

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



Н. Л. Королева
«05» июля 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.О.36 Защита персональных данных в информационных системах

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: 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 «26» ноября 2020 г. № 1461).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «18» мая 2021 г. Протокол № 9

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «05» июля 2021 г. № 5.

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.....	18
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	34
6. Учебно-методическое и информационное обеспечение дисциплины.....	36
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	37

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-5 Способен организовывать процедуру аттестации объектов вычислительной техники на соответствие требованиям по защите информации

1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- организационно-управленческий

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сферах: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере), 12 Обеспечение безопасности (в сфере защиты информации), Сфера правоохранительной деятельности

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

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	Индикаторы достижения компетенций
	ПК-5 Способен организовывать процедуру аттестации объектов вычислительной техники на соответствие требованиям по защите информации	Проводит аттестацию объектов вычислительной техники на соответствие требованиям защиты персональных данных в информационных системах

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-5 Способен организовывать процедуру аттестации объектов вычислительной техники на соответствие требованиям по защите информации

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения				
		Очная (семестр)				
		3	4	5	8	10
1	International information security			+		
2	Защита информационных процессов в компьютерных системах				+	
3	Международная информационная безопасность			+		
4	Микропроцессорная техника	+				
5	Основы электро- и радиоизмерений	+				

6	Преддипломная практика					+
7	Стандарты в области информационной безопасности			+		
8	Техническая защита информации		+	+		
9	Электроника и схемотехника	+				

2. Место дисциплины в структуре ОП специалиста:

Дисциплина «Защита персональных данных в информационных системах» относится к обязательной части учебного плана ОП по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере.

Дисциплина «Защита персональных данных в информационных системах» изучается в 7 семестре.

3. Объем и содержание дисциплины

3.1. Объем дисциплины: 3 з.е.

Очная: 3 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	108
Контактная работа	48
Лекции (Лекции)	16
Лабораторные (Лаб. раб.)	32
Самостоятельная работа (СР)	60
Зачет	-

3.2. Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
7 семестр					
1	Введение	2	4	10	Собеседование; Тестирование
2	Объекты информационной безопасности	2	4	10	Собеседование
3	Угрозы безопасности информации	2	4	10	Другие формы контроля; Тестирование
4	Информационная безопасность и организационные основы защиты информации	2	4	10	Тестирование

5	Правовое обеспечение информационной безопасности.	4	8	10	Тестирование
6	Организация работы с персоналом предприятия	4	8	10	Тестирование

Тема 1. Введение (ПК-5)

Лекция.

Предмет, цели, задачи и содержание курса технической защиты информации (ТЗИ). Роль и место курса в подготовке специалистов по организации защиты информации в государственных и коммерческих структурах. Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия.

Лабораторные работы.

Подготовить доклад на тему:

Роль и место курса в подготовке специалистов по организации защиты информации в государственных и коммерческих структурах

Понятия защиты персональных данных работников, порядок их сбора, обработки, хранения, использования, передачи.

Роль и место конституционных прав личности в защите персональных данных работника.

Роль законодательства в защите персональных данных работников в настоящий период.

Правовая защита персональных данных работника.

Задания для самостоятельной работы.

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

Тема 2. Объекты информационной безопасности (ПК-5)

Лекция.

Основные свойства информации как предмета технической защиты.

Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности ее защиты. Понятие о демаскирующих признаках объектов защиты. Характеристики и особенности семантической (смысловой) информации и информации о демаскирующих признаках объекта.

Демаскирующие признаки объектов защиты.

Классификация демаскирующих признаков. Оознавательные признаки и признаки деятельности объектов. Видовые, сигнальные и вещественные демаскирующие признаки. Информативность признаков. Понятие о признаковых структурах. Основные видовые демаскирующие признаки объектов наблюдения. Особенности видовых признаков в оптическом и радиодиапазонах. Источники и носители конфиденциальной информации.

Понятие об источниках, носителях и получателях информации. Классификация источников информации. Источники технической и экономической информации при научных исследованиях, разработке, производстве и эксплуатации продукции, на различных этапах и видах коммерческой деятельности. Виды носителей информации (люди, физические поля, электрические сигналы и материальные тела). Источники опасных сигналов.

Понятие об опасном сигнале и их источниках. Основные и вспомогательные технические средства и системы. Побочные электромагнитные излучения и наводки. Акустоэлектрические преобразователи, их виды и принципы работы. Принципы высокочастотного навязывания. Высокочастотные и низкочастотные побочные излучения технических средств и систем (ТСС). Паразитная генерация усилителей. Виды паразитных связей между цепями ТСС. Паразитные наводки в цепях электропитания, заземления, в токопроводящих конструкциях помещений и зданий.

Лабораторные работы.

Лабораторная работа 1

Мониторинг радиоэлектронной обстановки в защищаемом помещении с помощью скоростного поискового приемника радиосигналов «СКОРПИОН»

Лабораторная работа 2

Определение частоты работающей радиозакладки с использованием скоростного поискового приемника радиосигналов «СКОРПИОН».

Задания для самостоятельной работы.

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

Тема 3. Угрозы безопасности информации (ПК-5)

Лекция.

Виды угроз безопасности информации.

Виды потенциальных угроз безопасности информации. Преднамеренные и случайные воздействия на источники информации. Утечка информации и ее особенности. Подходы к оценке уровня угрозы. Факторы, влияющие на возможность реализации угроз.

Органы разведки.

Роль разведки в деятельности государств и коммерческих структур. Структура органов разведки. Виды зарубежной разведки и разведки коммерческих структур. Классификация технической разведки по физической природе носителя. Носители технических средств разведки. Принципы ведения разведки.

Технология разведки. Основные принципы и этапы добывания информации. Структура органов управления, добывания и информационной работы. Видовая и комплексная обработка данных и сведений.

Способы несанкционированного доступа к источникам информации.

Понятие о разведывательном контакте и его условиях. Виды доступа к источникам информации (физический контакт и дистанционный доступ). Принципы доступа к источникам информации без физического проникновения к контролируемую зону. Классификация и характеристики наземных средств дистанционного съема информации с носителей. Принципы доступа к источникам информации без нарушения государственной границы. Возможности зарубежной космической, воздушной и морской разведки в мирное время.

