

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

УТВЕРЖДАЮ:
Директор института



И. Н. Якунина
«20» января 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.В.ОД.2 Избранные вопросы информационной безопасности

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: 2020

Автор программы:

Кандидат педагогических наук, доцент Михайлова Елена Михайловна

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

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

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

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП Специалиста.....	6
3. Объем и содержание дисциплины.....	6
4.	19
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	61
6. Учебно-методическое и информационное обеспечение дисциплины.....	62
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	63

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ОК-12 Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации

ПК-18 Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации

1.2 Виды и задачи профессиональной деятельности по дисциплине:

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

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

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Знания и умения, необходимые для формирования трудового действия / компетенции
	ОК-12 Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	Знает и понимает: сущность и значение информации в развитии современного общества; основные теоретические положения информатики; об информационных ресурсах общества; основные методы обобщения, восприятия и анализа информации, основы информационной и библиографической культуры; основы реализации информационных технологий; современное состояние уровня и направлений развития вычислительной техники и программного обеспечения ПК.
		Умеет (способен продемонстрировать): работать с программными средствами общего назначения, в локальных и глобальных компьютерных сетях; решать стандартные задачи профессиональной деятельности с применением ИКТ.
		Владеет: навыками переработки больших объемов информации, навыками проведения целенаправленного поиска в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах.
	ПК-18 Способность	Знает и понимает:

	разрабатывать предложения по совершенствованию системы управления безопасностью информации	типы угроз информационной безопасности; законодательство РФ по защите информации, принципы обеспечения защиты информации; источники угроз ИБ РФ, современные методы и средства защиты от угроз ИБ
		Умеет (способен продемонстрировать): оценивать эффективность предлагаемых средств защиты с точки зрения экономической целесообразности
		Владеет: навыками составления документации по защите информации.

1.4 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ОК-12 Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения							
		Очная (семестр)							
		1	2	3	4	5	6	7	8
1	Аттестация и аудит объектов информатизации					+	+		
2	Базы данных		+	+					
3	Информатика	+							
4	Компьютерная экспертиза								+
5	Компьютерные сети					+	+	+	+
6	Методика обучения информатике и информационной безопасности			+					
7	Основы программирования в корпоративных информационных системах					+	+	+	
8	Программно-аппаратная защита информации						+	+	
9	Теория систем и системный анализ					+			
10	Техническая защита информации				+	+			

ПК-18 Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения
		Очная (семестр)
		10
1	Преддипломная практика	+

2. Место дисциплины в структуре ОП специалитета:

Дисциплина «Избранные вопросы информационной безопасности» относится к вариативной части учебного плана ОП по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере.

Дисциплина «Избранные вопросы информационной безопасности» изучается в 10 семестре.

3.Объем и содержание дисциплины

3.1.Объем дисциплины: 7 з.е.

Очная: 7 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	252
Контактная работа	112
Лекции (Лекции)	56
Лабораторные (Лаб. раб.)	56
Самостоятельная работа (СР)	104
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	
10 семестр					
1	Информация как объект правового регулирования.	2	-	2	Тестирование
2	Законодательство РФ в области информационной безопасности.	2	-	2	Тестирование
3	Правовые режимы защиты конфиденциальной информации.	2	-	4	Тестирование
4	Лицензирование и сертификация в информационной сфере.	2	-	4	Тестирование

5	Компьютерные правонарушения	2	-	4	Тестирование
6	Внутренние нормативные документы по ИБ.	2	-	4	Тестирование
7	Угрозы. Система управления информационной безопасностью предприятия.	2	-	4	Тестирование
8	Компьютерная экспертиза.	2	-	4	Тестирование
9	Основные свойства информации как предмета защиты	2	2	4	Тестирование
10	Организация технической защиты информации.	2	2	4	Тестирование
11	Интеллектуальная собственность и ее защита	2	2	4	Тестирование
12	Информационно-аналитическое обеспечение правоохранительной деятельности.	2	2	4	Тестирование
13	Информационно-психологическое обеспечение правоохранительной деятельности.	2	2	4	Тестирование
14	Организационная защита информации	2	2	4	Тестирование
15	Правоохранительные органы	2	2	4	Тестирование
16	Модель угроз. Угрозы безопасности информации	2	2	4	Тестирование
17	Стандарты по информационной безопасности	2	2	4	Тестирование
18	Виды источников и носителей информации	2	2	4	Тестирование
19	Источники опасных сигналов	2	4	4	Тестирование

20	Технические каналы утечки информации (особенности, характеристики, классификация).	2	4	4	Тестирование
21	Принципы технической защиты информации	2	4	4	Тестирование
22	Способы и средства инженерной защиты и технической охраны.	2	4	4	Тестирование
23	Способы и средства противодействия подслушиванию	2	4	4	Тестирование
24	Способы и средства предотвращения утечки информации с помощью закладных устройств.	2	4	4	Тестирование
25	Способы и средства предотвращения утечки информации через побочные излучения и наводки.	2	4	4	Тестирование
26	Системы идентификации и аутентификации	2	4	4	Тестирование
27	Биометрические системы идентификации и аутентификации.	4	4	4	Тестирование

Тема 1. Информация как объект правового регулирования. (ОК-12)

Лекция.

Правовой режим. Понятие информации. Документированная информация. Целостность, конфиденциальность и доступность информации. Виды тайн. Собственник, владелец и пользователь информации. Организация работы с различными источниками информации, информационными ресурсами и технологиями, применение основных методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации.

Лабораторные работы.

Тест.

Задания для самостоятельной работы.

1. Какие подходы существуют в определении понятия информации?
2. Что такое документированная информация?
3. Что такое целостность, конфиденциальность и доступность информации?
4. Какие виды тайн существуют в РФ?
5. В чем различие понятий собственник, владелец и пользователь информации?
6. Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации

Тема 2. Законодательство РФ в области информационной безопасности. (ОК-12)

Лекция.

Доктрина информационной безопасности Российской Федерации. Стратегия национальной безопасности Российской Федерации до 2020 года. Федеральный закон «О государственной тайне». Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера». Нормативные правовые акты ФСТЭК и ФСБ РФ.

Лабораторные работы.

Тест.

Задания для самостоятельной работы.

1. Что представляет собой доктрина информационной безопасности РФ?
2. Что представляет собой стратегия информационной безопасности РФ до 2020 года?
3. Какие виды отношений регулирует федеральный закон «О государственной тайне»?
4. Какие виды отношений регулирует федеральный закон «Об информации, информационных технологиях и о защите информации»?
5. Какие нормативные акты ФСТЭК и ФСБ РФ вы знаете?

Тема 3. Правовые режимы защиты конфиденциальной информации. (ОК-12)

Лекция.

Конфиденциальная информация: понятие, признаки, классификация. Административно-правовые отношения по поводу конфиденциальной информации. Структура административно-правовых режимов конфиденциальной информации. Административно-правовой режим персональных данных. Административно-правовой режим служебной тайны. Административно-правовой режим коммерческой тайны.

Лабораторные работы.

Тест.

Задания для самостоятельной работы.

1. Что такое конфиденциальная информация?
2. Какие виды сведений конфиденциального характера вы знаете?
3. Какой основной закон регулирует административно-правовые отношения по поводу конфиденциальной информации?
4. Что такое персональные данные и почему необходимо их защищать?
5. Какую информацию можно отнести к служебной тайне?

Тема 4. Лицензирование и сертификация в информационной сфере. (ОК-12)

Лекция.

Понятия лицензирования и сертификации. Нормативные и правовые документы в области лицензирования и сертификации. Органы лицензирования.

Лабораторные работы.

Тест.

Задания для самостоятельной работы.

1. Что называется лицензированием?
2. Что такое лицензия?
3. Дайте определение сертификации?
4. Что входит в организационную структуру системы лицензирования?
5. Перечислите нормативные и правовые документы в области лицензирования и сертификации.
6. Приведите пример органов лицензирования.
7. Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации

Тема 5. Компьютерные правонарушения (ПК-18)

Лекция.

Понятие компьютерных преступлений. Неправомерный доступ к компьютерной информации. Создание, использование и распространение вредоносных программ. Нарушение правил эксплуатации

Лабораторные работы.

Тест.

Задания для самостоятельной работы.

1. Что такое компьютерные преступления?
2. В чём заключается несанкционированный доступ к информации?
3. Перечислите причины несанкционированного доступа.
4. Какие программы называются вредоносными?
5. Приведите основные типы вредоносных программ.
6. Расскажите классификацию вредоносных программ.
7. Какое наказание грозит за неправомерный доступ к компьютерной информации?
8. Перечислите наказания предусмотренные за создание и распространение вредоносных программ.
9. Какие наказания предусмотрены Ст. 274 Уголовного кодекса РФ?

Тема 6. Внутренние нормативные документы по ИБ. (ОК-12)

Лекция.

Концепция обеспечения информационной безопасности. Политика ИБ. Обязательство о неразглашении защищаемых сведений. Перечень защищаемых сведений. Положение о работе с защищаемыми сведениями.

Лабораторные работы.

Тест.

Задания для самостоятельной работы.

1. Что определяет концепция обеспечения информационной безопасности?
2. Что такое политика ИБ и каково ее назначение?
3. Какие пункты содержит «Обязательство о неразглашении конфиденциальной информации»?
4. Какие сведения можно включить в «Перечень сведений конфиденциального характера»?
5. С какой целью разрабатывается «Положение о работе с защищаемыми сведениями»?

Тема 7. Угрозы. Система управления информационной безопасностью предприятия. (ПК-18)

Лекция.

Основные функции систем управления информационной безопасностью. Принципы управления информационной безопасностью. Понятие риска. Идентификация рисков. Оценка вероятности реализации угроз. Оценивание рисков. Измерение рисков. Допустимый уровень риска. Разработка предложений по совершенствованию системы управления безопасностью информации

Лабораторные работы.

Тест.

Задания для самостоятельной работы.

1. На основании положений каких международных стандартов должно осуществляться построение СУИБ?
2. Назовите три основные функции СУИБ.
3. Какова цель применения процессного подхода как одного из принципов управления ИБ?
4. Назовите этапы процесса оценки рисков ИБ.
5. Объясните цель и механизм применения количественного и качественного подхода к оценке рисков ИБ.
6. Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации

Тема 8. Компьютерная экспертиза. (ПК-18)

Лекция.

Механизм слеодообразования в компьютерных системах. Возможности исследования следов в компьютерных системах для восстановления цепочек событий. Задачи, решаемые при расследовании инцидентов, связанных с компьютерной техникой. Инструментарий компьютерного исследования. Порядок действий по организации и проведению расследований компьютерных инцидентов. Восстановление удаленной информации.

Лабораторные работы.

Анализ радиоэлектронной обстановки с использованием прибора «скорпион». Общая характеристика анализа радиоэлектронной обстановки. Использование прибора «Скорпион» для анализа радиоэлектронной обстановки.

Задания для самостоятельной работы.

1. Опишите механизм слеодообразования в компьютерных системах?
2. Какие возможности исследования следов в компьютерных системах?
3. Как восстанавливать удаленную информацию?
4. Какой порядок действия по организации и проведению расследования компьютерных инцидентов?
5. Какой инструментарий используется при компьютерном исследовании?

Тема 9. Основные свойства информации как предмета защиты (ОК-12)

Лекция.

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

Лабораторные работы.

Тест.

Задания для самостоятельной работы.

1. Каким федеральным законом РФ установлено понятие термина «информация»?
2. Какие сведения относятся к государственной тайне?
3. Какая информация является признаковой?
4. Что такое прямые и косвенные демаскирующие признаки?
5. Что такое опасный сигнал?

Тема 10. Организация технической защиты информации. (ПК-18)

Лекция.

Общие положения по инженерно-технической защите информации в организации. Краткая характеристика государственной системы защиты информации. Основные руководящие и нормативные документы по организации инженерно-технической защиты информации в организации, их сущность. Организационные и технические меры по инженерно-технической защите информации в организации. Задачи и виды контроля эффективности защиты информации.

Лабораторные работы.

Блокирование информационных угроз для пользователя. Юридические методы. Организационные меры и основные правила работы за компьютером. Программные методы. WOT. Фильтрация контента. «Родительский контроль». Нормы этического поведения в информационной среде.

Задания для самостоятельной работы.

1. Какие выделяют принципы защиты информации?
2. Что и кто обеспечивает функционирование государственной системы защиты информации?
3. Назовите основные руководящие документы по защите информации?
4. Какие выделяют организационные и технические меры по защите информации?
5. Назовите виды контроля защиты информации

Тема 11. Интеллектуальная собственность и ее защита (ОК-12)

Лекция.

Понятие интеллектуальной собственности, ее виды. Интеллектуальный продукт как объект интеллектуальной собственности и предмет защиты. Содержание гражданско-правовых норм в области защиты интеллектуальной собственности. Авторское право. Патентное право. Товарный знак. Договорное право, авторские и лицензионные договоры.

Лабораторные работы.

