

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

УТВЕРЖДАЮ:
Директор института



Н. Л. Королева
«05» июля 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.О.29 Аудит и аттестация объектов информатизации

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

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

Уровень высшего образования: специалитет

Квалификация: Специалист по защите информации

год набора: 2021

Автор программы:

Кандидат технических наук, доцент Зауголков Игорь Алексеевич

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере (уровень специалитета) (приказ Министерства образования и науки РФ от «26» ноября 2020 г. № 1461).

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

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

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП Специалиста.....	4
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	11
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	28
6. Учебно-методическое и информационное обеспечение дисциплины.....	30
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	30

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-6 Способен организовывать процедуру аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации

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

- организационно-управленческий

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

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Индикаторы достижения компетенций
	ПК-6 Способен организовывать процедуру аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации	Проводит аттестацию и аудит объектов информатизации, выделенных (защищаемых) помещений на соответствие требованиям по защите информации

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-6 Способен организовывать процедуру аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения	
		Очная (семестр)	
		9	10
1	Информационно-аналитическое обеспечение правоохранительной деятельности	+	
2	Преддипломная практика		+

2. Место дисциплины в структуре ОП специалиста:

Дисциплина «Аудит и аттестация объектов информатизации» относится к обязательной части учебного плана ОП по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере.

Дисциплина «Аудит и аттестация объектов информатизации» изучается в 8, 9 семестрах.

3.Объем и содержание дисциплины

3.1.Объем дисциплины: 8 з.е.

Очная: 8 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	288
Контактная работа	128
Лекции (Лекции)	64
Лабораторные (Лаб. раб.)	64
Самостоятельная работа (СР)	124
Экзамен	36
Зачет	-

3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
8 семестр					
1	Введение.	11	-	26	Собеседование
2	Основы Законодательства РФ, руководящие и нормативные документы ФСТЭК (Гостехкомиссии) России, регламентирующие вопросы защиты информации.	11	16	26	Выполнение лабораторных работ ; Собеседование; Тестирование
3	Организация защиты автоматизированн ых систем и их компонентов от несанкционирован ного доступа.	10	16	28	Выполнение лабораторных работ ; Собеседование; Реферат
9 семестр					
4	Порядок подготовки и проведения аттестации объектов информатизации по требованиям ФСТЭК России.	11	11	14	Выполнение лабораторных работ ; Собеседование

5	Порядок проведения сертификационных испытаний средств защиты информации.	11	11	14	Выполнение лабораторных работ ; Собеседование
6	Порядок лицензирования деятельности по защите информации ФСТЭК России.	10	10	16	Выполнение лабораторных работ ; Собеседование

Тема 1. Введение. (ПК-6)

Лекция.

Предмет, цели, задачи и содержание курса «Аттестация объектов информатизации». Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия.

Лабораторные работы.

1. Понятие аттестации ОИ. Объекты информатизации, аттестуемые по требованиям безопасности информации. ОИ, подлежащие аттестации.
2. Назначение проведения аттестации.
3. Перечень проводимых работ при проведении аттестации.
4. Описание концепции проведения работ по аттестации.
5. Завершение работ по аттестации с последующим выводом.

Задания для самостоятельной работы.

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

Тема 2. Основы Законодательства РФ, руководящие и нормативные документы ФСТЭК (Гостехкомиссии) России, регламентирующие вопросы защиты информации. (ПК-6)

Лекция.

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) — федеральный орган исполнительной власти России, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности.

Приказ ФСТЭК России от «14» марта 2014 г. n 31 "об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами

Приказ ФСТЭК России № 21 от 18 февраля 2013 г. Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Лабораторные работы.

1. Основной проблемой реализации систем защиты явля-ется:
 - а) исключение случай-ного и преднамеренного получения информации посто-ронними лицами;
 - б) разграничение доступа к устройствам и ресурсам системы всех пользователей, администрации и обслуживающего персонала;
 - с) системы защиты не должны со-здавать заметных неудобств пользователям в ходе их рабо-ты с ресурсами системы.

d) все вышеперечисленное.

2. Комплексный (системный) подход к построению любой системы включает в себя:

- a) изучение объекта внедряемой системы; оценку угроз безопасности объекта; анализ средств, которыми будем оперировать при построении системы; оценку экономической целесообразности; изучение самой системы, ее свойств, принципов работы и возможность увеличения ее эффективности; соотношение всех внутренних и внешних факторов; возможность дополнительных изменений в процессе построения системы и полную организацию всего процесса от начала до конца; +
- b) совокупности научных, научно-технических и организационных мероприятий и применения специальных средств и методов, а создания целостной системы организационно-технологических мероприятий и применения комплекса специальных средств и методов;
- c) разработку единой концепции как полной совокупности научно обоснованных взглядов, положений и решений, необходимых и достаточных для оптимальной организации и обеспечения надежности защиты информации.

3. Какими бывают стратегии защиты информации?