Способы и средства добывания информации техническими средствами. Способы и средства наблюдения. Факторы, влияющие на эффективность обнаружения и распознавания объектов наблюдения. Структура и основные характеристики средств наблюдения. Параметры зрительной системы человека. Классификация и основные характеристики объективов. Виды и технические характеристики визуально-оптических приборов.

Способы и средства перехвата сигналов. Задачи, решаемые при перехвате сигналов. Структура средств перехвата и их функции. Классификация и характеристики антенн. Структура радиоприемника и его характеристики. Особенности и основные характеристики сканирующих радиоприемников. Принципы определения координат источников радиоизлучений и анализа сигналов.

Способы и средства подслушивания акустических сигналов. Параметры слуховой системы человека. Структура и характеристики технических средств подслушивания. Классификация и характеристики микрофонов. Виды и принципы работы остронаправленных микрофонов. Стетоскопы. Принципы работы и характеристики диктофонов для скрытной записи. Классификация и характеристики закладных устройств. Варианты камуфлирования закладных устройств. Способы и средства лазерного подслушивания и ВЧ-навязывания. Способы и средства добывания информации о демаскирующих признаках веществ. Способы и возможности определения демаскирующих признаков веществ.

Технические каналы утечки информации. Характеристики каналов утечки информации. Структура технических каналов утечки информации. Отличия технического канала утечки информации от канала связи. Виды технических каналов утечки информации. Типовая структура технического канала утечки информации. Основные характеристики технических каналов утечки информации. Способы комплексного использования злоумышленниками технических каналов утечки информации.

Оптические каналы утечки информации. Структура оптического канала утечки информации. Условия освещенности объектов наблюдения в видимом и ИК-диапазонах в различные периоды времени. Характеристики среды распространения оптических лучей. Основные показатели оптоэлектронных линий связи и способы снятия с них информации. Варианты оптических каналов утечки информации для типовых контролируемых зон организации.

Радиоэлектронные каналы утечки информации. Особенности радиоэлектронных каналов утечки информации. Виды и структура радиоэлектронных каналов утечки информации. Акустические каналы утечки информации.

Структура акустического канала утечки информации. Отражение и поглощение акустических волн в среде распространения. Понятие о реверберации и влияние времени реверберации на разборчивость речи. Способы увеличения протяженности акустического канала утечки информации. Материально-вещественные каналы утечки информации. Структура материально-вещественного канала утечки информации и характеристики ее элементов.

Лабораторные работы.

Лабораторная работа.

Определение частоты работающей радиозакладки с использованием скоростного поискового приемника радиосигналов "СКОРПИОН"

Лабораторная работа.

Определение мощности работающей радиозакладки с использованием портативного измерителя частоты и мощности MFP – 8000

Лабораторная работа.

Определение электромагнитных излучений работающей радиозакладки с использованием генератора шума ЛГШ-503.

Задания для самостоятельной работы.

1. проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы
2. подготовка к тестированию, контрольной работе

Тема 4. Информационная безопасность и организационные основы защиты информации (ПК-5)

Лекция.

В лекции рассматриваются базовые вопросы информационной безопасности и организационные основы защиты информации. Информационная безопасность, виды и источники угроз информационной безопасности, методы обеспечения информационной безопасности Российской Федерации, регулирование отношений в сфере ИБ.

Лабораторные работы.

1. Основными источниками угроз информационной безопасности являются все указанное в списке:
 - Хищение жестких дисков, подключение к сети, инсайдерство

- Перехват данных, хищение данных, изменение архитектуры системы+
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

2. К основным угрозам иб относятся:

- Фишинг / Социально-технические атаки, Атаки на основе IoT, Программы-вымогатели, Инсайдерские атаки;+
- DDoS-атаки, Неисправленные уязвимые места и ошибки системы безопасности, хакерские атаки;
- Асинхронные вызовы процедур в системных ядрах, Неравномерность мер по обеспечению информационной безопасности, DDoS-атаки, Неисправленные уязвимые места и ошибки системы безопасности.+

3. Под информационной безопасностью понимается...

- Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре;+
- Программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия;
- Нет правильного ответа.

4. Основные объекты информационной безопасности:

- Компьютерные сети, базы данных+
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

5. К основным принципам обеспечения информационной безопасности относится:

- Экономической эффективности системы безопасности+
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

6. Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний
- органы права, государства, бизнеса+
- сетевые базы данных, фаерволлы

7. К основным функциям системы безопасности можно отнести все перечисленное:

- Установление регламента, аудит системы, выявление рисков+
- Установка новых офисных приложений, смена хостинг-компаний
- Внедрение аутентификации, проверки контактных данных пользователей

8. Принципом политики информационной безопасности является принцип:

- Невозможности миновать защитные средства сети (системы)+
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

9. Принципом политики информационной безопасности является принцип:

- Усиления защищенности самого незащищенного звена сети (системы)+
- Перехода в безопасное состояние работы сети, системы

- Полного доступа пользователей ко всем ресурсам сети, системы

10. К ОСНОВНЫМ ТИПАМ СРЕДСТВ ВОЗДЕЙСТВИЯ НА КОМПЬЮТЕРНУЮ СЕТЬ ОТНОСИТСЯ:

- Компьютерный сбой
- Логические закладки («мины») +
- Аварийное отключение питания

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 5. Правовое обеспечение информационной безопасности. (ПК-5)

Лекция.

Информационная безопасность в системе национальной безопасности Российской Федерации. Информационные отношения как объект правового регулирования. Источники угроз информационной безопасности РФ. Понятие информационной войны. Правовой режим защиты государственной тайны. Правовые режимы защиты информации конфиденциального характера.

Лабораторные работы.

