

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

УТВЕРЖДАЮ:
Директор института



И. Н. Якунина
«20» января 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.Б.26 Комплексная система защиты информации 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: 2020

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 «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. Контроль знаний обучающихся и типовые оценочные средства.....	11
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	33
6. Учебно-методическое и информационное обеспечение дисциплины.....	35
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	35

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

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

ПК-1 Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз

ПК-3 Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации

1.2 Виды и задачи профессиональной деятельности по дисциплине:

- эксплуатационная

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов технических систем обеспечения безопасности информации
- участие в проведении специальных проверок и исследований, аттестации объектов, помещений, технических средств, систем, сертификационных испытаний программных средств на предмет соответствия требованиям защиты информации
- администрирование подсистем обеспечения информационной безопасности на объекте

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

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Знания и умения, необходимые для формирования трудового действия / компетенции
	ОК-4 Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета	Знает и понимает: принципы и тенденции изменений законодательства в области информации, требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности.
		Умеет (способен продемонстрировать): анализировать основные изменения законодательства в области информации и применять их на практике, осуществлять логику взаимосвязей информационных систем и ресурсов
		Владеет: навыками поиска актуальной правовой информации, знаниями основ государства и права, основными понятиями и категориями информационного права
	ПК-1 Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	Знает и понимает: основных тенденций создания комплекса мер по обеспечению безопасности информации,
		Умеет (способен продемонстрировать): самостоятельно анализировать меры по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну

	информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	Владеет: формальной постановки и решения задач защиты информации
	ПК-3 Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации	Знает и понимает: основных целей, задач, методов по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, анализа эффективности системы защиты информации Умеет (способен продемонстрировать): администрировать подсистемы ИБ определять рациональные меры защиты на объектах и оценивать их эффективность Владеет: эксплуатации подсистем ИБ, разработки практических рекомендаций и реализацией их в системе информационной безопасности или ее элементах

1.4 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

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

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

безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения		
		Очная (семестр)		
		8	9	10
1	Практика по получению профессиональных умений и опыта профессиональной деятельности	+	+	
2	Преддипломная практика			+

ПК-3 Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения	
		Очная (семестр)	
		8	9
1	Компьютерная экспертиза	+	
2	Практика по получению профессиональных умений и опыта профессиональной деятельности	+	+

2. Место дисциплины в структуре ОП специалиста:

Дисциплина «Комплексная система защиты информации объектов информатизации» относится к базовой части учебного плана ОП по направлению подготовки 10.05.05 - Безопасность информационных технологий в правоохранительной сфере.

Дисциплина «Комплексная система защиты информации объектов информатизации» изучается в 7, 8, 9 семестрах.

3. Объем и содержание дисциплины

3.1. Объем дисциплины: 9 з.е.

Очная: 9 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	324

Контактная работа	138
Лекции (Лекции)	48
Лабораторные (Лаб. раб.)	90
Самостоятельная работа (СР)	148
Курсовая работа	2
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	
7 семестр					
1	Законодательно-правовые и организационные основы обеспечения информационной безопасности предприятия	10	17	28	Защита лабораторных работ ; Собеседование
2	Принципы организации и этапы разработки КСЗИ	8	17	28	Защита лабораторных работ ; Собеседование; Тестирование
8 семестр					
3	Моделирование КСЗИ	8	8	19	Собеседование; Защита лабораторных работ
4	Функционирование КСЗИ	8	8	19	Собеседование; Защита лабораторных работ; Тестирование
9 семестр					
5	Способы обеспечения информационной безопасности информационных систем	6	12	18	Собеседование; Защита лабораторных работ

6	Обеспечение безопасности персональных данных, обрабатываемых в информационных системах	4	14	16	Собеседование; Защита лабораторных работ
7	Обеспечение безопасности информации в ключевых системах информационной инфраструктуры	4	Пп 14	20	Собеседование; Защита лабораторных работ; Тестирование; Практическое задание для практической подготовки

Тема 1. Законодательно-правовые и организационные основы обеспечения информационной безопасности предприятия (ОК-4)

Лекция.

Законодательно-правовые и организационные основы обеспечения информационной безопасности предприятия. Сущность и задачи комплексной системы защиты информации (КСЗИ) на предприятии.

Лабораторные работы.

