

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Институт математики, физики и информационных технологий
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:
Директор института



И. Н. Якунина
«20» января 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.Б.19 Правовая защита информации

Направление подготовки/специальность: 10.05.05 - Безопасность информационных технологий в правоохранительной сфере

Профиль/направленность/специализация: Технологии защиты информации в правоохранительной сфере

Уровень высшего образования: специалитет

Квалификация: Специалист по защите информации

год набора: 2019

Тамбов, 2021

Автор программы:

Кандидат педагогических наук, доцент Михайлова Елена Михайловна

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере (уровень специалитета) (приказ Министерства образования и науки РФ от «19» декабря 2016 г. № 1612).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «22» декабря 2020 г. Протокол № 4

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «20» января 2021 г. № 1.

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП Специалиста.....	5
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	10
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	35
6. Учебно-методическое и информационное обеспечение дисциплины.....	37
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	38

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ОК-4 Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета

ПК-19 Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности

1.2 Виды и задачи профессиональной деятельности по дисциплине:

- организационно-управленческая
 - организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов
 - разработка и контроль эффективности осуществления системы мер по формированию и использованию информационных ресурсов, систем обеспечения информационной безопасности
 - организация работы малых групп и коллективов исполнителей, сформированных для решения конкретных профессиональных задач

1.3 В результате освоения дисциплины у обучающихся должны быть сформированы следующие компетенции:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Знания и умения, необходимые для формирования трудового действия / компетенции
	ОК-4 Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета	Знает и понимает: принципы и тенденции изменений законодательства в области информации, требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности.
		Умеет (способен продемонстрировать): анализировать основные изменения законодательства в области информации и применять их на практике, осуществлять логику взаимосвязей информационных систем и ресурсов.
		Владеет: навыками поиска актуальной правовой информации, знаниями основ государства и права, основными понятиями и категориями информационного права.
	ПК-19 Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности	Знает и понимает: принципы и тенденции изменений законодательства в области информации, требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности.
		Умеет (способен продемонстрировать): анализировать основные изменения законодательства в области информации и применять их на практике, осуществлять логику взаимосвязей информационных систем и ресурсов
		Владеет:

	навыками поиска актуальной правовой информации, знаниями основ государства и права, основными понятиями и категориями информационного права
--	---

1.4 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ОК-4 Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения					
		Очная (семестр)					
		3	6	7	8	9	10
1	Досудебное производство в уголовном процессе			+			
2	Информационно-аналитическое обеспечение правоохранительной деятельности					+	
3	Информационное право	+					
4	Комплексная система защиты информации объектов информатизации			+	+	+	
5	Криминалистика и криминалистическая техника			+	+		
6	Психология профессиональной деятельности		+				
7	Специальные информационные технологии в правоохранительной деятельности						+

ПК-19 Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения			
		Очная (семестр)			
		3	7	8	9
1	Досудебное производство в уголовном процессе		+		
2	Информационное право	+			

3	Практика по получению профессиональных умений и опыта профессиональной деятельности			+	+
---	---	--	--	---	---

2. Место дисциплины в структуре ОП специалитета:

Дисциплина «Правовая защита информации» относится к базовой части учебного плана ОП по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере.

Дисциплина «Правовая защита информации» изучается в 4 семестре.

3. Объем и содержание дисциплины

3.1. Объем дисциплины: 5 з.е.

Очная: 5 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	180
Контактная работа	68
Лекции (Лекции)	34
Лабораторные (Лаб. раб.)	34
Самостоятельная работа (СР)	76
Экзамен	36

3.2. Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
4 семестр					
1	Информация как объект правового регулирования	2	2	8	Тестирование
2	Законодательство РФ в области информационной безопасности	4	4	8	Тестирование
3	Правовой режим защиты государственной тайны	4	4	8	Тестирование
4	Правовые режимы защиты конфиденциальной информации	4	4	8	Тестирование

5	Лицензирование и сертификация в информационной сфере	4	4	8	Тестирование
6	Защита интеллектуальной собственности	4	4	8	Тестирование
7	Компьютерные правонарушения	4	4	8	Тестирование
8	Правовое регулирование оперативно-розыскных мероприятий (ОРМ) в оперативно-розыскной (ОРД) и частной детективной и охранной деятельности (ЧДОД)	4	4	10	Тестирование
9	Международное законодательство в области защиты информации	4	4	10	Тестирование

Тема 1. Информация как объект правового регулирования (ОК-4)

Лекция.

Определение информация, право. Смысл понятия «Нормативный акт» Проблемы правового регулирования защиты информации. Соблюдение в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности.

Лабораторные работы.

не предусмотрено

Задания для самостоятельной работы.

1. Какой Государственный стандарт в области информационной безопасности является основным?
2. Какой стандарт устанавливает классификацию и перечень факторов, воздействующих на безопасность защищаемой информации?
3. Какие существуют виды угроз информационной безопасности Российской Федерации по общей направленности?
4. Что относится к внешним источникам угроз информационной безопасности Российской Федерации?
5. На какие виды разделяются общие методы обеспечения информационной безопасности Российской Федерации?
6. Кто играет основную роль в создании правовых механизмов защиты информации?
7. Функции межведомственной комиссии?
8. Какой орган формирует законодательную базу в области защиты информации?
9. Функции службы внешней разведки Российской Федерации?
10. Основные задачи ФСТЭК?

Тема 2. Законодательство РФ в области информационной безопасности (ОК-4)

Лекция.

Определение информации, право. Смысл понятия «Нормативный акт» Проблемы правового регулирования защиты информации. Соблюдение в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности.

Лабораторные работы.

Обзор нормативных актов регулирующих сферу информационной безопасности в РФ

Задания для самостоятельной работы.

1. Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы
2. Подготовка к тестированию

Тема 3. Правовой режим защиты государственной тайны (ПК-19)

Лекция.

Понятие «государственная тайна», главные черты государственной тайны, правовые основы реализации защиты государственной тайны. Соблюдение в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечение соблюдения режима секретности.

Лабораторные работы.

Анализ систем защиты информации на объектах информатизации обрабатывающие сведения, составляющие государственную тайну.

Задания для самостоятельной работы.

- 1 Что относится к государственной тайне?
- 2 Кто может иметь доступ к государственной тайне?
- 3 Какие ограничения могут быть для лиц, допущенных к сведениям составляющих государственную тайну?
- 4 Что относится к основным составляющим национальных интересов Российской Федерации в информационной сфере?
- 5 Что может служить основанием для рассекречивания сведений, составляющих государственную тайну?
- 6 Какие грифы секретности могут быть присвоены информации?
- 7 Какие сведения не подлежат отнесению к государственной тайне и засекречиванию?
- 8 Что можно отнести к актуальным проблемам защиты государственной информации?
- 9 Способы защиты государственной тайны?
- 10 Какие органы занимаются защитой государственной информации?

Тема 4. Правовые режимы защиты конфиденциальной информации (ПК-19)

Лекция.

Понятие «конфиденциальная информация», главные черты конфиденциальной информации, правовые основы реализации защиты конфиденциальной информации

Лабораторные работы.

Анализ систем защиты информации на объектах информатизации обрабатывающие конфиденциальные данные

Задания для самостоятельной работы.

1. Понятие и виды информации. информация в системе правового регулирования общественных отношений.
2. Правовые режимы информации.

3. Понятие и виды конфиденциальной информации.
4. Правовые режимы конфиденциальности информации в частном праве.
5. Правовой режим семейной тайны.
6. Правовой режим личной тайны.
7. Правовой режим секретов производства (ноу-хау).
8. Правовой режим коммерческой тайны.
9. Правовой режим конфиденциальности информации в договорных отношениях.
10. Виды правовых режимов конфиденциальности информации в публичных правоотношениях.
12. Правовой режим служебной тайны.
13. Правовой режим профессиональной тайны.
14. Конфиденциальность персональных данных.
15. Гражданско-правовая ответственность при нарушении правовых режимов конфиденциальности информации.
16. Административно-правовая ответственность при нарушении правовых режимов конфиденциальности информации.
17. Уголовно-правовая ответственность при нарушении правовых режимов конфиденциальности информации.
18. Правовые последствия нарушения правового режима конфиденциальности информации.

Тема 5. Лицензирование и сертификация в информационной сфере (ОК-4)

Лекция.

Закон "О лицензировании отдельных видов деятельности", правовые акты общего назначения, Государственные структуры занимающиеся лицензированием в информационной сфере. Выполнение профессиональных задач в соответствии с нормами морали, профессиональной этики и служебного этикета.

Лабораторные работы.

Не предусмотрено

Задания для самостоятельной работы.