Классификация сканеров безопасности: по отношению к объекту сканирования, по назначению, уязвимости. Классификация, основные характеристики и особенности использования сканеров безопасности: по отношению к объекту сканирования, по назначению, уязвимости.

Задания для самостоятельной работы.

1. В чем отличие авторского от патентного права?
2. Какие виды интеллектуальной собственности существуют?
3. Что такое «интеллектуальный продукт»?
4. В чем особенность договорного права?
5. Какое содержание гражданско-правовых норм в области защиты интеллектуальной собственности?
6. Что общего между авторским и лицензионным договором?
7. Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации

Тема 12. Информационно-аналитическое обеспечение правоохранительной деятельности. (ПК-18)

Лекция.

Понятие, сущность, задачи информационно-аналитического обеспечения правоохранительной деятельности. Методика информационно-аналитической работы. Основа работы с информацией. Основные свойства и возможности юридических информационных систем. Содержание аналитической деятельности. Информационно-аналитические технологии в аналитической деятельности. Представление результатов аналитической деятельности. Информационно-аналитическое обеспечение организационно-управленческой деятельности в правоохранительных органах. Информационно-аналитическое обеспечение оперативно-розыскной деятельности в правоохранительных органах. Информационно-аналитическое обеспечение раскрытия и расследования преступлений

Лабораторные работы.

Межсетевые экраны. Классификация межсетевых экранов: по виду (типу) исполнения, по назначению, по функциональным возможностям. Определение надёжности персональных межсетевых экранов. Лик-тесты (leak-tests). Принципы работы leak-тестов

Задания для самостоятельной работы.

1. Информационное обеспечение правоохранительных органов.
2. Информационные технологии правоохранительной деятельности.
3. Правовые автоматизированные системы учета и управления.
4. Правовые автоматизированные информационные системы.
5. Правовые автоматизированные информационно-справочные

Тема 13. Информационно-психологическое обеспечение правоохранительной деятельности. (ПК-18)

Лекция.

Психологические аспекты формирования профессиональных качеств сотрудника. Основные задачи психологической подготовки. Формирование психологической готовности к борьбе с преступностью. Психологические особенности сотрудников правоохранительной сферы. Психологические особенности деятельности сотрудников. Психологические особенности личности сотрудника органов внутренних дел. Психологическая подготовка сотрудников органов внутренних дел.

Лабораторные работы.

Электронные ключи. Типизация, внутренняя структура, назначение. Базовые способы и возможности защиты программного обеспечения с помощью электронных ключей. Типовые решения в области организации ключевых систем. Утверждение о подмене эталона

Задания для самостоятельной работы.

1. Понятие информационная коммуникация.
2. Свойства информации.
3. Задачи информационно-психологической безопасности.
4. Угрозы информационно-психологической безопасности личности.
5. Средства информационно-психологического воздействия.

Тема 14. Организационная защита информации (ПК-18)

Лекция.

Концептуальные положения организационного обеспечения информационной безопасности. Организация службы безопасности объекта. Функции, задачи и особенности службы безопасности объекта. Организация внутриобъектового режима. Организация аналитической работы по предупреждению утечки конфиденциальной информации. Защита информации при проведении совещаний и переговоров. Работа с кадрами, владеющие конфиденциальной информацией. Методы обеспечения информационной безопасности российской федерации. Организация охраны объектов. Цели и задачи, объекты, виды и способы охраны. Классификация

Лабораторные работы.

Электронная подпись. Понятие целостности данных и аутентификации источника данных.

Задачи защиты информации, решаемые с помощью электронной подписи. Понятие о проверке электронной подписи. Пример реализации ЭП с помощью криптосистемы Эль-Гамала.

Понятие о проверке электронной подписи.

Задания для самостоятельной работы.

1. Дать определение организационной защите информации.
2. Назовите этапы аналитической работы.
3. Как защитить информацию при проведении конфиденциальных переговорах?
4. Что включает в себя работа с персоналом владеющим конфиденциальной информацией?
5. Назовите метода обеспечения информационной безопасности.
6. Назовите цели и задачи охраны предприятия.
7. На какие группы делятся информационные ресурсы?

Тема 15. Правоохранительные органы (ОК-12)

Лекция.

Правоохранительная деятельность: понятие, основные направления, функции. Признаки правоохранительной деятельности. Общая характеристика органов, осуществляющих ее. Система правоохранительных органов. Судебная власть: понятие и основные признаки. Ее соотношение с законодательной и исполнительной властями. Суд как орган судебной власти. Общие понятия судебной системы: Конституционный суд РФ, Верховный суд РФ и возглавляемые им общие и военные суды, Высший Арбитражный суд РФ и арбитражные суды. Понятие звена судебной системы. Основные суды, суды среднего звена и высшие суды. Понятие судебной инстанции. Понятие правосудия и его признаки. Органы, осуществляющие правоохранительную функцию; роль органов юстиции. Министерство юстиции РФ и его органы. Государственные нотариальные конторы. Понятие прокурорского надзора. Принципы организации прокуратуры. Система органов прокуратуры.

Лабораторные работы.

Симметричные шифры. Понятие симметричной системы шифрования. Преимущества и недостатки систем с симметричными ключами. Алгоритмы симметричного шифрования: 3DES, IDEA, AES, ГОСТ 29147-98

Задания для самостоятельной работы.

1. Как определяется понятие «правоохранительный орган» в учебной юридической литературе?
2. Каковы существенные признаки понятия «правоохрана»?
3. Каковы виды (формы) правоохраны?
4. Что понимать под правоохранительным органом?
5. Какие государственные органы входят в перечень правоохранительных органов? Чем определяется ограниченность этого перечня?
6. Что понимать под органами, содействующими правоохране (правоприменительными органами)? Каково практическое значение их выделения?
7. Почему теорию правоохраны следует рассматривать в качестве одной из отраслей научного знания или отраслей юридической науки?
8. Что представляет собой теория правоохраны как отрасль юридической науки?
9. Каковы объект и предмет теории правоохраны?
10. Каковы методы теории правоохраны?
11. Какова задача теории правоохраны?
12. Что является предметом учебной дисциплины «Правоохранительные органы»?

Тема 16. Модель угроз. Угрозы безопасности информации (ПК-18)

Лекция.

Понятие уязвимости. Классификация угроз. Стихийные бедствия и пожары; сбои и отказы технических средств. Угрозы утечки информации по техническим каналам. Непреднамеренные и умышленные действия пользователей. Понятие модели нарушителя. Классификация нарушителей: внешние и внутренние нарушители. Предположения об имеющейся у нарушителя информации. Описание каналов атак. Описание объектов и целей атаки. Средства осуществления атак. Способы осуществления атаки.

Лабораторные работы.

Асимметричные шифры. Шифр RSA. Понятие асимметричной системы шифрования.

Понятие открытого и секретного ключа. Алгоритм шифрования и расшифрования RSA и его математическое обоснование. Стойкость алгоритма. Рекомендуемые требования к параметрам ключа

Задания для самостоятельной работы.

1. Что такое уязвимость информационной системы?
2. По каким признакам могут быть классифицированы угрозы ИБ?
3. На какие группы делятся ТКУИ по физической природе носителя?
4. Что такое модель нарушителя, и какова ее базовая структура?
5. Какие способы атак могут использовать нарушители?

Тема 17. Стандарты по информационной безопасности (ОК-12)

Лекция.

Показатели требований к безопасности информации. Практические рекомендации по организации ИБ. Стандарт по информационной безопасности ГОСТ 17799, ГОСТ 27001. Модель и требования для создания, внедрения, эксплуатации, сопровождения и совершенствования системы управления ИБ (СУИБ).

Лабораторные работы.

Асимметричные шифры. Шифр Эль-Гамала. Понятие асимметричной системы шифрования.

Понятие односторонней функции и функции-"ловушки". Алгоритм шифрования и расшифрования Эль-Гамала и его математическое обоснование. Рекомендации по выбору параметров ключа.

Задания для самостоятельной работы.

1. Какие практические рекомендации по организации ИБ приведены в разделах ГОСТРИСО/МЭК17799?
2. Какие три основных показателя требований к безопасности информации приведены в ГОСТРИСО/МЭК17799-2005?
3. Для чего предназначен ГОСТРИСО/МЭК17799-2005?
4. С какой целью был введен ГОСТРИСО/МЭК27001-2006?
5. Каковы требования для создания, внедрения, эксплуатации, сопровождения и совершенствования системы управления ИБ?
6. Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации

Тема 18. Виды источников и носителей информации (ОК-12)

Лекция.

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). Принципы записи и съема информации с носителя. Способы записи информации на различные виды носителей. Виды модуляции (манипуляции) сигналов. Характеристики модулированных сигналов. Принципы съема информации путем демодуляции (детектирования).

Лабораторные работы.

Режимы использования шифра ГОСТ 28147-89. Режим простой замены, режим шифрования с обратной связью, режим гаммирования с обратной связью, режим гаммирования. Получение ключевой хэш-функции с использованием режима выработки имитовставки.

Задания для самостоятельной работы.

1. Каким федеральным законом РФ установлено понятие термина «информация»?
2. Приведите примеры источников, носителей и получателей информации.
3. Назовите способы организации промышленного шпионажа.
4. Назовите цели осуществления экономического шпионажа.
5. Перечислите способы записи информации на различные виды носителей.
6. Перечислите особенности амплитудной, частотной и фазовой модуляции.
7. Дайте определения термину «среда распространения носителя».
8. Перечислите функции приёмника информации.

Тема 19. Источники опасных сигналов (ПК-18)

Лекция.

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.

Поиск и устранение неисправностей в сети. Методы поиска и устранения неисправностей в сети. Выявление физических проблем. Программные средства для поиска и устранения неполадок, команды ping, tracert, nslookup, netstat, ipconfig. Поиск и устранение неполадок беспроводных подключений. Устранение неисправностей регистрации и аутентификации. Неполадки DHCP. Неисправности, связанные с подключением к интернет - провайдеру

Задания для самостоятельной работы.

1. Для чего нужны функциональные сигналы?
2. Что такое случайные опасные сигналы?
3. Какой частотный диапазон ПЭМИ?

Тема 20. Технические каналы утечки информации (особенности, характеристики, классификация) (ПК-18)

Лекция.

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.

Лабораторные работы.

Тесты на проникновение (пен-тесты). Место сканеров безопасности в комплексе средств защиты. Задачи локальных и сетевых сканеров безопасности. Объекты сканирования

Задания для самостоятельной работы.

1. Какие три основных элемента содержит любой канал передачи информации?
2. По каким техническим каналам возможна утечка семантической информации?
3. По каким каналам получают сигнальные демаскирующие признаки?

Тема 21. Принципы технической защиты информации (ПК-18)

Лекция.

Уровни безопасности информации. Методы защиты информации. Сущность инженерной защиты и технической охраны источников информации. Понятие об информационном портрете объекта защиты. Способы изменения информационного портрета при маскировке и дезинформировании. Зависимость качества информации от отношения мощностей носителя информации и помехи. Сущность энергетического скрытия. Показатели эффективности инженерно-технической защиты информации

Лабораторные работы.

Классификация сканеров безопасности: по отношению к объекту сканирования, по назначению, уязвимости. Классификация, основные характеристики и особенности использования сканеров безопасности: по отношению к объекту сканирования, по назначению, уязвимости.

Задания для самостоятельной работы.

1. Что такое политика безопасности?
2. Что включает в себя комплексная система защиты?
3. Какие способы изменения информационного портрета существуют?
4. Какие основные показатели эффективности системы защиты информации?
5. Что играет главную роль при выборе системы защиты информации?

Тема 22. Способы и средства инженерной защиты и технической охраны. (ПК-18)

Лекция.

Модели злоумышленников. Уровни физической безопасности объектов охраны. Типовая структура системы охраны. Системы автономной и централизованной охраны. Основные показатели системы охраны. Показатели эффективности инженерно-технической охраны объектов. Типовые инженерные конструкции.

Лабораторные работы.

Стеганографические методы защиты информации, принципы скрытия информации в текстовых документах, в графических изображениях. Основные особенности, характеристика стенографических методов защиты информации, электронная подпись, методы скрытия информации в текстовых документах, в графических изображениях.

Задания для самостоятельной работы.

1. Перечислите модели злоумышленников. Охарактеризуйте каждый из них.
2. В чем заключаются задачи физической защиты?
3. Опишите типовую структуру системы охраны.
4. Дайте рекомендации по повышению укреплённости зданий и помещений.

Тема 23. Способы и средства противодействия подслушиванию (ПК-18)

Лекция.

Способы и средства информационного скрытия акустических сигналов и речевой информации. Способы и средства информационного скрытия информации от подслушивания. Виды информационного скрытия речевой информации. Классификация способов технического закрытия. Сущность способов технического закрытия. Методы энергетического скрытия акустических сигналов: звукоизоляция и звукопоглощение

Лабораторные работы.