Оценка состояния защищенности предприятия

Оценка состояния защищенности по направлениям обеспечения безопасности:

- Состав и структура службы безопасности.
- Правовое обеспечение безопасности.
- Организационные меры защиты.
- Инженерно-техническое обеспечение безопасности.
- Управление безопасностью.

Задания для самостоятельной работы.

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

Тема 2. Принципы организации и этапы разработки КСЗИ (ОК-4)

Лекция.

Факторы, влияющие на организацию КСЗИ. Определение и нормативное закрепление состава защищаемой информации, определение объектов защиты, анализ и оценка угроз безопасности информации.

Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию. Выбор методов и способов предотвращения угроз безопасности информации.

Этапы разработки КСЗИ.

Лабораторные работы.

Определение защищенности информации при несанкционированном доступе.

1. Подсчитать вероятности событий 1-8 при T=500 часов.
2. Найти вероятности сложных событий:

$$P\{D(1) + E\} = P\{D(1)\} + P\{E\} - P\{D(1)\} \times P\{E\},$$

$$P\{D(2) + E\} = P\{D(2)\} + P\{E\} - P\{D(2)\} \times P\{E\},$$

$$P\{CB(1) A(1)\} = P\{C\} \times P\{B(1)\} \times P\{A(1)\},$$

$$P\{CB(2) A(2)\} = P\{C\} \times P\{B(2)\} \times P\{A(2)\},$$

$$P\{CB(1) A(1) + CB(2) A(2)\} = 1 - (1 - P\{CB(1) A(1)\})(1 - P\{CB(2) A(2)\}),$$

$$P\{E + CB(1) A(1) + CB(2) A(2)\} = 1 - (1 - P\{E\})(1 - P\{CB(1) A(1)\})(1 - P\{CB(2) A(2)\}).$$

Задания для самостоятельной работы.

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

Тема 3. Моделирование КСЗИ (ПК-1)

Лекция.

Определение условий функционирования КСЗИ. Разработка модели КСЗИ. Определение компонентов КСЗИ, технологическое и организационное построение КСЗИ.

Кадровое, материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ.

Лабораторные работы.

Перечень персональных данных.

Контрольные задания:

Составить перечень персональных данных, обрабатываемых в выбранном объекте (организация, фирма, предприятие и т.д.).

Задания для самостоятельной работы.

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

Тема 4. Функционирование КСЗИ (ПК-1)

Лекция.

Назначение, структура и содержание управления КСЗИ, принципы и методы планирования функционирования КСЗИ.

Сущность и содержание контроля функционирования КСЗИ. Управление КСЗИ в условиях чрезвычайных ситуаций. Методы оценки эффективности КСЗИ.

Лабораторные работы.

Определение уровня исходной защищенности ИСДн.

Контрольные задания. Определить уровень исходной защищенности ИСПДн выбранного объекта (организация, фирма, предприятие и т.д.).

Задания для самостоятельной работы.

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

Тема 5. Способы обеспечения информационной безопасности информационных систем (ПК-1)

Лекция.

Понятие и классификации информационных систем предприятия. Специфика построения корпоративных ИС. Угрозы информации в корпоративных ИС. Противодействия угрозам в корпоративных ИС.

Лабораторные работы.

1. Определение актуальности угроз безопасности персональных данных в ИСПДН. Контрольные задания.
2. Составить перечень возможных УБПДн.
3. Определить вероятности реализации угроз нарушителем в ИСПДн.
4. Определение возможности реализации угрозы в ИСПДн АС.
5. Составить перечень актуальных угроз безопасности ПДн в ИСПДн АС.

Задания для самостоятельной работы.

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

Тема 6. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах (ПК-3)

Лекция.

Нормативно-правовое регулирование обеспечения безопасности персональных данных, обрабатываемых в информационных системах.

Лабораторные работы.

Расчет рисков информационной системы на основе модели угроз и уязвимостей. Расчет рисков по угрозе информационной безопасности

На первом этапе рассчитываем уровень угрозы по уязвимости T_h на основе критичности и вероятности реализации угрозы через данную уязвимость. Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации.

Задания для самостоятельной работы.

1. Законодательно-правовые обеспечения информационной безопасности предприятия.
2. Организационные основы обеспечения информационной безопасности предприятия.
3. Задачи комплексной системы защиты информации (КСЗИ) на предприятии.
4. Определение объектов защиты, состава защищаемой информации предприятия.
5. Нормативное закрепление состава защищаемой информации предприятия.
6. Определение функций КСЗИ по защите информации предприятия.