1. Понятие, цель и критерии лицензирования отдельных видов деятельности.
2. Порядок лицензирования отдельных видов деятельности.
3. Юридические санкции за осуществление предпринимательской деятельности без лицензии и с нарушением лицензионных требований?
4. Уведомительный порядок начала осуществления предпринимательской деятельности?
5. Какие виды деятельности подлежат обязательному лицензированию?
6. На какие виды деятельности выдаётся лицензия ФСТЭК?

7. На какие виды деятельности выдаётся лицензия ФСБ?

Тема 6. Защита интеллектуальной собственности (ОК-4)

Лекция.

Понятие интеллектуальной собственности, методы защиты интеллектуальной собственности, сравнение систем лицензирования и сертификации в РФ и Европе

Лабораторные работы.

Обзор нормативных актов регулирующих сферу информационной безопасности в Европе

Задания для самостоятельной работы.

1. Что является объектом интеллектуальной собственности?
2. Дайте определение понятия авторского права.
3. Перечислите закрепленные в Гражданском кодексе РФ объекты авторского права
4. Дайте общую характеристику прав, смежных с авторскими
5. Какие общественные отношения регулирует патентное законодательство?
6. Назовите правовые механизмы защиты патентных прав и дайте их общую характеристику.
7. Дайте характеристику исключительного права на фирменное наименование
8. В чем заключается режим правовой охраны наименования места происхождения товара?
9. Каковы правовые формы защиты интеллектуальных прав на секрет производства?

Тема 7. Компьютерные правонарушения (ПК-19)

Лекция.

Понятие компьютерное правонарушение, правовые акты общего назначения регулирующие сферу компьютерных правонарушений. . Выполнение профессиональных задач в соответствии с нормами морали, профессиональной этики и служебного этикета.

Лабораторные работы.

Не предусмотрено

Задания для самостоятельной работы.

1. Уголовно-правовая характеристика компьютерных преступлений
2. Неправомерный доступ к компьютерной информации
3. Создание, использование и распространение вредоносных программ
4. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.
5. Способы совершения компьютерных преступлений.
6. Предупреждение компьютерных преступлений.
7. Методика и практика расследования преступлений в сфере компьютерной информации.

Тема 8. Правовое регулирование оперативно-розыскных мероприятий (ОРМ) в оперативно-розыскной (ОРД) и частной детективной и охранной деятельности (ЧДОД) (ПК-19)

Лекция.

Федеральный закон "Об оперативно-розыскной деятельности", правовые акты общего назначения, правовые акты общего назначения и другие подзаконные акты регулирующие ОРД, Закон РФ "О частной детективной и охранной деятельности в Российской Федерации".

Лабораторные работы.

Не предусмотрено

Задания для самостоятельной работы.

1. Понятие и сущность оперативно-розыскной деятельности.
2. Задачи, решаемые в процессе осуществления оперативно-розыскной деятельности.
3. Понятие, роль и значение правового регулирования оперативно-розыскной деятельности.
4. Система и классификация правовых норм, регулирующих оперативно-розыскную деятельность.
5. Виды органов, осуществляющих оперативно-розыскную деятельность, их компетенция.

6. Лица, участвующие в оперативно-розыскной деятельности, их социальная и правовая защита.
7. Содержание и значение оперативно-розыскных мероприятий.
8. Основания и условия осуществления оперативно-розыскных мероприятий.
9. Роль и значение соблюдения прав и свобод человека в процессе оперативно-розыскной деятельности.

Тема 9. Международное законодательство в области защиты информации (ПК-19)

Лекция.

Международные правовые акты общего и специального назначения. Сравнение объёма правовых актов и подходов к построению правовых основ защиты информации. Выполнение профессиональных задач в соответствии с нормами морали, профессиональной этики и служебного этикета.

Лабораторные работы.

Не предусмотрено

Задания для самостоятельной работы.

1. Ответьте на вопросы:

Основными направлениями международного сотрудничества в области обеспечения информационной безопасности является?

Цель Федерального закона «Об участии в международном информационном обмене» является?

2. Заполните таблицу:

Зарубежное законодательство

Область применения нормативного акта

США: «Закон об информационной безопасности»

Computer Security Act of 1987

США: «Закон о совершенствовании информационной безопасности»

Computer Security Enhancement Act of 1997 & 2001

ФРГ: «Закон о защите данных» Federal Data Protection Act of 1990 & 1994

Великобритания: Семейство добровольных стандартов программ безопасности BS7799

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

4 семестр

- посещаемость – 8 баллов
- текущий контроль – 42 балла
- контрольные срезы – 2 среза по 10 баллов каждый
- премиальные баллы – 17 баллов
- ответ на экзамене: не более 30 баллов

Распределение баллов по заданиям:

№ те мы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки

1.	Информация как объект правового регулирования	Тестирование	6	Тест состоит из вопросов с выбором ответа. 4-6 баллов - студент правильно отвечает более чем на 90% вопросов. 3 балла – студент правильно отвечает на 50-80% вопросов в тесте. 2 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
2.	Законодательство РФ в области информационной безопасности	Тестирование	6	Тест состоит из вопросов с выбором ответа. 4-6 баллов - студент правильно отвечает более чем на 90% вопросов. 3 балла – студент правильно отвечает на 50-80% вопросов в тесте. 2 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
3.	Правовой режим защиты государственной тайны	Тестирование	6	Тест состоит из вопросов с выбором ответа. 4-6 баллов - студент правильно отвечает более чем на 90% вопросов. 3 балла – студент правильно отвечает на 50-80% вопросов в тесте. 2 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
4.	Правовые режимы защиты конфиденциальной информации	Тестирование(контрольный срез)	10	Тест состоит из вопросов с выбором ответа. 10 баллов - студент правильно отвечает более чем на 90% вопросов. 7-9 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 4-6 баллов - студент правильно отвечает на 30-50% вопросов. 1-2 балла - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
5.	Лицензирование и сертификация в информационной сфере	Тестирование	6	Тест состоит из вопросов с выбором ответа. 4-6 баллов - студент правильно отвечает более чем на 90% вопросов. 3 балла – студент правильно отвечает на 50-80% вопросов в тесте. 2 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
6.	Защита интеллектуальной собственности	Тестирование	6	Тест состоит из вопросов с выбором ответа. 4-6 баллов - студент правильно отвечает более чем на 90% вопросов. 3 балла – студент правильно отвечает на 50-80% вопросов в тесте. 2 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
7.	Компьютерные правонарушения	Тестирование	6	Тест состоит из вопросов с выбором ответа. 4-6 баллов - студент правильно отвечает более чем на 90% вопросов. 3 балла – студент правильно отвечает на 50-80% вопросов в тесте. 2 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.

8.	Правовое регулирование оперативно-розыскных мероприятий (ОРМ) в оперативно-розыскной (ОРД) и частной детективной и охранной деятельности (ЧДОД)	Тестирование(контрольный срез)	10	Тест состоит из вопросов с выбором ответа. 7-10 баллов - студент правильно отвечает более чем на 90% вопросов. 4-6 баллов – студент правильно отвечает на 50-80% вопросов в тесте. 2-3 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
9.	Международное законодательство в области защиты информации	Тестирование	6	Тест состоит из вопросов с выбором ответа. 4-6 баллов - студент правильно отвечает более чем на 90% вопросов. 3 балла – студент правильно отвечает на 50-80% вопросов в тесте. 2 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
10.	Посещаемость		8	8 баллов – стопроцентное посещение занятий студентом 5-7 баллов – посещаемость студента составляет не менее 80 % занятий 3-4 баллов – посещаемость студента составляет не менее 50 % занятий 1-2 балла – посещаемость студента составляет не менее 25 % занятий
11.	Премиальные баллы		17	Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 17 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 17 баллов; - участие в выставке по тематике изучаемой дисциплины – 17 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20

12.	Ответ на экзамене	30	<p>Оценка «удовлетворительно»- студент имеет достаточный минимальный объем знаний по дисциплине; студентом усвоена основная литература, рекомендованная учебной программой; студент умеет ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; студент умеет делать выводы без существенных ошибок;</p> <p>Оценка «хорошо» – «достаточно полные и систематизированные знания по дисциплине;» умение ориентироваться в основном теориях, концепциях и направлениях дисциплины и давать им критическую оценку; использование научной терминологии, лингвистически и логически правильное изложение ответа на вопросы, умение делать обоснованные выводы; владение инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач; усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; средний уровень сформированности заявленных в рабочей программе компетенций.</p> <p>- Оценка «отлично» – систематизированные и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; точное использование научной терминологии систематически грамотное и логически правильное изложение ответа на вопросы; безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; выраженная способность самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; полное и глубокое усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; умение ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин; творческая самостоятельная работа; активное участие в групповых обсуждениях.</p>
13.	Итого за семестр	100	