1. Какая информация подлежит защите?
 - информация, циркулирующая в системах и сетях связи;
 - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
 - информация, составляющая государственные информационные ресурсы;
 - любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. +
2. Как называется информация, которую следует защищать (по нормативам, правилам сети, системы)?
 - Регламентированной
 - Правовой
 - Защищаемой +
3. Что относится к правовым методам, обеспечивающим информационную безопасность:
 - Разработка аппаратных средств защиты данных;
 - Разработка и установка во всех компьютерных правовых сетях журналов учета действий;

-Разработка и конкретизация правовых нормативных актов обеспечения безопасности+

4. По категориям доступа информация делится:

- открытую информацию и государственную тайну;
- конфиденциальную информацию и информацию свободного доступа;
- информацию с ограниченным доступом и общедоступную информацию. +

5. Какой из нижеперечисленных законодательных актов обладает наибольшей юридической силой, в вопросах информационного права:

- Указ президента "об утверждении перечня сведений, относящихся к государственной тайне";
- Постановления Правительства РФ;
- закон "об информации, информатизации и защите информации";
- Конституция. +

6. Система защиты государственных секретов определяется Законом

- "Об информации, информатизации и защите информации";
- "Об органах ФСБ";
- "О государственной тайне"; +
- "О безопасности".

7. К органам защиты государственной тайны относятся:

- 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, уполномоченный в области противодействия техническим разведкам и технической защиты информации, и их территориальные органы;
- органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны; +
- Правительство Российской Федерации;
- Межведомственная комиссия по защите государственной тайны.

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

- уполномоченными федеральными органами исполнительной власти; +
- Федеральная служба безопасности РФ;
- Государственная Дума РФ и Президент РФ;
- Президент РФ и Правительство РФ.

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

- рассекречивание
- доступ;
- пропуск;
- допуск. +

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

- Правительство РФ; +
- Федеральная служба безопасности РФ;

- Президент РФ;
- орган местного самоуправления.

11. На кого возлагается сертификация средств защиты информации РФ:

- ФСБ;
- 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;+
- Министерство обороны;
- ФСТЭК+

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

- только уголовную;
- только гражданско-правовую;
- административную, дисциплинарную;+
- уголовную, гражданско-правовую.+

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

- "особой важности", "совершенно секретно" и "секретно".+
- "особо секретно", "совершенно секретно" и "секретно".
- "особой важности", "абсолютно секретно" и "важно".
- "особой важности", "абсолютно секретно" и "секретно".

14. Перечень сведений, отнесенных к государственной тайне формирует:

- Президент Российской Федерации.
- Межведомственная комиссия.
- Правительство Российской Федерации.
- Органов государственной власти.+

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

- обращаться в территориальные органы ФСБ по засекречиванию информации, находящейся в собственности.
- обращаться в Межведомственную комиссию по засекречиванию информации, находящейся в собственности.
- принимать решения о засекречивании информации, находящейся в собственности.+
- обращаться в Органы государственной власти по засекречиванию информации, находящейся в собственности.

16. В течении какого срока принимается решение о дополнении (изменении) перечня сведений, составляющих гос. тайну:

- в течении 5 месяцев.
- в течении 6 месяцев.
- в течении 3 месяцев.+
- в течении года.

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

-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;

-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.+

-об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя, о регистрационном номере.

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

-лицензии;+

-аттестата соответствия;

-наличие соответствующих специалистов;

-наличие сертифицированных средств защиты.

19. К объектам интеллектуальной собственности относятся:

-селекционные достижения;

-товары и услуги;

-произведения прикладного искусства;+

-секреты производства (ноу-хау); +

-фонограммы;+

-фирменные наименования; +

-логотипы;+

-юридические лица;

-музыкальные произведения. +

20. Результат интеллектуальной деятельности может одновременно использоваться:

-одним лицом;

-группой лиц до 10 человек;

-группой лиц более 10 человек;

-неограниченным кругом лиц.+

21. Правовая охрана каких объектов интеллектуальной собственности возникает в силу факта их создания:

-произведения науки, литературы и искусства;+

-исполнения, фонограммы, передачи организаций вещания+

-товарный знак, программы для ЭВМ;

-программы для ЭВМ и базы данных;+

-топологии интегральных микросхем.+

22. Какой из объектов не является объектом интеллектуальной собственности:

-селекционное достижение;

-предприятие как имущественный комплекс;+

-секрет производства (ноу-хау);

-фонограмма;

-товарный знак.

23. Какие права субъектов интеллектуальной собственности охраняются бессрочно:

-имущественные права;

-личные неимущественные права;+

-как имущественные, так и личные неимущественные права.

24. Какие права субъектов интеллектуальной собственности охраняются бессрочно:

-имущественные права;

-личные неимущественные права;+

-как имущественные, так и личные неимущественные права.

25. К объектам авторского права относятся:

-новые сорта растений;

-музыкальные произведения;+

-товарные знаки;

-базы данных;+

-идеи, концепции, открытия;

-монографии;+

-научные статьи. +

26. Какой из объектов охраняется правом интеллектуальной собственности:

а) недвижимое имущество;

б) идея;

в) герб;

г) товарный знак;+

д) открытие.

27. Основные источники угроз информационной безопасности это:

а) Хищение жестких дисков, подключение к сети, инсайдерство;

б) Перехват данных, хищение данных, изменение архитектуры системы;+

в) Хищение данных, подкуп системных администраторов, нарушение регламента работы.

28. Выберите наиболее важный момент при реализации защитных мер политики безопасности:

а) Аудит, анализ затрат на проведение защитных мер;

б) Аудит, анализ безопасности;

в) Аудит, анализ уязвимостей, риск-ситуаций. +

29. Какой нормативный документ регламентирует отношения в области авторских и смежных прав?

-Доктрина информационной безопасности РФ;

-Гражданский кодекс; +

-Уголовный кодекс РФ;

-Указ Президента РФ;

-Закон «Об информации, информатизации и защите информации».

30. Какой законодательный акт регулирует отношения в области защиты информационных ресурсов (личных и общественных) от искажения, порчи и уничтожения?

- Закон «Об информации, информатизации и защите информации»; +
- Закон «О правовой охране программ для ЭВМ и баз данных»;
- Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ;
- Пункты 1 и 3
- Указ Президента РФ.

