МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное
учреждение высшего образования
«УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ В.Ф. ЯКОВЛЕВА»

«Утверждено»
Решением Ученого Совета УрГЮУ
имени В.Ф. Яковлева
от «26» июня 2023 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Правовое обеспечение информационной безопасности»
Основная профессиональная образовательная программа высшего образования – программа специалитета по специальности
40.05.04 Судебная и прокурорская деятельность
Специализация №2 "Прокурорская деятельность"
(Профиль: Прокурорский работник)

1. Цели и задачи дисциплины:

В рамках учебной дисциплины осуществляется подготовка студентов к следующим видам профессиональной деятельности:

1. правоприменительная;
2. правоохранительная;

Целью освоения учебной дисциплины является:

формирование у студентов современных углубленных знаний, практических умений и навыков в области обеспечения информационной безопасности, в т.ч. государственной тайны, служебной тайны, коммерческой тайны, профессиональных тайн, персональных данных.

В ходе освоения дисциплины студент готовится к выполнению следующих профессиональных задач:

правоприменительная деятельность:

обоснование и принятие правовых решений, а также совершение действий, связанных с реализацией правовых норм, в соответствии с профилем профессиональной деятельности;

составление юридических документов;

правовое обеспечение служебной **деятельности;**

- обеспечение международного сотрудничества в правовой сфере;

правоохранительная деятельность:

- обеспечение законности, правопорядка, безопасности личности, общества и государства;
- предупреждение, пресечение, выявление, профилактика преступлений и правонарушений, своевременное реагирование и принятие мер к восстановлению нарушенных прав;
- выявление на основе анализа и обобщения судебной, прокурорской практики причин и условий, способствующих совершению правонарушений, разработка предложений, направленных на их устранение и недопущение;
- обеспечение реализации актов правоприменительной деятельности;

2. Место дисциплины в структуре образовательной программы:

Дисциплина относится к вариативной части учебного плана. Дисциплина по выбору.

3. Компетенции, формирующиеся у обучающегося и проверяемые в ходе освоения дисциплины:

После освоения дисциплины студент должен обладать следующими **профессиональными компетенциями** (ПК):

правоприменительная деятельность:

- способностью применять нормативные правовые акты, реализовывать нормы материального и процессуального права в профессиональной деятельности (ПК-5);

правоохранительная деятельность:

- способностью к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства (ПК-7);

4. Объем дисциплины и виды учебной работы:

Общая трудоемкость дисциплины составляет 2 зачетных единицы.

Вид учебной работы	Всего часов	Семестры					
		3					
Аудиторные занятия (всего)	**32**	**32**					
В том числе:	-	-	-	-	-		
Лекции	16	16					

Практические занятия	16	16						
Самостоятельная работа (всего)	**40**	**40**						
В т.ч. промежуточная аттестация	18	18						
Вид промежуточной аттестации (зачет, экзамен)	**зач**	**зач**						
Общая трудоемкость час	**72**	**72**						
зач. ед.	**2**	**2**						

5. Структура учебной дисциплины.

5.1 Тематический план

№ п/п	Модуль, темы учебной дисциплины	Виды учебной деятельности и трудоемкость (в часах)			Всего часов	Интерактивные образовательные технологии, применяемые на практических занятиях	
		Лекции	Практические занятия	Самостоятельная работа		В часах	Применяемые формы
	Входной контроль				0,5	-	-
I	**Модуль 1. Основы теории информационной безопасности**	**10**	**10**	**25**	**45**	**5**	
1	Тема 1. Понятие и система информационной безопасности. Угрозы информационной безопасности.	2	2	5	9		
2	Тема 2. Организационное обеспечение информационной безопасности	2	2	5	9	1,5	Дискуссии, ситуационные задачи
3	Тема 3. Правовое обеспечение информационной безопасности	2	2	5	9	1,5	Дискуссии, ситуационные задачи
4	Тема 4. Технические	2	2	5	9	1	Дискуссии, ситуационные

	средства обеспечение информационной безопасности						задачи
5	Тема 5. Технологическое обеспечение информационной безопасности	2	2	5	9	1	Дискуссии, ситуационные задачи
II	**Модуль 2. Режимы защиты информации**	**6**	**6**	**15**	**27**	**2**	
1	Тема 6. Лицензирование и сертификация в области защиты информации	1	1	2	4	1	Дискуссии, ситуационные задачи
2	Тема 7. Корпоративная система защиты информации	1	1	2	4		
3	Тема 8. Режим защиты государственной тайны	1	1	2	4	1	Дискуссии, ситуационные задачи
4	Тема 9. Режим защиты служебной тайны	1	1	2	4		
5	Тема 10. Режим защиты коммерческой тайны	0,5	0,5	2	3		
6	Тема 11. Режим защиты персональных данных	0,5	0,5	2	3		
7	Тема 12. Классификация и	1	1	3	5		

	проблемы предупреждения информационных преступлений						
	ВСЕГО:	**16**	**16**	**40**	**72**	**7**	

6. Планируемые результаты обучения по дисциплине, фонд оценочных средств по дисциплине для текущего контроля и промежуточной аттестации и критерии освоения компетенций:

6.1. Планируемые результаты обучения по дисциплине, фонд оценочных средств по дисциплине для текущего контроля и критерии освоения компетенций:

ПК-5 способностью применять нормативные правовые акты, реализовывать нормы материального и процессуального права в профессиональной деятельности;

Результаты обучения, достижение которых свидетельствует об освоении компетенции:

Знания: Организация информационной безопасности. Директивные документы по обеспечению информационной безопасности. Кадровое обеспечение информационной безопасности. Система государственных органов в сфере информационной безопасности. Базовые законы в сфере информационной безопасности. Подзаконные акты в сфере информационной безопасности. Локальные нормативные акты в сфере информационной безопасности. Стандарты и регламенты. Международные стандарты в сфере информационной безопасности.

