конституция Российской Федерации - Нормативно-правовые акты (Указы) Президента Российской Федерации;

в) Подзаконные акты Правительства Российской Федерации – Федеральные законы - Кодексы;
г) нет верного ответа.

Тест №9. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации состоит из:

а) Федерального закона «Об информации, информационных технологиях и о защите информации» и других федеральных законов, регулирующих отношения в области использования информации;
б) Федерального закона «О персональных данных» и других федеральных законов, регулирующих отношения в области использования информации;
в) Федерального закона «О коммерческой тайне» и других федеральных законов, регулирующих отношения в области использования информации;
г) Федерального закона «О государственной тайне» и других федеральных законов, регулирующих отношения в области использования информации.

Тест №10. Предметом правового регулирования в области информации, информационных технологий и защиты информации являются:

а) отношения, возникающие только при осуществлении права на поиск, получение, передачу, производство и распространение информации;
б) отношения, возникающие только при применении информационных технологий;
в) отношения, возникающие только при обеспечении защиты информации;
г) отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; при применении информационных технологий; при обеспечении защиты информации.

Вопросы для обсуждения

1. Что такое государственная тайна? Персональные данные?
2. Назовите перечень сведений, составляющих государственную тайну?
3. Что такое гриф секретности? Назовите степени секретности сведений, составляющих государственную тайну?
4. Что такое информационная система персональных данных?
5. Назовите категории (группы) информационных систем персональных данных?
6. Базовые источники правового обеспечения информационной безопасности.
7. Информация, относимая к государственной тайне. Способы защиты.
8. Структура законодательства РФ в области защиты информации.
9. Модель угроз безопасности информационных систем персональных данных.
10. Российские регуляторы в области защиты информации.
11. Какой документ занимает главное место в системе законодательства в области авторского права?
12. Перечислите способы защиты авторских и смежных прав?
13. Что является целью Федерального закона "Об электронной цифровой подписи"?
14. Как происходит использование электронной цифровой подписи в сфере государственного управления?
15. Какие сведения относят к коммерческой тайне?

Примерные задачи

Задача. Обстоятельства дела:

Задача 1

Сотрудники частной охранно-детективной фирмы создали собственный архив, в котором собирали наиболее интересную информацию о всех своих клиентах. Данная информация использовалась по мере необходимости в повседневной деятельности фирмы.

Вопрос: *Нарушила ли в этом случае контора законодательство об архивном деле в Российской Федерации*

Темы докладов

1.Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.
2.Организационные структуры системы обеспечения информационной безопасности предприятия (организации).
3.Физическая защита субъекта информационной сферы.
4.Корпоративная нормативная база по защите информации.
5.Принципы политики безопасности.
6.Общие положения по управлению персоналом на предприятиях и в организациях
7.Подбор и расстановка кадров.
8.Мотивация добросовестной деятельности.
9.Организация подготовки кадров в области обеспечения информационной безопасности.
10.Российские регуляторы в области информационной безопасности.
11.Области взаимодействия законодательных актов, приоритет применения и зоны ответственности.
12.Понятие конфиденциальной, деловой и технической информации.
13.Режимы защиты конфиденциальной информации.
14.Режимы защиты деловой и технической информации.
15.Требования регуляторов в сфере защиты персональных данных.
16.Регламент защиты персональных данных на предприятии.
17.Защита информации о частной жизни граждан.
18.Злоупотребления в области защиты персональной и личной информации.
19.Сфера международной охраны и государственной политики различных стран в области авторского права и смежных прав.
20.Виды компьютерных преступлений, закрепленные в Уголовном кодексе Российской Федерации.
21.Состав компьютерных преступлений.
22.Ответственность за компьютерные преступления.
23.Лицензирование частной детективной и охранной деятельности.
24.Регулирование использования специальных технических средств в оперативно-розыскной деятельности.
25.Правовая основа системы лицензирования и сертификации в Российской

Федерации.
26.Лицензирование деятельности по защите информации.
27.Сертификация средств защиты информации.

Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

Вопросы к зачету

1. Информационное общество. Перспективы развития.
2. Объекты информационного права.
3. Связь информационной безопасности с другими отраслями права.
4. Базовые источники правового обеспечения информационной безопасности.
5. Основные положения закона "Об информации, информационных технологиях и защите информации".
6. Международные правовые акты, регламентирующие деятельность в области информационного обмена и защиты информации.
7. Информация, относимая к коммерческой тайне. Способы защиты.
8. Информация, относимая к технической или служебной. Способы защиты.
9. Государственное регулирование использования средств криптографической защиты.
10.Лицензирование деятельности и сертификация средств криптографической защиты.
11.Уголовная ответственность за не исполнение Федеральных Законов.
12.Защита прав и законных интересов субъектов информационной сферы.
13.Процедура обращения в суд за судебной защитой.
14.Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.
15.Организационные структуры системы обеспечения информационной безопасности предприятия (организации).
16.Физическая защита субъекта информационной сферы.
17.Корпоративная нормативная база по защите информации.
18.Принципы политики безопасности.
19.Общие положения по управлению персоналом на предприятиях и в организациях
20.Подбор и расстановка кадров.
21.Мотивация добросовестной деятельности.
22.Организация подготовки кадров в области обеспечения информационной безопасности.
23.Российские регуляторы в области информационной безопасности.
24.Области взаимодействия законодательных актов, приоритет применения и зоны ответственности.
25.Понятие конфиденциальной, деловой и технической информации.
26.Режимы защиты конфиденциальной информации.
27.Режимы защиты деловой и технической информации.
28.Требования регуляторов в сфере защиты персональных данных.
29.Регламент защиты персональных данных на предприятии.
30.Защита информации о частной жизни граждан.
31.Злоупотребления в области защиты персональной и личной информации.