- a) оборонительная, наступательная, упреждающая;
- b) наступательная, инженерная, сигнализационная, адаптивная;
- c) инженерно-техническая, программно-аппаратная, программная, организационная.

1 4. Что должна включать в себя система защиты от утечки?

- a) защита от наблюдения, прослушивания, перехвата, контроль вещественных носителей (комплексы мероприятий по контролю звукопроницаемости помещений, предотвращение утечки информации путем шифрования, контроль за уничтожением носителей и т.д.)
- b) звукоизоляция, глушение, экранирование);
- c) защита от перехвата (шифрование, экранирование, зашумление, фильтрация);+ комплекс защиты от перехвата (шифрование, экранирование, зашумление, фильтрация) комплекс предотвр. утечки вещ.носителей (учет и скрытие отходов, уничтожение отходов)
- d) определение полномочий пользователя (учет и анализ потока информации, распределение полномочий пользователей, ведения журнала учета);
- e) установки пропускного режима (КПП на входе в здание, контроль доступа в помещения для совещаний и хранилищ конфиденциальных данных);

5. Какие элементы входят в состав информационных правоотношений ?

- a) должностные инструкции, обращение, фиксирование, хранение;
- b) права, ограничение прав, обязанности, ответственность;
- c) права, обязанности, фиксирование, хранение
- d) права, ограничение прав, должностные инструкции, ответственность

Задания для самостоятельной работы.

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

Тема 3. Организация защиты автоматизированных систем и их компонентов от несанкционированного доступа. (ПК-6)

Лекция.

Внедрение современных информационных технологий (ИТ) на базе компьютерной техники и телекоммуникационных средств радикально изменили информационную среду.

Как следствие, усложнились процессы регулирования отношений между субъектами и информационными объектами. При решении задач защиты информации от НСД в АСОД предметом рассмотрения являются отношения доступа между субъектами и информационными объектами в среде программно-технического комплекса (ПТК) АСОД.

Рассматриваются отношения доступа между субъектами и элементами программно-технического комплекса, то есть программно-техническими ресурсами АСОД, и между элементами ПТК и информационными объектами, то есть информационными ресурсами АСОД. Естественно, предметом рассмотрения могут быть отношения доступа между элементами ПТК в определённых процессах, когда анализируются тракты доступа субъектов к информационным объектам.

Лабораторные работы.

1. Законодательство о персональных данных.
2. Методы и средства защиты информации от НСД
3. Защита авторских прав.
4. Назначение, функции и типы систем видеозащиты.
5. Как подписывать с помощью ЭЦП электронные документы различных форматов.
6. Обзор угроз и технологий защиты Wi-Fi-сетей.
7. Проблемы внедрения дискового шифрования.
8. Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.
9. Особенности процессов аутентификации в корпоративной среде.
10. Квантовая криптография.
11. Утечки информации: как избежать. Безопасность смартфонов.
12. Безопасность применения пластиковых карт - законодательство и практика.
13. Защита CD- и DVD-дисков от копирования.
14. Современные угрозы и защита электронной почты.
15. Программные средства анализа локальных сетей на предмет уязвимостей.
16. Безопасность применения платежных систем - законодательство и практика.
17. Аудит программного кода по требованиям безопасности.
18. Антишпионское ПО (antispysware).
19. Обеспечение безопасности Web-сервисов.
20. Защита от внутренних угроз.
21. Технологии RFID.
22. Уничтожение информации на магнитных носителях.
23. Ботнеты - плацдарм современных кибератак.
24. Цифровые водяные знаки в изображениях.
25. Электронный документооборот. Модели нарушителя.
26. Идентификация по голосу. Скрытые возможности.
27. Безопасность океанских портов.
28. Безопасность связи.
29. Безопасность розничной торговли.
30. Банковская безопасность.
31. Информатизация управления транспортной безопасностью.
32. Биопаспорт.
33. Обзор современных платформ архивации данных.
34. Что такое консалтинг в области ИБ.
35. Бухгалтерская отчетность как источник рассекречивания информации.

36. Управление рисками: обзор употребительных подходов.
37. Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности.
38. Распределенные атаки на распределенные системы.
39. Оценка безопасности автоматизированных систем.
40. Windows и Linux: что безопаснее?
41. Функциональная безопасность программных средств.
42. Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств.
43. Информационная безопасность: экономические аспекты.

Задания для самостоятельной работы.

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

Тема 4. Порядок подготовки и проведения аттестации объектов информатизации по требованиям ФСТЭК России. (ПК-6)

Лекция.

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации определяется следующими документами:

«Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам», утверждены решением Гостехкомиссии России от 23 мая 1997 года № 55;

«Положение по аттестации объектов информатизации по требованиям безопасности информации», утверждено Председателем Гостехкомиссии России 25 ноября 1994 года;

«Методические рекомендации управлениям ФСТЭК России по федеральным округам об организации работ по аттестации объектов информатизации по требованиям безопасности информации, приказ Директора ФСТЭК России от 21 апреля 2006 года № 126.