Методы обнаружения и противодействия вредоносным программам. Обнаружение неизвестного вируса. Основные правила защиты. Восстановление пораженных объектов. Обнаружение троянской программы. Защита от программных закладок и шпионов. Антивирусное программное обеспечение. Обзор современных антивирусных программ. Методика использования антивирусных программ. Прогнозы развития антивирусного обеспечения.

Задания для самостоятельной работы.

- 1.Перечислите модели злоумышленников. Охарактеризуйте каждый из них.
- 2.В чем заключаются задачи физической защиты?
- 3.Опишите типовую структуру системы охраны.
- 4.Дайте рекомендации по повышению укрепленности зданий и помещений.

Тема 24. Способы и средства предотвращения утечки информации с помощью закладных устройств. (ПК-18)

Лекция.

Классификация средств обнаружения, локализации и подавления закладных устройств. Принципы работы и основные характеристики обнаружителей электромагнитного поля, их достоинства и недостатки, способы применения. Возможности бытовых приемников и селективных вольтметров. Особенности специальных радиоприемников. Типы и параметры сканирующих приемников. Состав, принципы работы, возможности и параметры автоматизированных комплексов радиоконтроля помещений. Способы контроля телефонных линий и цепей электропитания. Способы подавления сигналов закладных устройств. Типы генераторов радиопомех.

Лабораторные работы.

Системы идентификации и аутентификации. Парольные подсистемы идентификации и аутентификации личности. Количественная оценка стойкости парольной защиты. Аппаратные устройства идентификации и аутентификации.

Задания для самостоятельной работы.

- 1.Назовите средства обнаружения, локализации и подавления закладных устройств.
- 2.Опишите принцип работы идентификатора поля.
- 3.Что нужно для обнаружения и измерения основных характеристик ПЭМИ?
- 4.Какие устройства применяются для контроля телефонных линий?
- 5.Какие средства подавления закладных устройств вам известны?

Тема 25. Способы и средства предотвращения утечки информации через побочные излучения и наводки. (ПК-18)

Лекция.

Требования к средствам подавления сигналов побочных электромагнитных излучений и наводок. Методы и средства пассивного подавления опасных сигналов акустоэлектрических преобразователей. Экранирование электрических, магнитных и электромагнитных полей. Экранирование проводов и кабелей. Материалы для экранирования. Требования к заземлению и конструкция заземлителей. Развязка и фильтрация цепей электропитания. Средства активного линейного и пространственного зашумления.

Лабораторные работы.

Блочные шифры. Шифр DES. Понятие блочного шифра. Структура алгоритма DES. Стойкость алгоритма DES и возможность нахождения ключа полным перебором. Модификации DES: 3DES (DES-EDE) и DESX. Современный стандарт шифрования AES.

Задания для самостоятельной работы.

- 1.Какие выделяют требования к средствам подавления ПЭМИН?
- 2.Способы защиты от опасных сигналов акустоэлектрических преобразователей?
- 3.Какими материалами можно экранировать провода и кабели?
- 4.Назовите требования к заземлению?
- 5.Чем можно фильтровать сигналы в цепях электропитания?
- 6.Какие бывают средства активного и пространственного зашумления?

Тема 26. Системы идентификации и аутентификации (ПК-18)

Лекция.

Парольные подсистемы идентификации и аутентификации личности. Количественная оценка стойкости парольной защиты. Аппаратные устройства идентификации и аутентификации.

Лабораторные работы.

Блочные шифры. Шифр ГОСТ 28147-89. Понятие блочного шифра. Структура алгоритма ГОСТ 28147-89. Стойкость алгоритма ГОСТ 28147-89.

Задания для самостоятельной работы.

1. Что такое аутентификация?
2. Что такое идентификация?
3. На чем основана идентификация пользователя?
4. Каковы возможные реакции системы на неудачную попытку входа пользователя в систему?
5. На какие электронные СИА по способу обмена данными между идентификатором и устройством ввода-вывода подразделяются?

Тема 27. Биометрические системы идентификации и аутентификации. (ПК-18)

Лекция.

Типизация, режимы функционирования, архитектура, базовые отличия от других систем идентификации и аутентификации

Лабораторные работы.

Бесключевые хэш-функции. Понятие хэш-функции. Назначение бесключевых хэш-функций. Требования к бесключевым хэш-функциям. Примеры наиболее популярных бесключевых хэш-функций. Возможные атаки на бесключевые функции хеширования.

Задания для самостоятельной работы.

1. Назовите и поясните достоинства и недостатки биометрических систем идентификации и аутентификации.
2. Поясните принцип функционирования систем идентификации и аутентификации по отпечаткам пальцев, назовите их достоинства и недостатки.
3. Поясните принцип функционирования систем идентификации и аутентификации по геометрии кисти руки, назовите их достоинства и недостатки.
4. Поясните принцип функционирования систем идентификации и аутентификации по радужной оболочке глаза, назовите их достоинства и недостатки.
5. Поясните принцип функционирования систем идентификации и аутентификации по сетчатке глаза, назовите их достоинства и недостатки.
6. Поясните принцип функционирования систем идентификации и аутентификации по голосу, назовите их достоинства и недостатки.
7. Поясните принцип функционирования систем идентификации и аутентификации по геометрии лица, назовите их достоинства и недостатки.

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

10 семестр

- посещаемость – 10 баллов
- текущий контроль – 50 баллов
- контрольные срезы – 2 среза по 5 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.	Информация как объект правового регулирования.	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
2.	Законодательство РФ в области информационной безопасности.	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
3.	Правовые режимы защиты конфиденциальной информации.	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
4.	Лицензирование и сертификация в информационной сфере.	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
5.	Компьютерные правонарушения	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
6.	Внутренние нормативные документы по ИБ.	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
7.	Угрозы. Система управления информационной безопасностью предприятия.	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
8.	Компьютерная экспертиза.	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
9.	Основные свойства информации как предмета защиты	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.

10.	Организация технической защиты информации.	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
11.	Интеллектуальная собственность и ее защита	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
12.	Информационно-аналитическое обеспечение правоохранительной деятельности.	Тестирование(контрольный срез)	5	Тест состоит из вопросов с выбором ответа. 4-5 баллов - студент правильно отвечает более чем на 90% вопросов. 3 балла – студент правильно отвечает на 50-80% вопросов в тесте. 2 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
13.	Информационно-психологическое обеспечение правоохранительной деятельности.	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
14.	Организационная защита информации	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
15.	Правоохранительные органы	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
16.	Модель угроз. Угрозы безопасности информации	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
17.	Стандарты по информационной безопасности	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
18.	Виды источников и носителей информации	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
19.	Источники опасных сигналов	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.

20.	Технические каналы утечки информации (особенности, характеристики, классификация).	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
21.	Принципы технической защиты информации	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
22.	Способы и средства инженерной защиты и технической охраны.	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
23.	Способы и средства противодействия подслушиванию	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
24.	Способы и средства предотвращения утечки информации с помощью закладных устройств.	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
25.	Способы и средства предотвращения утечки информации через побочные излучения и наводки.	Тестирование(контрольный срез)	5	Тест состоит из вопросов с выбором ответа. 4-5 баллов - студент правильно отвечает более чем на 90% вопросов. 3 балла – студент правильно отвечает на 50-80% вопросов в тесте. 2 балла - студент правильно отвечает на 30-50% вопросов. 1 балл - студент правильно отвечает на 25-30% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
26.	Системы идентификации и аутентификации	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.
27.	Биометрические системы идентификации и аутентификации.	Тестирование	2	Тест состоит из вопросов с выбором ответов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте. 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает.

28.	Посещаемость	10	<p>10 баллов – стопроцентное посещение занятий студентом</p> <p>7-9 баллов – посещаемость студента составляет не менее 80 % занятий</p> <p>4-6 баллов – посещаемость студента составляет не менее 50 % занятий</p> <p>1-3 балла – посещаемость студента составляет не менее 25 % занятий</p>
29.	Премияльные баллы	20	<p>Дополнительные премиальные баллы могут быть начислены:</p> <ul style="list-style-type: none"> - 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

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

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

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

4.2 Типовые оценочные средства текущего контроля

Тестирование

Тема 1. Информация как объект правового регулирования.

1. Информация это -

- 1 сведения, поступающие от СМИ
- 2 только документированные сведения о лицах, предметах, фактах, событиях
- 3 сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления+
- 4 только сведения, содержащиеся в электронных базах данных

2. Информация

- 1 не исчезает при потреблении
- 2 становится доступной, если она содержится на материальном носителе
- 3 подвергается только "моральному износу"
- 4 характеризуется всеми перечисленными свойствами +

3. Информация, зафиксированная на материальном носителе, с реквизитами,

- 1 позволяющими ее идентифицировать, называется
- 2 достоверной
- 3 конфиденциальной+
- 4 документированной
- 5 коммерческой тайной

4. Формы защиты интеллектуальной собственности -

- 1 авторское, патентное право и коммерческая тайна+
- 2 интеллектуальное право и смежные права
- 3 коммерческая и государственная тайна
- 4 гражданское и административное право

5. По принадлежности информационные ресурсы подразделяются на

- 1 государственные, коммерческие и личные+
- 2 государственные, не государственные и информацию о гражданах
- 3 информацию юридических и физических лиц
- 4 официальные, гражданские и коммерческие

6. К негосударственным относятся информационные ресурсы

- 1 созданные, приобретенные за счет негосударственных учреждений и организаций
- 2 созданные, приобретенные за счет негосударственных предприятий и физических лиц
- 3 полученные в результате дарения юридическими или физическими лицами

указанные в п.1-3

4. указанные в п.1-3.+

7. По доступности информация классифицируется на

- 1 открытую информацию и государственную тайну
- 2 конфиденциальную информацию и информацию свободного доступа
- 3 информацию с ограниченным доступом и общедоступную информацию+
- 4 виды информации, указанные в остальных пунктах

8. К конфиденциальной информации относятся документы, содержащие

- 1 государственную тайну+
- 2 законодательные акты
- 3 "ноу-хау"

4 сведения о золотом запасе страны

9. Запрещено относить к информации ограниченного доступа:

- 1 информацию о чрезвычайных ситуациях
- 2 информацию о деятельности органов государственной власти
- 3 документы открытых архивов и библиотек
- 4 все, перечисленное в остальных пунктах+

Тема 2. Законодательство РФ в области информационной безопасности.

1. К конфиденциальной информации не относится

- 1 коммерческая тайна
- 2 персональные данные о гражданах
- 3 государственная тайна
- 4 "ноу-хау"+

2. Вопросы информационного обмена регулируются (...) правом

- 1 гражданским+
- 2 информационным
- 3 конституционным
- 4 уголовным

3. Согласно ст.132 ГК РФ интеллектуальная собственность это

- 1 информация, полученная в результате интеллектуальной деятельности индивида
- 2 литературные, художественные и научные произведения
- 3 изобретения, открытия, промышленные образцы и товарные знаки
- 4 исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности+

4. Интеллектуальная собственность включает права, относящиеся к

- 1 литературным, художественным и научным произведениям, изобретениям и
- 2 открытиям
- 3 исполнительской деятельности артиста, звукозаписи, радио- и телепередачам
- 4 промышленным образцам, товарным знакам, знакам обслуживания, фирменным+
- 5 наименованиям и коммерческим обозначениям
- 6 всему, указанному в остальных пунктах

5. Конфиденциальная информация это

- 1 сведения, составляющие государственную тайну
- 2 сведения о состоянии здоровья высших должностных лиц
- 3 документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ+
- 4 данные о состоянии преступности в стране

6. Какая информация подлежит защите?

- 1 информация, циркулирующая в системах и сетях связи
- 2 зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать
- 3 только информация, составляющая государственные информационные ресурсы

- 4 любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу+
7. Система защиты государственных секретов определяется Законом
- 1 "Об информации, информатизации и защите информации"
 - 2 "Об органах ФСБ"
 - 3 "О государственной тайне"+
 - 4 "О безопасности"
8. Государственные информационные ресурсы не могут принадлежать
- 1 физическим лицам
 - 2 коммерческим предприятиям
 - 3 негосударственным учреждениям
 - 4 всем перечисленным субъектам+
9. Из нижеперечисленных законодательных актов наибольшей юридической силой в вопросах информационного права обладает
- 1 Указ Президента "Об утверждении перечня сведений, относящихся к государственной тайне"+
 - 2 ГК РФ
 - 3 Закон "Об информации, информатизации и защите информации"
 - 4 Конституция
10. Классификация и виды информационных ресурсов определены
- 1 Законом "Об информации, информатизации и защите информации"+
 - 2 Гражданским кодексом
 - 3 Конституцией
 - 4 всеми документами, перечисленными в остальных пунктах

Тема 3. Правовые режимы защиты конфиденциальной информации.