32.Сфера международной охраны и государственной политики различных стран в области авторского права и смежных прав.
33.Виды компьютерных преступлений, закрепленные в Уголовном кодексе Российской Федерации.
34.Состав компьютерных преступлений.
35.Ответственность за компьютерные преступления.
36.Лицензирование частной детективной и охранной деятельности.
37.Регулирование использования специальных технических средств в оперативно-розыскной деятельности.
38.Правовая основа системы лицензирования и сертификации в Российской Федерации.
39.Лицензирование деятельности по защите информации.
40.Сертификация средств защиты информации.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники:

Основные

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149 –ФЗ (ред. от 11.06.2021).
2. Федеральный закон от 29.07.2004 г. №98-ФЗ «О коммерческой тайне» (ред. от 09.03.2021 г.)
3. Закон Российской Федерации от 21.07.1993 г. №5485-1 «О государственной тайне» (ред. от 11.06.2021 г.)

Дополнительные

1. Федеральный закон от 03.04.1995 г. №40-ФЗ «О федеральной службе безопасности» (ред. от 09.11.2020 г.)
2. Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности» (ред. от 09.11.2020).

Литература:

Основная

1. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассоло Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469235
2. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/477968

Дополнительная

1. Иванова, С. А. Актуальные проблемы гражданского права : учебное пособие / С.А. Иванова, Д.А. Пашенцев, Л.В. Санникова. — Москва : ИНФРА-М, 2020. — 190 с. - (Высшее образование: Магистратура). — DOI 10.12737/972075. - ISBN 978-5-16-106732-1. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/972075

2. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467370

3. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/476294

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Информационно-правовое обеспечение «Гарант» // Режим доступа: www.garant.ru
Информационно-правовая система «Консультант+»//Режим доступа: www.consultant.ru
Официальные сайты:
Сайт Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации// Режим доступа:
https://digital.gov.ru/ru/
Сайт федеральных арбитражных судов Российской Федерации // Режим доступа:
http://www.arbitr.ru/
Сайт Верховного суда Российской Федерации // Режим доступа: http://www.vsrf.ru/
Сайт Министерства юстиции Российской Федерации // Режим доступа: http://minjust.ru
Ресурсный центр медиации // Режим доступа: http://mediators.ru
Центр медиации и права // Режим доступа: http://www.mediacia.com/
Третейский суд при Торгово-промышленной палате Российской Федерации // Режим доступа:
http://ts.tpprf.ru и др.

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 обеспечения дисциплины используется материально-техническая база образовательного учреждения: учебные аудитории, оснащённые компьютером и проектором для демонстрации учебных материалов.

Состав программного обеспечения:

1. Windows
2. Microsoft Office

3. Kaspersky Endpoint Security

Профессиональные полнотекстовые базы данных:
1. Национальная электронная библиотека (НЭБ) www.rusneb.ru
2. ELibrary.ru Научная электронная библиотека www.elibrary.ru
3. Электронная библиотека Grebennikon.ru www.grebennikon.ru
4. Cambridge University Press
5. ProQuest Dissertation & Theses Global
6. SAGE Journals
7. Taylor and Francis
8. JSTOR

Информационные справочные системы:
3. Консультант Плюс
4. Гарант

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 семинарских/ практических/ лабораторных занятий

Тема 1. ПРАВОВЫЕ РЕЖИМЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Вопросы

1. Понятие правового режима.
2. Понятие и виды информационных ресурсов.
3. Правовой режим государственной тайны
4. Правовой режим коммерческой тайны.
5. Правовой режим конфиденциальной информации.

Тема 2. СИСТЕМА ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ РЕГУЛИРУЮЩИХ ИНФОРМАЦИОННУЮ СФЕРУ

Вопросы

1. Государственное управление в информационной сфере.
2. Система и полномочия органов государственной власти, обеспечивающих охрану государственной тайны.
3. Компетенция органов государственной власти, обеспечивающих правовой режим конфиденциальной информации.

Тема 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Вопросы

1. Понятие и виды информационной безопасности.
2. Задачи, методы, средства обеспечения информационной безопасности. Информационная безопасность личности.
3. Информационная безопасность государства.
4. Информационная безопасность общества.
5. Обеспечение безопасности в глобальном информационном пространстве.

Тема 4. ОТВЕТСТВЕННОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ

Вопросы

1. Общая характеристика и виды ответственности за нарушения в информационной сфере.
2. Дисциплинарная ответственность в информационной сфере.

3. Административная ответственность в информационной сфере.
4.Уголовная ответственность в информационной сфере.
5.Материальная ответственность в информационной сфере.
6.Особенности ответственности в области массовой информации.
7.Особенности ответственности в сети интернет.

9.2 Методические рекомендации по подготовке письменных работ

Методические рекомендации и темы для подготовки докладов-презентаций

Презентация представляется в распечатанном виде на кафедру предпринимательского права.

Текст набирается в программе PowerPoint и состоит **СТРОГО** из 5 слайдов (не допускается увеличение или сокращение количества слайдов).

Титул (см. приложение), а также «Список использованной литературы», на основании которого выполнена работа, в общий объем слайдов не входит.

Поскольку презентация должна быть представлена в распечатанном виде, то нецелесообразно использовать «заливку» цветом поля страниц;

Презентация должна быть использована студентом на семинарском занятии как сопровождение своего выступления, поэтому рекомендуется соотнести тему презентации и выступления с темой и вопросом семинарского занятия.

Рекомендуется ознакомиться со смежными темами выступающих (см. список), чтобы правильно определить границы своего предмета, не повторять и не пересекаться с первыми.

Требования к содержанию слайдов:

1) слайды должны раскрывать содержание вопроса темы, т.е. отражать самое главное в презентуемом вопросе;
2) быть непосредственно связанными с проблемами юридической науки;
3) характеризоваться наглядностью, т.е. демонстрировать структуру элементов, свойств, характеристик и проч. знания о том или ином объекте, его связей со смежными научными положениями;
4) материал не должен копировать текст (т.е. не быть конспектом), а представлять собой схему (или таблицу) с минимальным количеством слов, позволяющую визуально быстро «схватить» суть вопроса;
5) слайды не должны быть перегружены информацией, но при этом должны содержать достаточный ее объем для раскрытия темы.

На семинарском занятии после выступления студента с презентацией группа задает вопросы по теме, на которые выступающему необходимо отвечать кратко, грамотно и доходчиво.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Правовые основы информационной безопасности» реализуется на факультете архивоведения и документоведения кафедрой предпринимательского права.

Цель дисциплины: формирование у обучающихся системных представлений о современном состоянии законодательства, обеспечивающего информационную безопасность.

Задачи:

– всестороннее понимание студентами природы и сущности основных понятий, правового регулирования информационной безопасности;

– формирование умения применять нормы законодательства, закрепляющего информационную безопасность к конкретным жизненным ситуациям, анализировать и давать им правовое толкование;

– формирование разносторонней творческой личности, профессионального правосознания будущих специалистов.

Дисциплина направлена на формирование следующих компетенций:

УК-1 способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

УК-1.1 знать принципы стратегического развития и системного подхода в условиях цифровой экономики;

ПК-4 способен организовывать разработку и внедрение корпоративной системы электронного документооборота

ПК-4.1 использует в работе принципы организации электронного документооборота, в том числе на межведомственном уровне

ПК-4.2 организует внедрение системы электронного документооборота

В результате освоения дисциплины обучающийся должен:

Знать: нормативные-правовые акты, закрепляющие информационную безопасность; примерные проблемные ситуации, для разрешения которых требуется знание правовых основ информационной безопасности. Правовые принципы организации электронного документооборота с соблюдением правовых основ информационной безопасности, в том числе на межведомственном уровне. Правовые основы информационной безопасности организации внедрения системы электронного документооборота

Уметь: использовать нормативные-правовые акты, закрепляющие правовые основы информационной безопасности; осуществлять критический анализ проблемных ситуаций с применением правовых основы информационной безопасности. Применять нормативные-правовые акты, закрепляющие правовые основы информационной безопасности с целью осуществления критического анализа проблемных ситуаций с применением правовых механизмов, обеспечивающих информационную безопасность. Использовать правовые основы информационной безопасности при организации электронного документооборота, в том числе на межведомственном уровне. Применять правовые основы информационной безопасности при организации электронного документооборота, в том числе на межведомственном уровне. Использовать нормативные-правовые акты в области информационной безопасности при организации электронного документооборота. Применять правовые основы информационной безопасности при организации внедрения электронного документооборота.

Владеть: навыками применения нормативных-правовых актов, закрепляющих информационную безопасность с целью осуществления критического анализа проблемных ситуаций с применением механизмов, обеспечивающих информационную безопасность. Навыками использования правовых основ информационной безопасности при организации электронного документооборота, в том числе на межведомственном уровне. Навыками

использования правовых основы информационной безопасности при организации внедрения электронного документооборота.

По дисциплине *(модулю)* предусмотрена промежуточная аттестация в форме *зачета.*

Общая трудоемкость освоения дисциплины составляет __2_зачетные единицы.