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает: 1. Подача заявки на аттестацию объекта информатизации. Заявитель для получения аттестата соответствия направляет в управление ФСТЭК России по федеральному округу (далее - Управление) заявку на проведение аттестации объекта информатизации с необходимыми исходными данными по установленной форме (приложение № 1). 2. Рассмотрение заявки на аттестацию, принятие решения на ее проведение, доведение решения до заявителя и органа по аттестации объектов информатизации.

Лабораторные работы.

1. Документы, определяющие порядок проведения аттестации объектов информатизации по требованиям безопасности информации
2. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации
3. Рассмотрение заявки на аттестацию, принятие решения на ее проведение, доведение решения до заявителя и органа по аттестации объектов информатизации.

Задания для самостоятельной работы.

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

Тема 5. Порядок проведения сертификационных испытаний средств защиты информации. (ПК-6)

Лекция.

Сертификация средств защиты информации производится в соответствии с "Положением о сертификации средств защиты информации", утвержденным постановлением Правительства Российской Федерации от 26 июня 1995 г.

Сертификация - форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

Сертификат соответствия - документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации.

Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации

Лабораторные работы.

1. "Положение о сертификации средств защиты информации"
2. Понятие сертификации
3. Понятие сертификата соответствия
4. Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну
5. Технические средства, подлежащие обязательной сертификации

Задания для самостоятельной работы.

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

Тема 6. Порядок лицензирования деятельности по защите информации ФСТЭК России. (ПК-6)

Лекция.

Лицензирование деятельности по технической защите конфиденциальной информации-это вид деятельности направленный на выполнение работ и оказание услуг по ее защите от несанкционированного доступа, от ее утечки по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

В соответствии с Постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79 г. Москва "О лицензировании деятельности по технической защите конфиденциальной информации" лицензию по технической защите конфиденциальной информации обязаны получить организации, которые собираются осуществлять перечисленные ниже виды деятельности:

- 1) контроль защищенности конфиденциальной информации от утечки по техническим каналам;
- 2) контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
- 3) сертификационные испытания на соответствие требованиям по безопасности информации продукции, используемой в целях защиты конфиденциальной информации;
- 4) аттестационные испытания и аттестация на соответствие требованиям по защите информации;
- 5) установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

Лабораторные работы.

1. Лицензирование деятельности по технической защите конфиденциальной информации
2. Контроль защищенности конфиденциальной информации от утечки по техническим каналам

3. Контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации
4. Сертификационные испытания на соответствие требованиям по безопасности информации продукции, используемой в целях защиты конфиденциальной информации
5. Установка, монтаж, испытания, ремонт средств защиты информации

Задания для самостоятельной работы.

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

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

8 семестр

- посещаемость – 10 баллов
- текущий контроль – 70 баллов
- контрольные срезы – 2 среза по 10 баллов каждый
- премиальные баллы – 20 баллов

Распределение баллов по заданиям:

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

1.	Введение.	Собеседование	10	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>10 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>7 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>5 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
2.	Основы Законодательства РФ, руководящие и нормативные документы ФСТЭК (Гостехкомиссии) России, регламентирующие вопросы защиты информации.	Выполнение лабораторных работ	20	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>30 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>20 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>10 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>

		Собеседование(контрольный срез)	10	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>10 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>7 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>5 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
		Тестирование	10	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>10 балла – студент правильно отвечает на 50-100% вопросов в тесте. 5 балл - студент правильно отвечает на 25-50% вопросов в тесте.</p>
3.	Организация защиты автоматизированных систем и их компонентов от несанкционированного доступа.	Выполнение лабораторных работ	20	<p>Лабораторные работы выполняются по текущему разделу или теме дисциплины. 20 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>10 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>5 баллов - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>

Собеседование(контрольный срез)	10	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>10 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>7 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>5 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
---------------------------------	----	--

	Реферат	10	<p>8-10 баллов – реферат выполнен обучающимся самостоятельно, в полном объеме, с соблюдением необходимых технических параметров; стиль изложения отвечает специфике жанра научной работы; во введении логично, объективно и аргументировано характеризуется научная проблема; содержание реферата включает самостоятельное исследование, а заключение содержит выводы, логично вытекающие из содержания основной части; список литературы оформлен в соответствии с правилами ГОСТа</p> <p>6-7 баллов – во введении четко сформулированы основные позиции реферата, а содержание соответствует теме реферата; в содержании реферата логично, связно, но недостаточно полно излагается теоретическая или практическая часть; заключение содержит выводы, логично вытекающие из содержания основной части; стиль изложения соответствует специфике жанра научной работы; в оформлении списка литературы встречаются незначительные погрешности</p> <p>3-5 балла – во введении основные позиции реферата сформулированы нечетко или не вполне соответствуют теме исследования; в основной части реферата (теоретической и эмпирической главах) исследование выполнено недостаточно логично (убедительно) и последовательно; выводы в заключение отражают содержание глав не полностью или неточно; в оформлении списка литературы нет единообразия; стиль изложения не отвечает специфике жанра научной работы</p> <p>1-2 балла – текст реферата представляет несамостоятельное (компиляция; плагиат) научное исследование; реферат написан с несоблюдением технических и научных требований</p>
4.	Посещаемость	10	<p>10 баллов – студент посетил все 100% занятий 6-7 баллов – студент посетил не менее 80% занятий 4-5 баллов – студент посетил не менее 50% занятий 1-3 балла – студент посетил не менее 25% занятий Если студент посетил менее 25% занятий, баллы не начисляются.</p>
5.	Премияльные баллы	20	<p>Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции</p>
6.	Итого за семестр	100	

