

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.21 Организационная 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: 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.....	22
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	40
6. Учебно-методическое и информационное обеспечение дисциплины.....	42
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	43

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-1 Способен разрабатывать требования по защите, формировать политику безопасности компьютерных систем и сетей

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-1 Способен разрабатывать требования по защите, формировать политику безопасности компьютерных систем и сетей	Разрабатывает требования по защите, формирует политику безопасности компьютерных систем и сетей на основе методов организационной защиты информации

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-1 Способен разрабатывать требования по защите, формировать политику безопасности компьютерных систем и сетей

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения			
		Очная (семестр)			
		2	3	5	6
1	Автоматизация деятельности предприятий		+		
2	Защита компьютерных систем от вредоносных программ		+		
3	Компьютерные сети			+	+
4	Ознакомительная практика				+
5	Основы программирования в корпоративных информационных системах		+		

6	Современные технологии обеспечения информационной безопасности	+			
7	Теоретические основы защиты информации на английском языке	+			
8	Теоретические основы информационной безопасности	+			

2. Место дисциплины в структуре ОП специалитета:

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

Дисциплина «Организационная защита информации» изучается в 9 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	64
Лекции (Лекции)	32
Лабораторные (Лаб. раб.)	32
Самостоятельная работа (СР)	80
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	
9 семестр					
1	Информационная безопасность и организационные основы защиты информации	4	4	10	Тестирование
2	Организация внутриобъектного режима предприятия	4	4	10	Тестирование

3	Организация и функции службы безопасности предприятия	4	4	12	Тестирование
4	Организация информационно-аналитической работы	4	Пп 4	12	Практическое задание для практической подготовки; Тестирование
5	Организация конфиденциального делопроизводства	4	4	12	Тестирование
6	Организация работы с персоналом предприятия	6	6	12	Тестирование
7	Правовое обеспечение информационной безопасности.	6	6	12	Тестирование

Тема 1. Информационная безопасность и организационные основы защиты информации (ПК-1)

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 2. Организация внутриобъектного режима предприятия (ПК-1)

Лекция.

В лекции рассматриваются организация внутриобъектного режима и его задачи. Организация охраны объектов предприятия: контрольно-пропускной режим на предприятии, оборудование пропускных пунктов, транспортные КПП. Организация инженерно-техническая ЗИ

Лабораторные работы.

1. Кому выдаются материальные пропуска?

-выдаются лицам, ответственным за сохранность материальных средств+

-выдаются сотрудникам при поступлении на работу на основании приказа о зачислении в штат

-выдаются лицам, работающим временно, или прикомандированным посетителям предприятия

2. Инструкция по пропускному и внутриобъектовому режимам предназначена для организации

-Для сохранения материальных ценностей.

-для устранения внутренних угроз.

-Для организации эффективного режима безопасности.+

3. Каково время действия разового пропуска?

-30 минут со времени выдачи до входа в здание+

-Действует до выхода из здания

-45 минут с момента выдачи до входа в здание

-60 минут с момента выдачи до входа в здание

4. Какие из перечисленных видов пропусков существуют

-Постоянные, временные, разовые+

-одноразовые, двухразовые

-оба варианта верно

5. Какие из перечисленных видов охраны существуют?

-Охрана с помощью технических средств

-Комбинированная охрана

-оба варианта верно+

6. Для организации внутриобъектного пропускного режима на предприятии необходимы:

-Положение

-Инструкция+

-Нормативно-правовые акты вышестоящих организаций

Задания для самостоятельной работы.

1. Что такое внутриобъектный режим?

2. Что является основной задачей службы безопасности по обеспечению охраны и внутриобъектового режима?

3. Какие основные задачи организации внутриобъектового режима?

4. Какие бывают виды пропусков?

5. Как оценивается эффективность системы защиты?

6. Что относится к факторам, влияющих на выбор приемов и средств охраны?
7. В зависимости от чего выбирается режим охраны объекта по времени?
8. Каким может быть режим охраны объекта по времени?
9. Перечислите виды охраны.
10. Что включает в себя многорубежная защита для охраны помещений?

Тема 3. Организация и функции службы безопасности предприятия (ПК-1)

Лекция.