1. Формой правовой защиты литературных, художественных и научных произведений является (...) право
- 1 литературное
 - 2 художественное
 - 3 авторское+
 - 4 патентное
2. Запрещено относить к информации с ограниченным доступом
- 1 законодательные акты, информацию о чрезвычайных ситуациях и информацию ограниченного доступа
 - 2 деятельности органов государственной власти (кроме государственной тайны)+
 - 3 только информацию о чрезвычайных ситуациях
 - 4 только информацию о деятельности органов государственной власти (кроме государственной тайны)
 - 5 документы всех библиотек и архивов
3. Формой правовой защиты изобретений является
- 1 институт коммерческой тайны
 - 2 патентное право+
 - 3 авторское право

4 все, перечисленное в остальных пунктах

4. К коммерческой тайне могут быть отнесены

- 1 сведения не являющиеся государственными секретами
- 2 сведения, связанные с производством и технологической информацией
- 3 сведения, связанные с управлением и финансами
- 4 сведения, перечисленные в остальных пунктах+

5. Является ли авторское право, патентное право и КТ формами защиты интеллектуальной собственности?

- 1 да+
- 2 нет
- 3 только авторское и патентное
- 4 только КТ

6. «Ноу-хау» это -

- 1 незащищенные новшества
- 2 защищенные новшества+
- 3 общеизвестные новые технологии
- 4 опубликованные технические и технологические новинки

7. Каким законом в РФ защищаются права исполнителей и производителей фонограмм?

- 1 "О правовой охране программ для ЭВМ и баз данных"
- 2 "Об авторском праве и смежных правах"+
- 3 "Патентный закон РФ"
- 4 закон еще не принят

8. Закон "Об авторском праве и смежных правах" защищает права

- 1 исполнителей (актеров, певцов и т.д.)
- 2 производителей фонограмм
- 3 организации эфирного и кабельного вещания+
- 4 всех лиц, перечисленных в остальных пунктах

9. Какой законодательный акт содержит сведения по защите коммерческой тайны?

- 1 Закон "Об авторском праве и смежных правах"
- 2 Закон "О коммерческой тайне"+
- 3 Патентный закон
- 4 Закон "О правовой охране программ для ЭВМ и баз данных"

10. К информации ограниченного доступа не относится

- 1 государственная тайна
- 2 размер золотого запаса страны
- 3 персональные данные+
- 4 коммерческая тайна

11. Система защиты государственных секретов

- 1 основывается на Уголовном Кодексе РФ
- 2 регулируется секретными нормативными документами
- 3 определена Законом РФ "О государственной тайне"+

4 осуществляется в соответствии с п.1-3

12. Действие Закона "О государственной тайне" распространяется

- 1 на всех граждан и должностных лиц РФ
- 2 только на должностных лиц
- 3 на граждан, которые взяли на себя обязательство выполнять требования законодательства о государственной тайне
- 4 на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения+

13. К государственной тайне относится...

- 1 информация в военной области
- 2 информация о внешнеполитической и внешнеэкономической деятельности государства
- 3 информация в области экономики, науки и техники и сведения в области разведывательной и оперативно-розыскной деятельности
- 4 все выше перечисленное+

14. Документы, содержащие государственную тайну снабжаются грифом

- 1 "секретно"
- 2 "совершенно секретно"
- 3 "особой важности"
- 4 указанным в п.1-3+

15. Гриф "ДСП" используется

- 1 для секретных документов
- 2 для документов, содержащих коммерческую тайну
- 3 как промежуточный для несекретных документов+
- 4 в учебных целях

16. Порядок засекречивания состоит в установлении следующих принципов:

- 1 целесообразности и объективности
- 2 необходимости и обязательности
- 3 законности, обоснованности и своевременности
- 4 всех выше перечисленных+

17. Предельный срок пересмотра ранее установленных грифов секретности составляет

- 1 5 лет+
- 2 1 год
- 3 10 лет
- 4 15 лет

18. Срок засекречивания сведений, составляющих государственную тайну

- 1 составляет 10 лет
- 2 ограничен 30 годами+
- 3 не ограничен

Тема 4. Лицензирование и сертификация в информационной сфере.

1. Лицензированием в области защиты информации называется:

- 1 деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации. +

- 2 деятельность, заключающаяся в обработке или хранение документов
- 3 защита информации

2. Лицензией называется:

- 1 информация о внешнеполитической и внешнеэкономической деятельности государства
- 2 разрешение на право проведения работ в области защиты информации.+
- 3 все выше перечисленное

3. На какой срок выдается лицензия?:

- 1 5 лет
- 2 1 год
- 3 3 года+

4. Что нужно делать после истечения срока действия лицензии?:

- 1 перерегистрация в порядке, установленном для выдачи лицензии+
- 2 купить пробную версию лицензии
- 3 продолжать пользоваться продуктом без лицензии

5. Какие условия нужны для предприятия что бы получить лицензию:

- 1 производственную и испытательную базу
- 2 нормативную и методическую документацию
- 3 располагает научным и инженерно-техническим персоналом
- 4 все выше перечисленное+

6. Организационную структуру лицензирования образуют(два варианта ответа):

- 1 государственные органы по лицензированию+
- 2 лицензионные центры+
- 3 лицензируемые объекты

7. Государственные органы по лицензированию:

- 1 организуют обязательное государственное лицензирование деятельности предприятий+
- 2 планируют и проводят работы по экспертизе предприятий-заявителей;
- 3 контролируют полноту и качество выполненных лицензиатами работ.

8. Лицензионные центры:

- 1 выдают государственные лицензии предприятиям-заявителям;
- 2 согласовывают составы экспертных комиссий, представляемые лицензионными центрами
- 3 формируют экспертные комиссии и представляют их состав на согласование руководителям соответствующих государственных органов по лицензированию, которыми являются ФСТЭК и ФСБ;+

Тема 5. Компьютерные правонарушения

1. Компьютерное преступление(два правильных ответа):

- 1 любое противоправное действие, при котором компьютер выступает либо как объект, против которого совершается преступление, либо как инструмент, используемый для совершения преступных действий.+
- 2 хищение, шпионаж, незаконное собирание сведений, которые составляют коммерческую тайну, и т.д., если оно совершается с использованием компьютера+

- 3 доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

2. Несанкционированный доступ:

- 1 доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.+
- 2 преступления, при совершении которых компьютерная техника, информация или электронная обработка информации выступают в качестве предмета или средства совершения преступления
- 3 хищение, шпионаж, незаконное собирание сведений, которые составляют коммерческую тайну, и т.д., если оно совершается с использованием компьютера

3. Причины возникновения компьютерных преступлений:

- 1 изменение идеологии хранения, обработки и передачи информации;
- 2 использование программных средств, имеющих ошибки в кодах приложений;
- 3 использование программных продуктов, не включающих системы защиты информации;
- 4 все выше перечисленное+

4. Неправомерный доступ к охраняемой законом компьютерной информации несет за собой денежный штраф в размере:

- 1 до 500 т.р
- 2 до 100 т.р
- 3 до 200 т.р+

5. Использование вредоносных компьютерных программ предназначены:

- 1 для несанкционированного уничтожения
- 2 блокирования
- 3 модификации
- 4 все выше перечисленное+

6. типы вредоносных программ:

- 1 вирусы, черви, троянские и хакерские программы+
- 2 шпионское, рекламное программное обеспечение, Вирусы
- 3 потенциально опасное программное обеспечение, программы скрытого дозвола

7. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации наказывается штрафом в размере:

- 1 до 500 т.р+
- 2 до 100 т.р
- 3 до 200 т.р

8. Расположите вирусы по вредоносной нагрузке:

- 1 Похищение данных, представляющих ценность или тайну.4
- 2 Саботирование промышленных процессов, управляемых компьютером (этим известен червь Stuxnet).2
- 3 Распаковка другой вредоносной программы, уже содержащейся внутри файла (dropper).3
- 4 Блокировка антивирусных сайтов, антивирусного ПО и административных функций ОС с целью усложнить лечение.1

Тема 6. Внутренние нормативные документы по ИБ.

1. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
 - 1 меры обеспечения целостности;+
 - 2 административные меры;
 - 3 меры обеспечения конфиденциальности.+
2. Дублирование сообщений является угрозой:
 - 1 доступности;
 - 2 конфиденциальности;
 - 3 целостности.+
3. Вредоносное ПО Melissa подвергает атаке на доступность:
 - 1 системы электронной коммерции;
 - 2 геоинформационные системы;
 - 3 системы электронной почты.+
4. Выберите вредоносную программу, которая открыла новый этап в развитии данной области.
 - 1 Melissa.+
 - 2 Bubble Boy.
 - 3 ILO VE YOU.
5. Самыми опасными источниками внутренних угроз являются:
 - 1 некомпетентные руководители;+
 - 2 обиженные сотрудники;+
 - 3 любопытные администраторы.
6. Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности.
 - 1 просчеты при администрировании информационных систем;
 - 2 необходимость постоянной модификации информационных систем;
 - 3 сложность современных информационных систем.+
7. Агрессивное потребление ресурсов является угрозой:
 - 1 доступности+
 - 2 конфиденциальности
 - 3 целостности
8. Программа Melissa — это:
 - 1 бомба;
 - 2 вирус;+
 - 3 червь.
9. Для внедрения бомб чаще всего используются ошибки типа:
 - 1 отсутствие проверок кодов возврата;
 - 2 переполнение буфера;+
 - 3 нарушение целостности транзакций.
10. Окно опасности появляется, когда:

- 1 становится известно о средствах использования уязвимости;
- 2 появляется возможность использовать уязвимость;+
- 3 устанавливается новое ПО.

Тема 7. Угрозы. Система управления информационной безопасностью предприятия.

1. Криптография необходима для реализации следующих сервисов безопасности:
 - 1 идентификация;
 - 2 экранирование;
 - 3 аутентификация.+
2. Криптография необходима для реализации следующих сервисов безопасности:
 - 1 контроль конфиденциальности;+
 - 2 контроль целостности;
 - 3 контроль доступа.
3. Экран выполняет функции:
 - 1 разграничения доступа;+
 - 2 облегчения доступа;
 - 3 усложнения доступа.
4. Демилитаризованная зона располагается:
 - 1 перед внешним межсетевым экраном;
 - 2 между межсетевыми экранами;+
 - 3 за внутренним межсетевым экраном.
5. Экранирование на сетевом и транспортном уровнях может обеспечить:
 - 1 разграничение доступа по сетевым адресам;+
 - 2 выборочное выполнение команд прикладного протокола;
 - 3 контроль объема данных, переданных по ТСП-соединению.
6. Системы анализа защищенности помогают предотвратить:
 - 1 известные атаки;
 - 2 новые виды атак;+
 - 3 нетипичное поведение пользователей.
7. Среднее время наработки на отказ:
 - 1 пропорционально интенсивности отказов;
 - 2 обратно пропорционально интенсивности отказов;+
 - 3 не зависит от интенсивности отказов.
8. Туннелирование может использоваться на следующем уровне эталонной семиуровневой модели OSI:
 - 1 сетевом;+
 - 2 сеансовом;
 - 3 уровне представления.
9. Принцип усиления самого слабого звена можно переформулировать как:
 - 1 принцип равной прочности обороны;+
 - 2 принцип удаления слабого звена;

3 принцип выявления главного звена, ухватившись за которое, можно вытянуть всю цепь.

10. Политика безопасности:

- 1 фиксирует правила разграничения доступа;
- 2 отражает подход организации к защите своих информационных активов;+
- 3 описывает способы защиты руководства организации.

11. При анализе стоимости защитных мер следует учитывать:

- 1 расходы на закупку оборудования+
- 2 расходы на закупку программ+
- 3 расходы на обучение персонала+

Тема 8. Компьютерная экспертиза.

1.Виды компьютерно-технической экспертизы:

- 1 Аппаратно-компьютерная экспертиза;
- 2 Программно-компьютерная экспертиза
- 3 Компьютерно-сетевая экспертиза;
- 4 все вышеперечисленные+

2.Обычно перед экспертом ставятся вопросы:

- 1 о возможности (пригодности) использования исследуемых объектов для определённых целей (например, для доступа в сеть);+
- 2 о стоимости компьютеров, носителей, лицензий на содержащиеся там программы;
- 3 о переводах найденных текстов, интерфейсов программ, переписки и т. п.