Тема 7. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры (ПК-3)

Лекция.

Информационная структура предприятия. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры.

Лабораторные работы.

Технология оценки угроз и уязвимостей.

Для оценки угроз и уязвимостей применяются различные методы, в основе которых могут лежать:

- экспертные оценки;
- статистические данные;
- учет факторов, влияющих на уровни угроз и уязвимостей.

Задания для самостоятельной работы.

1. Современные технические средства несанкционированного доступа к информации.
2. Анализ и оценка угроз безопасности информации.

- 3 Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.
- 4 Современные технические средства охраны и защиты информации.
- 5 Выбор методов и способов предотвращения угроз безопасности информации.
- 6 Определение условий функционирования КСЗИ.
- 7 Определение компонентов КСЗИ
- 8 Технологическое и организационное построение КСЗИ.
- 9 Кадровое, материально-техническое обеспечение функционирования КСЗИ.

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

7 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.	Законодательно-правовые и организационные основы обеспечения информационной безопасности предприятия	Защита лабораторных работ (контрольный срез)	10	Лабораторные работы выполняются по тематике практических занятий. 24 балла – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию 14 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы 8 баллов - 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

		Собеседование	19	<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>19 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>12 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>6 баллов – 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.	Принципы организации и этапы разработки КСЗИ	Защита лабораторных работ	32	<p>Лабораторные работы выполняются по тематике практических занятий. 32 балла – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>16 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>8 баллов - 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	19	<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>19 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>12 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>6 баллов – 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(контрольный срез)	10	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>14 баллов – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>5 баллов - студент правильно отвечает на 25-50% вопросов в тесте.</p>
3.	Посещаемость		10	<p>10 баллов – стопроцентное посещение занятий студентом</p> <p>7-5 баллов – посещаемость студента составляет не менее 80 % занятий</p> <p>3 баллов – посещаемость студента составляет не менее 50 % занятий</p> <p>1 балла – посещаемость студента составляет не менее 25 % занятий</p>

4.	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 / журнале из перечня ВАК – 10 / 15 / 20
5.	Итого за семестр	100	

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.	Моделирование КСЗИ	Собеседование	19	<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>19 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>12 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>6 баллов – 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>
		Защита лабораторных работ(контрольный срез)	10	<p>Лабораторные работы выполняются по тематике практических занятий. 24 балла – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>14 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>8 баллов - 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>

2.	Функционирование КСЗИ	Собеседование	19	<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>19 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>12 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>6 баллов – 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>
		Защита лабораторных работ	32	<p>Лабораторные работы выполняются по тематике практических занятий. 32 балла – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>16 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>8 баллов - 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>
		Тестирование(контрольный срез)	10	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>10 баллов – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>5 баллов - студент правильно отвечает на 25-50% вопросов в тесте.</p>

3.	Посещаемость	10	10 баллов – стопроцентное посещение занятий студентом 7-5 баллов – посещаемость студента составляет не менее 80 % занятий 3 баллов – посещаемость студента составляет не менее 50 % занятий 1 балла – посещаемость студента составляет не менее 25 % занятий
4.	Премияльные баллы	20	Дополнительные премияльные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20
5.	Итого за семестр	100	

9 семестр

- посещаемость – 10 баллов
- текущий контроль – 44 балла
- контрольные срезы – 2 среза: 10 баллов, 6 баллов
- премияльные 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.	Способы обеспечения информационной безопасности информационных систем	Собеседование	8	<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>8 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>5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>2 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>
		Защита лабораторных работ	10	<p>Лабораторные работы выполняются по тематике практических занятий. 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>5 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>2 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>

2.	Обеспечение безопасности персональных данных, обрабатываемых в информационных системах	Собеседование	8	<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>8 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>5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>2 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>
		Защита лабораторных работ(контрольный срез)	10	<p>Лабораторные работы выполняются по тематике практических занятий. 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>5 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>2 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>

3.	Обеспечение безопасности информации в ключевых системах информационной инфраструктуры	Собеседование	8	<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>8 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>5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>2 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>
		Защита лабораторных работ	8	<p>Лабораторные работы выполняются по тематике практических занятий.</p> <p>8 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>5 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>2 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>
		Тестирование(контрольный срез)	6	<p>Оценка теста по текущему разделу или теме дисциплины</p> <p>6 баллов – студент правильно отвечает на 50-100% вопросов в тесте.</p> <p>2 баллов - студент правильно отвечает на 25-50% вопросов в тесте.</p>