Итоговая оценка по экзамену выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
85 - 100 баллов	Отлично
70 - 84 баллов	Хорошо
50 - 69 баллов	Удовлетворительно
Менее 50	Неудовлетворительно

4.2 Типовые оценочные средства текущего контроля

Тестирование

Тема 1. Информация как объект правового регулирования

1. В системе права информация делится на:

а) нормативную;

- b) **ненормативную;**
 - c) **законодательную.**
2. По категориям доступа информация делится:
- a) открытую информацию и государственную тайну;
 - b) конфиденциальную информацию и информацию свободного доступа;
 - c) информацию с ограниченным доступом и общедоступную информацию.
3. Какая информация подлежит защите?
- a) информация, циркулирующая в системах и сетях связи;
 - b) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
 - c) только информация, составляющая государственные информационные ресурсы;
 - d) любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.
4. Какой из нижеперечисленных законодательных актов обладает наибольшей юридической силой, в вопросах информационного права:
- a) Указ президента "об утверждении перечня сведений, относящихся к государственной тайне";
 - b) Постановления Правительства РФ;
 - c) закон "об информации, информатизации и защите информации";
 - d) **Конституция.**
5. Из каких компонентов состоит право собственности информации как продукта:
- a) **право распоряжения;**
 - b) **право владения и пользования;**
 - c) право распоряжения и владения.
6. Принципы информационного права базируются на:
- a) **Конституции РФ;**
 - b) **Федеральных законах и других нормативных актах;**
 - c) Конституции РФ; и ФЗ «Об информации, информатизации и защите информации»;
 - d) Указов Президента РФ.
7. Информационное право это наука:
- a) **о предметах, принципах и методах правового регулирования деятельности и отношений в областях формирования и использования информационных ресурсов, технологий и коммуникаций и их сетей;**
 - b) **организации управления процессами информатизации и обеспечения информационной безопасности граждан, государства и общества в целях удовлетворения их информационных потребностей и обеспечения процессов развития общества;**
 - c) организации управления процессами информатизации и обеспечения информационной безопасности граждан.

Тема 2. Законодательство РФ в области информационной безопасности

1. Отношения, связанные с обработкой персональных данных, регулируются законом...
- a) Федеральным законом «О персональных данных»;
 - b) «Об информации, информационных технологиях»;
 - v) Федеральным законом «О конфиденциальной информации»;
 - г) «О защите информации».

2. Какую ответственность влечет нарушение Федерального закона "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ?

- а) гражданскую ответственность;
- б) дисциплинарная, гражданско-правовая, административная или уголовная ответственность в соответствии с законодательством Российской Федерации;
- в) нет никакого наказания;
- г) административная или уголовная ответственность;
- д) гражданско-правовая.

3. Электронно-цифровая подпись – это...

- а) такой подписи не бывает т.к. подлинность документа заверяется личной подписью руководителя организации и печатью;
- б) отсканированная подпись руководителя организации и помещенная в электронный документ для заверения подлинности данного документа;
- в) реквизит электронного документа, предназначенный для защиты данного документа от подделки, позволяющий идентифицировать владельца, а также установить отсутствие искажения информации в электронном документе;
- г) электронный ключ, предназначенный для заверения подлинности данного документа.

4. Какой из типов нормативно-правовых документов регламентирует Информационную безопасность в Российской Федерации?

- а) акты федерального законодательства;
- б) нормативно-методические документы государственных органов;
- в) стандарты информационной безопасности;
- г) все выше перечисленные.

5. Определены принципы и условия обработки персональных данных. Что не входит в эти принципы?

- а) общий запрет на обработку персональных данных без согласия субъекта персональных данных;
- б) обязанность операторов и третьих лиц, получивших доступ к персональным данным, обеспечивать их общедоступность;
- в) обязанность операторов и третьих лиц, получивших доступ к персональным данным, обеспечивать их конфиденциальность;
- г) право субъекта персональных данных на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

6. Система защиты государственных секретов определяется Законом

- а) "Об информации, информатизации и защите информации";
- б) "Об органах ФСБ";
- в) "О государственной тайне";
- г) "О безопасности".

7. Система защиты государственных секретов

- а) основывается на Уголовном Кодексе РФ;
- б) регулируется секретными нормативными документами;
- в) определена Законом РФ "О государственной тайне";
- г) осуществляется в соответствии с Конституцией РФ.

8. Действие Закона "О государственной тайне" распространяется

- а) на всех граждан и должностных лиц РФ;
- б) только на должностных лиц;
- в) на граждан, которые взяли на себя обязательство выполнять требования законодательства о государственной тайне;
- г) на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения.

9. Какой документ в РФ закладывает основы информационной политики государства?

- а) Гражданский кодекс РФ;

б) Доктрина информационной безопасности;

в) Конституция РФ;

г) закон «О защите данных».

10. Какой термин определяет фактические расходы, понесенные субъектом в результате нарушения его прав, утраты или повреждения имущества, а также расходы, которые он должен будет произвести для восстановления нарушенного права и стоимости поврежденного или утраченного имущества?

а) угроза;

б) риск;

в) ущерб;

г) утрата.

11. Внешние источники угроз информационной безопасности Российской Федерации...

а) увеличение технологического отрыва ведущих стран мира, их противодействие созданию конкурентоспособных информационных технологий;

б) недостаточное финансирование мероприятий по обеспечению информационной безопасности РФ;

в) недостаточная экономическая мощь государства;

г) обострение международной конкуренции за обладание информационными технологиями и ресурсами.

12. Ответственность за преступления против компьютерной безопасности наступает с ... лет.

а) 14

б) 16

в) 18

г) 21

13. Внутренние источники угроз информационной безопасности Российской Федерации...

а) снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

б) недостаточный государственный контроль за развитием информационного рынка;

в) разработка рядом государств концепции информационных войн;

г) стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынков.

14. Какой нормативно-правовой документ определяет перечень объектов информационной безопасности личности, общества, государства и методы ее обеспечения?

а) Уголовный кодекс РФ;

б) Гражданский кодекс РФ;

в) Указ Президента РФ №260;

г) Доктрина информационной безопасности РФ.

15. Какие правовые документы решают вопросы информационной безопасности?

а) Уголовный кодекс РФ;

б) Конституция РФ;

в) Закон "Об информации, информатизации и защите информации";

г) Закон РФ "О государственной тайне";

д) Закон РФ "О коммерческой тайне";

е) Закон РФ "О лицензировании отдельных видов деятельности";

з) Закон РФ "Об электронной цифровой подписи";

и) все вышеперечисленное.

Тема 3. Правовой режим защиты государственной тайны

1. Государственную тайну составляют сведения ...

а) в области образования, в области экономики, науки и техники

- б) в военной области, в области экономики, науки и техники, в области внешней политики и экономики, сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности
- с) в области здравоохранения, в области внешней политики и экономики
- д) в области учета населения, в военной области, в области разведывательной, контрразведывательной и оперативно-розыскной деятельности

2. К органам защиты государственной тайны относятся:

- а) федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, федеральный орган исполнительной власти, уполномоченный в области обороны, федеральный орган исполнительной власти, уполномоченный в области внешней разведки, федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, и их территориальные органы;
- б) органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны;
- с) Правительство Российской Федерации;
- д) Межведомственная комиссия по защите государственной тайны.

3. Степень секретности сведений зависит от ...

- а) объема предоставленных сведений
- б) органов, имеющих эти сведения
- с) степени ущерба, нанесенного конкретным лицам
- д) тяжести ущерба, который может быть нанесен государству

4. На кого возлагается ответственность за обеспечение режима секретности, разработку и осуществления необходимых мероприятий по защите сведений, составляющих государственную тайну в организации?

- а) начальника отдела кадров
- б) начальника секретного отдела
- с) руководителя организации
- д) заместителя руководителя организации по секретному делопроизводству

5. Принципы отнесения сведений к государственной тайне

- а) законности, обоснованности и своевременности
- б) законности и своевременности
- с) обоснованности и своевременности

6. К сведениям, не подлежащим к засекречиванию, относятся:

- а) о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях; о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности; о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- б) о фактах нарушения прав и свобод человека и гражданина; о размерах золотого запаса и государственных валютных резервах Российской Федерации; о состоянии здоровья высших должностных лиц Российской Федерации; о фактах нарушения законности органами государственной власти и их должностными лицами.
- с) о чрезвычайных происшествиях и катастрофах, о фактах нарушения прав и свобод человека и гражданина, а также о стихийных бедствиях, демографии

7. Выберите степени секретности сведений, составляющих государственную тайну, в соответствии с законом РФ от 21.07.1993 №5485-1:

- a) "особой важности", "совершенно секретно" и "секретно".
- b) "особо секретно", "совершенно секретно" и "секретно".
- c) "особой важности", "абсолютно секретно" и "важно".
- d) "особой важности", "абсолютно секретно" и "секретно".