3.Следующие вопросы не должны относиться к данному виду экспертизы, их включение в постановление представляется ошибочным:

- 1 о свойствах программ для ЭВМ, в частности, о принадлежности их к вредоносным;
- 2 об идентификации найденных электронных документов, программ для ЭВМ, пользователей компьютера.
- 3 о лицензионности/контрафактности экземпляров программ, записанных на исследуемых объектах;+

4.Используемые программы:

- 1 DeFacto+
- 2 CCleaner
- 3 Booster

5.Класс аппаратных объектов:

- 1 компьютеры персональные (ноутбуки, настольные, портативные);+
- 2 стол
- 3 шкаф

6.Вопросы для компьютерно-технической экспертизы аппаратных средств(два ответа):

- 1 определить, относится ли представленное устройство к аппаратным компьютерным средствам;+
- 2 определить совместимость конкретного программного средства с программным и аппаратным обеспечением компьютерной системы;
- 3 определить, используется ли данное программное средство для решения определенной функциональной задачи;

4 определить, к какому типу (марке, модели) относится аппаратное (компьютерное) средство;+

7. Вопросы компьютерно-технической экспертизе программных средств (два ответа):

- 1 определить, какую классификацию имеют конкретные программные средства (системные или прикладные) представленного программного обеспечения;+
- 2 определить общую характеристика представленного на судебную компьютерно-техническую экспертизу программного обеспечения, из каких компонент (программных средств) оно состоит;+
- 3 определить, какое запоминающее устройство предназначено для работы с данным носителем информации;
- 4 определить, имеется ли в составе представленного компьютера, какое-либо запоминающее устройство для работы с этим носителем информации;

8. Вопросы компьютерно-технической экспертизе информации (данных) (два ответа):

- 1 определить, имеются ли в программном средстве отклонения от нормальных параметров (например, свойства инфицирования, недокументированных функций);
- 2 определить характеристики физического размещения данных на носителе информации (компьютере);+
- 3 определить, каким образом организованы ввод и вывод данных в представленном компьютере (программном средстве);
- 4 определить, каким образом был отформатирован носитель информации (компьютер) и в каком виде на него записаны данные;+

Тема 9. Основные свойства информации как предмета защиты

1. В соответствии с терминологией Закона №149 ФЗ «Об информации, информационных технологиях и защите информации» информация это

- 1 сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления+
- 2 защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.
- 3 характерное свойство объекта защиты, которое может быть использовано технической разведкой для обнаружения и распознавания объекта, а также для получения необходимых сведений о нем.

2. Защите не подлежит информация:

- 1 секретная
- 2 конфиденциальная
- 3 своевременная+

3. Дайте определение Государственной тайны:

- 1 сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
- 2 защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.+

- 3 характерное свойство объекта защиты, которое может быть использовано технической разведкой для обнаружения и распознавания объекта, а также для получения необходимых сведений о нем.
4. Под конфиденциальной понимается информация с:
 - 1 ограниченным доступом, не содержащая государственную тайну+
 - 2 неограниченным доступом
 - 3 с ограниченным доступом, содержащая государственную тайну
5. Под демаскирующим признаком понимается свойство объекта:
 - 1 связанное с функционированием объекта защиты и проявляющееся через их физические поля
 - 2 которое может быть использовано технической разведкой для обнаружения и распознавания объекта
 - 3 отличаться по каким-либо характеристикам от других объектов.+
6. Что не относится к основным источникам функциональных сигналов относятся:
 - 1 источники систем связи
 - 2 передатчики радиотехнических систем
 - 3 распространители электромагнитных сигналов+
7. Обнаружение объекта это
 - 1 процесс функционирования средства технической разведки (ТР), в результате которого фиксируются технические демаскирующие признаки объекта и делается заключение о его наличии.+
 - 2 процесс функционирования средства ТР, в результате которого определяются параметры демаскирующего признака объекта и делается заключение о его характеристиках
 - 3 техническое средство, предназначенное для устранения или ослабления демаскирующих признаков объекта, создания ложных (имитирующих) признаков, а также для создания помех техническим средствам доступа к информации
8. Что такое семантическая информация:
 - 1 процесс функционирования средства технической разведки
 - 2 продукт абстрактного мышления человека и обработки данных рецепторов других живых существ+
 - 3 сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления

Тема 10. Организация технической защиты информации.

1. Что представляет собой ресурс системы защиты информации?
 - 1 количество специалистов по защите информации
 - 2 состав инженерно-технических сооружений
 - 3 выделенные денежные средства
 - 4 все вместе+
2. Что надо определить перед выбором мер защиты информации?
 - 1 квалификацию персонала
 - 2 угрозы безопасности информации+
 - 3 систему пожарно-охранной сигнализации
3. Локальные показатели эффективности защиты информации подразделяются на:

- 1 тактические и стратегические
 - 2 оперативные и постоянные
 - 3 функциональные и экономические+
 - 4 территориальные и пространственные
4. Что означает принцип экономичности защиты информации?
- 1 минимизация затрат на защиту информации
 - 2 затраты на защиту информации не должны превышать возможный ущерб от реализации угроз+
 - 3 численность службы защиты информации не должна превышать 7 чел.
 - 4 комплексное использование различных способов и средств защиты информации
5. Что означает принцип рациональности защиты информации?
- 1 использование только сертифицированных средств защиты
 - 2 системный подход к инженерно—технической защите информации
 - 3 минимизацию ресурсов на обеспечение необходимого уровня безопасности информации+
 - 4 все вместе
6. Зоны защиты объектов информатизации бывают:
- 1 независимыми, пересекающимися и вложенными+
 - 2 автономными, многоярусными и многозвенными
 - 3 укрепленными, локальными и общими
7. Чем отличаются ОТСС от ВТСС?
- 1 потребляемой мощностью
 - 2 наличием принятых мер по защите информации+
 - 3 не могут использоваться для обработки открытой информации
 - 4 большей скоростью обработки информации
8. По способу формирования электрического сигнала активные акустоэлектрические преобразователи могут быть
- 1 индуктивными, электродинамическими и пьезоэлектрическими
 - 2 емкостными, электродинамическими и электромагнитными
 - 3 электродинамическими, электромагнитными и пьезоэлектрическими+
 - 4 индуктивными, емкостными и резистивными
9. Чувствительность электродинамического микрофона лежит в пределах
- 1 30 - 45 мВ/Па
 - 2 4 - 6 мВ/Па+
 - 3 0,1 – 0,5 мВ/Па
 - 4 0,001 – 0,2 мВ/Па
10. Чувствительность вторичных электрических часов как акустоэлектрических преобразователей
- 1 30 - 45 мВ/Па
 - 2 4 - 6 мВ/Па
 - 3 0,1 – 0,5 мВ/Па+
 - 4 0,001 – 0,2 мВ/Па
 - 5 Ключ к тесту:

1. К объектам интеллектуальной собственности относятся:

- 1 селекционные достижения;
- 2 товары и услуги;
- 3 произведения прикладного искусства;+
- 4 секреты производства (ноу-хау);+
- 5 фонограммы;+
- 6 логотипы;+
- 7 музыкальные произведения.+

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

- 1 литературных произведений;+
- 2 изобретений;
- 3 компьютерных программ;+
- 4 фотографий;+
- 5 промышленных образцов.

3. Результат интеллектуальной деятельности может одновременно использоваться:

1. одним лицом;
2. группой лиц до 10 человек;
3. группой лиц более 10 человек;
4. неограниченным кругом лиц.+

4. К объектам авторского права относятся:

- 1 новые сорта растений;
- 2 музыкальные произведения;+
- 3 товарные знаки;
- 4 идеи, концепции, открытия;
- 5 научные статьи.+

5. Авторское право возникает:

- 1 с момента возникновения идеи произведения;
- 2 после регистрации произведения и получения свидетельства;
- 3 с момента создания произведения.+

6. Какой из объектов охраняется правом интеллектуальной собственности:

- 1 недвижимое имущество;
- 2 идея;
- 3 герб;
- 4 товарный знак;+
- 5 открытие.

7. Выберите объект, правовая охрана которого удостоверяется патентом:

- 1 картина;
- 2 песня;
- 3 изобретение;+
- 4 товар;
- 5 курсовая работа.

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

- 1 картина;+
- 2 изобретение;
- 3 промышленный образец;
- 4 произведение архитектуры;+
- 5 дипломная работа.+

Тема 12. Информационно-аналитическое обеспечение правоохранительной деятельности.

1. Сущность информационного обеспечения правоохранительных органов определяется как:

- 1 целесообразная деятельность человека, направленная на исходные фактические данные с тем, чтобы, используя соответствующие технические средства, преобразовать их в форму, пригодную для решения управленческих либо конкретных задач выявления, предупреждения, пресечения и раскрытия правонарушений и преступлений, розыска скрывшихся правонарушителей и преступников, а также без вести пропавших граждан.+
- 2 системность информации, а также непрерывность ее сбора и анализа.
- 3 механизм управления правоохранительными органами

2. Одним из основных требований, предъявляемых к организации информационно-аналитического обеспечения правоохранительных органов, является:

- 1 автономность системы
- 2 системность информации, а также непрерывность ее сбора и анализа.+
- 3 решение управленческих либо конкретных задач

3. Основным объектом информационной деятельности правоохранительных органов является:

- 1 интеллектуальная обработка информации
- 2 информационно-аналитическая работа
- 3 информация социального характера+

4. Информационно-аналитическая деятельность является целостной частью:

- 1 ведомственного механизма управления правоохранительными органами+
- 2 управленческой деятельности
- 3 системы включающей в себя два взаимосвязанных компонента

5. Важной процедурой информационно-аналитической работы является:

- 1 оптимизации информационного обеспечения деятельности правоохранительных органов
- 2 интеллектуальная обработка информации
- 3 первичный анализ и отбор релевантной информации+

6. Информационное обеспечение правоохранительных органов ориентировано прежде всего на:

- 1 интеллектуальную обработку информации+
- 2 поддержание устойчивого состояния информационных связей
- 3 сборе, накоплении, обработке, хранении и выдаче информации потребителям в максимально короткие сроки

7. Информационное обеспечение административной деятельности органов внутренних дел включает в себя:

- 1 правовую информацию
- 2 массив различных неправовых источников информации
- 3 все вышеперечисленное+

8.В целях защиты интересов Российской Федерации и граждан от преступных посягательств, действуя в рамках своей компетенции, органы внутренних дел используют возможности:

- 1 информационного обеспечения в процессе розыска и идентификации лиц, выявления, предупреждения, пресечения и раскрытия преступлений по находящимся в их производстве материалам и уголовным делам+
- 2 систематизации и анализа информации
- 3 выявление детерминант того или иного явления

9.Роль прокуратуры в системе правоохранительных органов и возложение на нее функций общего надзора за соблюдением законодательства в России обуславливает:

- 1 необходимость учета в организации информационно-аналитического обеспечения ее деятельности огромного объема самой разнообразной информации+
- 2 получения информации должностными лицами прокуратуры
- 3 информационным взаимодействием с органами государственной власти

Тема 13. Информационно-психологическое обеспечение правоохранительной деятельности.

1.Психологическое обеспечение в сфере правоохранения имеет одну из форм осуществления:

- 1 консультационная помощь специалиста-психолога+
- 2 конкретные меры психологического характера, направленные на достижение определенной цели
- 3 потребности системы, цели и задачи, соответствующие требованию повышения эффективности работы

2.К консультационной помощи специалиста прибегают в том случае, когда

- 1 показания специалиста – сообщение сведений о фактах, из-вестных ему как лицу
- 2 правоохранительным органам могут потребоваться специальные знания, умения и навыки+
- 3 критический анализ заключения психолога в форме документа «мнение специалиста»

3.Консультационная помощь не включает в себя:

- 1 консультации в форме допроса специалиста по иным вопросам, входящим в его компетенцию, осуществляемые сведущим лицом;
- 2 критический анализ заключения психолога в форме документа «мнение специалиста»;
- 3 конкретные меры психологического характера, направленные на достижение определенной цели +

4.К экспертным учреждениям не относят:

- 1 судебно-психологические институты
- 2 комплексные экспертизы институты
- 3 суд+

5.Во главе системы экспертных учреждений в структуре Министерства юстиции стоит:

- 1 Российский Федеральный центр судебных экспертиз+
- 2 Министерства здравоохранения и медицинской промышленности
- 3 Государственный центр социальной и судебной психиатрии им. В.П. Сербского

6.Право производства комплексных судебных психолого-психиатрических экспертиз принадлежит экспертным учреждениям

- 1 Российский Федеральный центр судебных экспертиз
- 2 Министерства здравоохранения и медицинской промышленности+
- 3 Государственный центр социальной и судебной психиатрии им. В.П. Сербского

7. Где расположена сеть экспертных учреждений в Вооруженных Силах России:

- 1 не существует
- 2 только в крупных городах
- 3 в округах, на флотах, в некоторых войсковых соединениях+

8. Психолог, работающий в рамках экспертного учреждения, имеет особый:

- 1 отличительный знак
- 2 процессуальный статус эксперта+
- 3 документ

9. Под психологической службой понимают

- 1 комплексное использование данных психологической науки, ее средств, методов и технологий специально подготовленными или компетентными в этой сфере лицами в целях совершенствования деятельности органов правоохранения
- 2 возможность в соответствии с целями и направлениями обеспечения выделить направления, цели и задачи деятельности юридического психолога по осуществлению психологического обеспечения правоохранительной деятельности, которые составляют программу его профессиональной деятельности
- 3 централизованно управляемую систему специальных структурных подразделений и должностей специалистов+

10. В уголовно-исполнительной системе активное создание психологической службы обусловлено

- 1 историческим опытом использования психологических знаний в данном ведомстве+
- 2 ростом преступности
- 3 экономическим развитием

Тема 14. Организационная защита информации

1. Что является наилучшим описанием количественного анализа рисков?

- 1 Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
- 2 Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
- 3 Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков +
- 4 Метод, основанный на суждениях и интуиции

2. Почему количественный анализ рисков в чистом виде не достижим?

