МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

УТВЕРЖДАЮ
Зам. директора по УР
_____ Н.А. Андреева
«22» 04 2024 г.

Б1.В.16 Защита персональных данных

рабочая программа дисциплины

Кафедра: Инфокоммуникационные технологии и системы связи
Направление подготовки: **11.03.02 Инфокоммуникационные технологии и системы связи**
Профиль: **Защищенные инфокоммуникационные системы**
Формы обучения: **очная, заочная**

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО)), курсам (для заочной формы обучения (ЗФО))

Вид учебной работы	ОФО		ЗФО	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/8	4	36/4 108/5
Контактная работа, в том числе (по семестрам, курсам):		50/8		2/4 16/5
Лекции		20/8		2/4 4/5
Лабораторных работ				
Практических занятий		30/8		12/5
Семинаров				
Самостоятельная работа		58/8		34/4 83/5
Контроль		36/8		9/5
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с разбивкой по семестрам				
Число экзаменов с разбивкой по семестрам		1/8		1/5

Программу составил:

Доцент кафедры ИТСС, к. т. н., доцент Ершов В.В.

Рабочая программа дисциплины
«Защита персональных данных»

Разработана в соответствии с ФГОС ВО
направления подготовки 11.03.02 ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ СВЯЗИ, утвержденным приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 930.

Составлена на основании учебных планов
направления 11.03.02 Инфокоммуникационные технологии и системы связи, профиля: «Защищенные инфокоммуникационные системы», одобренного Учёным советом СКФ МТУСИ, Протокол № 9 от 22.04.2024 г., и утвержденного директором СКФ МТУСИ 22.04.2024 г.

Рассмотрена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «22» 04 2024 г. № 9

Зав. кафедрой _____Юхнов В.И.

1. Цели изучения дисциплины

Целями освоения дисциплины «Защита персональных данных» являются: изучение нормативно-правовых актов РФ по защите персональных данных; формирование правовой грамотности, понятия персональных данных, особенности защиты персональных данных, взаимосвязь нормативно-правового обеспечения защиты персональных данных с другими направлениями в области информационных систем и технологий.

2 Планируемые результаты обучения

Изучение дисциплины направлено на формирование у обучающихся способности, решать профессиональные задачи в соответствии с технологическим видом деятельности.

Результатом освоения дисциплины являются сформированные у обучающихся следующие компетенции:

Компетенции обучающегося, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ПК-1: Способен обеспечить защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи
Знать:
Основные понятия и определения. Содержание категории «персональные данные»; Порядок обработки персональных данных. Контроль и надзор за обработкой персональных данных; Ответственность за нарушение требований по обращению с персональными данными. Права субъектов персональных данных и их соблюдение при обработке; Трансграничная передача персональных данных. Ответственность за нарушение требований по обращению с персональными данными. Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных; Классификацию информационных систем персональных данных; Внутренние нормативные документы организации по охране конфиденциальности сведений; Модель угроз для информационных систем персональных данных; Организацию и обеспечение режимов защиты персональных данных; Оценку эффективности системы защиты информационных систем персональных данных. Порядок лицензирования операторов информационных систем персональных данных
Уметь:
Пользоваться нормативно-правовыми актами РФ по защите персональных данных; Определять административную ответственность за нарушение требований по обращению с персональными данными; Проводить разграничение прав доступа в информационных системах персональных данных; Реализовывать нормативно-правовой подход к защите информационной системы персональных данных; Проводить классификацию информационных систем персональных данных; Пользоваться моделью угроз для информационных систем персональных данных; Организовывать и обеспечивать режимы защиты персональных данных; Проводить оценку эффективности систем защиты информационных систем персональных данных.
Владеть:
Навыками применения Нормативно-правовых актов РФ по защите персональных данных; Методикой определения административной ответственности за нарушение требований по обращению с персональными данными;

Методикой разграничения прав доступа в информационных системах персональных данных; Нормативно-правовым подходом к защите информационной системы персональных данных. Методикой классификации информационных систем персональных данных; Навыками работы с моделью угроз для информационных систем персональных данных Организацией и обеспечением режимов защиты персональных данных; Методикой оценки эффективности систем защиты информационных систем персональных данных.