		Практическое задание для практической подготовки	2	<p>Практические задания выполняются по тематике практических занятий.</p> <p>2 баллов – практическое задание выполнено в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>1 балла – практическое задание выполнено, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p>
4.	Посещаемость		10	<p>10 баллов – стопроцентное посещение занятий студентом</p> <p>7-5 баллов – посещаемость студента составляет не менее 80 % занятий</p> <p>3 баллов – посещаемость студента составляет не менее 50 % занятий</p> <p>1 балла – посещаемость студента составляет не менее 25 % занятий</p>
5.	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

6.	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>
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

Распределение баллов по курсовой работе:

- представление содержательной части – не более 55 баллов,
- оформление и информационное сопровождение – не более 20 баллов,
- защита курсовой работы – не более 25 баллов.

Распределение баллов по видам учебной работы и методика начисления баллов:

№	Вид учебной работы	Мах. кол-во баллов	Методика начисления баллов
1.	Представление содержательной части	55	<p>41-55 баллов – содержание работы соответствует выбранному направлению подготовки/специальности и теме работы, работа актуальна, выполнена самостоятельно, имеет творческий характер, отличается определенной новизной; проведен обстоятельный анализ степени теоретического исследования проблемы, различных подходов к ее решению, показано знание информационной (при необходимости – нормативной) базы, использованы актуальные данные; проблема раскрыта глубоко и всесторонне, материал изложен логично; теоретические положения органично сопряжены с практикой, даны практические рекомендации, вытекающие из анализа проблемы; проведен количественный анализ проблемы, который подтверждает выводы автора, иллюстрирует актуальную ситуацию, приведены таблицы сравнений, графики, диаграммы, формулы, показывающие умение автора формализовать результаты исследования;</p> <p>21-40 баллов – содержание работы в целом соответствует выбранной теме, структура плана логична и пропорциональна; обоснование актуальности темы подкрепляется анализом степени теоретического исследования проблемы; основные положения работы раскрыты на достаточном теоретическом и методологическом уровне, большая часть теоретических положений сопряжена с практикой; практические рекомендации обоснованы; выводы по работе содержательны и в целом соответствуют поставленным задачам;</p> <p>1-20 баллов – имеет место определенное несоответствие содержания работы заявленной теме; исследуемая проблема в основном раскрыта, но не отличается новизной, теоретической глубиной и аргументированностью; выявлены недочеты в методологических характеристиках курсового исследования; есть нарушения логики изложения материала, поставленные задачи решены не полностью; теоретические положения слабо связаны с практикой, практические рекомендации носят формальный бездоказательный характер</p>
2.	Оформление и информационное сопровождение	20	<p>16-20 баллов – широко представлена библиография по теме работы, в том числе и зарубежные источники, приложения к работе иллюстрируют достижения автора и подкрепляют его выводы, оформление работы полностью соответствует требованиям, предъявляемым к курсовому исследованию;</p> <p>8-15 баллов – приложения, используемые в исследовании, составлены грамотно, прослеживается связь с положениями курсовой работы; список использованной литературы составлен, следуя ГОСТу, и в достаточной мере соответствует теме работы; имеются отдельные неточности в оформлении работы (отсутствует часть ссылок на используемые источники, есть отдельные стилистические, грамматические и орфографические ошибки);</p> <p>1-7 баллов – в работе не полностью использована необходимая для раскрытия темы научная литература, информационные базы данных, а также материалы исследований; библиографический список оформлен неверно; содержание приложений не отражает решения поставленных задач (отсутствуют необходимые приложения); имеются многочисленные неточности в оформлении работы</p>

3.	Защита курсовой работы	25	<p>19-25 баллов – защита отличается полнотой раскрытия темы и представления полученных результатов; студент демонстрирует уверенность и убедительность манеры выступления; стиль и грамотность речи соответствуют культуре представления результатов научного исследования; ответы на дополнительные вопросы характеризуются краткостью и аргументированностью;</p> <p>10-18 баллов – структура и регламент выступления в целом соблюдены; защита сопровождается грамматически правильной, эмоциональной речью; студент поддерживает хороший контакт с аудиторией; отмечается творческий подход в подготовке объектов наглядности презентации; дополнительные вопросы вызывают некоторые затруднения;</p> <p>1-9 баллов – студент демонстрирует невысокое качество устного доклада; доступность и образность представления проделанной работы и полученных результатов вызывает вопросы; отмечается частичное несоответствие презентации содержанию курсового исследования; дизайн визуальной интерпретации представленной работы затрудняет ее восприятие</p>
ИТОГО:		100	

Итоговая оценка по курсовой работе 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

Защита лабораторных работ

Тема 3. Моделирование КСЗИ

Перечень персональных данных.