В лекции рассматривается организационная структура службы безопасности и основные задачи и функции службы безопасности. Организация охраны объектов предприятия, организация инженерно-технической защиты, организация безопасности функционирования информационных систем. Проведение аналитико-разведывательной работы

Лабораторные работы.

1. В основу деятельности службы безопасности положены:
 - Гражданский Кодекс РФ, Уголовный Кодекс РФ, Кодекс основ о труде, Закон РФ «О безопасности».
 - Закон «О персональных данных», уголовный Кодекс РФ, Кодекс основ о труде, Гражданский Кодекс РФ.
 - Гражданский Кодекс РФ, Уголовный Кодекс РФ, Кодекс основ о труде, Закон РФ «О безопасности», Закон РФ «О частной детективной и охранной деятельности», Закон РФ «О предприятиях и предпринимательской деятельности», Закон РФ «О конкуренции и ограничении монополистической деятельности на товарных рынках», Инструкции министерств и ведомств, касающиеся соответствующих видов деятельности, Устав объекта (предприятия), коллективный договор, трудовые договоры, правила внутреннего трудового распорядка сотрудников, должностные обязанности руководителей и персонала объекта (предприятия).+
2. Служба безопасности состоит из
 - Режим охраны
 - Режим охраны, спец. Отдел+
 - Спец. Отдел
3. Мероприятия, проводимые сотрудниками службы, можно подразделить на категории:
 - Прогнозирование возможных угроз, организация деятельности по предупреждению возможных угроз (превентивные меры), выявление, анализ и оценка возникших реальных Угроз безопасности.+
 - принятие решений и организация деятельности по реагированию на возникшие угрозы, постоянное совершенствование системы обеспечения безопасности предприятия.+
 - Совершенствование систем безопасности и анализ внутренних угроз
4. Что предусматривают организационные мероприятия по охране?
 - определение границ охраняемой территории
 - реализацию мер локализации или воспрепятствования возможным каналам
 - верны оба варианта+
5. Целью создания службы безопасности
 - Обеспечение безопасности предприятия, производства, продукции и защита коммерческой, промышленной, финансовой, деловой и другой информации, независимо от ее назначения и форм+
 - Обеспечение защиты коммерческой тайны и анализ угроз
 - Обеспечение безопасности предприятия, производства, продукции
6. Какова функция организации безопасности функционирования информационных систем?
 - Защита ИС основывается на положениях и требованиях существующих

законов, стандартов и нормативно-методических документов по защите от НСД к информации.

- Защита средств вычислительной техники, входящей в состав ИС, обеспечивается комплексом программно-технических средств
- верны оба варианта+

7. Службы безопасности должна базироваться на следующих основных принципах

- Комплексность, своевременность, непрерывность, законность, плановость, совершенствование+
- Комплексность, своевременность, совершенствование
- Центральное управление, дублирование+

Задания для самостоятельной работы.

1. Что такое служба безопасности предприятия?
2. Кто принимает решение о создании системы безопасности?
3. Что такое кризисная ситуация?
4. Какие задачи решает анти-кризисная группа?
5. Что в себя включает инженерно-техническая защита информации?
6. Что относится к организационным мероприятиям по защите информации?
7. Что необходимо делать для пресечения несанкционированного доступ (НСД) к информационным системам?
8. Основными способами несанкционированного доступа к ИС являются?
9. Чему должна отводиться основная роль в деятельности службы безопасности предприятия?

Тема 4. Организация информационно-аналитической работы (ПК-1)

Лекция.

В лекции рассматриваются цели и задачи информационно-аналитической работы, направления и методы аналитической работы, этапы выполнения информационно-аналитических исследований производственных ситуаций, методы выполнения аналитических исследований. Организация аналитической работы по предупреждению утечки конфиденциальной информации

Лабораторные работы.