9 семестр

- посещаемость – 10 баллов
- текущий контроль – 45 баллов
- контрольные срезы – 2 среза: 5 баллов, 10 баллов
- 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.	Порядок подготовки и проведения аттестации объектов информатизации и по требованиям ФСТЭК России.	Выполнение лабораторных работ	20	<p>Лабораторные работы выполняются по текущему разделу или темы дисциплины.</p> <p>20 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>10 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>5 баллов - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>
		Собеседование	10	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>10 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>7 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>3 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>

2.	Порядок проведения сертификационных испытаний средств защиты информации.	Выполнение лабораторных работ (контрольный срез)	5	<p>Лабораторные работы выполняются по текущему разделу или теме дисциплины.</p> <p>5 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>3 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>1 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>
		Собеседование	5	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>5 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>3 балла - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>1 балл – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>

3.	Порядок лицензирования деятельности по защите информации ФСТЭК России.	Выполнение лабораторных работ	10	<p>Лабораторные работы выполняются по текущему разделу или теме дисциплины.</p> <p>10 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы, используя профессиональную терминологию.</p> <p>6 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы.</p> <p>3 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы.</p>
		Собеседование(контрольный срез)	10	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> - правильность ответа по содержанию; - полнота и глубина ответа; - сознательность ответа; - логика изложения материала; - рациональность использованных приемов и способов решения поставленной учебной задачи; - своевременность и эффективность использования наглядных пособий и технических средств при ответе; - использование дополнительного материала; - рациональность использования времени, отведенного на задание. <p>10 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>7 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>5 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
4.	Посещаемость		10	<p>10 баллов – студент посетил все 100% занятий 6-7 баллов – студент посетил не менее 80% занятий 4-5 баллов – студент посетил не менее 50% занятий 1-3 балла – студент посетил не менее 25% занятий Если студент посетил менее 25% занятий, баллы не начисляются.</p>

5.	Премияльные баллы	20	Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции
6.	Ответ на экзамене	30	25-30 баллов – студент раскрыл основные вопросы и задания билета на оценку «отлично». 18-24 баллов – студент раскрыл основные вопросы и задания билета на оценку «хорошо», 10-17 баллов – студент раскрыл основные вопросы и задания билета на оценку «удовлетворительно»
7.	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

Выполнение лабораторных работ

Тема 2. Основы Законодательства РФ, руководящие и нормативные документы ФСТЭК (Гостехкомиссии) России, регламентирующие вопросы защиты информации.

Тема Установление необходимости обработки (обсуждения) информации ограниченного доступа на объекте информатизации.

Цель работы Проанализировать перечень сведений конфиденциального характера, обрабатываемых в организации, и состав мероприятий по защите информации

Исполнение При проведении работ по защите государственных информационных ресурсов перечень сведений конфиденциального характера, обрабатываемых в организации, и состав мероприятий по защите информации устанавливаются в соответствии с требованиями нормативных и методических документов по защите информации

Защита ЛР. Разработка перечня сведений конфиденциального характера, обрабатываемых в организации

Тема 3. Организация защиты автоматизированных систем и их компонентов от несанкционированного доступа.

Тема Проверка документов на полноту и достаточность их содержания, а также проверка соответствия их содержания требованиям к безопасности информации.

Цель работы Проверка содержания документов на достаточность указанных в них сведений в соответствии с требованиями нормативных и методических документов по безопасности информации

Исполнение составление наименования и характеристики объекта информатизации;

- перечня технических и программных средств объекта информатизации;

определение класса защищенности объекта информатизации;

Защита ЛР. Разработка документов заявителя для проведения аттестации

Тема 4. Порядок подготовки и проведения аттестации объектов информатизации по требованиям ФСТЭК России.

Изучение технологического процесса автоматизированной обработки информации ограниченного доступа

Цель работы Изучается схема информационных потоков в автоматизированной системе.

Определяются возможности доступа к хранимой, обрабатываемой и передаваемой информации

Исполнение В описании технологического процесса обработки информации должны быть указаны:

- перечень субъектов доступа (сотрудников организации);
- перечень объектов доступа;
- режим обработки информации (однопользовательский и мно-гопользовательский);

особенности обработки, хранения, удаления, передачи и копирования информации, а также доступа к ней

Тема 5. Порядок проведения сертификационных испытаний средств защиты информации.