Контрольные задания. Составить перечень персональных данных, обрабатываемых в выбранном объекте (организация, фирма, предприятие и т.д.).

Тема 4. Функционирование КСЗИ

Определение уровня исходной защищенности ИСДн.

Контрольные задания. Определить уровень исходной защищенности ИСПДн выбранного объекта (организация, фирма, предприятие и т.д.).

Тема 5. Способы обеспечения информационной безопасности информационных систем

Определение актуальности угроз безопасности персональных данных в ИСПДн. Контрольные задания.

Составить перечень возможных УБПДн

Определить вероятности реализации угроз нарушителем в ИСПДн

Определение возможности реализации угрозы в ИСПДн АС

Составить перечень актуальных угроз безопасности ПДн в ИСПДн АС

Тема 6. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах

Расчет рисков информационной системы на основе модели угроз и уязвимостей. Расчет рисков по угрозе информационной безопасности

На первом этапе рассчитываем уровень угрозы по уязвимости Th на основе критичности и вероятности реализации угрозы через данную уязвимость. Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации.

Тема 7. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры

Технология оценки угроз и уязвимостей.

Для оценки угроз и уязвимостей применяются различные методы, в основе которых могут лежать: экспертные оценки;

статистические данные;

учет факторов, влияющих на уровни угроз и уязвимостей.

Защита лабораторных работ

Тема 1. Законодательно-правовые и организационные основы обеспечения информационной безопасности предприятия

Оценка состояния защищенности предприятия

Оценка состояния защищенности по направлениям обеспечения безопасности:

- Состав и структура службы безопасности.
- Правовое обеспечение безопасности.
- Организационные меры защиты.
- Инженерно-техническое обеспечение безопасности.
- Управление безопасностью.

Защита лабораторных работ

Тема 2. Принципы организации и этапы разработки КСЗИ

Определение защищенности информации при несанкционированном доступе.

1 Подсчитать вероятности событий 1-8 при $T=500$ часов.

2 Найти вероятности сложных событий:

$$P\{D(1) + E\} = P\{D(1)\} + P\{E\} - P\{D(1)\} \times P\{E\},$$

$$P\{D(2) + E\} = P\{D(2)\} + P\{E\} - P\{D(2)\} \times P\{E\},$$

$$P\{CB(1) A(1)\} = P\{C\} \times P\{B(1)\} \times P\{A(1)\},$$

$$P\{CB(2) A(2)\} = P\{C\} \times P\{B(2)\} \times P\{A(2)\},$$

$$P\{CB(1) A(1) + CB(2) A(2)\} = 1 - (1 - P\{CB(1) A(1)\})(1 - P\{CB(2) A(2)\}),$$

$$P\{E + CB(1) A(1) + CB(2) A(2)\} = 1 - (1 - P\{E\})(1 - P\{CB(1) A(1)\})(1 - P\{CB(2) A(2)\}).$$

Практическое задание для практической подготовки

Тема 7. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры

- 1 Современные технические средства несанкционированного доступа к информации.
- 2 Анализ и оценка угроз безопасности информации.
- 3 Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.
- 4 Современные технические средства охраны и защиты информации.
- 5 Выбор методов и способов предотвращения угроз безопасности информации.
- 6 Определение условий функционирования КСЗИ.
- 7 Определение компонентов КСЗИ
- 8 Технологическое и организационное построение КСЗИ.
- 9 Кадровое, материально-техническое обеспечение функционирования КСЗИ.

Собеседование

Тема 1. Законодательно-правовые и организационные основы обеспечения информационной безопасности предприятия

- 1 Законодательство о персональных данных.
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.

Тема 2. Принципы организации и этапы разработки КСЗИ

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.

Тема 3. Моделирование КСЗИ

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).