31. Какой закон содержит гарантии недопущения сбора, хранения, использования и распространения информации о частной жизни граждан:

- Указ Президента РФ;
- Закон «Об информации, информатизации и защите информации»; +
- Закон «О правовой охране программ для ЭВМ и баз данных»;
- Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ;
- Доктрина национальной безопасности РФ.

32. Для написания самостоятельной работы Вы скопировали из Интернет полный текст нормативно-правового акта. Нарушили ли Вы при этом авторское право?

- да, нарушено авторское право владельца сайта;
- нет, так как нормативно-правовые акты не являются объектом авторского права; +
- нет, если есть разрешение владельца сайта;
- да, нарушено авторское право автора документа;
- нет, если истек срок действия авторского права.

33. Можно ли разместить на своем сайте в Интернет опубликованную в печати статью какого-нибудь автора?

- можно, с указанием имени автора и источника заимствования;
- можно, с разрешения и автора статьи, и издателя;
- можно, но исключительно с ведома автора и с выплатой ему авторского вознаграждения;
- можно, поскольку опубликованные статьи не охраняются авторским правом;
- можно, с разрешения издателя, издавшего данную статью, или автора статьи. +

34. Что необходимо указать при цитировании статьи, размещенной на чьем-то сайте?

- имя автора, название статьи, адрес сайта, с которого заимствована статья; +
- адрес сайта и имя его владельца;
- имя автора и название статьи;
- электронный адрес сайта, с которого заимствована статья;
- название статьи и название сайта.

35. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это....

- информационная война; +
- информационное оружие;
- информационное превосходство.

36. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспреещения доступа к ним это:

- информационная война;
- информационное оружие;+
- информационное превосходство.

37. Определение коммерческой (торговой) деятельности содержится:

- в Уголовном кодексе РФ;
- в Гражданском кодексе РФ;+
- в Трудовом кодексе РФ;
- в Налоговом кодексе РФ.

38. Предметом коммерческого права является:

- управленческие отношения;
- отношения, возникающие в сфере товарного обращения;+
- отношения, возникающие в сфере административного права;
- управленческие отношения и отношения, возникающие в сфере товарного обращения и административного права.

39. Субъект коммерческой деятельности – это:

- несовершеннолетние;
- специалист, работающий в области юриспруденции;
- торговая сеть;
- юридические лица или индивидуальные предприниматели, занимающиеся торгово-предпринимательской деятельностью и зарегистрированные в установленном законом порядке;+
- ЭКОНОМИСТ.

40. Компьютерное преступление это...

- Незаконный доступ к компьютерной информации; +
- Создание, применение и распространение вредоносных компьютерных программ; +
- Кража компьютерной техники или комплектующих ЭВМ;
- Нарушение норм эксплуатации средств хранения, обработки или передачи компьютерной информации. +

41. Виды вредоносных компьютерных программ:

- логическая бомба;
- тройанский конь; +
- компьютерный вирус;+
- приложение.

Задания для самостоятельной работы.

1. Правовая охрана результатов интеллектуальной деятельности.
2. Преступления в сфере компьютерной информации. Правовые режимы защиты информации ведущих мировых держав.
3. Виды ответственности за нарушение законодательства в области защиты информации. УК и КАПП

Тема 6. Организация работы с персоналом предприятия (ПК-5)

Лекция.

В лекции рассматривается организация работы с персоналом предприятия. Подбор и подготовка кадров, методы добывания ценной информации у персонала, особенности приёма на работу, этапы процедуры отбора персонала, заключение контрактов и соглашений о неразглашении конфиденциальной информации. Доступ персонала к конфиденциальным сведениям, документам и базам данных. Текущая работа с персоналом, владеющим конфиденциальной информацией, а так же особенности увольнения сотрудников, владеющих конфиденциальной информацией.

Лабораторные работы.

1. Основные задачи работы с персоналом включают:

- затруднить работу злоумышленнику или его сообщнику +
- выявление недобросовестного персонала
- не допустить установления определенных взаимоотношений злоумышленника и сотрудника фирмы+

2. При подборе персонала для работы с конфиденциальной информацией проводят мероприятия:

- Проведение аналитических мероприятий, добровольного согласия лица не разглашать конфиденциальную информацию.+
- Инструктирование и обучение сотрудников практическим действиям по защите информации. Стимулирование ответственности к сохранению конфиденциальной информации.+
- Добровольное согласие и инструктирование по неразглашению.

3. Должна ли предусматривать разрешительная система доступ к конфиденциальной информации должностных лиц из внешних организаций, выполняющих совместную работу с организацией где введен режим конфиденциальности?

- нет, не должна
- да, должна+
- зависит от индивидуального решения руководителя, даже если это ставит под угрозу срыва выполнение совместных работ

4. Имеют ли право на доступ к различным видам конфиденциальной информации сотрудники уполномоченных органов государственной власти (налоговая служба, служба судебных приставов, органы МВД и др.)?

Выберите один из 3 вариантов ответа:

- нет, не имеют
- имеют, в пределах своей компетенции
- имеют, в пределах своей компетенции, при этом обязаны обеспечить защиту полученной информации от разглашения и неправомерного использования+

5. Кто входит в круг лиц, имеющих право давать разрешение на допуск и доступ к конфиденциальной информации? Ответов несколько.

Выберите несколько из 5 вариантов ответа:

- Руководитель организации+
- Любой сотрудник, имеющий доступ к КИ
- Руководитель структурного подразделения всем сотрудникам
- Руководитель структурного подразделения в пределах своей компетенции+
- Заместитель руководителя в пределах своей сферы деятельности+

6. Кто такой контрагент в рамках реализации работ с КИ со сторонней организацией?

- это постороннее для организации лицо
- это адресат
- это сторона гражданско-правового договора+

7. Обязан ли контрагент сообщить обладателю конфиденциальной информации о допущенном им же (контрагентом) факте разглашения КИ?

- да+
- нет

8. Кому сотрудник сообщит о попытке посторонних лиц получить от него КИ и кому сотрудник в случае увольнения сдаст все носители КИ?

- сотруднику службы конфиденциального делопроизводства и руководителю организации
- никому ничего не должен сообщать и передавать
- руководителю организации и сотруднику службы конфиденциального делопроизводства+
- в вариантах не перечислено этих лиц

Задания для самостоятельной работы.