1. Какие существуют направления информационно аналитической работы?
 - постоянными, периодическими и разовые+
 - разовые,периодические
 - оба варианта верны
2. Основной целью информационно-аналитической работы в области обеспечения информационной безопасности предприятия можно считать:
 - Целенаправленный сбор, обработку и анализ информации, которая служит для выявления и нейтрализации реальных и потенциальных внутренних и внешних угроз.+
 - Целенаправленный сбор, обработку и анализ информации, которая служит для выявления реальных и потенциальных внутренних и внешних угроз
 - Интерпретация представленной информации
3. Качество управления предприятием зависит напрямую...
 - от переработки экономической информации о состоянии предприятия в целом и каждой из его функциональных единиц в частности, и принятия управленческих решений, носящей комплексный характер.
 - от переработки социальной и экономической информации о состоянии предприятия в целом и каждой из его функциональных единиц в частности, и принятия управленческих решений, носящей комплексный характер.+

-от переработки социальной информации о состоянии предприятия в целом и каждой из его функциональных единиц в частности, и принятия управленческих решений, носящей комплексный характер.

4. Информационно-аналитический подход включает в себя:

- тактический и стратегический методы принятия управленческих решений
- экономический, оперативный методы принятия управленческих решений
- оперативный, тактический и стратегический методы принятия управленческих решений+

5. Одним из ключевых элементов информационно-аналитического обеспечения являются:

- современные информационные технологии+
- нормативно-правовые акты
- оба варианта

6. Информационно-аналитический подход представляет собой непрерывный процесс

- выявление и классификацию информации
- обработки и анализа информации+
- классификацию и интерпретацию информации

7. Что предусматривает аналитическая работа с источником угрозы конфиденциальной информации?

- выявление и классификацию максимального состава источников угрозы конфиденциальной информации,
- анализ риска возникновения угрозы
- оба варианта верны+

8. Информационно-аналитический подход подразделяется на...

- информационный
- информационный, аналитический+
- аналитический

Задания для самостоятельной работы.

1. Что такое информационно-аналитическая деятельность?
2. Какие направления информационно – аналитической работы вы знаете?
3. Что предусматривает аналитическая работа с источником угрозы конфиденциальной информации?
4. Что является одним из самых важных разделов аналитической работы?
5. Что является первым этапом информационно-аналитической работы?
6. Что отражает частоту взаимодействия субъектов за определенный период времени?
7. Какие графики используются для регистрации событий?
8. Что представляют собой экспертные системы?
9. Что включает в себя обнаружение каналов НСД к конфиденциальной информации предприятия?
10. На каком этапе информационно-аналитической работы происходит выделение посторонней информации?

Тема 5. Организация конфиденциального делопроизводства (ПК-1)

Лекция.

В лекции рассматривается организация конфиденциального делопроизводства: конфиденциальная информация, угрозы конфиденциальной информации, электронный документооборот, классификация систем электронного документооборота

Лабораторные работы.

1. Где обрабатывается конфиденциальная информация

- Выделенное помещение
- Защищаемое помещение+
- Охраняемое помещение
- 1, 2 вариант

2. Какие документы подвергают регистрации?

- внутренние, входящие
- входящие, исходящие
- только внутренние
- правильного ответа нет+

3. Почему на пакетах (конвертах) с конфиденциальными документами не проставляют гриф конфиденциальности?

- гриф проставляют всегда+
- чтобы не привлекать внимания
- т.к. это не имеет никакого значения, важно лишь содержание конверта

4. Что делать с ошибочно присланными конфиденциальными документами (выберите верные ответы)?

- Их нужно сжечь по согласованию с отправителем
- Их нужно отправить обратно+
- По согласованию с отправителем переслать в нужный адрес+

5. Стоит ли принимать надорванный пакет (конверт) с конфиденциальными документами, если он адресован в вашу организацию?

- нет, не стоит, нужно составить акты и вернуть обратно+
- да, стоит, но составить акты
- нет, не стоит принимать, и акты составлять тоже не стоит

6. Какая отметка должна стоять в журнале учета входящих документов, если конфиденциальный документ пришел с сопроводительным письмом, которое, в свою очередь, не содержит конфиденциальной информации?

- сопроводительное письмо не нужно регистрировать

-"без приложения не конфиденциально"+

- письмо регистрируют отдельно, а приложение отдельно

7. За что отвечает служба конфиденциального делопроизводства?