Проверка соответствия состава и структуры программно-технических средств автоматизированной системы представленной документации

Цель работы Выявляются программно-технические средства, потенциально опасные с точки зрения обеспечения безопасности обработки, хранения и передачи информации ограниченного доступа

Исполнение При наличии установленных в автоматизированной системе средств разработки и отладки программного обеспечения проверяются условия эксплуатации этих программных средств на соответствие требованиям нормативных и методических документов по защите информации

Тема 6. Порядок лицензирования деятельности по защите информации ФСТЭК России.

Тема Разграничение доступа пользователей на объекте информатизации

Цель работы Определение уровней полномочий пользователей по доступу к информации ограниченного доступа, обрабатываемой и (или) обсуждаемой на объекте информатизации

Исполнение Проверяется соответствие разрешительной системы доступа требованиям нормативных и методических документов по безопасности информации

Реферат

Тема 3. Организация защиты автоматизированных систем и их компонентов от несанкционированного доступа.

1. Законодательство о персональных данных.
2. Методы и средства защиты информации от НСД
3. Защита авторских прав.
4. Назначение, функции и типы систем видеозащиты.
5. Как подписывать с помощью ЭЦП электронные документы различных форматов.
6. Обзор угроз и технологий защиты Wi-Fi-сетей.
7. Проблемы внедрения дискового шифрования.

8. Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.
9. Особенности процессов аутентификации в корпоративной среде.
10. Квантовая криптография.
11. Утечки информации: как избежать. Безопасность смартфонов.
12. Безопасность применения пластиковых карт - законодательство и практика.
13. Защита CD- и DVD-дисков от копирования.
14. Современные угрозы и защита электронной почты.
15. Программные средства анализа локальных сетей на предмет уязвимостей.
16. Безопасность применения платежных систем - законодательство и практика.
17. Аудит программного кода по требованиям безопасности.
18. Антишпионское ПО (antispware).
19. Обеспечение безопасности Web-сервисов.
20. Защита от внутренних угроз.
21. Технологии RFID.
22. Уничтожение информации на магнитных носителях.
23. Ботнеты - плацдарм современных кибератак.
24. Цифровые водяные знаки в изображениях.
25. Электронный документооборот. Модели нарушителя.
26. Идентификация по голосу. Скрытые возможности.
27. Безопасность океанских портов.
28. Безопасность связи.
29. Безопасность розничной торговли.
30. Банковская безопасность.
31. Информатизация управления транспортной безопасностью.
32. Биопаспорт.
33. Обзор современных платформ архивации данных.
34. Что такое консалтинг в области ИБ.
35. Бухгалтерская отчетность как источник рассекречивания информации.
36. Управление рисками: обзор потребительских подходов.
37. Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности.
38. Распределенные атаки на распределенные системы.
39. Оценка безопасности автоматизированных систем.
40. Windows и Linux: что безопаснее?
41. Функциональная безопасность программных средств.
42. Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств.
43. Информационная безопасность: экономические аспекты.

Собеседование

Тема 1. Введение.

1. Понятие аттестации ОИ. Объекты информатизации, аттестуемые по требованиям безопасности информации. ОИ, подлежащие аттестации.
2. Назначение проведения аттестации.
3. Перечень проводимых работ при проведении аттестации.
4. Описание концепции проведения работ по аттестации.
5. Завершение работ по аттестации с последующим выводом.

Тема 2. Основы Законодательства РФ, руководящие и нормативные документы ФСТЭК (Гостехкомиссии) России, регламентирующие вопросы защиты информации.

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России)
2. Приказ ФСТЭК России от «14» марта 2014 г. n 31 "об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами
3. Приказ ФСТЭК России № 21 от 18 февраля 2013 г. Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Тема 3. Организация защиты автоматизированных систем и их компонентов от несанкционированного доступа.

1. Внедрение современных ИТ на базе компьютерной техники и телекоммуникационных средств
2. Задачи защиты информации от НСД в АСОД
3. Тракты доступа субъектов к информационным объектам
4. Список лиц, допущенных к объектам информатизации
5. Перечень средств защиты объектов информатизации от НСД

Тема 4. Порядок подготовки и проведения аттестации объектов информатизации по требованиям ФСТЭК России.

1. Документы, определяющие порядок проведения аттестации объектов информатизации по требованиям безопасности информации
2. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации
3. Рассмотрение заявки на аттестацию, принятие решения на ее проведение, доведение решения до заявителя и органа по аттестации объектов информатизации.

Тема 5. Порядок проведения сертификационных испытаний средств защиты информации.

1. "Положение о сертификации средств защиты информации"
2. Понятие сертификации
3. Понятие сертификата соответствия
4. Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну
5. Технические средства, подлежащие обязательной сертификации

Тема 6. Порядок лицензирования деятельности по защите информации ФСТЭК России.

1. Лицензирование деятельности по технической защите конфиденциальной информации
2. Контроль защищенности конфиденциальной информации от утечки по техническим каналам
3. Контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации
4. Сертификационные испытания на соответствие требованиям по безопасности информации продукции, используемой в целях защиты конфиденциальной информации
5. Установка, монтаж, испытания, ремонт средств защиты информации

Тестирование

Тема 2. Основы Законодательства РФ, руководящие и нормативные документы ФСТЭК (Гостехкомиссии) России, регламентирующие вопросы защиты информации.