1. В чём заключается сложность персонала как объекта защиты?
2. Под обеспечением безопасности деятельности предприятия понимается?
3. Какова цель кадровой политики?
4. Кто является источником получения конфиденциальной информации?
5. Какие определяются сложности в работе с персоналом?
6. Метод поиска кандидатов внутри компании позволяет?
7. Как проводятся плановые полиграфные проверки?
8. Как проводятся внеплановые полиграфные проверки?
9. Как проводятся целевые полиграфные проверки?
10. Что представляет собой обязательство о неразглашении конфиденциальных сведений представляет собой?

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

7 семестр

- посещаемость – 10 баллов
- текущий контроль – 79 баллов
- контрольные срезы – 2 среза: 4 балла, 7 баллов
- премиальные баллы – 20 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.	Введение	Собеседование	15	<p>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.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - 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. <p>15 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>10 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>5 балл – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
		Тестирование	4	<p>Тест состоит из 15 вопросов.</p> <p>4 балла – студент правильно отвечает на 50-100% вопросов в тесте</p> <p>2 балла - студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает</p>

2.	Объекты информационн ой безопасности	Собеседо вание	20	<p>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.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - 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. <p>20 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>15 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>10 балл – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
3.	Угрозы безопасности информации	Другие формы контроля	26	<p>Лабораторные работы выполняются по тематике практических занятий.</p> <p>30-25 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>20-15 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>15-10 балл - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p>
		Тестиров ание(кон трольны й срез)	4	<p>Тест состоит из 15 вопросов.</p> <p>4 балла – студент правильно отвечает на 50-100% вопросов в тесте</p> <p>2 балла - студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает</p>

4.	Информационная безопасность и организационные основы защиты информации	Тестирование	7	Тест состоит из вопросов с выбором ответа. 7 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.
5.	Правовое обеспечение информационной безопасности.	Тестирование(контрольный срез)	7	Тест состоит из вопросов с выбором ответа. 7 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.
6.	Организация работы с персоналом предприятия	Тестирование	7	Тест состоит из вопросов с выбором ответа. 7 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.
7.	Посещаемость		10	1-3 балла – посещаемость студента составляет не менее 25 % занятий
8.	Премиальные баллы		20	Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 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 – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20
9.	Итого за семестр		100	

Итоговая оценка по зачету 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
50 - 100 баллов	Зачтено
0 - 49 баллов	Не зачтено

4.2 Типовые оценочные средства текущего контроля

Другие формы контроля

Тема 3. Угрозы безопасности информации

Лабораторная работа.

Определение частоты работающей радиозакладки с использованием скоростного поискового приемника радиосигналов "СКОРПИОН"

Лабораторная работа.

Определение мощности работающей радиозакладки с использованием портативного измерителя частоты и мощности MFP – 8000

Лабораторная работа.

Определение электромагнитных излучений работающей радиозакладки с использованием генератора шума ЛГШ-503.

Собеседование

Тема 1. Введение

Подготовить доклад на тему:

Роль и место курса в подготовке специалистов по организации защиты информации в государственных и коммерческих структурах

Понятия защиты персональных данных работников, порядок их сбора, обработки, хранения, использования, передачи.

Роль и место конституционных прав личности в защите персональных данных работника.

Роль законодательства в защите персональных данных работников в настоящий период.

Правовая защита персональных данных работника.

Тема 2. Объекты информационной безопасности

1. Определить место информационной безопасности в обеспечении системы общественной безопасности.
2. Дать определение информационной безопасности.
3. Назвать основные направления и задачи обеспечения информационной безопасности общества.
4. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.
5. Охарактеризовать уровни реализации информационной безопасности.
6. Дать определение и классификацию информационных ресурсов.
7. Определить основные виды угроз информационным ресурсам.
8. Охарактеризовать особенности угроз конфиденциальной информации.
9. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.
10. Описать причины возникновения каналов несанкционированного доступа к информации.
11. Классифицировать виды каналов несанкционированного доступа к информации.

Тестирование

Тема 1. Введение

Вашему вниманию предлагаются ответы на итоговый тест курса повышения квалификации “Обработка персональных данных в образовательных организациях” сайта Единый урок. Искренне верю, что кому-нибудь они будут полезны.

- 1 Данные, полученные при сканировании паспорта оператором персональных данных для подтверждения осуществления определенных действий конкретным лицом, относят
 - к биометрическим персональным данным
 - к специальной категории персональных данных
 - к персональным данным
2. Оператор до начала обработки персональных данных обязан уведомить территориальный орган Роскомнадзора о своем намерении осуществлять обработку персональных данных. Верно ли данное суждение?
 - Да
 - Нет
3. Неавтоматизированная обработка персональных данных это:
 - обработка персональных данных с помощью средств вычислительной техники
 - обработка персональных данных, осуществляемая при непосредственном участии человека
 - смешенная обработка персональных данных
4. Фотографические изображения обучающихся, сотрудников и посетителей организации относят:
 - К биометрическим персональным данным
 - К специальной категории персональных данных
5. Согласие на обработку персональных данных может быть дано путем получения на мобильный телефон и (или) электронную почту уникальной последовательности символов?
 - Да
 - Нет
6. Источником получения персональных данных может быть лицо, не имеющее правовых оснований для раскрытия конфиденциальной информации о субъекте персональных данных. Верно ли данное суждение?
 - Да
 - Нет
7. Согласие на обработку персональных данных может быть дано если иное не установлено федеральным законом в любой позволяющей подтвердить факт его получения форме. Верно ли данное суждение?
 - Да
 - Нет
8. Сбор, хранение, использование и распространение информации о частной жизни человека без его согласия допускается согласно Конституции РФ?
Нет

9. При обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных, ...

- Соблюдаются требования Закона о персональных данных
- **Не соблюдаются требования Закона о персональных данных**

10. Осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом. В данном случае необходимо согласие субъекта персональных данных или нет?