Режим защиты государственной тайны. Государственная тайна как особый вид информации ограниченного доступа. Перечень сведений, составляющих государственную тайну. Условия допуска к государственной тайне. Порядок защиты государственной тайны. Ответственность за нарушение режима государственной тайны.

Режим защиты служебной тайны. Понятие служебной тайны. Нормативное закрепление правового режима служебной тайны. Порядок работы с информацией, составляющей служебную тайну.

Режим защиты коммерческой тайны. Понятие и природа коммерческой тайны. Нормативное закрепление правового режима коммерческой тайны. Методическое обеспечение определения сведений, составляющей коммерческую тайну. Субъекты коммерческой тайны. Условия передачи информации, составляющей коммерческую тайну.

Режим защиты персональных данных. Персональные данные как форма защиты частной жизни. Система законодательства о защите персональных данных. Условия работы с персональными данными. Методическое обеспечение защиты персональных данных. Ответственность за нарушения порядка обработки персональных данных.

Понятие и система информационных преступлений. Классификация информационных преступлений. Проблемы предупреждения информационных преступлений. Международные проблемы борьбы с информационными преступлениями.

Умения: анализировать правовые нормы об обеспечении государственной политики в области информатики и информационной безопасности. Классифицировать национальные интересы в области информационной безопасности. Определять допустимые нормативно-правовыми актами виды технических и технологических средств

обеспечения информационной безопасности, описывать в локальных нормативных актах инженерно-технические, методические, криптографические и программно-аппаратные способы обеспечения информационной безопасности.

Осуществлять обеспечение защиты государственной тайны, служебной тайны, коммерческой тайны, персональных данных. Совершать юридически значимые действия в области информации ограниченного доступа. Анализировать нормы правовых актов в области тайн.

Навыки: элементарные навыки создания локальных нормативных актов в сфере информационной безопасности. Применения правовых норм в области обеспечения информационной безопасности. Элементарные навыки создания локальных нормативных актов в области обеспечения защиты государственной тайны, коммерческой тайны, персональных данных. Элементарные навыки предупреждения опасностей и угроз, возникающих в информационных процессах

Оценочные средства, используемые для оценки сформированности компетенции:

1. Теоретические вопросы (для дискуссии и контрольной работы)

1.1. Понятие информационной безопасности
1.2. Базовые нормативные акты в сфере информационной безопасности
1.3. Директивные документы по обеспечению информационной безопасности
1.4. Силы и средства обеспечения информационной безопасности
1.5. Понятие государственной тайны
1.6. Перечень сведений, составляющих государственную тайну
1.7. Условия допуска к государственной тайне
1.8. Ответственность за нарушение режима государственной тайны
1.9. Понятие служебной тайны
1.10. Порядок работы с информацией, составляющей служебную тайну
1.11. Понятие и природа коммерческой тайны
1.12. Субъекты коммерческой тайны
1.13. Условия передачи информации, составляющей коммерческую тайну
1.14. Понятие персональных данных
1.15. Условия работы с персональными данными
1.16. Ответственность за нарушения порядка обработки персональных данных
1.17. Понятие и система информационных преступлений
1.18. Проблемы предупреждения информационных преступлений
1.19. Международные проблемы борьбы с информационными преступлениями

2. Тестовые задания (для контрольной работы)

2.1. Доктриной информационной безопасности понятие «информационная безопасность» определяется как

- состояние защищенности национальных интересов РФ в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства
- невозможность нанесения вреда кому-нибудь или чему-нибудь вследствие проявления угроз, т.е. защищенность от угроз
- совокупность внутренних и внешних потребностей государства в обеспечении защищенности и устойчивого развития личности, общества и государства
- состояние защищенности информации и информационных систем

2.2. В системе норм в области обеспечения информационной безопасности Доктрина информационной безопасности РФ определяет:

- основные положения информационной безопасности России

- базовые условия обеспечения национальной безопасности
- правовые режимы информации ограниченного доступа
- основные положения правового статуса субъектов информационных отношений

2.3. Преступлениями в сфере компьютерной информации являются:
- Неправомерный доступ к компьютерной информации
- Создание, использование и распространение вредоносных компьютерных программ
- Незаконный сбор персональных данных в автоматизированном режиме
- Разглашение сведений, составляющих банковскую тайну, в сети Интернет.

2.4. Обязанность по созданию условий, обеспечивающих охрану конфиденциальности сведений, составляющих коммерческую тайну законом возлагается на (несколько вариантов ответа):
- уполномоченных сотрудников органа государственной власти;
- обладателя информации, составляющей коммерческую тайну;
- работодателя;
- руководитель службы безопасности организации;
- органы государственной власти, иные государственные органы, органы местного самоуправления.

2.5. Обладатели информации, составляющей коммерческую тайну, обязаны предоставить сведения, составляющие коммерческую тайну, органам государственной власти:
- по запросу руководителя органа государственной власти;
- по мотивированному требованию, подписанному уполномоченным должностным лицом;
- при условии заключения гражданско-правового договора о передаче информации, составляющей коммерческую тайну.

2.6. Документы с пометкой "Для служебного пользования" (несколько вариантов ответа):
- печатаются на компьютерах, имеющих ограниченный доступ;
- печатаются в специальном машинописном бюро;
- учитываются отдельно от несекретной документации;
- передаются всем работникам подразделений под расписку;
- пересылаются сторонним организациям фельдъегерской связью, заказными или ценными почтовыми отправлениями;
- размножаются (тиражируются) исключительно только с письменного разрешения лица, подписывающего или утверждающего документ;
- хранятся в специальных хранилищах.

2.7. Обеспечение безопасности персональных данных достигается, в частности (несколько вариантов ответа):
- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- учетом печатных носителей персональных данных;
- регистрацией всех фактов использования персональных данных в информационной системе персональных данных;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных.