Тема 4. Функционирование КСЗИ

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.

Тема 5. Способы обеспечения информационной безопасности информационных систем

- 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.

Тема 6. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах

- 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.

Тема 7. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры

- 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.

Тестирование

Тема 2. Принципы организации и этапы разработки КСЗИ

- 1. Из перечисленных разделов, криптография включает: а) управление ключами б) системы электронной подписи в) асимметричные криптосистемы г) симметричные криптосистемы д) стеганография
- 2. Из перечисленного для аутентификации по личной подписи терминальных пользователей используются методы: а) исследование траектории движения руки б) исследование динамических характеристик движения руки в) визуальное сканирование г) фрагментарное сканирование
- 3. Если средство защиты способно противостоять отдельным атакам, то согласно "Европейским критериям" безопасность считается: а) стандартной б) базовой в) средней г) низкой
- 4. Полномочия ядра безопасности ОС ассоциируются с: а) приложениями б) процессами в) пользователями г) периферийными устройствами
- 5. Согласно "Оранжевой книге" дискреционную защиту имеет группа критериев: а) В б) А в) D г) С

6. Два ключа используются в криптосистемах: а) двойного шифрования б) симметричных в) с закрытым ключом г) с открытым ключом
7. На многопользовательские системы с информацией одного уровня конфиденциальности согласно "Оранжевой книге" рассчитан класс: а) C2 б) B2 в) C1 г) B1
8. Согласно "Оранжевой книге" с объектами должны быть ассоциированы: а) уровни доступа б) электронные подписи в) метки безопасности г) типы операций
9. Административные действия в СУБД позволяют выполнять привилегии: а) безопасности б) чтения
10. Как предотвращение неавторизованного использования ресурсов определена услуга защиты: а) пр контроль доступа г) целостность

Тема 4. Функционирование КСЗИ

1. Основной проблемой реализации систем защиты является:
 - 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 работы с ресурсами системы.
 - д) все вышеперечисленное.+
2. Комплексный (системный) подход к построению любой системы включает в себя:
 - а) изучение объ-екта внедряемой системы; оценку угроз безопасности объ-екта; анализ средств которыми будем оперировать при построении системы; оценку экономической целесооб-разности; изучение самой системы, ее свойств, принципов работы и возможность увеличения ее эффективности; со-отношение всех внутренних и внешних факторов; возмоз-ность 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 ме-роприятий и применения комплекса специальных средств и методов;
 - с) разработку единой концепции как полной совокупности научно обос-нованных взглядов, положений и решений, необходимых и достаточных для оптимальной организации и обеспечения надежности защиты информации.

Тема 7. Обеспечение безопасности информации в ключевых системах информационной и

1. Какими бывают стратегии защиты информации?
 - а) оборонительная, наступательная, упреждающая; +
 - б) наступательная, инженерная, сигнализационная, адаптивная;
 - с) инженерно-техническая, программно-аппаратная, программная, организационная.
2. 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);

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета, экзамена

Типовые вопросы зачета (ОК-4, ПК-1, ПК-3)

1. Определение условий функционирования КСЗИ.
2. Разработка модели КСЗИ.
3. Определение компонентов КСЗИ, технологическое и организационное построение КСЗИ.
4. Кадровое, материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ.
5. Назначение, структура и содержание системы управления КСЗИ.
6. Принципы и методы планирования функционирования КСЗИ.
7. Сущность и содержание контроля функционирования КСЗИ.
8. Управление КСЗИ в условиях чрезвычайных ситуаций.
9. Методы оценки эффективности КСЗИ.

Типовые задания для зачета (ОК-4, ПК-1, ПК-3)

Не предусмотрено

Типовые вопросы экзамена (ОК-4, ПК-1, ПК-3)

1. Законодательно-правовые и организационные основы обеспечения информационной безопасности предприятия.
2. Задачи комплексной системы защиты информации (КСЗИ) на предприятии.
3. Определение объектов защиты и нормативное закрепление состава защищаемой информации предприятия.
4. Определение функций КСЗИ по защите информации предприятия.
5. Современные технические средства несанкционированного доступа к информации.
6. Анализ и оценка угроз безопасности информации.
7. Выявление и оценка источников, способов и результатов дестабилизирующего воздействия информации.
8. Современные технические средства охраны и защиты информации.
9. Выбор методов и способов предотвращения угроз безопасности информации.