- за учет и регистрацию конфиденциальных документов+
- за передачу документов между исполнителями+
- за контроль за сроками исполнения документов+
- правильного ответа нет

8. Какие документы берут на инвентарное хранение

- пронумерованные
- сброшюрованные, документы большого формата, чертежно-графические. научно- технические, в том числе являющиеся приложениями к основным, фотографии, рисунки, электронные документы на соответствующих носителях (дискеты, флэш-памяти)+
- документы большого формата, чертежно-графические. научно- технические, в том числе являющиеся приложениями к основным, фотографии, рисунки, электронные документы на соответствующих носителях (дискеты, флэш-памяти)

9. Сущность конфиденциального делопроизводства:

- Коллективная система доступа для сотрудников структурных подразделений государственного органа;
- Идентификация пользователей в соответствии с правами доступа+
- Совместная ответственность сотрудников структурных подразделений государственного органа за организацию работы с конфиденциальными документами;
- Визуальное отображение этапов прохождения документов.

10. При отправке по электронной почте подписанного ЭЦП документа будет отправлен:

- сам файл и подпись файла;
- только файл;+
- только подпись.

11. При подписании файла электронной цифровой подписью:

- создается новая версия файла, в которую добавляется подпись;
- все версии файла преобразуются с помощью крипто-алгоритмов ЭЦП;
- к файлу добавляется подпись, при этом сам файл не меняется.+

12. Разрешается ли редактирование файла, подписанного ЭЦП:

- нет;+
- да;
- разрешается только пользователю с полными правами.

13. Может ли документ одновременно быть зашифрованным и подписанным ЭЦП:

- да;+
- нет.

14. При подписании документа ЭЦП используется:

- открытый ключ;
- секретный ключ;+
- сертификат ключа.

15. Хэш-функция используется {несколько верных ответов):

- для создания сжатого образа сообщения, применяемого в ЭЦП;+
- быстрой передачи данных;
- идентификации отправителя;

- построения кода аутентификации сообщений.+

16. При верификации подписи получатель отделяет цифровую подпись от основного текста и выполняет проверку (последовательность из двух действий):

- дополнительной информации;
- применяет к тексту полученного сообщения хэш-функцию;+
- проверяет соответствие хэш-образа сообщения полученной цифровой подписи с использованием открытого ключа проверки подписи;+
- проверяет исходный код.

17. В объеме документооборота следует учитывать:

- все входящие и исходящие документы за определенный период времени все внутренние документы и все копии за определенный период времени

- все входящие и исходящие документы за определенный период времени

- все входящие, исходящие и внутренние документы, а также все копии за определенный период времени +

18. Главное правило организации документооборота – это:

- стабильный маршрут движения, который зависит от состава и содержания документов и от принятой в организации технологии работ с документами

- оперативное прохождение документа по наиболее короткому и прямому маршруту с наименьшими затратами времени +

- стереотипные маршруты движения свойственные входящим документам с наименьшими затратами времени

Задания для самостоятельной работы.

1. Что является угрозой внутренней ИТ?
2. На какие два типа делятся документы?
3. Перечислить сведения, которые составляют гос.тайну?
4. Сколько дается времени должностным лицам на оценку поступивших предложений?
5. Перечислить степени секретности информации?
6. Конфиденциальность информации-это?
7. Какая информация содержится в законе «О коммерческой тайне»?
8. Какая статья ГК определяет секрет производства (ноу-хау)?
9. Перечислить угрозы конфиденциальной информации?
10. ЭДО-это?

Тема 6. Организация работы с персоналом предприятия (ПК-1)

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?

Тема 7. Правовое обеспечение информационной безопасности. (ПК-1)

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

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

9 семестр

- посещаемость – 10 баллов
- текущий контроль – 40 баллов
- контрольные срезы – 2 среза по 10 баллов каждый
- премиальные баллы – 20 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.	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.
2.	Организация внутриобъектного режима предприятия	Тестирование(контрольный срез)	10	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.
3.	Организация и функции службы безопасности 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.
4.	Организация информационно-аналитической работы	Практическое задание для практической подготовки	5	Практические задания выполняются по тематике практических занятий. 3-5 баллов – практическое задание выполнено в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию 1-2 балла – практическое задание выполнено, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы

		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.	Организация конфиденциального делопроизводства	Тестирование(контрольный срез)	10	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.	Правовое обеспечение информационной безопасности.	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.
8.	Посещаемость		10	10 баллов – студент посетил все 100% занятий 6-7 баллов – студент посетил не менее 80% занятий 4-5 баллов – студент посетил не менее 50% занятий 1-3 балла – студент посетил не менее 25% занятий Если студент посетил менее 25% занятий, баллы не начисляются.
9.	Премияльные баллы		20	Дополнительные премияльные 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
10.	Ответ на экзамене		30	25-30 баллов – студент раскрыл основные вопросы и задания билета на оценку «отлично». 18-24 баллов – студент раскрыл основные вопросы и задания билета на оценку «хорошо», 10-17 баллов – студент раскрыл основные вопросы и задания билета на оценку «удовлетворительно»
11.	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

Практическое задание для практической подготовки

Тема 4. Организация информационно-аналитической работы

Практическое занятие № 1. Информационноаналитические технологии, их задачи

Практическое занятие № 2. Информационноаналитическое обеспечение

Практическое занятие № 3. Отчетно–информационные документы и методы их разработки

Практическое занятие № 4. Разработка рекомендаций по обеспечению защиты информации

Практическое занятие № 5. Изучение и анализ нормативно-правовых актов по обеспечению защиты информации

Тестирование

Тема 1. 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 2. Организация внутриобъектного режима предприятия

1. Кому выдаются материальные пропуска?

- выдаются лицам, ответственным за сохранность материальных средств+
- выдаются сотрудникам при поступлении на работу на основании приказа о зачислении в штат
- выдаются лицам, работающим временно, или прикомандированным посетителям предприятия

2. Инструкция по пропускному и внутриобъектовому режимам предназначена для организации

- Для сохранения материальных ценностей.
- для устранения внутренних угроз.
- Для организации эффективного режима безопасности.+

3. Каково время действия разового пропуска?

-30 минут со времени выдачи до входа в здание+

-Действует до выхода из здания

-45 минут с момента выдачи до входа в здание

-60 минут с момента выдачи до входа в здание

4. Какие из перечисленных видов пропусков существуют

-Постоянные,временные,разовые+

-одноразовые,двухразовые

-оба варианта верно

5. Какие из перечисленных видов охраны существуют?

-Охрана с помощью технических средств

-Комбинированная охрана

-оба варианта верно+

6. Для организации внутриобъектного пропускного режима на предприятии необходимы:

-Положение

-Инструкция+

-Нормативно-правовые акты вышестоящих организаций

Тема 3. Организация и функции службы безопасности предприятия

1. В основу деятельности службы безопасности положены:

- Гражданский Кодекс РФ, Уголовный Кодекс РФ, Кодекс основ о труде, Закон РФ «О безопасности».

-Закон «О персональных данных», уголовный Кодекс РФ, Кодекс основ о труде, Гражданский Кодекс РФ.

- Гражданский Кодекс РФ, Уголовный Кодекс РФ, Кодекс основ о труде, Закон РФ «О безопасности», Закон РФ «О частной детективной и охранной деятельности», Закон РФ «О предприятиях и предпринимательской деятельности», Закон РФ «О конкуренции и ограничении монополистической деятельности на товарных рынках», Инструкции министерств и ведомств, касающиеся соответствующих видов деятельности, Устав объекта (предприятия), коллективный договор, трудовые договоры, правила внутреннего трудового распорядка сотрудников, должностные обязанности руководителей и персонала объекта (предприятия).+

2. Служба безопасности состоит из

-Режим охраны

-Режим охраны, спец. Отдел+

-Спец. Отдел

3. Мероприятия, проводимые сотрудниками службы, можно подразделить на категории:

-Прогнозирование возможных угроз,организация деятельности по предупреждению возможных угроз (превентивные меры), выявление, анализ и оценка возникших реальных Угроз безопасности.+

-принятие решений и организация деятельности по реагированию на возникшие угрозы, постоянное совершенствование системы обеспечения безопасности предприятия.+

-Совершенствование систем безопасности и анализ внутренних угроз

4. Что предусматривают организационные мероприятия по охране?