3. Ситуационные задачи (для работы на семинаре и контрольной работы)

3.1. В ГУВД по Самарской области обратился гр. Петров с заявлением о подготовке проживающими в соседней квартире гражданами взрыва плотины шламонакопителя (гидросооружения с отходами химического производства) Волжского химкомбината. К заявлению были приобщены аудио и видеозаписи, в которых содержались признаки подготавливаемого взрыва. Оперуполномоченный отдела по борьбе с терроризмом вынес постановление о проведении прослушивания телефонных переговоров всех подозреваемых лиц без судебного решения.

О каком виде информации ограниченного доступа здесь идет речь? Дайте правовую оценку данной ситуации и действиям представителя ГУВД.

Критерии освоения компетенции:

«пороговый уровень» (удовлетворительно) – знает основной директивный документ по обеспечению информационной безопасности; систему федеральных государственных органов в сфере информационной безопасности; базовые законы и подзаконные акты в сфере информационной безопасности; основные стандарты и регламенты в сфере информационной безопасности. Знает режим защиты государственной тайны; примерный перечень сведений, составляющих государственную тайну; основные условия допуска к государственной тайне; примерные виды ответственности за нарушение режима государственной тайны. Понятие служебной тайны; основные нормы правового режима служебной тайны; порядок работы с информацией, составляющей служебную тайну. Понятие коммерческой тайны; нормативное закрепление правового режима коммерческой тайны; субъекты коммерческой тайны; примерные условия передачи информации, составляющей коммерческую тайну. Понятие персональных данных; систему законодательства о защите персональных данных; условия работы с персональными данными; примерные виды ответственности за нарушения порядка обработки персональных данных. Понятие и систему информационных преступлений; основные проблемы предупреждения информационных преступлений.

Умеет анализировать правовые нормы об обеспечении государственной политики в области информационной безопасности. Классифицировать основные национальные интересы в области информационной безопасности. Определять допустимые нормативно-правовыми актами виды технических и технологических средств обеспечения информационной безопасности, описывать в локальных нормативных актах инженерно-технические, методические, криптографические и программно-аппаратные способы обеспечения информационной безопасности. Умеет осуществлять обеспечение защиты государственной тайны, служебной тайны, коммерческой тайны, персональных данных. Совершать юридически значимые действия в области информации ограниченного доступа. Анализировать нормы правовых актов в области тайн.

Владеет элементарными навыками создания локальных нормативных актов в сфере информационной безопасности и применения правовых норм в области обеспечения информационной безопасности. Владеет элементарными навыками создания локальных нормативных актов в области обеспечения защиты государственной тайны, коммерческой тайны, персональных данных; Элементарными навыками предупреждения опасностей и угроз, возникающих в информационных процессах.

«базовый уровень» (хорошо) – уверенно знает основной директивный документ по обеспечению информационной безопасности; систему федеральных и региональных государственных органов в сфере информационной безопасности; базовые законы и подзаконные акты в сфере информационной безопасности, систематизирует их; основные стандарты и регламенты в сфере информационной безопасности, систематизирует их. Знает режим защиты государственной тайны; перечень сведений, составляющих государственную тайну; условия допуска к государственной тайне; виды ответственности

за нарушение режима государственной тайны. Понятие служебной тайны; нормы правового режима служебной тайны; порядок работы с информацией, составляющей служебную тайну. Понятие коммерческой тайны; нормативное закрепление правового режима коммерческой тайны; субъекты коммерческой тайны; условия передачи информации, составляющей коммерческую тайну. Понятие персональных данных; систему законодательства о защите персональных данных; условия работы с персональными данными; виды ответственности за нарушения порядка обработки персональных данных. Понятие и систему информационных преступлений; проблемы предупреждения информационных преступлений.

Умеет анализировать и применять правовые нормы об обеспечении государственной политики в области информационной безопасности. Классифицировать и систематизировать национальные интересы в области информационной безопасности. Определять допустимые нормативно-правовыми актами виды технических и технологических средств обеспечения информационной безопасности, описывать в локальных нормативных актах инженерно-технические, методические, криптографические и программно-аппаратные способы обеспечения информационной безопасности. Умеет осуществлять обеспечение защиты государственной тайны, служебной тайны, коммерческой тайны, персональных данных. Совершать юридически значимые действия в области информации ограниченного доступа. Анализировать нормы правовых актов в области тайн.

Владеет уверенными навыками создания локальных нормативных актов в сфере информационной безопасности и применения правовых норм в области обеспечения информационной безопасности. Владеет уверенными навыками создания локальных нормативных актов в области обеспечения защиты государственной тайны, коммерческой тайны, персональных данных; Элементарными навыками предупреждения опасностей и угроз, возникающих в информационных процессах.

«повышенный уровень» (отлично) - уверенно знает директивные документы по обеспечению информационной безопасности и использует их при решении задач; систему федеральных и региональных государственных органов в сфере информационной безопасности, органов местного самоуправления в сфере обеспечения информационной безопасности; базовые законы и подзаконные акты в сфере информационной безопасности, систематизирует их и правоотношения, регулируемые ими; основные стандарты и регламенты в сфере информационной безопасности, систематизирует их. Знает режим защиты государственной тайны; перечень сведений, составляющих государственную тайну, систематизирует их; условия допуска к государственной тайне, льготы и ограничения при допуске к государственной тайне; виды ответственности за нарушение режима государственной тайны. Понятие служебной тайны; нормы правового режима служебной тайны; порядок работы с информацией, составляющей служебную тайну. Понятие коммерческой тайны; нормативное закрепление правового режима коммерческой тайны; субъекты коммерческой тайны; условия передачи информации, составляющей коммерческую тайну. Понятие персональных данных; систему законодательства о защите персональных данных; условия работы с персональными данными; виды ответственности за нарушения порядка обработки персональных данных. Понятие и систему информационных преступлений; проблемы предупреждения информационных преступлений, международные проблемы борьбы с информационными правонарушениями.