8. Перечень сведений, отнесенных к государственной тайне формирует:

- a) Президент Российской Федерации.
- b) Межведомственная комиссия.
- c)) Правительство Российской Федерации.
- d) Органов государственной власти.

9. Должностные лица, наделенные в порядке, предусмотренном законом полномочиями по отнесению сведений к государственной тайне, вправе:

- a) обращаться в территориальные органы ФСБ по засекречиванию информации, находящейся в собственности.
- b) обращаться в Межведомственную комиссии по засекречиванию информации, находящейся в собственности.
- c) принимать решения о засекречивании информации, находящейся в собственности.
- d) обращаться в Органы государственной власти по засекречиванию информации, находящейся в собственности.

10. В течении какого срока принимается решение о дополнении (изменении) перечня:

- a) в течении 5 месяцев.
- b) в течении 6 месяцев.
- c) в течении 3 месяцев.
- d) в течении года.

11. На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные:

- a) об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя, о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.
- b) о регистрационном номере;
- c) об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя, о дате или условии рассекречивания сведений либо о событии, после наступления которого, сведения будут рассекречены, о регистрационном номере.
- d) об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя, о регистрационном номере.

12. Основаниями для рассекречивания сведений являются:

- a) изменение объективных обстоятельств.
- b) взятие на себя Российской Федерацией международных обязательств по открытому обмену.
- c) обращение в Межведомственную комиссию.
- d) обращение в территориальные органы ФСБ.

13. В течении которого времени необходимо пересматривать содержание действующих в органах государственной власти, на предприятиях, в учреждениях и организациях перечней сведений, подлежащих засекречиванию:

- a) в течении 5 месяцев.
- b) в течении 6 месяцев.
- c) в течении 3 месяцев.
- d) в течении года.

14. Допуск должностных лиц и граждан к государственной тайне предусматривает:

- а) принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну, согласие на частичные, временные ограничения их прав;
- б) письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий, ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;
- в) отсутствие родственников за границей, принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну;
- г) принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну.

15. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне:

- а) постоянное проживание его самого и (или) его близких родственников за границей или включение его в список физических лиц, выполняющих функции иностранного агента, ;
- б) признание его недееспособным, наличие медицинских противопоказаний;
- в) уклонение его от проверочных мероприятий и (или) сообщение им заведомо ложных анкетных данных;
- г) постоянное проживание его самого и (или) его близких родственников за границей.

16. Должностные лица и граждане, виновные в нарушении законодательства Российской Федерации о государственной тайне, несут:

- а) только уголовную;
- б) только гражданско-правовую;
- в) административную, дисциплинарную;
- г) уголовную, гражданско-правовую.

17. Основанием для допуска предприятий, учреждений и организаций является:

- а) лицензии;
- б) аттестата соответствия;
- в) наличие соответствующих специалистов;
- г) наличие сертифицированных средств защиты.

18. На кого возлагается сертификация средств защиты информации РФ:

- а) ФСБ;
- б) Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области обороны, в соответствии с функциями, возложенными на них законодательством Российской Федерации;
- в) Министерство обороны;
- г) ФСТЭК

19. Процедура оформления прав граждан на получение сведений, составляющих государственную тайну, называется:

- а) рассекречивание
- б) доступ
- в) пропуск
- г) допуск

20. Решение о передаче сведений, составляющих государственную тайну, другому государству принимает ...

- а) Правительство РФ
- б) Федеральная служба безопасности РФ
- в) Президент РФ

d) орган местного самоуправления

21. В особом порядке (без проведения проверочных мероприятий) допускаются к государственной тайне ...

- a) члены Совета Федерации, депутаты Государственной Думы, судьи, адвокаты, участвующие в судебном процессе, связанном с государственной тайной
- b) Президент РФ
- c) послы России за рубежом
- d) члены Правительства РФ

22. Контроль за обеспечением защиты государственной тайны осуществляет...

- a) уполномоченными федеральными органами исполнительной власти;
- b) Федеральная служба безопасности РФ;
- c) Государственная Дума РФ и Президент РФ;
- d) Президент РФ и Правительство РФ.

Тема 4. Правовые режимы защиты конфиденциальной информации

1. Конфиденциальная информация это

- a) сведения, составляющие государственную тайну
- b) сведения о состоянии здоровья высших должностных лиц
- c) документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ
- d) данные о состоянии преступности в стране

2. К конфиденциальной информации относятся документы, содержащие

- a) государственную тайну
- b) законодательные акты
- c) "ноу-хау"
- d) сведения о золотом запасе страны

3. Какая информация подлежит защите?

- a) информация, циркулирующая в системах и сетях связи
- b) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать
- c) только информация, составляющая государственные информационные ресурсы
- d) любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу

4. К коммерческой тайне могут быть отнесены

- a) сведения не являющиеся государственными секретами
- b) сведения, связанные с производством и технологической информацией
- c) сведения, связанные с управлением и финансами
- d) сведения, перечисленные в остальных пунктах

5. Действие Закона "О государственной тайне" распространяется

- a) на всех граждан и должностных лиц РФ
- b) только на должностных лиц
- c) на граждан, которые взяли на себя обязательство выполнять требования законодательства о государственной тайне
- d) на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения

6. Отношения, связанные с обработкой персональных данных, регулируются законом...

- a) «Об информации, информационных технологиях»

- б) «О защите информации»
- с) Федеральным законом «О персональных данных»
- д) Федеральным законом «О конфиденциальной информации»
- е) «Об утверждении перечня сведений конфиденциального характера»

Тема 5. Лицензирование и сертификация в информационной сфере

1. Положение «О лицензировании деятельности по технической защите конфиденциальной информации» (Постановление Правительства РФ от 03.02.2012 №79) определяет:
 - а) порядок лицензирования деятельности по программно-аппаратной защите конфиденциальной, осуществляемой юридическими лицами и индивидуальными предпринимателями;
 - б) порядок лицензирования деятельности по технической защите конфиденциальной, осуществляемой юридическими лицами и индивидуальными предпринимателями;
 - с) порядок лицензирования деятельности по инженерно-технической защите конфиденциальной, осуществляемой юридическими лицами и индивидуальными предпринимателями.
2. Под технической защитой конфиденциальной информации понимается выполнение работ и (или) оказание услуг по защите от:
 - а) несанкционированного доступа;
 - б) от утечки по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к информации;
 - с) уничтожения, искажения или блокирования доступа к информации.
3. Лицензирование деятельности по технической защите конфиденциальной информации (далее - лицензируемый вид деятельности) осуществляет:
 - а) Министерство обороны;
 - б) Межведомственная комиссия;
 - с) ФСТЭК России.
4. Виды лицензий ФСТЭК:
 - а) на техзащиту конфиденциальной информации;
 - б) на разработку и производство средств защиты конфиденциальной информации;
 - с) на охрану гостайны в части техзащиты данных и по части сопротивления разведкам;
 - д) на разработку документов на охрану гостайны.
5. Лицензия востребована организациям, которые:
 - а) следят за безопасностью секретных сведений и исключают и контролируют их утечку, и исключают незаконный допуск к ним;
 - б) проводят мониторинг ИБ, аттестацию по нормам ИБ, занимаются проектированием зданий для работы с секретными данными;
 - с) занимаются сборкой, настройкой, починкой средств защиты информации (СЗИ), разрабатывают и производят СЗИ;
 - д) обрабатывают, хранят и передают информацию Пд;
 - е) защищают гостайны в части техзащиты данных и по части сопротивления разведкам;
 - ф) исключают, контролируют утечку Пд.
6. Срок получения лицензии:
 - а) 2 месяца;
 - б) от 2 -6 месяцев
 - с) от 1,5-2 года.
7. Сертификация ФСТЭК это процедура получения документа подтверждающего, что средства защиты информации:
 - а) соответствует требованиям нормативно-методических документов ФСТЭК;
 - б) соответствует законодательству РФ;
 - с) соответствует нормативно-методических документов в сфере ИБ РФ.