-определение границ охраняемой территории

-реализацию мер локализации или воспреещения возможных каналов

-верны оба варианта+

5. Целью создания службы безопасности

- Обеспечение безопасности предприятия, производства, продукции и защита коммерческой, промышленной, финансовой, деловой и другой информации, независимо от ее назначения и форм+
- Обеспечение защиты коммерческой тайны и анализ угроз
- Обеспечение безопасности предприятия, производства, продукции

6. Какова функция организации безопасности функционирования информационных систем?

- Защита ИС основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от НСД к информации.
- Защита средств вычислительной техники, входящей в состав ИС, обеспечивается комплексом программно-технических средств
- верны оба варианта+

7. Службы безопасности должна базироваться на следующих основных принципах

- Комплексность, своевременность, непрерывность, законность, плановость, совершенствование+
- Комплексность, своевременность, совершенствование
- Центральное управление, дублирование+

Тема 4. Организация информационно-аналитической работы

1. Какие существуют направления информационно аналитической работы?

- постоянными, периодическими и разовые+
- разовые,периодические
- оба варианта верны

2. Основной целью информационно-аналитической работы в области обеспечения информационной безопасности предприятия можно считать:

- Целенаправленный сбор, обработку и анализ информации, которая служит для выявления и нейтрализации реальных и потенциальных внутренних и внешних угроз.+
- Целенаправленный сбор, обработку и анализ информации, которая служит для выявления реальных и потенциальных внутренних и внешних угроз
- Интерпретация представленной информации

3. Качество управления предприятием зависит напрямую...

- от переработки экономической информации о состоянии предприятия в целом и каждой из его функциональных единиц в частности, и принятия управленческих решений, носящей комплексный характер.
- от переработки социальной и экономической информации о состоянии предприятия в целом и каждой из его функциональных единиц в частности, и принятия управленческих решений, носящей комплексный характер.+
- от переработки социальной информации о состоянии предприятия в целом и каждой из его функциональных единиц в частности, и принятия управленческих решений, носящей комплексный характер.

4. Информационно-аналитический подход включает в себя:

- тактический и стратегический методы принятия управленческих решений
- экономический, оперативный методы принятия управленческих решений
- оперативный, тактический и стратегический методы принятия управленческих решений+

5. Одним из ключевых элементов информационно-аналитического обеспечения являются:

- современные информационные технологии+
- нормативно-правовые акты
- оба варианта

6. Информационно-аналитический подход представляет собой непрерывный процесс

- выявление и классификацию информации
- обработки и анализа информации+
- классификацию и интерпретацию информации

7. Что предусматривает аналитическая работа с источником угрозы конфиденциальной информации?

- выявление и классификацию максимального состава источников угрозы конфиденциальной информации,
- анализ риска возникновения угрозы
- оба варианта верны+

8. Информационно-аналитический подход подразделяется на...

- информационный
- информационный, аналитический+
- аналитический

Тема 5. Организация конфиденциального делопроизводства

1. Где обрабатывается конфиденциальная информация

- Выделенное помещение
- Защищаемое помещение+
- Охраняемое помещение
- 1, 2 вариант

2. Какие документы подвергают регистрации?

- внутренние, входящие
- входящие, исходящие
- только внутренние
- правильного ответа нет+

3. Почему на пакетах (конвертах) с конфиденциальными документами не проставляют гриф конфиденциальности?

- гриф проставляют всегда+
- чтобы не привлекать внимания
- т.к. это не имеет никакого значения, важно лишь содержание конверта

4. Что делать с ошибочно присланными конфиденциальными документами (выберите верные ответы)?

- Их нужно сжечь по согласованию с отправителем
- Их нужно отправить обратно+
- По согласованию с отправителем переслать в нужный адрес+

5. Стоит ли принимать надорванный пакет (конверт) с конфиденциальными документами, если он адресован в вашу организацию?

- нет, не стоит, нужно составить акты и вернуть обратно+
- да, стоит, но составить акты
- нет, не стоит принимать, и акты составлять тоже не стоит

6. Какая отметка должна стоять в журнале учета входящих документов, если конфиденциальный документ пришел с сопроводительным письмом, которое, в свою очередь, не содержит конфиденциальной информации?

- сопроводительное письмо не нужно регистрировать
- "без приложения не конфиденциально" +
- письмо регистрируют отдельно, а приложение отдельно

7. За что отвечает служба конфиденциального делопроизводства?