Умеет уверенно анализировать и применять правовые нормы об обеспечении государственной политики в области информационной безопасности. Классифицировать и систематизировать национальные интересы в области информационной безопасности. Определять допустимые нормативно-правовыми актами виды технических и технологических средств обеспечения информационной безопасности, описывать в

локальных нормативных актах инженерно-технические, методические, криптографические и программно-аппаратные способы обеспечения информационной безопасности. Умеет осуществлять обеспечение защиты государственной тайны, служебной тайны, коммерческой тайны, персональных данных. Совершать юридически значимые действия в области информации ограниченного доступа. Анализировать нормы правовых актов в области тайн.

Владеет уверенными навыками создания локальных нормативных актов в сфере информационной безопасности и применения правовых норм в области обеспечения информационной безопасности. Владеет уверенными навыками создания локальных нормативных актов в области обеспечения защиты государственной тайны, коммерческой тайны, персональных данных; Элементарными навыками предупреждения опасностей и угроз, возникающих в информационных процессах.

ПК-7 способностью к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства

Результаты обучения, достижение которых свидетельствует об освоении компетенции:

Знания: понятие и систему информационной безопасности. Угрозы информационной безопасности понятие защищенности интересов личности, общества и государства в информационной сфере. Классификацию национальных интересов в области информационной безопасности. Понятие системы обеспечения информационной безопасности. Силы и средства обеспечения информационной безопасности. Технические и технологические средства обеспечения информационной безопасности. Понятие угроз информационной безопасности. Угрозы интересам личности в информационной сфере. Угрозы интересам общества в информационной сфере. Угрозы интересам государства в информационной сфере. Понятие информационных войн в системе угроз информационной безопасности.

Информация юридических лиц и ее место в информационном обществе. Особенности и порядок защиты информации в корпорациях. Кадровое обеспечение в организациях в области защиты информации. Управление рисками в области защиты информации.

Понятие и виды технических средств обеспечения информационной безопасности. Методическое обеспечение информационной безопасности. Криптографические методы обеспечения информационной безопасности. Программно-аппаратное обеспечение информационной безопасности.

Понятие защиты информации. Концепция комплексной системы защиты информации. Модель защиты информации. Классификация уровней защищенности информации. Практические проблемы реализации комплексной системы защиты информации. Понятие системы лицензирования в области защиты информации. Аттестация объектов информатизации по требованиям безопасности информации. Сертификация продукции и услуг в области защиты информации. Система органов по сертификации средств защиты информации. Ответственность в области защиты информации.

Умения: Правильно применять современные информационные технологии для оформления юридических документов в области информационной безопасности. Совершать юридически значимые действия в области управления рисками в информационной безопасности. Осуществлять поиск информации о лицензировании и аттестации в области защиты информации.

получать новые и применять полученные знания в практической деятельности по укреплению законности и правопорядка в сфере информационной безопасности. Определять юридическую природу и характер информационных правоотношений, отличать их от смежных отношений. Давать квалифицированные юридические заключения, проводить консультации по вопросам обеспечения информационной безопасности.

Навыки: Элементарные навыки соблюдения основных требований информационной безопасности. Выявления обстоятельств, способствующих совершению информационных правонарушений.

элементарные навыки совершенствования профессиональных знаний и профессионального опыта в сфере правового обеспечения информационной безопасности. Навыками оценки направлений дальнейшего профессионального развития.

Оценочные средства, используемые для оценки сформированности компетенции:

1. Теоретические вопросы (для дискуссии и для контрольной работы)

1.1. Система информационной безопасности
1.2. Угрозы информационной безопасности
1.3. Национальные интересы в области информационной безопасности
1.4. Система обеспечения информационной безопасности
1.5. Угрозы информационной безопасности
1.6. Понятие информационных войн в системе угроз безопасности
1.7. Особенности и порядок защиты информации в корпорациях.
1.8. Кадровое обеспечение в организациях в области защиты информации.
1.9. Управление рисками в области защиты информации.
1.10. Понятие и виды технических средств обеспечения информационной безопасности.
1.11. Понятие защиты информации.
1.12. Концепция комплексной системы защиты информации.
1.13. Практические проблемы реализации комплексной системы защиты информации.
1.14. Понятие системы лицензирования в области защиты информации.
1.15. Аттестация объектов информатизации по требованиям безопасности информации.
1.16. Сертификация продукции и услуг в области защиты информации.
1.17. Ответственность в области защиты информации.

2. Тестовые задания (для контрольной работы)

2.1. Информационная безопасность рассматривается в Стратегии развития информационного общества в качестве:
- одного из направлений реализации государственной политики
- принципа развития информационного общества
- основной задачи развития информационного общества
- одной из функций государства

2.2. Государственным органом по противодействию техническим разведкам и технической защите информации является:
- ФСТЭК РФ
- МВД РФ
- ФСО РФ
- ФСБ РФ

2.3. Жизненно важные интересы личности в информационной сфере заключаются в (выбрать два ответа):

- реализации конституционных прав человека и гражданина на доступ к информации
- защите информации, обеспечивающей личную безопасность
- упрочении правового и социального статуса человека
- создании условий для гармоничного развития российской информационной инфраструктуры

3. Ситуационные задачи (для работы на семинаре и контрольной работы)

3.1. В банк «Российский капитал» обратился оперуполномоченный отдела по борьбе с коррупцией ГУВД центрального административного округа г. Москвы с запросом о предоставлении информации, составляющей коммерческую тайну. При этом названный работник ГУВД не стал указывать мотивы под предлогом государственной тайны. Руководитель банка поручил начальнику юридического отдела разобраться и подготовить ответ о том, что банк может предоставить запрашиваемую информацию только на основании решения суда.

О каком виде информации ограниченного доступа здесь идет речь? Дайте правовую оценку данной ситуации. Как должно быть разрешено дело?