8. Сферы деятельности с обязательной сертификацией средств защиты информации:
 - a) государственные информационные системы (гис), государственная тайна (ЗГТ);
 - b) автоматизированные системы управления технологическим процессом (асу тп);
 - c) персональные данные (ЗПДн), конфиденциальная информация (служебная информация критическая информационная инфраструктура (КИИ));
 - d) государственные и муниципальные информационные системы.
9. Сертификат соответствия это:
 - a) совокупность правил выполнения работ по сертификации, её участников и правил функционирования системы в целом;
 - b) документ, удостоверяющий, что сертифицированная продукция (процесс) соответствует установленным требованиям технических регламентов, положениям стандартов или условиям договора;
 - c) деятельность, связанная с прямым или косвенным определением того, что соответствующие требования к объекту выполняются;
 - d) процедура, результатом которой является документальное удостоверение того, что продукция, процессы соответствуют установленным требованиям технических регламентов или стандартов, условиям договоров.
10. Нарушение условий, предусмотренных лицензией, на осуществление деятельности в области защиты конфиденциальной информации влечет:
 - a) уголовную ответственность;
 - b) гражданско-правовую ответственность;
 - c) административную- ответственность.
11. Добровольная сертификация:
 - a) способствует завоеванию места на рынке;
 - b) официальное признание компетентности физического или юридического лица выполнять работы в определённой области;
 - c) даёт право допуска продукции на рынок.
12. Знак соответствия – это знак, информирующий потребителя о соответствии продукции (услуги) требованиям:
 - a) систем добровольной сертификации;
 - b) договора на поставку;
 - c) национальных стандартов;
 - d) технических регламентов.

Тема 6. Защита интеллектуальной собственности

1. К объектам интеллектуальной собственности относятся:
 - a) селекционные достижения;
 - б) товары и услуги;
 - в) произведения прикладного искусства;
 - г) секреты производства (ноу-хау);
 - д) фонограммы;
 - е) фирменные наименования;
 - ж) логотипы;
 - з) юридические лица;
 - и) музыкальные произведения.
2. Правовая охрана каких объектов интеллектуальной собственности возникает в силу факта их создания:
 - a) литературных произведений;
 - б) изобретений;
 - в) компьютерных программ;

- г)фотографий;
- д)промышленных образцов;
- е)музыкальных произведений.

3.Правовая охрана каких объектов интеллектуальной собственности возникает вследствие предоставления правовой охраны уполномоченным государственным органом:

- а)товарных знаков и знаков обслуживания;
- б)секретов производства (ноу-хау);
- в)селекционных достижений;
- г)изобретений;
- д)полезных моделей;
- е)литературных произведений;
- ж)промышленных образцов.

4.Результат интеллектуальной деятельности может одновременно использоваться:

- а)одним лицом;
- б)группой лиц до 10 человек;
- в)группой лиц более 10 человек;
- г)неограниченным кругом лиц.

5.Какой из объектов не является объектом интеллектуальной собственности:

- а)селекционное достижение;
- б)предприятие как имущественный комплекс;
- в)секрет производства (ноу-хау);
- г)фонограмма;
- д)товарный знак.

6.В рамках права интеллектуальной собственности можно выделить следующие институты:

- а)авторского права и смежных прав;
- б)патентного права;
- в)наследственного права;
- г)обязательственного права;
- д)средств индивидуализации участников гражданского оборота и е)произведенной ими продукции (работ, услуг);+
- ж)охраны нетрадиционных объектов интеллектуальной собственности.

7.Нормами института авторского права и смежных прав регулируются:

- а)имущественные, а также связанные с ними личные неимущественные отношения, возникающие в связи с созданием, правовой охраной и использованием изобретений, полезных моделей и промышленных образцов;
- б)имущественные и личные неимущественные отношения, связанные с созданием, правовой охраной и использованием топологий интегральных микросхем, рационализаторских предложений;
- в)отношения, связанные с регистрацией, правовой охраной и использованием исключительных прав на фирменные наименования, товарные знаки, знаки обслуживания, а также географические указания;
- г)отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства, исполнений, фонограмм, передач организаций эфирного и кабельного вещания.

8.Нормами института патентного права регулируются:

- а)имущественные, а также связанные с ними личные неимущественные отношения, возникающие в связи с созданием, правовой охраной и б)использованием изобретений, полезных моделей и промышленных образцов;
- в)имущественные и личные неимущественные отношения, связанные с созданием, правовой охраной и использованием топологий интегральных микросхем, рационализаторских предложений;

г) отношения, связанные с регистрацией, правовой охраной и использованием исключительных прав на фирменные наименования, товарные знаки, знаки обслуживания, а также географические указания;

д) отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства, исполнений, фонограмм, передач организаций эфирного и кабельного вещания.

9. Нормами института средств индивидуализации участников гражданского оборота, товаров (работ, услуг) регулируются:

а) имущественные, а также связанные с ними личные неимущественные отношения, возникающие в связи с созданием, правовой охраной и использованием изобретений, полезных моделей и промышленных образцов;

б) имущественные и личные неимущественные отношения, связанные с созданием, правовой охраной и использованием топологий интегральных микросхем, рационализаторских предложений;

в) отношения, связанные с регистрацией, правовой охраной и использованием исключительных прав на фирменные наименования, товарные знаки, знаки обслуживания, а также географические указания;

г) отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства, исполнений, фонограмм, передач организаций эфирного и кабельного вещания.

10. Нормами института охраны нетрадиционных объектов интеллектуальной собственности регулируются:

а) имущественные, а также связанные с ними личные неимущественные отношения, возникающие в связи с созданием, правовой охраной и использованием изобретений, полезных моделей и промышленных образцов;

б) имущественные и личные неимущественные отношения, связанные с созданием, правовой охраной и использованием топологий интегральных микросхем, рационализаторских предложений;

в) отношения, связанные с регистрацией, правовой охраной и использованием исключительных прав на фирменные наименования, товарные знаки, знаки обслуживания, а также географические указания;

г) отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства, исполнений, фонограмм, передач организаций эфирного и кабельного вещания.

11. Какие права субъектов интеллектуальной собственности охраняются бессрочно:

а) имущественные права;

б) личные неимущественные права;

в) как имущественные, так и личные неимущественные права.

13. К объектам смежных прав относятся:

а) произведения, созданные двумя и более авторами;

б) перевод;

в) исполнение;

г) курсовая работа;

д) реферат;

е) фонограмма.

14. К объектам права промышленной собственности относятся:

а) чертежи;

б) изобретения;

в) компьютерные программы;

г) предприятия;

д) научные статьи;

е) селекционные достижения;

ж) монографии;

з) промышленные образцы;

и) полезные модели;

к) товары, работы, услуги;

- л) товарные знаки;
- м) секреты производства;
- н) юридические лица;
- о) дипломные работы;
- п) идеи;
- р) знаки обслуживания.

15. К объектам авторского права относятся:

- а) новые сорта растений;
- б) музыкальные произведения;
- в) товарные знаки;
- г) базы данных;
- д) идеи, концепции, открытия;
- е) монографии;
- ж) научные статьи.

16. Какой из объектов охраняется правом интеллектуальной собственности:

- а) недвижимое имущество;
- б) идея;
- в) герб;
- г) товарный знак;
- д) открытие.

17. Выберите объект, правовая охрана которого удостоверяется патентом:

- а) картина;
- б) песня;
- в) изобретение;
- г) товар;
- д) курсовая работа.

18. Для правовой охраны каких объектов не требуется получение патента:

- а) картина;
- б) селекционное достижение;
- в) изобретение;
- г) промышленный образец;
- д) произведение архитектуры;
- е) новый сорт растения;
- ж) дипломная работа.

18. Согласно ст. 132 ГК РФ интеллектуальная собственность это-

- а) информация, полученная в результате интеллектуальной деятельности индивида;
- б) литературные, художественные и научные произведения;
- в) изобретения, открытия, промышленные образцы и товарные знаки;
- г) исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности.

19. Интеллектуальная собственность включает права, относящиеся к:

- а) литературным, художественным и научным произведениям, изобретениям и открытиям;
- б) исполнительской деятельности артиста, звукозаписи, радио- и телепередачам;
- в) промышленным образцам, товарным знакам, знакам обслуживания, фирменным наименованиям и коммерческим обозначениям;
- г) всему, указанному в остальных пунктах.

Тема 7. Компьютерные правонарушения

- 1) Компьютерные правонарушения – это...

- а) нарушение работы ЭВМ, системы ЭВМ или их сети, использование либо распространение вредоносных программ или машинописных носителей с такими программами
- б) разработка и распространение компьютерных вирусов
- в) деяние совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения в области IT
- г) предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных

2) Что понимается под архитектурой безопасности?