- Да
- **Нет**

Тема 3. Угрозы безопасности информации

1. Распределенным случайным антеннам:

- a) (?) компактное техническое средство;
- b) (!) кабели, провода, металлические трубы.

2. Носителем речевой акустической информации являются:

- a) (!) механические колебания частиц упругой среды;
- b) (?) электрический ток;
- c) (?) электромагнитные волны.

3. Сигнал – это:

- a) (!) отображение процесса изменения данных во времени при их обработке;
- b) (?) физическая величина, изменяющаяся во времени.

4. Информационный сигнал – это:

- a) (!) сигнал однозначно отображающий информацию;
- b) (?) информация, зафиксированная на материальном носителе.

Тема 4. Информационная безопасность и организационные основы защиты информации

1. Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство
- Перехват данных, хищение данных, изменение архитектуры системы+
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

2. К основным угрозам иб относятся:

- Фишинг / Социально-технические атаки, Атаки на основе IoT, Программы-вымогатели, Инсайдерские атаки;+
- DDoS-атаки, Неисправленные уязвимые места и ошибки системы безопасности, хакерские атаки;
- Асинхронные вызовы процедур в системных ядрах, Неравномерность мер по обеспечению информационной безопасности, DDoS-атаки, Неисправленные уязвимые места и ошибки системы безопасности.+

3. Под информационной безопасностью понимается...

- Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре;+
- Программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия;
- **Нет правильного ответа.**

4. Основные объекты информационной безопасности:

- Компьютерные сети, базы данных+
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

5. К основным принципам обеспечения информационной безопасности относится:

- Экономической эффективности системы безопасности+
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

6. Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний
- органы права, государства, бизнеса+
- сетевые базы данных, фаерволлы

7. К основным функциям системы безопасности можно отнести все перечисленное:

- Установление регламента, аудит системы, выявление рисков+
- Установка новых офисных приложений, смена хостинг-компаний
- Внедрение аутентификации, проверки контактных данных пользователей

8. Принципом политики информационной безопасности является принцип:

- Невозможности миновать защитные средства сети (системы)+
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

9. Принципом политики информационной безопасности является принцип:

- Усиления защищенности самого незащищенного звена сети (системы)+
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

10. К ОСНОВНЫМ ТИПАМ СРЕДСТВ ВОЗДЕЙСТВИЯ НА КОМПЬЮТЕРНУЮ СЕТЬ ОТНОСИТСЯ:

- Компьютерный сбой
- Логические закладки («мины») +
- Аварийное отключение питания

Тема 5. Правовое обеспечение информационной безопасности.

1.Какая информация подлежит защите?

- информация, циркулирующая в системах и сетях связи;
- зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
- информация, составляющая государственные информационные ресурсы;
- любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. +

2. Как называется информация, которую следует защищать (по нормативам, правилам сети, системы)?

- Регламентированной
- Правовой
- Защищаемой+

3. Что относится к правовым методам, обеспечивающим информационную безопасность:

- Разработка аппаратных средств защиты данных;
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий;
- Разработка и конкретизация правовых нормативных актов обеспечения безопасности+

4. По категориям доступа информация делится:

- открытую информацию и государственную тайну;
- конфиденциальную информацию и информацию свободного доступа;
- информацию с ограниченным доступом и общедоступную информацию.+

5. Какой из нижеперечисленных законодательных актов обладает наибольшей юридической силой, в вопросах информационного права:

- Указ президента "об утверждении перечня сведений, относящихся к государственной тайне";
- Постановления Правительства РФ;
- закон "об информации, информатизации и защите информации";
- Конституция.+

6. Система защиты государственных секретов определяется Законом

- "Об информации, информатизации и защите информации";
- "Об органах ФСБ";
- "О государственной тайне";+
- "О безопасности".

7. К органам защиты государственной тайны относятся:

- 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, уполномоченный в области противодействия техническим разведкам и технической защиты информации, и их территориальные органы;
- органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны;+
- Правительство Российской Федерации;
- Межведомственная комиссия по защите государственной тайны.

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

- уполномоченными федеральными органами исполнительной власти;+
- Федеральная служба безопасности РФ;
- Государственная Дума РФ и Президент РФ;
- Президент РФ и Правительство РФ.

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

- рассекречивание
- доступ;

- пропуск;
- допуск. +

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

- Правительство РФ;+
- Федеральная служба безопасности РФ;
- Президент РФ;
- орган местного самоуправления.

11. На кого возлагается сертификация средств защиты информации РФ:

- ФСБ;
- 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;+
- Министерство обороны;
- ФСТЭК+

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

- только уголовную;
- только гражданско-правовую;
- административную, дисциплинарную;+
- уголовную, гражданско-правовую. +

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

- "особой важности", "совершенно секретно" и "секретно". +
- "особо секретно", "совершенно секретно" и "секретно".
- "особой важности", "абсолютно секретно" и "важно".
- "особой важности", "абсолютно секретно" и "секретно".

14. Перечень сведений, отнесенных к государственной тайне формирует:

- Президент Российской Федерации.
- Межведомственная комиссия.
- Правительство Российской Федерации.
- Органов государственной власти. +

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

- обращаться в территориальные органы ФСБ по засекречиванию информации, находящейся в собственности.
- обращаться в Межведомственную комиссию по засекречиванию информации, находящейся в собственности.
- принимать решения о засекречивании информации, находящейся в собственности. +
- обращаться в Органы государственной власти по засекречиванию информации, находящейся в собственности.

16. В течении какого срока принимается решение о дополнении (изменении) перечня сведений, составляющих гос. тайну:

- в течении 5 месяцев.
- в течении 6 месяцев.
- в течении 3 месяцев.+
- в течении года.

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

- 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;
- 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.+
- об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя, о регистрационном номере.

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

- лицензии;+
- аттестата соответствия;
- наличие соответствующих специалистов;
- наличие сертифицированных средств защиты.