Критерии освоения компетенции:

«пороговый уровень» (удовлетворительно) – знает понятие и систему информационной безопасности. Основные виды угроз информационной безопасности; понятие защищенности интересов личности, общества и государства в информационной сфере. Основную классификацию национальных интересов в области информационной безопасности. Понятие системы обеспечения информационной безопасности. Силы и средства обеспечения информационной безопасности. Технические и технологические средства обеспечения информационной безопасности. Понятие угроз информационной безопасности. Угрозы интересам личности в информационной сфере. Угрозы интересам общества в информационной сфере. Угрозы интересам государства в информационной сфере. Понятие информационных войн в системе угроз информационной безопасности. знает понятие информации юридических лиц и ее место в информационном обществе; особенности и порядок защиты информации в корпорациях; кадровое обеспечение в организациях в области защиты информации; управление рисками в области защиты информации. Понятие и основные виды технических средств обеспечения информационной безопасности; примерные методические способы обеспечения информационной безопасности; примерные криптографические методы обеспечения информационной безопасности; примерные программно-аппаратные способы обеспечения информационной безопасности. Понятие защиты информации; модель защиты информации. Классификацию уровней защищенности информации. Понятие системы лицензирования в области защиты информации; способы аттестации объектов информатизации по требованиям безопасности информации; сертификации продукции и услуг в области защиты информации; систему органов по сертификации средств защиты информации. Ответственность в области защиты информации.

Умеет правильно применять современные информационные технологии для оформления юридических документов в области информационной безопасности. Совершать юридически значимые действия в области управления рисками в информационной безопасности. Осуществлять поиск информации о лицензировании и аттестации в области защиты информации. Умеет получать новые и применять полученные знания в практической деятельности по укреплению законности и правопорядка в сфере информационной безопасности. Определять юридическую природу и характер информационных правоотношений, отличать их от смежных отношений.

Давать юридические заключения, проводить консультации по вопросам обеспечения информационной безопасности.

Владеет элементарными навыками соблюдения основных требований информационной безопасности. Выявления обстоятельств, способствующих совершению информационных правонарушений. Владеет элементарными навыками совершенствования профессиональных знаний и профессионального опыта в сфере правового обеспечения информационной безопасности. Навыками оценки направлений дальнейшего профессионального развития

«базовый уровень» (хорошо) – знает понятие и систему информационной безопасности. Виды угроз информационной безопасности; понятие защищенности интересов личности, общества и государства в информационной сфере. Различные классификации национальных интересов в области информационной безопасности. Понятие системы обеспечения информационной безопасности. Силы и средства обеспечения информационной безопасности, приводит содержание прав и обязанностей сил обеспечения информационной безопасности. Технические и технологические средства обеспечения информационной безопасности. Понятие и систему угроз информационной безопасности. Угрозы интересам личности в информационной сфере. Угрозы интересам общества в информационной сфере. Угрозы интересам государства в информационной сфере. Понятие информационных войн в системе угроз информационной безопасности. знает понятие и виды информации юридических лиц и ее место в информационном обществе; особенности и порядок защиты информации в корпорациях; способы кадрового обеспечения в организациях в области защиты информации; различные способы управления рисками в области защиты информации. Понятие и виды технических средств обеспечения информационной безопасности; основные методические способы обеспечения информационной безопасности; основные криптографические методы обеспечения информационной безопасности; основные программно-аппаратные способы обеспечения информационной безопасности. Понятие защиты информации; модель защиты информации. Классификацию уровней защищенности информации. Понятие системы лицензирования в области защиты информации; способы аттестации объектов информатизации по требованиям безопасности информации; сертификации продукции и услуг в области защиты информации; систему органов по сертификации средств защиты информации. Ответственность в области защиты информации.

Умеет правильно и оперативно применять современные информационные технологии для оформления юридических документов в области информационной безопасности. Совершать юридически значимые действия в области управления рисками в информационной безопасности. Осуществлять поиск информации о лицензировании и аттестации в области защиты информации. Умеет получать новые и применять полученные знания в практической деятельности по укреплению законности и правопорядка в сфере информационной безопасности. Определять юридическую природу и характер информационных правоотношений, отличать их от смежных отношений. Давать юридические заключения, проводить консультации по вопросам обеспечения информационной безопасности.

Владеет уверенными навыками соблюдения основных требований информационной безопасности. Выявления обстоятельств, способствующих совершению информационных правонарушений. Владеет уверенными навыками совершенствования профессиональных знаний и профессионального опыта в сфере правового обеспечения информационной безопасности. Навыками оценки направлений дальнейшего профессионального развития

«повышенный уровень» (отлично) – знает понятие и систему информационной безопасности. Виды угроз информационной безопасности; понятие защищенности интересов личности, общества и государства в информационной сфере. Различные

классификации национальных интересов в области информационной безопасности. Понятие системы обеспечения информационной безопасности. Силы и средства обеспечения информационной безопасности, приводит содержание прав и обязанностей сил обеспечения информационной безопасности. Технические и технологические средства обеспечения информационной безопасности, их виды и классификацию, возможности их применения. Понятие и систему угроз информационной безопасности. Угрозы интересам личности в информационной сфере. Угрозы интересам общества в информационной сфере. Угрозы интересам государства в информационной сфере. Понятие информационных войн в системе угроз информационной безопасности. знает понятие и виды информации юридических лиц и ее место в информационном обществе, систематизирует их; особенности и порядок защиты информации в корпорациях; способы кадрового обеспечения в организациях в области защиты информации; различные способы управления рисками в области защиты информации. Понятие и виды технических средств обеспечения информационной безопасности; различные методические способы обеспечения информационной безопасности; различные криптографические методы обеспечения информационной безопасности; различные программно-аппаратные способы обеспечения информационной безопасности. Понятие защиты информации; модель защиты информации. Классификацию уровней защищенности информации. Понятие системы лицензирования в области защиты информации; способы аттестации объектов информатизации по требованиям безопасности информации; сертификации продукции и услуг в области защиты информации; систему органов по сертификации средств защиты информации. Ответственность в области защиты информации.