- 1 Он достижим и используется
- 2 Он присваивает уровни критичности. Их сложно перевести в денежный вид.
- 3 Это связано с точностью количественных элементов
- 4 Количественные измерения должны применяться к качественным элементам +

3. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

- 1 Много информации нужно собрать и ввести в программу +
- 2 Руководство должно одобрить создание группы
- 3 Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
- 4 Множество людей должно одобрить данные

4. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

- 1 Стандарты
- 2 Должный процесс (Due process)
- 3 Должная забота (Due care) +
- 4 Снижение обязательств

5. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

- 1 Список стандартов, процедур и политик для разработки программы безопасности
- 2 Текущая версия ISO 17799
- 3 Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
- 4 Открытый стандарт, определяющий цели контроля +

6. Из каких четырех доменов состоит CobiT?

- 1 Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка +
- 2 Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
- 3 Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
- 4 Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

7. Что представляет собой стандарт ISO/IEC 27799?

- 1 Стандарт по защите персональных данных о здоровье +
- 2 Новая версия BS 17799
- 3 Определения для новой серии ISO 27000
- 4 Новая версия NIST 800-60

8. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?

- 1 COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
- 2 COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень +
- 3 COSO учитывает корпоративную культуру и разработку политик
- 4 COSO – это система отказоустойчивости

9. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления р компаниях. В чем заключаются различия между этими методами?

- 1 NIST и OCTAVE являются корпоративными
- 2 NIST и OCTAVE ориентирован на ИТ +
- 3 AS/NZS ориентирован на ИТ
- 4 NIST и AS/NZS являются корпоративными

10. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойде

- 1 Анализ связующего дерева
- 2 AS/NZS
- 3 NIST
- 4 Анализ сбоев и дефектов+

Тема 15. Правоохранительные органы

1. Согласно Конституции РФ судьей может стать:

- 1 гражданин, достигший совершеннолетия
- 2 честный и принципиальный человек, поступивший на службу в правоохранительные органы
- 3 студент юридического факультета, практикующийся в адвокатуре
- 4 профессиональный юрист с пятилетним стажем ра-боты+

2. Поддерживает в суде государственное обвинение:

- 1 адвокат
- 2 народный заседатель
- 3 мировой судья
- 4 прокурор+

3. Верно ли, что:

- 1) нотариус удостоверяет сделки, оформляет наследственные права;
- 2) нотариат участвует в расследовании и защищает права подозреваемых?

- 1 верно только 1+
- 2 верно только 2
- 3 верны оба суждения
- 4 оба суждения неверны

4. Верно ли, что:

- 1) различают государственные и негосу-дарственные правоохранительные органы;
- 2) правоохра-нительные органы обеспечивают безопасность граждан?

- 1 верно только 1
- 2 верно только 2
- 3 верны оба суждения +
- 4 оба суждения неверны

5. Последняя судебная инстанция по правам человека в РФ:

- 1 Европейский Суд по правам человека+
- 2 Верховный Суд РФ
- 3 городской (районный) суд
- 4 областной суд

6. За исполнением законов различными учреждениями, должностными лицами, гражданами следит:

- 1 нотариат
- 2 ФСБ России
- 3 адвокатура
- 4 прокуратура+

7. Верно ли, что:

- 1) присяжным заседателем может стать любой человек, достигший совершеннолетия;
- 2) суд при-сяжных рассматривает уголовные дела об особо тяжких преступлениях?

- 1 верно только 1

- 2 верно только 2 +
- 3 верны оба суждения
- 4 оба суждения неверны

8. Верно ли, что:

- 1) адвокат может заключить договор с доверителем независимо от его места жительства;
- 2) ад-вокатура входит в систему органов местного самоуправления?

- 1 верно только 1+
- 2 верно только 2
- 3 верны оба суждения
- 4 оба суждения неверны

Тема 16. Модель угроз. Угрозы безопасности информации

1. Источники угроз безопасности ИС вызванные случайными или преднамеренными действиями субъектов:

- 1 антропогенные +
- 2 техногенные
- 3 стихийные

2. Атакующая сторона этого класса, не имеет никаких полномочий доступа к информационным ресурсам КС:

- 1 внешний наблюдатель+
- 2 зарегистрированный внешний абонент
- 3 зарегистрированный пользователь

3. Атакующая сторона этого класса обладает более широкими правами доступа к массивам информации в БД и ЦБД:

- 1 зарегистрированный пользователь с полномочиями системного администратора
- 2 зарегистрированный привилегированный пользователь+
- 3 зарегистрированный пользователь с полномочиями администратора безопасности

4. В качестве объекта защиты могут выступать:

- 1 автономный компьютер, сервер, сетевое оборудование+
- 2 ПК, коммутатор, терминатор
- 3 сетевые адаптеры, концентраторы, маршрутизаторы

5. Этот источник угроз подразделяется на: внутренние и внешние, преднамеренные и случайные источники:

- 1 антропогенные +
- 2 техногенные
- 3 стихийные

6. Эти источники угроз приводят к отказам и сбоям технических и программных средств из-за устаревших программных и аппаратных средств или ошибок в ПО:

- 1 техногенные+
- 2 антропогенные
- 3 стихийные

7. По методам осуществления атаки могут быть:

- 1 внутренними и внешними
- 2 локальными и удаленными
- 3 активными и пассивными+

8. Угрозы информационной безопасности КС рассматриваются с позиций оценки трех основных взаимодействующих факторов:

- 1 объект защиты, субъект атаки, метод осуществления атаки +
- 2 организационно-технологических мер, программно-технических средств и правовых норм
- 3 перехват информации, модификация информации, подмена авторства информации

9. Источники угроз безопасности ИС вызванные природными катаклизмами или форс-мажорными обстоятельствами:

- 1 стихийные +
- 2 техногенные
- 3 антропогенные

10. Для обеспечения безопасности ИС применяют системы защиты информации, которые представляют собой комплекс:

- 1 аппаратно-технических, административно-технических мер
- 2 администрирования, конфигурирования систем и средств защиты
- 3 организационно-технологических мер, программно-технических средств и правовых норм+

Тема 17. Стандарты по информационной безопасности

1. Кто является основным ответственным за определение уровня классификации информации?

- 1 Руководитель среднего звена
- 2 Высшее руководство
- 3 Владелец+
- 4 Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

- 1 Сотрудники +
- 2 Хакеры
- 3 Атакующие
- 4 Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

- 1 Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
- 2 Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
- 3 Улучшить контроль за безопасностью этой информации +
- 4 Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?

- 1 Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
- 2 Необходимый уровень доступности, целостности и конфиденциальности +

- 3 Оценить уровень риска и отменить контрмеры
 - 4 Управление доступом, которое должно защищать данные
5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
- 1 Владельцы данных
 - 2 Пользователи
 - 3 Администраторы
 - 4 Руководство +
6. Что такое процедура?
- 1 Правила использования программного и аппаратного обеспечения в компании
 - 2 Пошаговая инструкция по выполнению задачи +
 - 3 Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
 - 4 Обязательные действия
7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
- 1 Поддержка высшего руководства +
 - 2 Эффективные защитные меры и методы их внедрения
 - 3 Актуальные и адекватные политики и процедуры безопасности
 - 4 Проведение тренингов по безопасности для всех сотрудников
8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
- 1 Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
 - 2 Когда риски не могут быть приняты во внимание по политическим соображениям
 - 3 Когда необходимые защитные меры слишком сложны
 - 4 Когда стоимость контрмер превышает ценность актива и потенциальные потери+
9. Что такое политики безопасности?
- 1 Пошаговые инструкции по выполнению задач безопасности
 - 2 Общие руководящие требования по достижению определенного уровня безопасности
 - 3 Широкие, высокоуровневые заявления руководства +
 - 4 Детализированные документы по обработке инцидентов безопасности
10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
- 1 Анализ рисков
 - 2 Анализ затрат / выгоды +
 - 3 Результаты ALE
 - 4 Выявление уязвимостей и угроз, являющихся причиной риска

Тема 18. Виды источников и носителей информации

1. Информацию, изложенную на доступном для получателя языке называют:
- 1 полной;
 - 2 полезной;
 - 3 актуальной;
 - 4 достоверной;
 - 5 понятной.+

2. Информацию, достаточную для решения поставленной задачи, называют:

- 1 полной;+
- 2 понятной.
- 3 достоверной;
- 4 актуальной;
- 5 полезной;

3. Информацию, не зависящую от личного мнения или суждения, называют:

- 1 достоверной;
- 2 актуальной;
- 3 объективной;+
- 4 полной;
- 5 понятной.

4. Информацию, отражающую истинное положение вещей, называют:

- 1 полной;
- 2 полезной;
- 3 актуальной;
- 4 достоверной;+
- 5 понятной.

5. Информацию, существенную и важную в настоящий момент, называют:

- 1 полной;
- 2 полезной;
- 3 актуальной;+
- 4 достоверной;
- 5 понятной.

6. По форме представления информацию можно условно разделить на следующие виды:

- 1 математическую, биологическую, медицинскую, психологическую и пр.
- 2 обыденную, производственную, техническую, управленческую;
- 3 текстовую, числовую, графическую, звуковую и пр.;+
- 4 научную, социальную, политическую, экономическую, религиозную и пр.;
- 5 зрительную, слуховую, тактильную, обонятельную, вкусовую;

7. По способу восприятия информации человеком различают следующие виды информации:

- 1 обыденную, производственную, техническую, управленческую;
- 2 математическую, биологическую, медицинскую, психологическую и пр.
- 3 зрительную, слуховую, тактильную, обонятельную, вкусовую;+
- 4 научную, социальную, политическую, экономическую, религиозную и пр.;
- 5 текстовую, числовую, графическую, звуковую и пр.;

8. Примером текстовой информации может служить:

- 1 фотография;
- 2 правило в учебнике русского языка;+
- 3 таблица умножения на обложке школьной тетради;
- 4 музыкальное произведение.
- 5 иллюстрация в книге;

9. Наибольший объем информации человек получает при помощи:

- 1 органов слуха;
- 2 органов зрения;+
- 3 органов осязания;
- 4 органов обоняния;
- 5 вкусовых рецепторов.

10. Тактильную информацию человек получает посредством:

- 1 специальных приборов;
- 2 термометра;
- 3 барометра;
- 4 органов осязания;+
- 5 органов слуха.

Тема 19. Источники опасных сигналов

1. Как называется умышленно искаженная информация?

- 1 Дезинформация +
- 2 Информативный поток
- 3 Достоверная информация
- 4 Перестает быть информацией

2. Как называется информация, к которой ограничен доступ?

- 1 Открытая
- 2 Противозаконная
- 3 Конфиденциальная +
- 4 Недоступная

3. Какими путями может быть получена информация?

- 1 проведением, покупкой и противоправным добыванием информации научных исследований +
- 2 захватом и взломом ПК информации научных исследований
- 3 добыванием информации из внешних источников и скремблированием информации научных исследований
- 4 захватом и взломом защитной системы для информации научных исследований

4. Как называются компьютерные системы, в которых обеспечивается безопасность информации?

- 1 защищенные КС +
- 2 небезопасные КС
- 3 Само достаточные КС
- 4 Саморегулирующиеся КС

5. Основной документ, на основе которого проводится политика информационной безопасности?

- 1 программа информационной безопасности +
- 2 регламент информационной безопасности
- 3 политическая информационная безопасность
- 4 Протекторат

6. В зависимости от формы представления информация может быть разделена на?

- 1 Речевую, документированную и телекоммуникационную +

- 2 Мысль, слово и речь
- 3 цифровая, звуковая и тайная
- 4 цифровая, звуковая

7. К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации

- 1 Мыслительным процессам
- 2 Машинным процессам
- 3 Микропроцессам
- 4 Информационным процессам+

8. Что называют защитой информации?

- 1 Все ответы верны +
- 2 Называют деятельность по предотвращению утечки защищаемой информации
- 3 Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
- 4 Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию

9. Под непреднамеренным воздействием на защищаемую информацию понимают?

- 1 Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений+
- 2 Процесс ее преобразования, при котором содержание информации изменяется на ложную
- 3 Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию
- 4 Не ограничения доступа в отдельные отрасли экономики или на конкретные производства

10. Шифрование информации это

- 1 Процесс преобразования, при котором информация удаляется
- 2 Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов +
- 3 Процесс ее преобразования, при котором содержание информации изменяется на ложную
- 4 Процесс преобразования информации в машинный код

Тема 20. Технические каналы утечки информации (особенности, характеристики, классификация).