19. К объектам интеллектуальной собственности относятся:

- селекционные достижения;
- товары и услуги;
- произведения прикладного искусства;+
- секреты производства (ноу-хау); +
- фонограммы;+

- фирменные наименования; +
- логотипы;+

- юридические лица;
- музыкальные произведения. +

20. Результат интеллектуальной деятельности может одновременно использоваться:

- одним лицом;
- группой лиц до 10 человек;
- группой лиц более 10 человек;
- неограниченным кругом лиц.+

21. Правовая охрана каких объектов интеллектуальной собственности возникает в силу факта их создания:

- произведения науки, литературы и искусства;+
- исполнения, фонограммы, передачи организаций вещания+
- товарный знак, программы для ЭВМ;
- программы для ЭВМ и базы данных;+

-топологии интегральных микросхем.+

22. Какой из объектов не является объектом интеллектуальной собственности:

- селекционное достижение;
- предприятие как имущественный комплекс;+
- секрет производства (ноу-хау);
- фонограмма;

-товарный знак.

23. Какие права субъектов интеллектуальной собственности охраняются бессрочно:

- имущественные права;
- личные неимущественные права;+
- как имущественные, так и личные неимущественные права.

24. Какие права субъектов интеллектуальной собственности охраняются бессрочно:

- имущественные права;
- личные неимущественные права;+
- как имущественные, так и личные неимущественные права.

25. К объектам авторского права относятся:

- новые сорта растений;
- музыкальные произведения;+
- товарные знаки;
- базы данных;+
- идеи, концепции, открытия;
- монографии;+
- научные статьи.+

26. Какой из объектов охраняется правом интеллектуальной собственности:

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

27. Основные источники угроз информационной безопасности это:

- а) Хищение жестких дисков, подключение к сети, инсайдерство;
- б) Перехват данных, хищение данных, изменение архитектуры системы;+
- в) Хищение данных, подкуп системных администраторов, нарушение регламента работы.

28. Выберите наиболее важный момент при реализации защитных мер политики безопасности:

- а) Аудит, анализ затрат на проведение защитных мер;
- б) Аудит, анализ безопасности;
- в) Аудит, анализ уязвимостей, риск-ситуаций. +

29. Какой нормативный документ регламентирует отношения в области авторских и смежных прав?

- Доктрина информационной безопасности РФ;
- Гражданский кодекс; +
- Уголовный кодекс РФ;
- Указ Президента РФ;
- Закон «Об информации, информатизации и защите информации».

30. Какой законодательный акт регулирует отношения в области защиты информационных ресурсов (личных и общественных) от искажения, порчи и уничтожения?

- Закон «Об информации, информатизации и защите информации»; +
- Закон «О правовой охране программ для ЭВМ и баз данных»;
- Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ;
- Пункты 1 и 3
- Указ Президента РФ.

31. Какой закон содержит гарантии недопущения сбора, хранения, использования и распространения информации о частной жизни граждан:

- Указ Президента РФ;
- Закон «Об информации, информатизации и защите информации»; +
- Закон «О правовой охране программ для ЭВМ и баз данных»;
- Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ;
- Доктрина национальной безопасности РФ.

32. Для написания самостоятельной работы Вы скопировали из Интернет полный текст нормативно-правового акта. Нарушили ли Вы при этом авторское право?

- да, нарушено авторское право владельца сайта;
- нет, так как нормативно-правовые акты не являются объектом авторского права; +
- нет, если есть разрешение владельца сайта;
- да, нарушено авторское право автора документа;
- нет, если истек срок действия авторского права.

33. Можно ли разместить на своем сайте в Интернет опубликованную в печати статью какого-нибудь автора?

- можно, с указанием имени автора и источника заимствования;
- можно, с разрешения и автора статьи, и издателя;
- можно, но исключительно с ведома автора и с выплатой ему авторского вознаграждения;
- можно, поскольку опубликованные статьи не охраняются авторским правом;
- можно, с разрешения издателя, издавшего данную статью, или автора статьи. +

34. Что необходимо указать при цитировании статьи, размещенной на чьем-то сайте?

- имя автора, название статьи, адрес сайта, с которого заимствована статья; +
- адрес сайта и имя его владельца;
- имя автора и название статьи;
- электронный адрес сайта, с которого заимствована статья;
- название статьи и название сайта.

35. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это....

- информационная война;+
- информационное оружие;
- информационное превосходство.

36. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспреещения доступа к ним это:

- информационная война;
- информационное оружие;+
- информационное превосходство.

37. Определение коммерческой (торговой) деятельности содержится:

- в Уголовном кодексе РФ;
- в Гражданском кодексе РФ;+
- в Трудовом кодексе РФ;
- в Налоговом кодексе РФ.

38. Предметом коммерческого права является:

- управленческие отношения;
- отношения, возникающие в сфере товарного обращения;+
- отношения, возникающие в сфере административного права;
- управленческие отношения и отношения, возникающие в сфере товарного обращения и административного права.

39. Субъект коммерческой деятельности – это:

- несовершеннолетние;
- специалист, работающий в области юриспруденции;
- торговая сеть;
- юридические лица или индивидуальные предприниматели, занимающиеся торгово-предпринимательской деятельностью и зарегистрированные в установленном законом порядке;+
- ЭКОНОМИСТ.

40. Компьютерное преступление это...

- Незаконный доступ к компьютерной информации; +
- Создание, применение и распространение вредоносных компьютерных программ; +
- Кража компьютерной техники или комплектующих ЭВМ;
- Нарушение норм эксплуатации средств хранения, обработки или передачи компьютерной информации. +

41. Виды вредоносных компьютерных программ:

- логическая бомба;
- троянский конь; +
- компьютерный вирус;+
- приложение.

1. Основные задачи работы с персоналом включают:

- затруднить работу злоумышленнику или его сообщнику +
- выявление недобросовестного персонала
- не допустить установления определенных взаимоотношений злоумышленника и сотрудника фирмы+

2. При подборе персонала для работы с конфиденциальной информацией проводят мероприятия:

- Проведение аналитических мероприятий, добровольного согласия лица не разглашать конфиденциальную информацию.+
- Инструктирование и обучение сотрудников практическим действиям по защите информации. Стимулирование ответственности к сохранению конфиденциальной информации.+
- Добровольное согласие и инструктирование по неразглашению.