Умеет правильно и оперативно применять современные информационные технологии для оформления юридических документов в области информационной безопасности. Совершать юридически значимые действия в области управления рисками в информационной безопасности. Осуществлять поиск информации о лицензировании и аттестации в области защиты информации. Умеет получать новые и применять полученные знания в практической деятельности по укреплению законности и правопорядка в сфере информационной безопасности. Определять юридическую природу и характер информационных правоотношений, отличать их от смежных отношений. Давать юридические заключения, проводить консультации по вопросам обеспечения информационной безопасности.

Владеет уверенными навыками соблюдения основных требований информационной безопасности. Выявления обстоятельств, способствующих совершению информационных правонарушений. Владеет уверенными навыками совершенствования профессиональных знаний и профессионального опыта в сфере правового обеспечения информационной безопасности. Навыками оценки направлений дальнейшего профессионального развития

6.2. Фонд оценочных средств по дисциплине для промежуточной аттестации.

При проведении промежуточной аттестации проверяется сформированность у обучающихся всех компетенций (полностью или в части), заявленных в п. 3 данной программы дисциплины.

Оценочные средства:

1. Теоретические вопросы к зачету:

1.Понятие информационной безопасности.
2.Интересы личности в информационной сфере.
3.Интересы общества в информационной сфере.
4.Интересы общества и государства в информационной сфере.
5. Понятие угроз информационной безопасности.

6.Угрозы интересам личности в информационной сфере.
7.Угрозы интересам общества в информационной сфере.
8.Угрозы интересам государства в информационной сфере.
9.Информационные войны в системе угроз информационной безопасности.
10.Понятие системы информационной безопасности.
11.Силы и средства обеспечения информационной безопасности.
12.Технические средства обеспечение информационной безопасности
13.Технологические средства обеспечения информационной безопасности.
14.Организационное обеспечение информационной безопасности
15.Система государственных органов в сфере информационной безопасности.
16.Правовое обеспечение информационной безопасности
17.Локальные нормативные акты в сфере информационной безопасности.
18.Международные стандарты в сфере информационной безопасности.
19.Криптографические методы обеспечение информационной безопасности.
20.Программно-аппаратное обеспечение информационной безопасности.
21.Понятие защиты информации
22.Концепция комплексной системы защиты информации.
23.Модель защиты информации.
24.Классификация уровней защищенности информации.
25.Понятие системы лицензирования в области защиты информации.
26.Аттестация объектов информатизации по требованиям безопасности информации.
27.Сертификация продукции и услуг в области защиты информации.
28.Система органов по сертификации средств защиты информации.
29.Ответственность в области защиты информации.
30.Корпоративная система защиты информации.
31.Государственная тайна как особый вид информации ограниченного доступа.
32.Перечень сведений, составляющих государственную тайну.
33.Условия допуска к государственной тайне.
34. Доступ и допуск к государственной тайне
35.Ответственность за нарушение режима государственной тайны.
36.Понятие служебной тайны.
37.Порядок работы с информацией, составляющей служебную тайну.
38.Понятие и природа коммерческой тайны.
39.Нормативное закрепление правового режима коммерческой тайны.
40.Методическое обеспечение определения сведений, составляющей коммерческую тайну.
41.Условия передачи информации, составляющей коммерческую тайну.
42.Персональные данные как форма защиты частной жизни.
43.Система законодательства о защите персональных данных.
44.Условия работы с персональными данными.
45.Методическое обеспечение защиты персональных данных.
46.Ответственность за нарушения порядка обработки персональных данных.
47.Понятие и виды профессиональных тайн.
48.Понятие и система информационных преступлений.
49.Понятие и виды информационных преступлений.
50.Проблемы предупреждения информационных правонарушений

2. Типовые практические задачи для экзамена

1.Гр. Иванов заключил договор на оказание услуг хостинга с компанией Ростелеком. На размещенном в хостинге веб-сайте Иванов дал возможность всем желающим вести дискуссию и размещать материалы на тему политического устройства России.

Во время длительного отпуска Иванова на веб-сайте были размещены экстремистские материалы. Один из посетителей сайта написал об этом заявление в прокуратуру и Роскомнадзор.

Дайте правовую оценку ситуации. Как должно быть разрешено дело?

2. Гр. Иванов десять лет назад имел допуск по первой форме (особой важности) к сведениям составляющим государственную тайну и уволился из НИИ спустя 6 лет. Имея желание выехать из Российской Федерации в Великобританию он обратился в полицию с заявлением на получение загранпаспорта и разрешением на выезд. В выдаче загранпаспорта и разрешения на выезд ему было отказано. Основанием для отказа явилось заключение Межведомственной комиссии по защите государственной тайны о том, что сведения, к которым был в свое время допущен Иванов, сохраняют режим секретности. Иванов посчитал, что его права нарушены и обратился в коллегию адвокатов за юридической помощью.

О каком виде информации ограниченного доступа здесь идет речь? Дайте правовую оценку данной ситуации. Как должно быть разрешено дело?

Билеты для зачета включают в себя 2 теоретических вопроса и 1 практическую задачу. Каждый теоретический вопрос оценивается преподавателем в 0-15 баллов, задача оценивается в 20 баллов.

Критерии оценивания:

Критерии начисления баллов за ответ **на теоретический вопрос**:

13-15 баллов ставится студенту, проявившему всесторонние и глубокие знания программного материала, освоившему в полном объеме содержание нормативно-правовых актов, изученных в течение курса, обнаружившему творческие способности в понимании и практическом использовании материала, проявившему высокие знания базовых категорий и понятий по изучаемой дисциплине. Баллы внутри критерия определяются в зависимости от количества допущенных неточностей.