1. Какие способы перехвата речевой информации требуют проникновения в выделенное помещение

- 1 Перехват акустических колебаний, возникающих при ведении разговоров, закладными устройствами с датчиками микрофонного типа. +
- 2 Перехват вибрационных колебаний, возникающих при ведении разговоров в ограждающих конструкциях и инженерных коммуникациях, закладными устройствами с датчиками контактного типа.
- 3 Перехват вибрационных колебаний, возникающих при ведении разговоров в ограждающих конструкциях и инженерных коммуникациях, электронными стетоскопами.
- 4 Перехват информативных электрических сигналов, возникающих вследствие акустоэлектрических преобразований акустических сигналов элементами ВТСС, техническими средствами, построенными на базе низкочастотных усилителей, подключаемыми к соединительных линий ВТСС.
- 5 Перехват акустической (речевой) информации методом «высокочастотного облучения» ВТСС, имеющих в своем составе акустоэлектрические преобразователи.

2. Причины, вызывающие появление опасных сигналов в цепях электропитания

- 1 наведение в цепях ЭДС полями НЧ и ВЧ побочных излучений ОТСС
- 2 модуляция тока электропитания токами радиоэлектронного средства
- 3 попадание опасного сигнала в цепи электропитания через паразитные связи элементов схемы и блоков питания
- 4 наличие в радиоэлектронном средстве импульсного блока питания
- 5 все ответы верны+

3. Оптическая разведка включает

- 1 визуально-оптическую, телевизионную и инфракрасную
- 2 визуально-оптическую, фотографическую и лазерную
- 3 визуально-оптическую, фотографическую и оптикоэлектронную+
- 4 визуально-оптическую, фотографическую и телевизионную

4. Что не относится к методам структурного скрытия информации?

- 1 маскировка
- 2 шифрование
- 3 дезинформирование
- 4 все относится+

5. Что не относится к методам энергетического скрытия?

- 1 уменьшение яркости и освещенности объекта
- 2 маскировка+
- 3 засветка
- 4 ослепление

6. От чего зависит эффективность электрического экранирования?

- 1 от электропроводности экрана и сопротивления заземления+
- 2 от толщины экрана и его магнитных свойств
- 3 все ответы верны

7. Эффективность электромагнитного экранирования измеряется

- 1 в децибелах
- 2 в неперах
- 3 все ответы верны+

8. От чего зависит эффективность магнитного экранирования?

- 1 от электропроводности экрана и сопротивления заземления
- 2 от толщины экрана и его магнитных свойств+
- 3 все ответы верны

9. Наибольшей чувствительностью обладают

- 1 электромагнитные микрофоны
- 2 электродинамические микрофоны
- 3 пьезоэлектрические микрофоны
- 4 угольные порошковые микрофоны+

10. При отражении лазерного луча от вибрирующей поверхности оконного стекла происходит его

- 1 частотная, угловая и фазовая модуляция+

- 2 частотная, амплитудная и фазовая модуляция
- 3 амплитудная, широтно-импульсная и фазовая модуляция

Тема 21. Принципы технической защиты информации

1. Когда возникает паразитная гальваническая связь?
 - 1 в результате воздействия магнитного поля
 - 2 в результате воздействия электрического поля
 - 3 через общее активное сопротивление+
 - 4 все ответы верны
2. Чем отличается технический канал утечки информации от канала связи?
 - 1 средой распространения сигнала
 - 2 типом получателя информации+
 - 3 видом помехи в канале
 - 4 все ответы верны
3. Под направлением физической защиты в ИТЗИ понимается
 - 1 инженерная защита за счет использования естественных и искусственных преград на маршрутах возможного распространения источников угроз воздействия
 - 2 техническая охрана объектов защиты
 - 3 все ответы верны+
4. Что относится к методам скрытия информации?
 - 1 пространственное и временное скрытие
 - 2 структурное и энергетическое скрытие
 - 3 пространственное и подземное скрытие
 - 4 верны ответы А и В+
 - 5 верны ответы В и С
5. В структуру системы технической разведки входят
 - 1 объекты разведки, органы добывания и органы сбора и обработки
 - 2 потребители информации, органы планирования и управления, органы добывания
 - 3 органы планирования и управления, органы добывания и органы сбора и обработки+
6. Наибольшей чувствительностью обладают
 - 1 электромагнитные микрофоны
 - 2 электродинамические микрофоны
 - 3 пьезоэлектрические микрофоны
 - 4 угольные порошковые микрофоны+
7. При отражении лазерного луча от вибрирующей поверхности оконного стекла происходит его
 - 1 частотная, угловая и фазовая модуляция+
 - 2 частотная, амплитудная и фазовая модуляция
 - 3 амплитудная, широтно-импульсная и фазовая модуляция
8. Разрешающая способность оптического средства наблюдения
 - 1 оценивается минимальным уровнем световой энергии, при котором обеспечивается требуемое качество изображения объекта наблюдения

- 2 характеризуется минимальными линейными или угловыми размерами между двумя соседними точками изображения, которые наблюдаются как отдельные+
- 3 определяет интервал силы света на входе оптического приемника, при котором обеспечивается заданное качество изображения

9. Чувствительность оптического средства наблюдения

- 1 оценивается минимальным уровнем световой энергии, при котором обеспечивается требуемое качество изображения объекта наблюдения+
- 2 характеризуется минимальными линейными или угловыми размерами между двумя соседними точками изображения, которые наблюдаются как отдельные
- 3 определяет интервал силы света на входе оптического приемника, при котором обеспечивается заданное качество изображения

10. Динамический диапазон оптического средства наблюдения

- 1 оценивается минимальным уровнем световой энергии, при котором обеспечивается требуемое качество изображения объекта наблюдения
- 2 характеризуется минимальными линейными или угловыми размерами между двумя соседними точками изображения, которые наблюдаются как отдельные
- 3 определяет интервал силы света на входе оптического приемника, при котором обеспечивается заданное качество изображения+

Тема 22. Способы и средства инженерной защиты и технической охраны.

1. Коэффициент направленного действия антенны

- 1 определяет величину энергетического выигрыша+
- 2 равен отношению мощности сигнала на выходе реальной антенны к мощности сигнала идеальной антенны без потерь
- 3 оба утверждения не верны

2. По назначению антенны бывают

- 1 передающие
- 2 приемные
- 3 приемопередающие
- 4 все утверждения верны+

3. Избирательность реального радиоприемника

- 1 оценивается шириной полосы пропускания и коэффициентом прямоугольности АЧХ радиоприемника+
- 2 оценивается шириной полосы пропускания и динамическим диапазоном радиоприемника
- 3 оценивается динамическим диапазоном и коэффициентом прямоугольности АЧХ радиоприемника

4. Для снижения влияния последовательно подключенного к линии средства перехвата информации

- 1 увеличивают величину входного сопротивления средства перехвата
- 2 уменьшают величину входного сопротивления средства перехвата+
- 3 используют индуктивные и емкостные связи

5. Для идентификации персонала применяются

- 1 атрибутные, биометрические и психофизические идентификаторы
- 2 атрибутные и биометрические идентификаторы+

3 вещественные и логические

6. Извещатели пожарно-охранной сигнализации бывают

- 1 точечными, многоточечными, линейными и поверхностными
- 2 многоточечными, поверхностными и объемными
- 3 точечными, линейными, поверхностными и объемными+

7.Тревожная сигнализация предназначена

- 1 для формирования сигнала тревоги
- 2 для психологического воздействия на нарушителя+
- 3 для включения механизмов блокировки прохода в охраняемую зону
- 4 для автоматизации процессов пожаротушения

8.Зоной R2 называется

- 1 пространство вокруг ОТСС, на границе и за пределами которого напряженность электромагнитного поля не превышает допустимого (нормированного)значения+
- 2 пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в сосредоточенных антеннах не превышает допустимого (нормированного)значения
- 3 пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в распределенных антеннах не превышает допустимого (нормированного)значения

9.Зоной R1 называется

- 1 пространство вокруг ОТСС, на границе и за пределами которого напряженность электромагнитного поля не превышает допустимого (нормированного)значения
- 2 пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в сосредоточенных антеннах не превышает допустимого (нормированного)значения+
- 3 пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в распределенных антеннах не превышает допустимого (нормированного)значения

10.Что входит в организационную составляющую ИТЗИ?

- 1 подбор и расстановка персонала
- 2 регламентация деятельности сотрудников и технических средств защиты+
- 3 выявление технических каналов утечки информации

Тема 23. Способы и средства противодействия подслушиванию

1.Подслушивание с помощью технических средств осуществляется путем:

- 1 приема и прослушивания акустических сигналов, распространяющихся в воздухе, воде и твердых телах;
- 2 прослушивания речи, выделяемой из перехваченных радио- и электрических сигналов функциональных каналов связи и из сигналов побочных излучений и наводок;
- 3 применения лазерных систем подслушивания;
- 4 использования закладных устройств;
- 5 все вышеперечисленное+

2.Для подслушивания применяют следующие технические средства(два ответа):

- 1 акустические приемники, в том числе с направленными микрофонами;
- 2 приемники опасных сигналов;+
- 3 высокочастотного навязывания.

3.информационное сккрытие, предусматривающее:

- 1 техническое закрытие и шифрование семантической и акустической информации в функциональном канале связи;
- 2 дезинформирование.+
- 3 средства звукоизоляции и звукопоглощения акустического сигнала

4.Энергетическое сккрытие путем:

- 1 звукоизоляции акустического сигнала+
- 2 техническое закрытие и шифрование семантической и акустической информации в функциональном канале связи
- 3 зашумления помещений или твердой среды распространения другими широкополосными звуками (шумами), обеспечивающими маскировку акустических сигналов;

5.Способы защиты делятся на(два ответа):

- 1 активные+
- 2 пассивные+
- 3 негативные

6.Способы экранирования:

- 1 электростатическое+
- 2 линейное зашумление
- 3 пространственное зашумление

7.Признаковые структуры не камуфлируемой радиозакладки включают:

- 1 радиоизлучение с модуляцией радиосигнала акустическим сигналом, циркулирующим в помещении;
- 2 признаки внешнего вида — малогабаритный предмет непонятного назначения в форме параллелепипеда, цилиндра без выступающих деталей и органов управления на поверхности;
- 3 одно или несколько отверстий малого диаметра в кожухе;
- 4 наличие отрезка провода (антенны);
- 5 все вышеперечисленное+

8.Типовой комплекс для поиска средств негласного съема акустической информации включает(два ответа):

- 1 сканирующий радиоприемник с широкополосными антеннами;+
- 2 коммутатор антенн для комплексов, контролирующих несколько помещений;+
- 3 средства звукоизоляции и звукопоглощения акустического сигнала

9.Минимальный набор для обнаружения закладных устройств включает(два ответа):

- 1 фонарь для освещения темных мест при визуальном поиске;+
- 2 портативный металлоискатель;
- 3 генератор помех в радиодиапазоне.
- 4 индикатор поля+

10.Средний набор для обнаружения закладных устройств включает(два ответа):

- 1 досмотровое зеркало;+
- 2 досмотровое зеркало;
- 3 индикатор поля- частотомер;+
- 4 индикатор поля- частотомер;

Тема 24. Способы и средства предотвращения утечки информации с помощью закладных устройств.

1. Для обнаружения и измерения основных характеристик ПЭМИ используются:

- a. измерительные приемники+
- b. индикаторы
- c. универсальные поисковые приборы

2. Многофункциональный приемник ближнего поля Xplorer сканирует за 1 секунду

- a. от 10 до 1000 МГц
- b. от 30 до 2000 МГц+
- c. от 20 до 4000 МГц

3. Узко-диапазонные приемники ориентируется на прием сигналов с

- a. высоким обхватом сигналов на большом уровне
- b. обнаружение сигналов с достаточной вероятностью их выявления при минимальном числе приемников.
- c. определенных участках спектра радиоволн: КВ, УКВ, метровом, сантиметровом и других.+

4. Частота принимаемого сигнала равна

- a. 150,43 МГц.+
- b. 180,54 МГц.
- c. 200,20 МГц.

5. Сканирующие приемники (как переносимые, так и перевозимые) могут работать в одном из следующих режимов:

- a. режим автоматического сканирования в заданном диапазоне частот;
- b. режим автоматического сканирования по фиксированным частотам
- c. оба суждения верны+

6. Автоматизированные комплексы обладают следующими характеристиками:

- a. производят автоматический панорамный анализ сигналов участка диапазона шириной до 15-20 МГц путём идентификации спектрограмм текущих сигналов с заложенными в память эталонными спектрограммами сигналов закладных устройств+
- b. имеют наименьшую скорость сканирования, до 10 МГц/с и более;
- c. автоматически не могут определять координаты закладного устройства по времени

7. В настоящее время основными техническими средствами, предназначенными для выявления радиоэфирных специальных технических средств (СТО) несанкционированного съема информации (НСИ) являются:

- a. измерители мощности и другие специальные устройства.
- b. автоматизированные многоканальные комплексы радиомониторинга.+
- c. оба суждения верны

8. К классификации специальных радиоприёмников по режиму настройки можно отнести

- a. ручную, автоматическую+

- б.поисковую, обнаружительную
- с.широкополосную, узкополосную

9. Средства обнаружения, локализации и подавления закладных устройств

- а. Средства радиоконтроля помещений
- б. Средства поиска неизлучающих закладных устройств
- с. оба суждения верны+

Тема 25. Способы и средства предотвращения утечки информации через побочные излучения и наводки.

