

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.22 Комплексная система защиты информации объектов информатизации

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2021

Автор программы:

Кандидат технических наук, доцент Зауголков Игорь Алексеевич

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства образования и науки РФ от «17» ноября 2020 г. № 1427).

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 бакалавра.....	4
3. Объем и содержание дисциплины.....	4
4. Контроль знаний обучающихся и типовые оценочные средства.....	8
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	21
6. Учебно-методическое и информационное обеспечение дисциплины.....	23
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	23

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями

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 сфере: 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)

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
	ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	Оценивает уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями к комплексным системам защиты информации

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Комплексная система защиты информации объектов информатизации» относится к обязательной части учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Комплексная система защиты информации объектов информатизации» изучается в 7 семестре.

3. Объем и содержание дисциплины

3.1. Объем дисциплины: 3 з.е.

Очная: 3 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	108
Контактная работа	80
Лекции (Лекции)	48
Лабораторные (Лаб. раб.)	32
Самостоятельная работа (СР)	28
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	6	4	2	Защита лабораторных работ ; Собеседование
2	Принципы организации и этапы разработки КСЗИ	6	2	4	Защита лабораторных работ
3	Моделирование КСЗИ	10	Пп 4	4	Защита лабораторных работ ; Тестирование; Практическое задание для практической подготовки
4	Функционирование КСЗИ	8	Пп 6	2	Защита лабораторных работ ; Реферат; Практическое задание для практической подготовки
5	Способы обеспечения информационной безопасности информационных систем	6	6	6	Защита лабораторных работ ; Собеседование
6	Обеспечение безопасности персональных данных, обрабатываемых в информационных системах	6	4	4	Защита лабораторных работ

7	Обеспечение безопасности информации в ключевых системах информационной инфраструктуры	6	6	6	Собеседование
---	---	---	---	---	---------------

Тема 1. Законодательно-правовые и организационные основы обеспечения информационной безопасности предприятия (ОПК-1.4)

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 (ОПК-1.4)

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 (ОПК-1.4)

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.

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

Задания для самостоятельной работы.

Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы.

Подготовка к тестированию.

Тема 4. Функционирование КСЗИ (ОПК-1.4)

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 (ОПК-1.4)

Лекция.

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

Лабораторные работы.

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

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 (ОПК-1.4)

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 (ОПК-1.4)

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 – 82 балла
- контрольные срезы – 2 среза: 6 баллов, 2 балла
- 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	4	Лабораторные работы выполняются по тематике практических занятий. 4 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию 2 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы 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

		Собеседование(контрольный срез)	6	<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>6 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 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>
2.	Принципы организации и этапы разработки КСЗИ	Защита лабораторных работ	6	<p>Лабораторные работы выполняются по тематике практических занятий.</p> <p>6 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>4 балла – 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.	Моделирование КСЗИ	Защита лабораторных работ	10	<p>Лабораторные работы выполняются по тематике практических занятий.</p> <p>10 балла – 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)	2	Тест состоит из 15 вопросов. 2 балла – студент правильно отвечает на 50-100% вопросов в тесте 1 балл - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает
		Практическое задание для практической подготовки	3	Практические задания выполняются по тематике практических занятий. 3 баллов – практическое задание выполнено в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию 1 балла – практическое задание выполнено, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы
		Защита лабораторных работ	4	Лабораторные работы выполняются по тематике практических занятий. 4 балла – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию 3 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы 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
4.	Функционирование КСЗИ			

		Реферат	10	<p>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 содержат выводы, логично вытекающие из содержания основной части; список литературы оформлен в соответствии с правилами ГОСТа</p> <p>5 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>3-4 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>
		Практическое задание для практической подготовки	5	<p>Практические задания выполняются по тематике практических занятий.</p> <p>5 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>
		Защита лабораторных работ	10	<p>Лабораторные работы выполняются по тематике практических занятий.</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>4 балла – 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>
5.	Способы обеспечения информационной безопасности информационных систем			

		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>3 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>
6.	Обеспечение безопасности персональных данных, обрабатываемых в информационных системах	Защита лабораторных работ	10	<p>Лабораторные работы выполняются по тематике практических занятий.</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>4 балла – 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>