3 Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.24 Основы информационной безопасности
2	Б1.В.14 Основы организационно-правового обеспечения информационной безопасности сетей и систем
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б2.О.03(Пд) Производственная практика (преддипломная)

4 Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 144 часа, 50 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
1	2	3	4	5	6
Курс 4 , Семестр 8					
Модуль 1. Защита персональных данных в инфокоммуникационных системах 24 часа (Лек 10+ПЗ 14) контактной работы 28 часов СР					
1.1	**Персональные данные в Федеральном законе и Трудовом кодексе Российской Федерации**. 1. Основные понятия и определения. Содержание категории «персональные данные». 2. Обработка персональных данных: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (передача), обезличивание, блокирование, уничтожение.	Лек.	2	ПК-1	Л1.1 Л1.2
1.2	Законность видеосъемки, фотосъемки и звукозаписи в общественных местах. Охрана изображения гражданина. Нарушение неприкосновенности частной жизни. Статья 137 УК РФ, статьи 151, 152, 152.1 Гражданского Кодекса РФ.	СРС	4	ПК-1	Л1.1 Л1.2 Л 2.1
1.3	**Принципы обработки персональных данных** 1. Принципы обработки персональных данных. Условия обработки персональных данных. Согласие субъекта. 2. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований по обращению с персональными данными. 3. Права субъектов персональных данных и их соблюдение при обработке.	Лек.	2	ПК-1	Л1.1 Л1.2

1.4	**Защита персональных данных в нормативно-правовых актах РФ** 1.Конституция РФ о защите персональных данных. 2. Защита персональных данных в трудовом кодексе РФ.	ПЗ	4	ПК-1	Л1.1 Л1.2 Л 2.1 Л 3.1
1.5	Обработка биометрических данных.	СРС	4	ПК-1	Л1.1 Л1.2
1.6	**Трансграничная передача персональных данных.** 1. Обработка персональных данных третьим лицом в интересах оператора. 2. Обязанности оператора персональных данных в ходе сбора и обработки персональных данных, ответы на запросы субъектов.	Лек.	**2**	ПК-1	Л1.1 Л1.2
1.7	**Административная ответственность за нарушение требований по обращению с персональными данными** 1. Безопасность обработки персональных данных. 2. Ответственность в Кодексе об Административных Правонарушениях Российской Федерации за нарушение требований ФЗ «О персональных данных».	ПЗ	2	ПК-1	Л1.1 Л1.2 Л 2.1 Л 3.1
1.8	Специальные категории персональных данных и особенности их обработки.	СРС	4	ПК-1	Л1.1 Л1.2 Л 2.1
1.9	**Ответственность за нарушение требований по обращению с персональными данными** 1. Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных. 2. Ответственность за нарушение требований по обращению с персональными данными.	Лек.	2	ПК-1	Л1.1 Л1.2
1.10	**Уничтожение электронных данных.** 1. Уровни уничтожения электронных данных (очистка, очищение, разрушение). 2. Стандартизация уничтожения электронных данных.	СРС	8	ПК-1	Л1.1 Л1.2 Л 2.1
1.11	**Хранение персональных данных в «облаке»** 1. Необходимые свойства «облака» для построения «облачной» системы хранения персональных данных. 2. Требования регулирующих органов по защите персональных данных в «облаке».	СРС	8	ПК-1	Л1.1 Л1.2 Л 2.1
1.12	**Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных** 1. Мероприятия по защите сведений конфиденциального характера. 2. Основные внутренние нормативные документы, меры по охране конфиденциальности. 3. Формирование перечня персональных данных.	Лек.	2	ПК-1	Л1.1 Л1.2
1.13	**Разграничение прав доступа в информационных системах персональных данных** 1. Структура механизмов разграничения доступа	ПЗ	4	ПК-1	Л1.1 Л1.2 Л 2.1