1.Средства ЗИ от утечки через ПЭМИН должны удовлетворять следующие требования:

- а. Опасные сигналы должны быть ослаблены до уровня, исключающего съём с них информации на границе КЗ+
- б. излучения в экранированном шкафу или в экранировании помещения целиком
- с.оба суждения верны

2. Активный метод подавления сигналов побочных электромагнитных излучений и наводок —это:

- а. экранирование источника излучения, размещении источника излучения в экранированном шкафу или в экранировании помещения целиком
- б. применение специальных широкополосных передатчиков помех.+
- с. Местонахождение по отношению к полезному сигналу

3. Пассивные методы подавления сигналов побочных электромагнитных излучений и наводок защиты:

- а. Линейное зашумление, Пространственное зашумление
- б. Отключение опасных сигналов, Фильтрация опасных сигналов, Ограничение опасных сигналов, Применение буферных устройств+
- с.оба суждения верны

4. Толщина стального листа выбирается исходя из прочности конструкции и возможности создания сплошного шва

- а. металлические листы+
- б. металлические сетки
- с. Фольговые материалы

5. Заземление или зануление электроустановок следует выполнять

- а. при напряжении 24 В
- б. при напряжении 12 В
- с. при напряжении 380 В и выше переменного тока и 440 В выше постоянного тока - во всех электроустановках+

6. Системы линейного зашумления применяются для

- а. для маскировки наведенных опасных сигналов в посторонних проводниках и соединительных линиях ВТСС, выходящих за пределы контролируемой зоны+
- б. границе контролируемой зоны
- с.оба суждения не верны

7. К системе линейного зашумления, применяемой для создания маскирующих электромагнитных помех в цепях электропитания СВТ, предъявляются следующие требования

- a. система должна создавать электромагнитные помехи в диапазоне частот возможных наводок побочных электромагнитных излучений СВТ (от 150 кГц до 300 МГц)
- b. создаваемые помехи не должны иметь регулярной структуры (энтропийный коэффициент качества шума должен быть не менее 0,6)
- c. система должна иметь сертификат по требованиям безопасности информации ФСТЭК РФ
- d. Все суждения верны+

8. К системе пространственного зашумления предъявляются следующие требования

- a. система должна создавать электромагнитные помехи в диапазоне частот возможных побочных электромагнитных излучений ТСПИ;
- b. создаваемые помехи не должны иметь регулярной структуры
- c. система должна создавать помехи как с горизонтальной, так и с вертикальной поляризацией
- d. все суждения верны+

Тема 26. Системы идентификации и аутентификации

1. Аутентификация - это

- a. это присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных
- b. проверка принадлежности пользователю предъявленного им идентификатора+

2. К группе методов аутентификации относят

- a. методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной оболочки глаза+
- b. знании некоторой секретной информации
- c. владении некоторым специальным предметом или устройством

3. При выборе пароля необходимо руководствоваться двумя правилами

- a. Пароли должны легко запоминаться, но трудно подбираться.
- b. Пароль нигде не должен записываться
- c. оба суждения верны+

4. Реакции системы на неудачную попытку входа пользователя в систему могут быть

- a. Блокировка учетной записи, под которой осуществляется попытка входа при превышении максимально возможного количества попыток+
- b. Не повторяемость пароля одного пользователя
- c. Макс. срок действия пароля

5. По способу обмена данными между идентификатором и устройством ввода-вывода электронные СИА подразделяются на:

- a. контактные+
- b. контактируемые
- c. все суждения верны

6. Гораздо более сильным средством, устойчивым к пассивному прослушиванию сети, являются

- a. постоянный пароль
- b. одноразовый пароль+
- c. новый пароль

7. Динамическое разделение обязанностей отличается от статического только тем, что

- a. рассматриваются роли, одновременно активные для данного пользователя+
- b. не рассматриваются роль для данного пользователя
- c. оба суждения верны

8. Административные функции

- a. создать/удалить роль/пользователя, приписать пользователя/право роли или ликвидировать существующую ассоциацию, создать/удалить отношение наследования между существующими ролями+
- b. открыть сеанс работы пользователя с активацией подразумеваемого набора ролей; активировать новую роль, деактивировать роль; проверить правомерность доступа
- c. Здесь проводится разделение на обязательные и необязательные функции

9. К традиционным моделям относится

- a. дискреционная и мандатная+
- b. Java-среды и системы Safe-Tcl

Тема 27. Биометрические системы идентификации и аутентификации.

1. Понятие "биометрия" появилось в

- a. XX веке
- b. в конце XIX века+
- c. в начале XVIII века

2. Наиболее популярным биометрическим параметром является

- a. Геометрия кисти руки
- b. отпечаток пальца+
- c. оба суждения неверны

3. Биометрическая аутентификация

- a. опознание индивидуума на основе его физиологических характеристик и поведения+
- b. опознание внутренних качеств
- c. оба суждения верны

4. Основная же слабость биометрии, по мнению специалистов, состоит в том, что

- a. биометрические данные не похищаются
- b. биометрические данные можно похитить после того, как они получены+
- c. оба суждения верны

5. Идентификация человека по чертам лица -это

- a. Геометрия лица+
- b. Голосовая идентификация
- c. Сетчатка глаза

6. Сканирование сетчатки глаза происходит с использованием

- a. обычного света
- b. инфракрасного света низкой интенсивности+
- c. Оба суждения неверны

7. Для чего используются биометрические системы безопасности

- а. для определения пола человека
- б. для удостоверения личности человека и его биометрические данные+
- с. для определения возраста человека

8. Что такое авторизация?

- а. проверка атрибутов безопасности пользователя на наличие полномочий
- б. выполнение определённого конкретного действия с проверкой
- с. оба суждения верны+

9. Динамические методы идентификации

- а. голос, почерк+
- б. код ДНК
- с. сетчатка глаза

10. К статическим методам относят

- а. клавиатурный почерк
- б. форма лица +
- с. почерк

4.3 Промежуточная аттестация по дисциплине проводится в форме экзамена

Типовые вопросы экзамена (ОК-12, ПК-18)

- 1 Конфиденциальная информация: понятие, признаки, классификация.
- 2 Понятия лицензирования и сертификации.
- 3 Понятие компьютерных преступлений. Неправомерный доступ к компьютерной информации
- 4 Политика ИБ. Обязательство о неразглашении защищаемых сведений.
- 5 Основные функции систем управления информационной безопасностью. Принципы управления информационной безопасностью
- 6 Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности ее защиты
- 7 Организационные и технические меры по инженерно-технической защите информации в организации
- 8 Интеллектуальный продукт как объект интеллектуальной собственности и предмет защиты.

Типовые задания для экзамена (ОК-12, ПК-18)

- 1 Организационные меры и основные правила работы за компьютером.
- 2 Определение надёжности персональных межсетевых экранов
- 3 Базовые способы и возможности защиты программного обеспечения с помощью электронных ключей
- 4 Понятие о проверке электронной подписи
- 5 Преимущества и недостатки систем с симметричными ключами
- 6 Понятие блочного шифра

4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
--------	-------------	--

«отлично» (85 - 100 баллов)	ОК-12	Демонстрирует высокий уровень знаний основных теоретических положений информатики. Эффективно использует программные средства общего и специального назначения. Свободно ориентируется в современной вычислительной технике и программном обеспечении ПК. Демонстрирует знание основ информационной и библиографической культуры. Способен продемонстрировать решение стандартных задач профессиональной деятельности с применением ИКТ.¶Практическое задание выполнено полностью.¶Ответ построен логично, материал излагается четко, ясно, хорошим языком, аргументировано. На вопросы отвечает кратко, аргументировано, уверенно, по существу.¶
	ПК-18	Демонстрирует высокий уровень знаний методологического базиса решения поставленных задач защиты информации. Анализирует существующие методики определений требования к защите информации. Свободно ориентируется в законодательстве РФ по защите информации. Демонстрирует знание принципов обеспечения защиты информации и источников угроз ИБ. Способен продемонстрировать современные подходы к технологиям и методам обеспечения ИБ.¶Практическое задание выполнено полностью.¶Ответ построен логично, материал излагается четко, ясно, хорошим языком, аргументировано. На вопросы отвечает кратко, аргументировано, уверенно, по существу.¶
«хорошо» (70 - 84 баллов)	ОК-12	Демонстрирует достаточный уровень знаний основных теоретических положений информатики. Эффективно использует программные средства общего и специального назначения. Достаточно свободно ориентируется в современной вычислительной технике и программном обеспечении ПК. Демонстрирует достаточные знания основ информационной и библиографической культуры. Способен продемонстрировать решение стандартных задач профессиональной деятельности с применением ИКТ.¶Практическое задание выполнено полностью или с незначительными недочетами.¶Ответ построен логично, материал излагается хорошим языком. Вопросы, задаваемые преподавателем, не вызывают существенных затруднений.¶
	ПК-18	Демонстрирует достаточный уровень знаний методологического базиса решения задач защиты информации. Анализирует существующие методики определений требования к защите информации. Достаточно свободно ориентируется в законодательстве РФ по защите информации. Демонстрирует достаточные знания принципов обеспечения защиты информации и источников угроз ИБ. Способен продемонстрировать современные подходы к технологиям и методам обеспечения ИБ.¶Практическое задание выполнено полностью или с незначительными недочетами.¶Ответ построен логично, материал излагается хорошим языком. Вопросы, задаваемые преподавателем, не вызывают существенных затруднений.¶

«удовлетворительно» (50 - 69 баллов)	ОК-12	Демонстрирует не достаточный уровень знаний основных теоретических положений информатики. Не способен эффективно использовать программные средства общего и специального назначения. Слабо ориентируется в современной вычислительной технике и программном обеспечении ПК. Демонстрируется не достаточное знание основ информационной и библиографической культуры. Не способен продемонстрировать решение стандартных задач профессиональной деятельности с применением ИКТ.¶Практическое задание выполнено не полностью.¶Ответ не всегда логично выстроен, материал излагается без применения научной терминологии. Вопросы, задаваемые преподавателем, вызывают затруднения.¶
	ПК-18	Демонстрирует не достаточный уровень знаний методологического базиса решения задач защиты информации. Не анализирует существующие методики определений требования к защите информации. Слабо ориентируется в законодательстве РФ по защите информации. Демонстрирует не достаточное знание принципов обеспечения защиты информации и источников угроз ИБ.¶Не способен продемонстрировать современные подходы к технологиям и методам обеспечения ИБ.¶Практическое задание выполнено не полностью.¶Ответ не всегда логично выстроен, материал излагается без применения научной терминологии. Вопросы, задаваемые преподавателем, вызывают затруднения.¶
«неудовлетворительно» (менее 50 баллов)	ОК-12	Демонстрирует не достаточный уровень знаний основных теоретических положений информатики. Не способен использовать программные средства общего и специального назначения. Не ориентируется в современной вычислительной технике и программном обеспечении ПК. Демонстрируется не достаточное знание основ информационной и библиографической культуры. Не способен продемонстрировать решение стандартных задач профессиональной деятельности с применением ИКТ.¶Практическое задание не выполнено.¶Неуверенно и логически непоследовательно излагает материал. Неправильно отвечает на поставленные вопросы или затрудняется с ответом¶
	ПК-18	Демонстрирует не достаточный уровень знаний методологического базиса решения задач защиты информации. Не анализирует существующие методики определений требования к защите информации. Не способен использовать программные средства. Не ориентируется в законодательстве РФ по защите информации. Демонстрирует не достаточное знание принципов обеспечения защиты информации и источников угроз.¶Практическое задание не выполнено.¶Неуверенно и логически непоследовательно излагает материал. Неправильно отвечает на поставленные вопросы или затрудняется с ответом¶

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. Передков В.М., Митрошкин А.Г. Информационная безопасность и защита информации. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
2. Лопатин Д.В., Калинина Ю.В. Безопасные информационные технологии : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
3. Тамб гос. ун-т им. Г.Р. Державина, Ин-т математики, физики и информатики Техническая защита информации : учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

6.2 Дополнительная литература:

1. Загинайлов Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие. - Москва|Берлин: Директ-Медиа, 2015. - 105 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=362895>
2. 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>
3. Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Рудановский М. В. Аудит информационной безопасности органов исполнительной власти : учебное пособие. - 4-е изд., стер.. - Москва: Флинта, 2016. - 100 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=93259>

4. Петренко В. И. Теоретические основы защиты информации : учебное пособие. - Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2015. - 222 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=458204>

6.3 Иные источники:

1. Курс «Стандарты информационной безопасности» - <https://www.intuit.ru/studies/courses/30/30/info>
2. Курс «Основы информационной безопасности» - <https://www.intuit.ru/studies/courses/10/10/info>

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

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

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

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

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

Лицензионное программное обеспечение:

Google Chrome

Microsoft Windows 10

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. Российская государственная библиотека. – URL: <https://www.rsl.ru>
6. Российская национальная библиотека. – URL: <http://nlr.ru>
7. 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.