3. Должна ли предусматривать разрешительная система доступ к конфиденциальной информации должностных лиц из внешних организаций, выполняющих совместную работу с организацией где введен режим конфиденциальности?

- нет, не должна
- да, должна+
- зависит от индивидуального решения руководителя, даже если это ставит под угрозу срыва выполнение совместных работ

4. Имеют ли право на доступ к различным видам конфиденциальной информации сотрудники уполномоченных органов государственной власти (налоговая служба, служба судебных приставов, органы МВД и др.)?

Выберите один из 3 вариантов ответа:

- нет, не имеют
- имеют, в пределах своей компетенции
- имеют, в пределах своей компетенции, при этом обязаны обеспечить защиту полученной информации от разглашения и неправомерного использования+

5. Кто входит в круг лиц, имеющих право давать разрешение на допуск и доступ к конфиденциальной информации? Ответов несколько.

Выберите несколько из 5 вариантов ответа:

- Руководитель организации+
- Любой сотрудник, имеющий доступ к КИ
- Руководитель структурного подразделения всем сотрудникам
- Руководитель структурного подразделения в пределах своей компетенции+
- Заместитель руководителя в пределах своей сферы деятельности+

6. Кто такой контрагент в рамках реализации работ с КИ со сторонней организацией?

- это постороннее для организации лицо
- это адресат
- это сторона гражданско-правового договора+

7. Обязан ли контрагент сообщить обладателю конфиденциальной информации о допущенном им же (контрагентом) факте разглашения КИ?

- да+
- нет

8. Кому сотрудник сообщит о попытке посторонних лиц получить от него КИ и кому сотрудник в случае увольнения сдаст все носители КИ?

- сотруднику службы конфиденциального делопроизводства и руководителю организации
- никому ничего не должен сообщать и передавать
- руководителю организации и сотруднику службы конфиденциального делопроизводства+
- в вариантах не перечислено этих лиц

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета

Типовые вопросы зачета (ПК-5)

1. Законодательные основы организационной защиты информации
2. Определение информационной безопасности, виды и источники угроз информационной безопасности.
3. Документы, регламентирующие организационную защиту информации
4. Организация охраны объектов предприятия, организация инженерно-технической защиты
5. Охрана объекта в условиях чрезвычайных ситуаций
6. Направления и методы информационно-аналитической работы
7. Конфиденциальная информация, угрозы конфиденциальной информации
8. Электронный документооборот, классификация систем электронного документооборота
9. Организация работы с персоналом предприятия. Подбор и подготовка кадров, методы добывания ценной информации у персонала
10. Технология подбора персонала для работы с конфиденциальными документами

Типовые задания для зачета (ПК-5)

1. Внутриобъектный режим – это:
 - a) установленный на предприятии (организации) порядок выполнения правил внутреннего трудового распорядка, направленных на обеспечение комплексной безопасности, сохранения материальных средств и защиты конфиденциальной информации.;
 - b) это установленный на предприятии (организации) порядок выполнения правил внутреннего трудового распорядка;
 - c) сохранения материальных средств и защиты конфиденциальной информации;
2. Перечислите виды пропусков:
 - a) одноразовые и многоразовые
 - b) постоянные и непостоянные
 - c) разовые, временные постоянные
 - d) всё выше перечисленное
3. Кому выдаются материальные пропуска?
 - a) выдаются лицам, ответственным за сохранность материальных средств
 - b) выдаются сотрудникам при поступлении на работу на основании приказа о зачислении в штат
 - c) выдаются лицам, работающим временно, или прикомандированным
 - d) посетителям предприятия
4. В течении скольких минут действителен разовый пропуск ?
 - a) 15 минут
 - b) 30 минут;
 - c) 90 минут

d) 120 минут

5. Физические средства защиты объектов можно разделить на:

- a) средства предупреждения, обнаружения и ликвидации угроз
- b) средства расследования компьютерных инцидентов
- c) средства анализа межсетевого трафика и антивирусной защиты

4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«зачтено» (50 - 100 баллов)	ПК-5	Показывает высокий уровень теоретических знаний в вопросах, связанных с защитой персональных данных в информационных системах. Способен проводить практические работы по аттестации объектов вычислительной техники на соответствие требованиям по защите персональных данных
«не зачтено» (0 - 49 баллов)	ПК-5	Нет знаний по вопросам, связанным с защитой персональных данных в информационных системах. Не способен проводить практические работы по аттестации объектов вычислительной техники на соответствие требованиям по защите персональных данных

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>
4. 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>

6.2 Дополнительная литература:

1. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие. - Москва/Берлин: Директ-Медиа, 2015. - 253 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>
2. Лапина, М. А., Ревин, А. Г., Лапин, В. И. Информационное право : учебное пособие для студентов вузов, обучающихся по специальности 021100 «юриспруденция». - 2021-02-20; Информационное право. - Москва: ЮНИТИ-ДАНА, 2015. - 335 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/52038.html>
3. Корниенко С. А. Основы государственного регулирования использования радиочастотного спектра в Российской Федерации : учебное пособие. - Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2016. - 154 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=459067>
4. Аверченков В. И., Ерохин В. В., Голембиовская О. М. История развития системы государственной безопасности России : учебное пособие. - 3-е изд., стер.. - Москва: Флинта, 2016. - 192 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=93267>
5. Аверченков В. И., Рытов М. Ю. Служба защиты информации: организация и управление : учебное пособие для вузов. - 3-е изд., стер.. - Москва: Флинта, 2016. - 186 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=93356>

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 исполъз -
5. Указ Президента Российской Федерации от 30 ноября 1995 г. N 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне.» -
6. Указ Президента Российской Федерации от 6 марта 1997 г. N 188 «Об утверждении Перечня сведений конфиденциального характера.» -
7. Указ Президента РФ от 31 декабря 2015 г. N 683 "О Стратегии национальной безопасности Российской Федерации" -
8. Указ Президента РФ от 05 декабря 2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" -

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 и свободно распространяемое программное обеспечение:

Microsoft Windows 10

Google Chrome

Консультант Плюс

Профессиональные базы данных и информационные справочные системы:

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

Электронная информационно-образовательная среда

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.