- а) информационное пространство, основанное на новейших достижениях электронно-вычислительной техники
- б) комплексное рассмотрение и решение вопросов безопасности информации в компьютерных системах и сетях
- в) система доступа по категориям персонала к конфиденциальной документации
- г) строение системы защиты информации от несанкционированного доступа

3) В архитектуре безопасности выделяются ... (несколько вариантов)

- а) угрозы безопасности
- б) защищаемые ресурсы
- в) службы безопасности
- г) механизм обеспечения безопасности
- д) доступ к информационным ресурсам

4) Под угрозой безопасности понимается ...

- а) действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов сети, включая хранимую, обрабатываемую информацию, а также программные и аппаратные средства
- б) непосредственный несанкционированный доступ к информационным ресурсам автоматизированных информационных систем путем использования уже имеющихся или же дополнительных собственных терминалов пользователей и принятых в данной системе паролей, коды которых удалось получить тем или иным способом
- в) нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации
- г) действие или событие, направленное на нарушение законодательства в IT-сфере

5) Угрозы безопасности подразделяются на ...

- а) активные и пассивные
- б) незначительные и серьёзные
- в) случайные и умышленные
- г) локальные и глобальные

6) Задача пассивных угроз - ...

- а) несанкционированно получить информацию
- б) нарушить архитектуру безопасности
- в) нарушать нормальный процесс функционирования сетей путем разрушения или радиоэлектронного подавления линий, сетей, вывода из строя компьютеров, искажения баз данных
- г) вмешательство в работу компьютера

7) Активные угрозы преследуют цель ...

- а) несанкционированно получать информацию
- б) нарушать архитектуру безопасности
- в) нарушать нормальный процесс функционирования сетей путем разрушения или радиоэлектронного подавления линий, сетей, вывода из строя компьютеров, искажения баз данных
- г) вмешательство в работу компьютера

8) Основные угрозы безопасности (несколько вариантов):

- а) раскрытие конфиденциальной информации +

- б) компрометация информации +
 - в) ошибочные действия пользователей
 - г) несанкционированное использование ресурсов систем и сетей +
 - д) отказ от передачи информации
- 9) Компьютерные преступления можно подразделить на категории (несколько вариантов):
- а) преступления, использующие компьютеры как необходимые технические средства
 - б) преступления, направленные на несанкционированный доступ к информации в компьютере
 - в) преступления, использующие пользователей для доступа к компьютеру
 - г) преступления, связанные с вмешательством в работу компьютеров
- 10) Виды компьютерных преступлений, связанные с вмешательством в работу компьютеров (несколько вариантов):
- а) несанкционированный доступ к информации, хранящейся в компьютере
 - б) разработка и распространение компьютерных вирусов
 - в) преступная небрежность
 - г) разработка сложных математических моделей, входными данными, в которых являются возможные условия проведения преступления, а выходными данными - рекомендации по выбору оптимального варианта действий преступника
 - д) подделка компьютерной информации
 - е) хищение компьютерной информации
- 11) К компьютерным преступлениям, использующие компьютеры как необходимые технические средства (компьютер является "средством" достижения цели), относится:
- а) разработка и распространение компьютерных вирусов
 - б) преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям
 - в) разработка сложных математических моделей, входными данными, в которых являются возможные условия проведения преступления, а выходными данными - рекомендации по выбору оптимального варианта действий преступника
 - г) хищение компьютерной информации

Тема 8. Правовое регулирование оперативно-розыскных мероприятий (ОРМ) в оперативно-розыскной (ОРД) и частной детективной и охранной деятельности (ЧДОД)

1. На кого распространяется социальная и правовая защита в соответствии с ФЗ «Об ОРД»?

Варианты ответа:

- на всех субъектов ОРД
- (+) на всех участников ОРД
- только на должностных лиц оперативно-розыскных органов
- только на лиц, оказывающих содействие оперативно-розыскным органам

2. Укажите субъект организации и ведения криминалистической (уголовной) регистрации:

(+) ОВД

- ФСБ
- прокуратура
- ФСКН

3. Среди перечисленных выберите органы, не осуществляющие ОРД:

- МВД
- ФСБ
- (+) МЧС
- ФСИН
- (+) прокуратура
- ФСКН
- (+) ФССП

- все перечисленные органы могут осуществлять ОРД

4. Укажите оперативно-розыскные мероприятия, для проведения которых требуется судебное решение:

- исследование предметов и документов
- (+) прослушивание телефонных переговоров
- проверочная закупка
- контролируемая поставка

5. Укажите оперативно-розыскные мероприятия, при проведении которых сотрудники оперативно-технических подразделений не принимают участие:

- наблюдение
- (+) отождествление личности
- (+) проверочная закупка
- прослушивание телефонных переговоров

6. Укажите основания получения органами внутренних дел РФ в случае необходимости проверки за рубежом фирм, филиалов, совместных предприятий и других коммерческих структур, зарегистрированных за рубежом, интересующей их информации из Генерального секретариата Интерпола или НЦБ Интерпола зарубежных государств?

- профилактика преступной деятельности коммерческих структур, расположенных за рубежом
- (+) возбужденное уголовное дело о преступной деятельности сотрудников таких коммерческих структур
- наличие оперативной или иной информации о незаконной деятельности сотрудников фирм

7. Представление результатов ОРД органу дознания, следователю или в суд осуществляется на основании:

- постановления оперуполномоченного
- (+) постановления руководителя органа, осуществляющего ОРД
- постановления прокурора

8. Является ли сравнительное исследование оперативно-розыскным мероприятием?

- да
- (+) нет

9. Укажите основания продления срока проведения ОРМ, затрагивающего конституционные права и свободы граждан?

- письменное указание прокурора
- (+) постановление судьи
- постановление руководителя оперативно-розыскного органа
- постановление вышестоящего должностного лица оперативно-розыскного органа

10. Укажите основные направления деятельности Интерпола:

- (+) международный розыск
- розыск лиц, пропавших без вести
- розыск похищенных предметов
- расследование международных преступлений

11. К сведениям, отнесенным ФЗ «Об оперативно-розыскной деятельности» к государственной тайне относятся:

- сведения о сотрудниках оперативно-розыскных органов
- (+) сведения о лицах, оказывающих содействие на конфиденциальной основе
- (+) сведения об организации и тактике проведения ОРМ
- все ответы правильные

12. ОРД это вид деятельности (ст.1 ФЗ «Об ОРД»):

- Осуществляемый в целях обеспечения деятельности правоохранительных органов.
- Осуществляемый только негласно.
- (+)Осуществляемый посредством ОРМ.

-Осуществляемый в целях выявления и раскрытия преступлений.

-Осуществляемый только гласно.

13. Кем осуществляется ОРД?

-Работниками прокуратуры.

-Сотрудниками организаций, имеющих лицензию на осуществление частной охранной и детективной деятельности.

-Военнослужащими внутренних войск.

(+)Сотрудниками оперативных подразделений органов, осуществляющих ОРД.

-Сотрудниками оперативных подразделений налоговой полиции.

14. ОРД основывается на следующем конституционном принципе, определенном в ст.3 ФЗ «Об ОРД»:

- Принцип гласности.

-Принцип поступательности и высокой оперативной готовности.

(+)Принцип законности.

-Принцип конспирации.

-Принцип плановости.

15. ОРД осуществляется в полном объеме:

-Сотрудниками частных охранных предприятий.

(+)Сотрудниками оперативных подразделений федеральных органов государственной охраны.

-Сотрудниками оперативного подразделения органа внешней разведки МО РФ,

-Сотрудниками оперативных подразделений пограничной службы РФ.

16. Задачей ОРД, согласно ст. 2 ФЗ «Об ОРД» является:

(+)Розыск лиц скрывающихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания.

-Обнаружение неопознанных трупов, а также розыска без вести пропавших.

-Выявление и установление лиц, обладающих информацией о событиях или действиях создающих угрозу государственной безопасности РФ.

-Обеспечение деятельности политических партий.

-Обеспечение социальной и правовой защиты должностных лиц органов, осуществляющих ОРД, а также лиц, оказывающих им конфиденциальное содействие, в том числе по контракту.

17. Согласно ст.3. ФЗ «Об ОРД» принципом ОРД является:

-Принцип гуманности.

-Принцип плановости.

-Принцип неотвратимости ответственности за совершенное преступление.

-Принцип уважения прав человека и гражданина.

(+)Принцип конспирации.

18. Укажите ОРМ указанное в ст. 6 ФЗ «Об ОРД»:

-Снятие электронной информации.

-Снятие информации, передаваемой по компьютерным сетям.

(+) Снятие информации с технических каналов связи.