- за учет и регистрацию конфиденциальных документов+
- за передачу документов между исполнителями+
- за контроль за сроками исполнения документов+
- правильного ответа нет

8. Какие документы берут на инвентарное хранение

- пронумерованные
- сброшюрованные, документы большого формата, чертежно-графические. научно- технические, в том числе являющиеся приложениями к основным, фотографии, рисунки, электронные документы на соответствующих носителях (дискеты, флэш-памяти)+
- документы большого формата, чертежно-графические. научно- технические, в том числе являющиеся приложениями к основным, фотографии, рисунки, электронные документы на соответствующих носителях (дискеты, флэш-памяти)

9. Сущность конфиденциального делопроизводства:

- Коллективная система доступа для сотрудников структурных подразделений государственного органа;
- Идентификация пользователей в соответствии с правами доступа+
- Совместная ответственность сотрудников структурных подразделений государственного органа за организацию работы с конфиденциальными документами;
- Визуальное отображение этапов прохождения документов.

10. При отправке по электронной почте подписанного ЭЦП документа будет отправлен:

- сам файл и подпись файла;
- только файл;+
- только подпись.

11. При подписании файла электронной цифровой подписью:

- создается новая версия файла, в которую добавляется подпись;
- все версии файла преобразуются с помощью крипто-алгоритмов ЭЦП;
- к файлу добавляется подпись, при этом сам файл не меняется. +

12. Разрешается ли редактирование файла, подписанного ЭЦП:

- нет;+
- да;
- разрешается только пользователю с полными правами.

13. Может ли документ одновременно быть зашифрованным и подписанным ЭЦП:

- да;+
- нет.

14. При подписании документа ЭЦП используется:

- открытый ключ;
- секретный ключ;+
- сертификат ключа.

15. Хэш-функция используется {несколько верных ответов):

- для создания сжатого образа сообщения, применяемого в ЭЦП;+
- быстрой передачи данных;
- идентификации отправителя;
- построения кода аутентификации сообщений.+

16. При верификации подписи получатель отделяет цифровую подпись от основного текста и выполняет проверку (последовательность из двух действий):

- дополнительной информации;
- применяет к тексту полученного сообщения хэш-функцию;+
- проверяет соответствие хэш-образа сообщения полученной цифровой подписи с использованием открытого ключа проверки подписи;+
- проверяет исходный код.

17. В объеме документооборота следует учитывать:

- все входящие и исходящие документы за определенный период времени все внутренние документы и все копии за определенный период времени
- все входящие и исходящие документы за определенный период времени
- все входящие, исходящие и внутренние документы, а также все копии за определенный период времени +

18. Главное правило организации документооборота – это:

- стабильный маршрут движения, который зависит от состава и содержания документов и от принятой в организации технологии работ с документами
- оперативное прохождение документа по наиболее короткому и прямому маршруту с наименьшими затратами времени +
- стереотипные маршруты движения свойственные входящим документам с наименьшими затратами времени

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

Тема 7. 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 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.

4.3 Промежуточная аттестация по дисциплине проводится в форме экзамена

Типовые вопросы экзамена (ПК-1)

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 экзамена (ПК-1)

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 многократные
 - 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)
«отлично» (85 - 100 баллов)	ПК-1	Демонстрирует высокий уровень знаний основных нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации. Способен проводить работы по разработке требований по организационной защите информации и формированию политики безопасности компьютерных систем и сетей.
«хорошо» (70 - 84 баллов)	ПК-1	Демонстрирует хороший уровень знаний основных нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации. Способен проводить работы по разработке требований по организационной защите информации и формированию политики безопасности компьютерных систем и сетей.
«удовлетворительно» (50 - 69 баллов)	ПК-1	Демонстрирует низкий уровень знаний основных нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации. Способен частично проводить работы по разработке требований по организационной защите информации и формированию политики безопасности компьютерных систем и сетей.
«неудовлетворительно» (менее 50 баллов)	ПК-1	Не имеет знаний основных нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации. Не способен проводить работы по разработке требований по организационной защите информации и формированию политики безопасности компьютерных систем и сетей.

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.prlib.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.