1. **Основной проблемой реализации систем защиты явля-ется:**

- а) исключение случайного и преднамеренного получения информации посторонними лицами;
- б) разграничение доступа к устройствам и ресурсам системы всех пользователей, администрации и обслуживающего персонала;
- с) системы защиты не должны создавать заметных неудобств пользователям в ходе их работы с ресурсами системы.
- д) все вышеперечисленное.

2. Комплексный (системный) подход к построению любой системы включает в себя:

- а) изучение объекта внедряемой системы; оценку угроз безопасности объекта; анализ средств, которыми будем оперировать при построении системы; оценку экономической целесообразности; изучение самой системы, ее свойств, принципов работы и возможность увеличения ее эффективности; соотношение всех внутренних и внешних факторов; возможность дополнительных изменений в процессе построения системы и полную организацию всего процесса от начала до конца; +
- б) совокупности научных, научно-технических и организационных мероприятий и применения специальных средств и методов, а создания целостной системы организационно-технологических мероприятий и применения комплекса специальных средств и методов;
- с) разработку единой концепции как полной совокупности научно обоснованных взглядов, положений и решений, необходимых и достаточных для оптимальной организации и обеспечения надежности защиты информации.

3. Какими бывают стратегии защиты информации?

- а) оборонительная, наступательная, упреждающая;
- б) наступательная, инженерная, сигнализационная, адаптивная;
- с) инженерно-техническая, программно-аппаратная, программная, организационная.

1 4. Что должна включать в себя система защиты от утечки?

- а) защита от наблюдения, прослушивания, перехвата, контроль вещественных носителей (комплексы мероприятий по контролю звукопроницаемости помещений, предотвращение утечки информации путем шифрования, контроль за уничтожением носителей и т.д.)
- б) звукоизоляция, глушение, экранирование);
- с) защита от перехвата (шифрование, экранирование, зашумление, фильтрация);+ комплекс защиты от перехвата (шифрование, экранирование, зашумление, фильтрация) комплекс предотвр. утечки вещ.носителей (учет и скрытие отходов, уничтожение отходов)
- д) определение полномочий пользователя (учет и анализ потока информации, распределение полномочий пользователей, ведения журнала учета);
- е) установки пропускного режима (КПП на входе в здание, контроль доступа в помещения для совещаний и хранилищ конфиденциальных данных);

5. Какие элементы входят в состав информационных правоотношений ?

- а) должностные инструкции, обращение, фиксирование, хранение;
- б) права, ограничение прав, обязанности, ответственность;
- с) права, обязанности, фиксирование, хранение
- д) права, ограничение прав, должностные инструкции, ответственность

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета, экзамена

Типовые вопросы зачета (ПК-6)

1. Понятие аттестации ОИ. Объекты информатизации, аттестуемые по требованиям безопасности информации. ОИ, подлежащие аттестации.
2. Назначение проведения аттестации.
3. Перечень проводимых работ при проведении аттестации.
4. Основные руководящие документы ФСТЭК России по аттестации объектов информатизации
5. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации
6. Функции заявителя.
7. Перечень документов заявителя для аттестации защищаемого помещения.
8. Перечень документов заявителя для аттестации АС.
9. Порядок проведения аттестации объектов информатизации
10. Содержание заявки на проведения аттестации объектов информатизации
11. Исходные данные по аттестуемому ОИ
12. Перечень СЗИ, подлежащих сертификации по требованиям безопасности информации
13. Содержание программы аттестационных испытаний
14. Цели и виды аттестационных испытаний
15. Условия и порядок проведения аттестационных испытаний
16. Этапы программы аттестационных испытаний
17. Методика аттестационных испытаний
18. Анализ процесса обработки информации
19. Испытание подсистемы управления доступом
20. Испытание подсистемы регистрации и учета
21. Испытание подсистемы обеспечения целостности
22. Состав аттестационной комиссии
23. Документы, оформляемые по результатам спецпроверки и аттестации.
24. Содержание заключения по результатам аттестации
25. Оформление, регистрация и выдача аттестатов соответствия
26. Содержание аттестата соответствия

Типовые задания для зачета (ПК-6)

1. **Основной проблемой реализации систем защиты является:**
 1. исключение случайного и преднамеренного получения информации посторонними лицами;
 2. разграничение доступа к устройствам и ресурсам системы всех пользователей, администрации и обслуживающего персонала;
 3. системы защиты не должны создавать заметных неудобств пользователям в ходе их работы с ресурсами системы.
 4. все вышеперечисленное.(+)
5. **Комплексный (системный) подход к построению любой системы включает в себя:**
 1. изучение объекта внедряемой системы; оценку угроз безопасности объекта; анализ средств, которыми будем оперировать при построении системы; оценку экономической целесообразности; изучение самой системы, ее свойств, принципов работы и возможность увеличения ее эффективности; соотношение всех внутренних и внешних факторов; возможность дополнительных изменений в процессе построения системы и полную организацию всего процесса от начала до конца; (+)

2. совокупности науч-ных, научно-технических и организационных мероприятий и применения специальных средств и методов, а создания целостной системы организационно-технологических мероприятий и применения комплекса специальных средств и методов;
3. разработку единой концепции как полной совокупности научно обос-нованных взглядов, положений и решений, необходимых и достаточных для оптимальной организации и обеспечения надежности защиты информации.