-Снятие информации, передаваемой по телексной, факсимильной и электронной сетям.

-Все вышеперечисленные ответы верны.

19. Является ли препятствием для проведения ОРМ гражданство, национальность, социальное и имущественное положение, принадлежность к общественным объединениям, отношение к религии?

-Да.

(+) Нет.

-Препятствием для проведения ОРМ, в исключительных случаях, является гражданство.

-Препятствием для проведения ОРМ, в исключительных случаях, является отношение к религиям.

-Верны ответы №3 и №4.

20. В каких случаях согласно ст. 7 ФЗ «Об ОРД», оперативные аппараты в праве собирать данные, характеризующие личность гражданина?

-По письменному заданию должностных лиц.

(+) В связи с оказанием гражданами содействия в подготовке и проведения ОРМ.

-По заявлению граждан.

-По личной инициативе оперативного работника.

-Все указанные ответы правильные.

21. Укажите ОРМ указанное в ст. 6 ФЗ «Об ОРД»:

-Опознавание личности.

-Непосредственное отождествление.

(+) Отождествление личности

-Опосредованное опознавание.

-Предъявление к опознанию.

22. Организация и тактика проведения ОРМ составляет:

-Служебную тайну.

-Не составляет тайну.

(+) Государственную тайну.

-Государственную тайну составляет, организация и тактика проведения ОРМ только судебного санкционирования.

-Государственную тайну составляет, организация и тактика проведения ОРМ только ведомственного санкционирования.

23. Укажите название дела оперативного учета, которое в праве заводить оперативное подразделение ОВД:

-Дело оперативной проверки.

-Дело оперативного поиска.

(+) Дело предварительной оперативной проверки.

-Накопительное дело.

-Учетно-регистрационное дело.

24. Укажите органы, оперативные подразделения которых, в праве осуществлять ОРД:

-Федеральные органы налоговой полиции.

(+) 2. Органы внутренних дел.

-Органы пограничной службы РФ.

-Служба безопасности президента РФ.

-Все ответы правильные.

25. ОРД согласно ст. 1 ФЗ «Об ОРД» осуществляется:

(+) В целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечение безопасности общества и государства от преступных посягательств.

- В целях раскрытия и предупреждения преступлений.
- В целях обеспечения безопасности общества и государства от преступных посягательств.
- В целях обеспечения безопасности правоохранительных органов.
- В целях негласного контроля за лицами, подозреваемых в подготовке и совершающие преступления.

26. ОРД осуществляется сотрудниками оперативных подразделений следующих государственных органов:

- Пограничной службой РФ.
- (+) Таможенных органов РФ.
- Комитета по контролю за исполнением наказаний.
- Внутренних войск РФ.
- Налоговой полиции РФ.

27. Ст.2 ФЗ «Об ОРД» определяет следующую задачу:

- Выявление, предупреждение, пресечение и раскрытие неочевидных преступлений.
- Розыска лиц скрывающихся от правосудия.
- (+) Выявление лиц подготавливающих, совершающих или совершивших преступления.
- Сбор информации о событиях представляющих угрозу безопасности РФ.
- Осуществление контроля за деятельностью общественных и религиозных объединений.

28. Лицо полагающее, что действие органов, осуществляющих ОРД, привели к нарушению его прав и свобод, вправе обжаловать эти действия, согласно ст. 5 ФЗ «Об ОРД» в:

- Государственную Думу.
- (+) Вышестоящие органы, осуществляющие ОРД.
- В комитет по соблюдению законности в органах, осуществляющих ОРД.
- В орган допустивший нарушение прав и свобод лица, при проведении ОРМ.
- В Федеральное собрание РФ.

29. Укажите ОРМ определенное в ст. 6 ФЗ «Об ОРД»:

- (+) Опрос.
- Специальная беседа.
- Гипнотический опрос.
- Контролируемый опрос.
- Следственный опрос.

30. Укажите основания проведения ОРМ определенные в ст.7 ФЗ «Об ОРД»:

- Принятие решения о допуске лица к сведениям, составляющим государственную тайну.
- Постановление о применении мер безопасности в отношении защищаемых лиц.
- Принятие решения о выдаче разрешений на частную детективную и охранную деятельность.
- Запросы других органов, осуществляющих ОРД.
- (+) Все ответы правильные.

31. Укажите ОРМ ведомственного санкционирования:

- (+) Оперативное внедрение.
- Оперативное наблюдение.
- Отождествление личности.
- Оперативное отождествление.
- Оперативный опрос.

32. ОРМ «Оперативный эксперимент» наиболее эффективен в борьбе с:

-Терроризмом.

-Незаконным оборотом наркотиков.

(+) Серийными изнасилованиями.

-Серийными квартирными кражами.

-Верные ответы № 2, 3, 4.

33. Укажите вид ОРМ «Обследование помещений, сооружений, участков местности и т.д.» требующий судебного санкционирования:

-Гласное.

(+)2. Негласное.

-Зашифрованное.

-Независимое.

-Все ответы правильные.

34. Укажите максимальный срок проведения ОРМ «Контроль почтовых отправлений телеграфных и иных сообщений»:

-1 месяц.

-3 месяца.

(+)3. 6 месяцев.

-9 месяцев.

-12 месяцев.

35. Укажите виды непосредственного отождествления личности:

-По фото, видео учетам ОВД.

- В ходе оперативного поиска, в местах вероятного появления преступника (ов).

-С помощью служебно-розыскной собаки (выборка лиц).

(+)4. Верны ответы № 1, 2.

-Верны ответы № 1, 2, 3.

36. ОРМ «Оперативный эксперимент» наиболее эффективен в борьбе с:

-Незаконным оборотом оружия.

-ОРМ «Оперативный эксперимент» наиболее эффективен только в борьбе с серийными мошенничествами в отношении юридических лиц.

-С серийными квартирными кражами.

(+)4. С серийными кражами автотранспорта.

- Нет правильных ответов.

37. ОРМ «Наблюдение» осуществляется:

-На транспорте.

-На открытой местности.

-В помещениях.

-Правильные ответы № 1, 2.

(+) Правильные ответы № 1, 2, 3.

38. ФЗ «Об ОРД» (ст.1) определяет ОРД, как:

-Вид деятельности, осуществляемый, как правило посредством проведения негласных ОРМ.

(+) Вид деятельности осуществляемый гласно и негласно.

-Вид деятельности, осуществляемый в целях охраны общественного порядка.

- Вид деятельности, осуществляемый в целях добывания информации о событиях и действиях, создающих угрозу государственной, военной, экономической или экологической безопасности РФ.
- Вид деятельности, осуществляемый в целях выявления лиц, подготавливающих и совершающих преступления.

Тема 9. Международное законодательство в области защиты информации

1. В сфере международных отношений социальное государство реализуется в первую очередь в ...
 - (+) политике защиты прав человека
 - международных договорах и соглашениях
 - деятельности международных неправительственных организаций
 - внешней политике государства
2. В странах-организаторах ЕС (Германия, Франция, Италия и др.) улучшение социальной политики в зоне ЕС не связывается с ...
 - унификацией требований к бюджету стран-членов ЕС
 - совершенствованием институтов социального страхования
 - совершенствованием политики мультикультурализма и единой миграционной политики
 - (+) унификацией законодательства в области социального обеспечения
3. В "Оранжевой книге" фигурируют понятия:
 - (+) ядро безопасности
 - (+) периметр безопасности
 - центр безопасности
4. В "Гармонизированных критериях Европейских стран" фигурируют понятия:
 - (+) цель оценки
 - система оценки
 - (+) объект оценки
5. "Общие критерии" содержат следующие основные виды требований безопасности:
 - архитектурные требования
 - (+) функциональные требования
 - (+) требования доверия
6. В стандарте BS 7799 разъясняются следующие понятия и процедуры:
 - безопасность интерфейсов
 - (+) безопасность персонала
 - (+) физическая безопасность
7. Спецификация IPsec затрагивает вопросы
 - доступности
 - (+)конфиденциальности
 - (+)целостности
8. Рекомендации X.509 регламентируют формат
 - сертификата безопасности
 - (+)сертификата открытого ключа
 - сертификата директории
9. Международные стандарты аудита:
 - являются стабильными, неизменными;
 - (+) периодически обновляются с учетом экономической ситуации и уровня развития аудита;
 - изменяются каждые 5 лет.
10. Аудиторские стандарты выполняют следующие функции:
 - (+) обеспечивают высокое качество проверки и связь отдельных элементов аудиторского процесса;

- формируют доверие общества к аудиту;
- устраняют конкуренцию на рынке аудиторских услуг.