Типовые задания для экзамена (ОК-4, ПК-1, ПК-3)

1. Основной проблемой реализации систем защиты является:
 - a) исключение случайного и преднамеренного получения информации посторонними лицами;
 - b) разграничение доступа к устройствам и ресурсам системы всех пользователей, администрации и обслуживающего персонала;
 - c) системы защиты не должны создавать заметных неудобств пользователям в ходе их работы 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;

- 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.

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);

Типовые темы курсовых работ (ОК-4, ПК-1, ПК-3)

1.Система нормативных актов РФ в области защиты от НСД 2.Угрозы и уязвимости современных автоматизированных систем 3.Классы защищённости современных автоматизированных систем и программно-аппаратных средств 4.Авторизация как процесс доступа к информации 5.Реализация механизмов парольной защиты для организации банковского сектора 6.Межсетевые экраны как средство защиты информации от несанкционированного доступа 7.Анализ рынка средств усиления парольной защиты 8.Реализация добавочных механизмов усиления парольной защиты 9.Разработка политики информационной безопасности для государственной организации 10.Разработка политики информационной безопасности для организации оборонно-промышленного комплекса 11.Архитектура корпоративной системы защиты информации пищевого предприятия 12.Анализ современных способов разграничения доступа 13.Анализ защищённости внутренней инфраструктуры сети государственной организации 14.Анализ защищённости внутренней инфраструктуры организации 15.Применения инструментальных средств анализа защищённости внутренней инфраструктуры программно-аппаратных средств защиты информации от несанкционированного доступа 17.Технико-комплексирования средств защиты информации на примере коммерческой организации 18.Разработка информации коммерческой фирмы 19.Разработка модели угроз безопасности информации государственного рынка биометрических средств ввода пароля

4.4. Шкала оценивания промежуточной аттестации

Зачет

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

«зачтено» (50 - 100 баллов)	ОК-4	Демонстрирует высокий уровень знаний требований нормативн области защиты государственной тайны и информационн Анализирует основные изменения законодательства в обла прослеживает междисциплинарные связи.¶Свободно применяет защиты государственной тайны и информационной безопаснос владеет навыками поиска актуальной правовой информации.¶От материал излагается четко, ясно, хорошим языком, аргументиров
	ПК-1	Демонстрирует высокий уровень знаний теории Анализирует з дает оценку основным тенденциям развития. Ответ построен излагается четко, ясно, хорошим языком, аргументировано.
	ПК-3	Свободно ориентируется в основных целях, задачах, мето обеспечением защиты информации, в том числе сведени государственную тайну, анализирует эффективность системы зап вопросы отвечает кратко, аргументировано, уверенно, по существу
«не зачтено» (0 - 49 баллов)	ОК-4	Демонстрирует слабый уровень знаний законодательства в об требований нормативных правовых актов в области защиты госу информационной безопасности.¶Не может анализировать ос законодательства в области информации¶Не может применить ос области информации, требования нормативных правовых актов государственной тайны и информационной безопасности.¶Не вла актуальной правовой информации.¶Неуверенно и логически излагает материал.
	ПК-1	Демонстрирует слабый уровень знаний. Не может определить пр основным тенденциям развития. Неуверенно и логически непос материал.
	ПК-3	Не ориентируется в основных целях, задачах, методах контро защиты информации, в том числе сведений, составляющих гос анализа эффективность системы защиты информации.Не о информационном и иллюстративном материале (примеры из графики и т.д.). Неправильно отвечает на поставленные вопросы ответом.

Экзамен

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«ОТЛИЧНО» (95 - 100 баллов)	ОК-4	Демонстрирует высокий уровень знаний требований нормативн области защиты государственной тайны и информационн Анализирует основные изменения законодательства в обла прослеживает междисциплинарные связи.¶Свободно применяет защиты государственной тайны и информационной безопаснос владеет навыками поиска актуальной правовой информации.¶От материал излагается четко, ясно, хорошим языком, аргументиров