9-12 баллов ставится студенту, проявившему полное знание программного материала, освоившему в полном объеме содержание нормативно-правовых актов, изученных в течение курса, обнаружившему стабильный характер знаний и умений и способному к их самостоятельному применению и обновлению в ходе практической деятельности, обнаружившему знания базовых категорий и понятий по изучаемой дисциплине. Баллы внутри критерия определяются в зависимости от количества допущенных неточностей.

5-8 баллов ставится студенту, проявившему знания основного программного материала в объеме, необходимом для предстоящей практической деятельности, знакомому с содержанием нормативно-правовых актов, изученных в течение курса, допустившему неточности при подготовке ответа, но обладающему необходимыми знаниями и умениями для их устранения при корректировке со стороны преподавателя, допустившему неточности в знаниях базовых категорий и понятий по изучаемой дисциплине. Баллы внутри критерия определяются в зависимости от количества допущенных ошибок.

1-4 балл ставится студенту, обнаружившему пробелы в знании основного программного материала, допустившему грубые ошибки при применении нормативно-правовых актов, изученных в течение курса, допустившему грубые ошибки в знаниях базовых категорий и понятий по изучаемой дисциплине. Баллы внутри критерия определяются в зависимости от количества допущенных ошибок.

0 баллов ставится студенту, который не ответил на вопрос в билете, не знает базовых категорий и понятий по изучаемой дисциплине, не знает отдельных разделов программного материала, допускает существенные ошибки, с большим затруднением отвечает на задаваемые дополнительные вопросы.

Критерии начисления баллов за решение **практической задачи**:

15-20 баллов за решение задачи ставится студенту за умение правильно формулировать вопросы к решению задачи, умение правильно применять нормы права и судебные акты, умение правильно решать задачу и формулировать правильный вывод. Баллы внутри критерия определяются в зависимости от количества допущенных неточностей.

8-14 баллов за умение правильно применять нормы права и правильно решать задачу. Баллы внутри критерия определяются в зависимости от количества допущенных неточностей.

1-7 балла за правильный выбор нормативного правового акта, но неправильное решение задачи. Баллы внутри критерия определяются в зависимости от количества допущенных ошибок.

0 балла – за неправильное решение задачи и неправильный выбор нормативного правового акта.

7. Система оценивания по дисциплине:

Перечень тем/ модулей	Форма и описание контрольного мероприятия	Балловая стоимость контрольного мероприятия и критерии начисления баллов
Модуль 1 Модуль 2	АУДИТОРНОЯ САМОСТОЯТЕЛЬНАЯ РАБОТА Выполняется на практических занятиях после разъяснения темы преподавателем. Состоит из 3 практических заданий, выполняемого на компьютере (максимальное количество баллов за семестр – 12 баллов).	Максимальная сумма балов за контрольное мероприятие: 12 баллов за 4 работы. Работа состоит из 3 практических заданий, выполняемых на компьютере. Практическое задание оценивается в 1 балл. Задания выполняются на компьютере и сохраняются в соответствующем формате в указанной преподавателем папке. Задание, выполненное в соответствии со всеми указанными в задании требованиями и сохраненное в соответствующем формате в указанной папке, оценивается в 1 балла. Задание, выполненное правильно на 50% - 0,5 балла. Задание, выполненное неверно или не выполненное оценивается в 0 баллов.
Модуль 1 Модуль 2	ВНЕАУДИТОРНАЯ ИТОГОВАЯ КОНТРОЛЬНАЯ РАБОТА Представлено 3 вида работ: практическая домашняя работа на 6 баллов, 2 теста – по 16 баллов (максимальное количество баллов за семестр –38 баллов).	Максимальная сумма балов за контрольное мероприятие: 38 баллов. Практическая домашняя работа - 6 баллов. 6 баллов за каждый вопрос ставятся в случае: в ответе отражены определения всех понятий, указанных в задании; перечислены и раскрыты свойства и характеристики данных понятий; указаны нормативные акты, регулирующие правоотношения по поводу использования выделенных в задании объектов; дан самостоятельный творческий анализ используемых материалов. 5-4 балла за каждый вопрос письменной части ставятся в случае: в ответе отражены определения всех понятий, указанных в задании; перечислены свойства и характеристики понятий; указаны нормативные акты, регулирующие правоотношения по поводу использования выделенных в задании объектов. 3-2 балла за каждый вопрос письменной части ставятся в

		случае: в ответе отражены определения понятий, указанных в задании или свойства и характеристики понятий или указаны нормативные акты, регулирующие правоотношения по поводу использования выделенных в задании объектов. 1 балл за каждый вопрос письменной части ставятся в случае: в ответе отражены определения не всех понятий или отсутствуют существенные признаки, не указаны свойства и/или характеристики понятий, не указаны или указаны не верно НПА. 0 баллов за каждый вопрос письменной части ставятся в случае полного отсутствия ответа на поставленный вопрос. 2 теста – по 16 баллов (32 балла). Каждое тестовое задание (вопрос) оценивается в 1 балл.

Итоговая оценка складывается из суммы баллов текущего контроля и баллов по промежуточной аттестации.

- оценка «не зачтено» - до 39 баллов включительно;
- оценка «зачтено» - от 40 до 100 баллов;

8. Методические указания для обучающихся по освоению дисциплины:

Занятия по дисциплине проводятся в виде лекционных и семинарских занятий.

Тема лекционного занятия определяется и озвучивается преподавателем студентам на предыдущей лекции. Ко времени лекции студенту необходимо ознакомиться с текстом нормативно-правовых актов, изучаемых по указанной теме. Желательно ознакомление студентом с учебной и научной литературой по рассматриваемой теме. В ходе лекции для закрепления материала преподаватель рассматривает со студентами практические ситуации и предлагает студентам найти и обсудить варианты их решений, после чего преподаватель озвучивает принятую правовую позицию.