11. Какая организация разрабатывает и утверждает Международные стандарты аудита?

- Институт профессиональных бухгалтеров России
- Совет по международным стандартам аудита и уверенности;
- Ассоциация присяжных бухгалтеров Великобритании.

(+) МФБ.

12. В соответствии с Международными стандартами аудита рабочие документы аудитора должны храниться:

- в течение необходимого периода времени, достаточного с точки зрения практики и в соответствии с правовыми и профессиональными требованиями, предъявляемыми к хранению документов;
- не менее одного года;

(+) не менее пяти лет;

- бессрочно, в течение срока деятельности аудиторской организации.

13. В некоторых европейских странах в целях борьбы с кибератаками вводится специальная сертификация для больших компаний. Какие средства необходимо использовать для того, чтобы подтвердить защищенность продукта от основных киберугроз?

- Средства контроля доступа пользователей

-Патч-менеджмент

-Файервол

(+) Все перечисленные средства

4.3 Промежуточная аттестация по дисциплине проводится в форме экзамена

Типовые вопросы экзамена (ОК-4, ПК-19)

1. Законодательство РФ в области информационной безопасности
2. Государственная тайна
3. Конфиденциальная информация
5. Лицензирование и сертификация в информационной сфере
6. Нормативно правовые акты по обеспечению защиты интеллектуальной собственности
7. Правовое регулирование оперативно-розыскных мероприятий в оперативно-розыскной деятельности.
8. Методы защиты информации в экстремальных ситуациях

Типовые задания для экзамена (ОК-4, ПК-19)

1. Каким нормативным актом осуществляется правовое регулирование оперативно-розыскных мероприятий.
 - a. Конституция РФ
 - b. Закон РФ "О частной детективной и охранной деятельности в Российской Федерации"
 - c. **Закон РФ "Об оперативно-розыскной деятельности"**
2. Государственная тайна это:
 - a. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной, оперативно-розыскной деятельности, распространение которых может нанести ущерб государству.
 - b. защищаемые государством сведения в области его военной, распространение которых может нанести ущерб государству.
 - c. защищаемые государством сведения в области его военной, внешнеполитической, экономической, экологической, разведывательной, контрразведывательной, оперативно-розыскной деятельности, распространение которых может нанести ущерб государству.

3. Основные принципы построения отказоустойчивых систем:

- a. **Модульность, избыточность, самоконтроль, независимость**
- b. Модульность, избыточность, независимость
- c. Избыточность, актуальность, независимость, дублирование

4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«отлично» (85 - 100 баллов)	ОК-4	Демонстрирует высокий уровень знаний требований нормативных правовых актов в области защиты государственной тайны и информационной безопасности. Анализирует основные изменения законодательства в области информации, прослеживает междисциплинарные связи. Свободно применяет основные положения защиты государственной тайны и информационной безопасности. В полной мере владеет навыками поиска актуальной правовой информации. Ответ построен логично, материал излагается четко, ясно, хорошим языком, аргументировано.
	ПК-19	Демонстрирует высокий уровень знаний требований нормативных правовых актов в области защиты государственной тайны и информационной безопасности. Анализирует основные изменения законодательства в области информации, прослеживает междисциплинарные связи. Свободно применяет основные положения защиты государственной тайны и информационной безопасности. В полной мере владеет навыками поиска актуальной правовой информации. Ответ построен логично, материал излагается четко, ясно, хорошим языком, аргументировано.
«хорошо» (70 - 84 баллов)	ОК-4	Демонстрирует достаточный уровень знаний законодательства в области информации. Анализирует основные изменения законодательства в области информации, но допускает некоторые погрешности. В отдельных примерах может выделить междисциплинарные связи. Относительно свободно применяет основные навыки поиска актуальной правовой информации. Владеет отдельными понятиями и категориями информационного права. Ответ построен логично, материал излагается хорошим языком.
	ПК-19	Демонстрирует достаточный уровень знаний законодательства в области информации. Анализирует основные изменения законодательства в области информации, но допускает некоторые погрешности. В отдельных примерах может выделить междисциплинарные связи. Относительно свободно применяет основные навыки поиска актуальной правовой информации. Владеет отдельными понятиями и категориями информационного права. Ответ построен логично, материал излагается хорошим языком.

«удовлетворительно» (50 - 69 баллов)	ОК-4	<p>Демонстрирует не достаточный уровень знаний законодательства в области информации, требований нормативных правовых актов в области защиты государственной тайны и информационной безопасности.</p> <p>Плохо анализирует основные изменения законодательства в области информации.</p> <p>Затрудняется применять основные положения законодательства в области информации, требования нормативных правовых актов.</p> <p>Владеет единичными навыками использования поиска актуальной правовой информации Ответ не всегда логично выстроен, материал излагается без применения научной терминологии.</p>
	ПК-19	<p>Демонстрирует не достаточный уровень знаний законодательства в области информации, требований нормативных правовых актов в области защиты государственной тайны и информационной безопасности.</p> <p>Плохо анализирует основные изменения законодательства в области информации.</p> <p>Затрудняется применять основные положения законодательства в области информации, требования нормативных правовых актов.</p> <p>Владеет единичными навыками использования поиска актуальной правовой информации Ответ не всегда логично выстроен, материал излагается без применения научной терминологии.</p>
«неудовлетворительно» (менее 50 баллов)	ОК-4	<p>Демонстрирует слабый уровень знаний законодательства в области информации, требований нормативных правовых актов в области защиты государственной тайны и информационной безопасности.</p> <p>Не может анализировать основные изменения законодательства в области информации</p> <p>Не может применить основные положения в области информации, требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности.</p> <p>Не владеет навыками поиска актуальной правовой информации.</p> <p>Неуверенно и логически непоследовательно излагает материал.</p>
	ПК-19	<p>Демонстрирует слабый уровень знаний законодательства в области информации, требований нормативных правовых актов в области защиты государственной тайны и информационной безопасности.</p> <p>Не может анализировать основные изменения законодательства в области информации</p> <p>Не может применить основные положения в области информации, требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности.</p> <p>Не владеет навыками поиска актуальной правовой информации.</p> <p>Неуверенно и логически непоследовательно излагает материал.</p>

5. Методические указания для обучающихся по освоению дисциплины (модуля)

5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;
- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература:

1. Тамб. гос. ун-т им. Г.Р. Державина Организационная защита информации : электронное учебное пособие. - [Тамбов]: [Б.и.], 2012. - 1 электрон. опт. диск (CD-ROM)
2. Аверченков, В. И., Рытов, М. Ю. Организационная защита информации : учебное пособие для вузов. - Весь срок охраны авторского права; Организационная защита информации. - Брянск: Брянский государственный технический университет, 2012. - 184 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/7002.html>
3. Аверченков, В. И., Рытов, М. Ю. Служба защиты информации. Организация и управление : учебное пособие для вузов. - Весь срок охраны авторского права; Служба защиты информации. Организация и управление. - Брянск: Брянский государственный технический университет, 2012. - 186 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/7008.html>

6.2 Дополнительная литература:

1. Кармановский, Н. С., Михайличенко, О. В., Прохожев, Н. Н. Организационно-правовое и методическое обеспечение информационной безопасности : учебное пособие. - 2022-10-01; Организационно-правовое и методическое обеспечение информационной безопасности. - Санкт-Петербург: Университет ИТМО, 2016. - 169 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/67452.html>

2. Казанцев С.Я. Правовое обеспечение информационной безопасности : учеб. пособие для вузов. - 2-е изд., испр. и доп.. - М.: Издат. центр "Академия", 2007. - 239 с.
3. Тимакин А.Е. Защита и обработка конфиденциальных документов : информ. образоват. ресурс. - [Тамбов: б. и.], 2011. - 1 электрон. опт. диск (CD-ROM)

6.3 Иные источники:

1. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных.» -
2. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации.» -
3. Закон Российской Федерации от 21 июля 1993 г. N 5485-1 «О государственной тайне.» -
4. Указ Президента Российской Федерации от 17 марта 2008 г. N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использ -
5. Указ Президента Российской Федерации от 6 марта 1997 г. N 188 «Об утверждении Перечня сведений конфиденциального характера.» -

7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное программное обеспечение:

Консультант Плюс

Microsoft Windows 10

Google Chrome

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>
2. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: <https://www.studentlibrary.ru>
3. Университетская библиотека онлайн: электронно-библиотечная система. – URL: <https://biblioclub.ru>
4. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>
5. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>
6. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prilib.ru>
7. Российская государственная библиотека. – URL: <https://www.rsl.ru>
8. Российская национальная библиотека. – URL: <http://nlr.ru>
9. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>

https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.