(85 - 100 баллов)	ПК-1	Демонстрирует высокий уровень знаний теории. Анализирует и дает оценку основным тенденциям развития. Ответ построен логично, излагается четко, ясно, хорошим языком, аргументировано.
	ПК-3	Свободно ориентируется в основных целях, задачах, методах обеспечения защиты информации, в том числе сведений государственную тайну, анализирует эффективность системы защиты информации. Вопросы отвечает кратко, аргументировано, уверенно, по существу.
«хорошо» (70 - 84 баллов)	ОК-4	Демонстрирует достаточный уровень знаний законодательства в области информации. Анализирует основные изменения законодательства в области информации, но допускает некоторые погрешности. В отдельности выделяет междисциплинарные связи. Относительно свободно находит и излагает актуальную правовую информацию. Владеет отдельными категориями информационного права. Ответ построен логично, хорошим языком.
	ПК-1	Демонстрирует достаточный уровень знаний теории. Достаточно уверенно определяет проблемы, дает оценку основным тенденциям развития. Ответ не всегда логично выстроен,
	ПК-3	Достаточно ориентируется в основных целях, задачах, методах контроля за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, анализирует эффективность системы защиты информации. Достаточно уверенно ориентируется в информационном и иллюстративном материале. Вопросы, задаваемые преподавателем, вызывают затруднения.
«удовлетворительно» (50 - 69 баллов)	ОК-4	Демонстрирует не достаточный уровень знаний законодательства в области информации, требований нормативных правовых актов в области защиты государственной тайны и информационной безопасности. Плохо анализирует основные изменения законодательства в области информации. Затрудняется применять основные положения законодательства в области информации, требования нормативных правовых актов. Владеет единичными навыками использования поиска актуальной правовой информации. Ответ не всегда логично выстроен, материал излагается без применения научной терминологии.
	ПК-1	Демонстрирует не достаточный уровень знаний теории. Неуверенно определяет проблемы, дает оценку основным тенденциям развития. Ответ не всегда логично выстроен, материал излагается без применения научной терминологии.
	ПК-3	Слабо ориентируется в основных целях, задачах, методах контроля за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, анализирует эффективность системы защиты информации. Вопросы, задаваемые преподавателем, вызывают затруднения. Слабо ориентируется в информационном и иллюстративном материале (примеры из практики, таблицы, графики и т.д.).

«неудовлетворительно» (менее 50 баллов)	ОК-4	Демонстрирует слабый уровень знаний законодательства в области информации, требований нормативных правовых актов в области защиты государственной тайны и информационной безопасности.¶Не может анализировать основные изменения зако в области информации¶Не может применить основные положения в области информации, требования нормативных правовых актов в области защиты государственной тайны и инфо безопасности.¶Не владеет навыками поиска актуальной правои информации.¶Неуверенно и логически непоследовательно излагает материал.
	ПК-1	Демонстрирует слабый уровень знаний. Не может определить оценку основным тенденциям развития. Неуверенно и логичи излагает материал.
	ПК-3	Не ориентируется в основных целях, задачах, методах контроля за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, анализа эффективности системы защиты информации. Не ориентируется в информационном и иллюстративном материале (примеры из практики, таблицы, графики и т.д.). 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 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, инд. 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 техники ответа;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов выступления с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержанию, направленность, соответствие содержания заявленной форме, адекватность использования техники последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соотношение звуков, 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. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : учеб. пособие. - М.: И
2. Аверченков В. И., Рытов М. Ю., Кондрашин Г. В., Рудановский М. В. Системы защиты информац учебное пособие для вузов. - 4-е изд., стер.. - Москва: Флинта, 2016. - 224 с. - Текст : электронный // онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=93351>

6.2 Дополнительная литература:

1. Криптографическая защита информации. : учеб.-метод. комплекс, Блок 1: История. - [Тамбов]: Изд- (CD).
2. Программно-аппаратная защита информации : учеб.-метод. комплекс, Блок 3: Защита программ отладки. - [Тамбов]: Изд-во ТГУ, [200. - 1 электрон. опт. диск (CD-ROM).
3. Информационная безопасность и защита информации : сборник студенческих работ. - Москва: Студенческая наука, 2012. - 1322 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=227774>
4. Арутюнов В.В. Защита информации : учебно-методическое пособие. - Москва: Либерея-Бибинформ

6.3 Иные источники:

1. Федеральный портал «Российское образование» - <http://www.edu.ru/>
2. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» - <http://school-c>

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 информационно-образовательную среду Университета.

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

Лицензионное программное обеспечение:

LibreOffice

Microsoft Windows 10

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. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prlib.ru>
8. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>
9. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>

Электронная информационно-образовательная среда

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

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