Тема семинарского занятия определяется и озвучивается преподавателем студентам на предыдущем семинарском занятии. К семинарскому занятию студентам в обязательном порядке необходимо ознакомиться с текстом нормативно-правовых актов, учебной и научной литературой по указанной теме. Семинарское занятие проходит в форме диалога, который определяет уровень теоретической подготовки студента; решения практических задач с использованием сети интернет и справочных правовых систем; решения теста, который позволяет оценить уровень знаний, умений и владений студента по указанной теме.

Выполнение творческого домашнего задания (составление презентаций) предусматривает уверенное владение студентом информационными материалами, размещаемыми в сети интернет на сайтах органов государственной власти, умение ориентироваться в современной литературе по теме задания и знание нормативно-правовых актов, изучаемых в курсе дисциплины.

9. Учебно-методическое и информационное обеспечение дисциплины:

9.1. Основная литература:

1) Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498844. — Режим доступа: по подписке.

2) Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/1861657. – Режим доступа: по подписке.

9.2. Дополнительная литература:

1) Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. — Доступ на сайте ЭБС Znanium. URL: https://znanium.com/catalog/product/405000. — Режим доступа: по подписке.

2) Гродзенский Я. С. Информационная безопасность : учебное пособие. – Москва : РГ-Пресс, 2020. – 144 с. - Доступ на сайте ЭБС Проспект. URL: http://ebs.prospekt.org/book/43070. — Режим доступа: по подписке.

3) Гродзенский Я. С. Информационная безопасность : учебное пособие. – Москва : РГ-Пресс, 2020. – 144 с. - Доступ на сайте ЭБС Проспект. URL: http://ebs.prospekt.org/book/43070. — Режим доступа: по подписке.

Электронные учебные издания доступны для зарегистрированных в Электронной информационно-образовательной среде университета пользователей.

9.3. Нормативно-правовые и правоприменительные акты:

1. Федеральный закон от 27.07.2006, г., № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 21 июня 1993 № 5485-1 «О государственной тайне».
3. Федеральный закон от 29 июля 2004 № 98-ФЗ «О коммерческой тайне».
4. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».
5. Федеральный закон от 09.02.2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».
6. Федеральный закон № 262-ФЗ от 22 декабря 2008 г. «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».
7. Федеральный закон №126-ФЗ от 7 июля 2003 г. «О связи».
8. Федеральный закон № 63-ФЗ от 06 апреля 2011 г. «Об электронной подписи».
9. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
10. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы (утв. Указом Президента РФ 09.05.2017 № 203) // Российская газета, N 34, 16.02.2008
11. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ 05.12.2016 № 646) // Российская газета, № 187, 06.12.2016
12. Постановление Правительства РФ № 1233 от 3 ноября 1994 г. «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах государственной власти».
13. Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

9.4. Перечень современных профессиональных баз данных:

1. Государственная автоматизированная система Российской Федерации «Правосудие» - Режим доступа: https://bsr.sudrf.ru/bigs/portal.html;

2. Банк решений Конституционного Суда Российской Федерации - Режим доступа: http://www.ksrf.ru/ru/Decision/Pages/default.aspx;
3. Банк решений арбитражных судов - Режим доступа: https://ras.arbitr.ru/;
4. База решений и правовых актов Федеральной антимонопольной службы - Режим доступа: https://br.fas.gov.ru/;
5. Государственная система правовой информации – Режим доступа: http://www.pravo.gov.ru/;
6. Федеральный портал проектов нормативных актов - Режим доступа: https://regulation.gov.ru/;
7. Система обеспечения законодательной деятельности - Режим доступа: https://sozd.duma.gov.ru/.

9.5. Перечень информационных справочных систем:

1. Информационно-правовой портал «Система Гарант»;
2. Справочная правовая система «КонсультантПлюс»;
3. Информационно-правовая система «Кодекс»;
4. Информационно-правовая система (ИПС) «Законодательство стран СНГ».

9.6. Перечень электронных библиотечных систем:

1. «Электронно-библиотечная система ZNANIUM»;
2. «Образовательная платформа ЮРАЙТ»;
3. Электронно-библиотечная система «BOOK.ru»;
4. Электронно-библиотечная система «ЛАНЬ»;
5. Электронно-библиотечная система Издательства «Проспект».

Издания электронных библиотечных систем доступны для зарегистрированных в Электронной информационно-образовательной среде университета пользователей.

9.7 Перечень лицензионного программного обеспечения:

1. Microsoft WINEDUperDVC ALNG UpgrdSAPk OLV E 1Y AcdmemicEdition Enterprise;
2. Linux (Альт, Астра);
3. Kaspersky Endpoint Security 11 для Windows (до15.02.2024);
4. Libre Office (свободно распространяемое программное обеспечение).

9.8 Наборы демонстрационного оборудования и учебно-наглядные пособия, обеспечивающие тематические иллюстрации при проведении занятий лекционного типа:

По дисциплине имеются:

- учебно-наглядные пособия: «Структурная модель информационной безопасности» по Теме «Понятие и система информационной безопасности. Угрозы информационной безопасности».

10. Материально-техническое обеспечение дисциплины, в том числе оборудование и технические средства обучения.

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебная аудитория для проведения занятий лекционного типа	Специализированная мебель и технические средства обучения, служащие для представления учебной информации большой аудитории: рабочие места для обучающихся, рабочее место преподавателя, экран

	проекционный, проектор, доска магнитно-меловая, учебно-наглядные пособия, обеспечивающие тематические иллюстрации, видеонаблюдение
Учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Специализированная мебель и технические средства обучения, служащие для представления учебной информации большой аудитории: рабочие места для обучающихся, рабочее место преподавателя, доска магнитно-меловая, учебно-наглядные пособия, обеспечивающие тематические иллюстрации, моноблок, интерактивная доска
Помещение для самостоятельной работы	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации, проектор, экран, многофункциональное устройство