4. Какими бывают стратегии защиты информации?

1. оборонительная, наступательная, упреждающая; (+)
2. наступательная, инженерная, сигнализационная, адаптивная;
3. инженерно-техническая, программно-аппаратная, программная, организационная.

4. Что должна включать в себя система защиты от утечки?

1. защита от наблюдения, прослушивания, перехвата, контроль вещественных носителей (комплексы мероприятий по контролю звукопроницаемости помещений, предотвращение утечки информации путем шифрования, контроль за уничтожением носителей и т.д.)
2. звукоизоляция, глушение, экранирование);(+)
3. защита от перехвата (шифрование, экранирование, зашумление, фильтрация);(+)
- комплекс защиты от перехвата (шифрование, экранирование, зашумление, фильтрация)
- комплекс предотвр. утечки вещ.носителей (учет и скрытие отходов, уничтожение отходов)
4. определение полномочий пользователя (учет и анализ потока информации, распределение полномочий пользователей, ведения журнала учета);
5. установки пропускного режима (КПП на входе в здание, контроль доступа в помещения для совещаний и хранилищ конфиденциальных данных);

6. Какие элементы входят в состав информационных правоотношений ?

1. должностные инструкции, обращение, фиксирование, хранение;
2. права, ограничение прав, обязанности, ответственность;(+)
3. права, обязанности, фиксирование, хранение;
4. права, ограничение прав, должностные инструкции, ответственность.

Типовые вопросы экзамена (ПК-6)

1. Понятие аттестации ОИ. Объекты информатизации, аттестуемые по требованиям безопасности информации. ОИ, подлежащие аттестации.
2. Назначение проведения аттестации.
3. Перечень проводимых работ при проведении аттестации.
4. Основные руководящие документы ФСТЭК России по аттестации объектов информатизации
5. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации
6. Функции заявителя.
7. Перечень документов заявителя для аттестации защищаемого помещения.
8. Перечень документов заявителя для аттестации АС.
9. Порядок проведения аттестации объектов информатизации
10. Содержание заявки на проведения аттестации объектов информатизации
11. Исходные данные по аттестуемому ОИ
12. Перечень СЗИ, подлежащих сертификации по требованиям безопасности информации
13. Содержание программы аттестационных испытаний
14. Цели и виды аттестационных испытаний
15. Условия и порядок проведения аттестационных испытаний
16. Этапы программы аттестационных испытаний
17. Методика аттестационных испытаний
18. Анализ процесса обработки информации
19. Испытание подсистемы управления доступом

20. Испытание подсистемы регистрации и учета
21. Испытание подсистемы обеспечения целостности
22. Состав аттестационной комиссии
23. Документы, оформляемые по результатам спецпроверки и аттестации.
24. Содержание заключения по результатам аттестации
25. Оформление, регистрация и выдача аттестатов соответствия
26. Содержание аттестата соответствия

Типовые задания для экзамена (ПК-6)

1. Основной проблемой реализации систем защиты является:

1. исключение случайного и преднамеренного получения информации посторонними лицами;
2. разграничение доступа к устройствам и ресурсам системы всех пользователей, администрации и обслуживающего персонала;
3. системы защиты не должны создавать заметных неудобств пользователям в ходе их работы с ресурсами системы.
4. все вышеперечисленное.(+)

5. Комплексный (системный) подход к построению любой системы включает в себя:

1. изучение объекта внедряемой системы; оценку угроз безопасности объекта; анализ средств, которыми будем оперировать при построении системы; оценку экономической целесообразности; изучение самой системы, ее свойств, принципов работы и возможность увеличения ее эффективности; соотношение всех внутренних и внешних факторов; возможность дополнительных изменений в процессе построения системы и полную организацию всего процесса от начала до конца; (+)
2. совокупности научных, научно-технических и организационных мероприятий и применения специальных средств и методов, а создания целостной системы организационно-технологических мероприятий и применения комплекса специальных средств и методов;
3. разработку единой концепции как полной совокупности научно обоснованных взглядов, положений и решений, необходимых и достаточных для оптимальной организации и обеспечения надежности защиты информации.

4. Какими бывают стратегии защиты информации?

1. оборонительная, наступательная, упреждающая; (+)
2. наступательная, инженерная, сигнализационная, адаптивная;
3. инженерно-техническая, программно-аппаратная, программная, организационная.

4. Что должна включать в себя система защиты от утечки?