7.	Обеспечение безопасности информации в ключевых системах информационной инфраструктуры	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>3 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>
8.	Посещаемость		10	<p>10 баллов – стопроцентное посещение занятий студентом</p> <p>7-9 баллов – посещаемость студента составляет не менее 80 % занятий</p> <p>4-6 баллов – посещаемость студента составляет не менее 50 % занятий</p> <p>1-3 балла – посещаемость студента составляет не менее 25 % занятий</p>
9.	Премияльные баллы		20	<p>Дополнительные премияльные 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
10.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы		20	<p>Решение кейса (10 баллов)</p> <p>Прохождение тестирования (30 вопросов) по всему курсу дисциплины (10 баллов)</p>

11.	Итого за семестр	100	
-----	------------------	-----	--

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

100-балльная система	Традиционная система
50 - 100 баллов	Зачтено
0 - 49 баллов	Не зачтено

4.2 Типовые оценочные средства текущего контроля

Защита лабораторных работ

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

1. Разработать частную модель угроз безопасности распределенной информационной системы персональных данных (ИС ПДн) с подключением к сети международного информационного обмена по следующим исходным данным:

- локальная ИС ПДн, развернута в пределах нескольких близко расположенных зданий;
- имеет многоточечный выход в сеть общего пользования;
- позволяет запись, удаление, сортировку ПДн;
- имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн;
- используется одна база ПДн, принадлежащая организации - владельцу данной ИСПДн;
- данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;
- предоставляются сторонним пользователям ИС ПДн без предварительной обработки только часть ПДн.

2. Определить базовый уровень защищенности ИС ПДн по следующим исходным данным:

- обработка ПДн сотрудников организации; - категории биометрических и иных персональных данных;
- объем обработки менее 100000 субъектов персональных данных;
- возможны угрозы 2 типа. 3.

3. Определить состав и содержание организационных и технических мер по защите ИС ПДн в соответствии с уровнем защищенности, руководствуясь последовательностью действий:

- определить базовый набор мер для третьего уровня защищенности ПДн;
- адаптировать базовый набор мер, с учетом характеристик распределенной информационной системы;
- подготовить предложения для уточнения адаптированного базового набора мер для различных вариантов ИС ПДн. Подобрать необходимый для заданного уровня защищенности ПДн состав средств защиты информации.

4. Разработать структуру технического задания на создание автоматизированной системы в защищенном исполнении. Составить технический паспорт на автоматизированную систему в защищенном исполнении, включающий:

- общие сведения об автоматизированной системе;
- состав оборудования автоматизированной системы (состав основных и вспомогательных средств и систем);
- состав средств защиты информации.

Тема 3. Моделирование КСЗИ

Лабораторная работа. Перечень персональных данных.

Тема 4. Функционирование КСЗИ

Лабораторная работа. Определение уровня исходной защищенности ИСПДн.

Тема 5. Способы обеспечения информационной безопасности информационных систем

Лабораторная работа. Определение актуальности угроз безопасности персональных данных в ИСПДн.

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

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

Защита лабораторных работ

Тема 2. Принципы организации и этапы разработки КСЗИ

Лабораторная работа. Определение защищенности информации при несанкционированном доступе.

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

2. Найти вероятности сложных событий:

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

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

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

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

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

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

$$- P\{CB(2) A(2)\}).$$

Практическое задание для практической подготовки

Тема 3. Моделирование КСЗИ

1. Основной проблемой реализации систем защиты является:

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

Тема 4. Функционирование КСЗИ

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

Реферат

Тема 4. Функционирование КСЗИ

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

1. Понятие распределенной информационной системы и её безопасности. Отличительные свойства распределенной информационной системы по отношению к нераспределенной. Классификация распределенных информационных систем.
2. Классификация угроз для распределенных информационных систем. Внутренние и внешние угрозы. Основные факторы, характерные для распределенных информационных систем, реализующие угрозы.
3. Методы сбора информации о распределенной информационной системе. Принципы работы приложений для сбора информации об распределенной информационной системе. Анализ топологии системы, включенных в неё устройств, и внутренних сервисов и приложений.
4. Классификация уязвимостей в распределенных информационных системах по сетевой модели ISO/OSI (с физического по представительский уровни).
5. Классификация уязвимостей в распределенных информационных системах по сетевой модели ISO/OSI (прикладной уровень). Классификация уязвимостей по типам приложений (сетевой сервис, веб-приложение, СУБД и др).
6. Технические и программные методы и средства атак на типовые уязвимости распределенных информационных систем.
7. Технические и программные средства и методы противодействия анализу распределенной информационной системы.
8. Технические и программные средства для обнаружения вторжений в распределенную информационную систему.
9. Программные средства для мониторинга работоспособности и целостности распределенной информационной системы. Средства аудита безопасности распределенной информационной системы.
10. Программные средства для мониторинга целостности и неизменности распределенной информационной системы. Защитные системы контроля версий.
11. Внутренние способы защиты. Особенности проектирования и разработки защищаемых сервисов и приложений для распределенной информационной системы. Принципы защиты от реализации атак на сервис и приложение на уровне программного кода.

Тема 5. Способы обеспечения информационной безопасности информационных систем

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.

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.

Тестирование

Тема 3. Моделирование 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
 - в) доступа

г) тиражирования

10. Как предотвращение неавторизованного использования ресурсов определена услуга защиты:

а) причастность

б) аутентификация

в) контроль доступа

г) целостность

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета

Типовые вопросы зачета (ОПК-1.4)

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 на информацию.
8. Современные технические средства охраны и защиты информации.
9. Выбор методов и способов предотвращения угроз безопасности информации.
10. Определение условий функционирования КСЗИ.
11. Разработка модели КСЗИ.
12. Определение компонентов КСЗИ, технологическое и организационное построение КСЗИ.
13. Кадровое, материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ.
14. Назначение, структура и содержание системы управления КСЗИ.
15. Принципы и методы планирования функционирования КСЗИ.
16. Сущность и содержание контроля функционирования КСЗИ.
17. Управление КСЗИ в условиях чрезвычайных ситуаций.
18. Методы оценки эффективности КСЗИ.

Типовые задания для зачета (ОПК-1.4)

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

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 скрывание 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);

4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«зачтено» (50 - 100 баллов)	ОПК-1.4	Демонстрирует высокий уровень теоретических знаний в вопросах, связанных с комплексной защитой информации объектов информатизации. Может проанализировать существующие методики определений требования к защите информации, в том числе в соответствии с нормативными и корпоративными требованиями. Способен комплексно оценить уровень безопасности компьютерных систем и сетей.
«не зачтено» (0 - 49 баллов)	ОПК-1.4	Не имеет знаний в вопросах, связанных с комплексной защитой информации объектов информатизации. Не может проанализировать существующие методики определений требования к защите информации, в том числе в соответствии с нормативными и корпоративными требованиями. Не способен комплексно оценить уровень безопасности компьютерных систем и сетей.

5. Методические указания для обучающихся по освоению дисциплины (модуля)

5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;

- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;
- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература:

1. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : учеб. пособие. - М.: ИД "Форум", ИНФРА-М, 2013. - 591 с.
2. Соколов, В. П., Тарасова, Н. П. Кодирование в системах защиты информации : учебное пособие. - 2022-04-04; Кодирование в системах защиты информации. - Москва: Московский технический университет связи и информатики, 2016. - 94 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/61485.html>

6.2 Дополнительная литература:

1. Блок 1: История и современная система защиты информации в России, 2017. - 1 электрон. опт. диск (CD-ROM)
2. Тамб. гос. ун-т им. Г.Р. Державина Комплексная система защиты информации на предприятии : электрон. УМК. - [Тамбов]: Изд-во ТГУ, 2008. - 1 электрон. опт. диск (CD).
3. Аверченков В. И., Рытов М. Ю., Кондрашин Г. В., Рудановский М. В. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов. - 4-е изд., стер.. - Москва: Флинта, 2016. - 224 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=93351>

6.3 Иные источники:

1. Федеральный портал «Российское образование» - <http://www.edu.ru/>
2. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» - <http://school-collection.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 Windows 10

Microsoft Office Профессиональный плюс 2007

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.