1. защита от наблюдения, прослушивания, перехвата, контроль вещественных носителей (комплексы мероприятий по контролю звукопроницаемости помещений, предотвращение утечки информации путем шифрования, контроль за уничтожением носителей и т.д.)
2. звукоизоляция, глушение, экранирование);(+)
3. защита от перехвата (шифрование, экранирование, зашумление, фильтрация);(+)
- комплекс защиты от перехвата (шифрование, экранирование, зашумление, фильтрация)
- комплекс предотвр. утечки вещ.носителей (учет и скрытие отходов, уничтожение отходов)
4. определение полномочий пользователя (учет и анализ потока информации, распределение полномочий пользователей, ведения журнала учета);
5. установки пропускного режима (КПП на входе в здание, контроль доступа в помещения для совещаний и хранилищ конфиденциальных данных);

6. Какие элементы входят в состав информационных правоотношений ?

1. должностные инструкции, обращение, фиксирование, хранение;
2. права, ограничение прав, обязанности, ответственность;(+)
3. права, обязанности, фиксирование, хранение;
4. права, ограничение прав, должностные инструкции, ответственность.

4.4. Шкала оценивания промежуточной аттестации

Зачет

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«зачтено» (50 - 100 баллов)	ПК-6	Показывает хороший уровень теоретических знаний по вопросам аудита и аттестации объектов информатизации. использует нормативные правовые акты в профессиональной деятельности. Показывает хорошие навыки организации технологического процесса проведения аудита и аттестации объектов информатизации в соответствии с правовыми нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Может частично показать навыки организации аудита и аттестации объектов информатизации
«не зачтено» (0 - 49 баллов)	ПК-6	Не имеет знаний по вопросам аудита и аттестации объектов информатизации. Не может использовать нормативные правовые акты в профессиональной деятельности. Не может показать навыки организации технологического процесса проведения аудита и аттестации объектов информатизации в соответствии с правовыми нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Экзамен

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«отлично» (85 - 100 баллов)	ПК-6	Показывает высокий уровень теоретических знаний по вопросам аудита и аттестации объектов информатизации. Эффективно использует нормативные правовые акты в профессиональной деятельности. Показывает высокие навыки организации технологического процесса проведения аудита и аттестации объектов информатизации в соответствии с правовыми нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Может показать навыки организации аудита и аттестации объектов информатизации
«хорошо» (70 - 84 баллов)	ПК-6	Показывает хороший уровень теоретических знаний по вопросам аудита и аттестации объектов информатизации. использует нормативные правовые акты в профессиональной деятельности. Показывает хорошие навыки организации технологического процесса проведения аудита и аттестации объектов информатизации в соответствии с правовыми нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Может частично показать навыки организации аудита и аттестации объектов информатизации

«удовлетворительно» (50 - 69 баллов)	ПК-6	Показывает низкий уровень знаний по вопросам аудита и аттестации объектов информатизации. Частично использует нормативные правовые акты в профессиональной деятельности. Показывает низкие навыки организации технологического процесса проведения аудита и аттестации объектов информатизации в соответствии с правовыми нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Может частично показать навыки организации аудита и аттестации объектов информатизации
«неудовлетворительно» (менее 50 баллов)	ПК-6	Не имеет знаний по вопросам аудита и аттестации объектов информатизации. Не может использовать нормативные правовые акты в профессиональной деятельности. Не может показать навыки организации технологического процесса проведения аудита и аттестации объектов информатизации в соответствии с правовыми нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

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. Кияев В., Граничин О. Информатизация предприятия. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 235 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=429037>
2. Жихарев А. П. Автоматизированные информационные системы и ресурсы города Москвы : научное издание. - Москва: Юнити-Дана : Закон и право, 2014. - 255 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=447946>

6.2 Дополнительная литература:

1. Вязовова О.В. Информатизация образовательного пространства учителя информатики : дис. ... канд. пед. наук:13.00.01 : Защищена 28.04.05 : Утв. 21.10.05. - Тамбов, 2005. - 240 с.
2. Карминский А.М., Нестеров П.В. Информатизация бизнеса. - М.: Финансы и статистика, 1997. - 415 с.
3. Копытова Н.Е., Макаровский А.В. Информатизация научно-исследовательской деятельности : учебно-методический комплекс. - [Тамбов]: [Б.и.], 2011. - 1 электрон. опт. диск (CD-ROM)
4. Мельникова, Ю. В., Нургазиев, Р. Б., Фортунатов, А. В. Информатизация бизнес-процессов : сборник лабораторных и контрольных заданий. - Весь срок охраны авторского права; Информатизация бизнес-процессов. - Саратов: Тема, 2009. - 87 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/21780.html>

6.3 Иные источники:

1. Федеральный портал «Российское образование» - <http://www.edu.ru/>

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

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

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

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

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

Лицензионное и свободно распространяемое программное обеспечение:

LibreOffice

Microsoft Office Профессиональный плюс 2007

Microsoft Windows 10

Профессиональные базы данных и информационные справочные системы:

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

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.