	в информационной системе персональных данных. 2. Реализация механизмов разграничения доступа в информационной системе персональных данных.				Л 3.1
1.14	**Нормативно-правовой подход к защите информационной системы персональных данных** 1. Аттестации информационной системы обработки персональных данных. 2. Подготовка пакета документов, необходимого для аттестации информационной системы персональных данных.	ПЗ	4	ПК-1	Л1.1 Л1.2 Л 2.1 Л 3.1
Модуль 2. Методы защиты персональных данных в инфокоммуникационных системах и оценка эффективности 26 часов (Лек 10+ПЗ 16) контактной работы 30 часов СР					
2.1	**Классификация информационных систем персональных данных** 1. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 г. Москва «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». 2. Порядок проведения классификации информационных систем персональных данных.	Лек.	2	ПК-1	Л1.1 Л1.2
2.2	Определение порядка обращения с персональными данными, контроля над его соблюдением, организация доступа к персональным данным.	СРС	6	ПК-1	Л1.1 Л1.2 Л 2.1
2.3	Внутренние нормативные документы организации по охране конфиденциальности сведений 1. Внутренние нормативные документы по охране конфиденциальности сведений, их содержание, порядок разработки и ввода в действие. 2. Контроль над соблюдением режима конфиденциальности.	Лек.	2	ПК-1	Л1.1 Л1.2
2.4	Классификация информационных систем персональных данных 1.Уровни защищённости информационных систем персональных данных. 2. Исследование классов систем.	ПЗ	4	ПК-1	Л1.1 Л1.2 Л 2.1 Л 3.1
2.5	Определение уровня защищённости информационных систем персональных данных.	СРС	6	ПК-1	Л1.1 Л1.2 Л 2.1
2.6	Внутренние нарушители защиты персональных данных и негативные последствия их деятельности для предприятий и организаций.	СРС	6	ПК-1	Л1.1 Л1.2 Л 2.1
2.7	**Модель угроз для информационных систем персональных данных** 1.Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. 2.Модель злоумышленника информационных систем персональных данных. 3.Разработка частных моделей угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования.	Лек.	2	ПК-1	Л1.1 Л1.2

2.8	Модель угроз для информационных систем персональных данных 1. Разработка модели угроз для информационных систем персональных данных. 2. Разработка частной модели угроз информационной системы персональных данных.	ПЗ	4	ПК-1	Л1.1 Л1.2 Л 2.1 Л 3.1
2.9	Многофакторная аутентификация. Примеры многофакторной аутентификации. Протоколы аутентификации.	СРС	4	ПК-1	Л1.1 Л1.2 Л 2.1
2.10	**Мероприятия по обеспечению защиты персональных данных** 1. Организационные и технические мероприятия, направленные на минимизацию ущерба от возможной реализации угроз безопасности персональных данных. 2. Защита персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий.	Лек.	2	ПК-1	Л1.1 Л1.2
2.11	**Организация и обеспечение режимов защиты персональных данных** 1. Организация защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий. 2. Обеспечение защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий.	ПЗ	4	ПК-1	Л1.1 Л1.2 Л 2.1 Л 3.1
2.12	**Оценка эффективности системы защиты информационных систем персональных данных.** 1. Мероприятия по оценке соответствия принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных требованиям безопасности информации. 2. Мероприятия по контролю обеспечения безопасности персональных данных. Механизмы и средства контроля. 3. Периодичность и содержание работ. Ответственность оператора за нарушение правил обращения с персональными данными. Подготовка уведомлений об обработке персональных данных в уполномоченный орган.	Лек.	2	ПК-1	Л1.1 Л1. 2
2.13	Определение политик безопасности (ПБ). Представление ПБ. Закрытые, открытые, гибридные политики информационной безопасности.	СРС	4	ПК-1	Л1.1 Л1.2 Л 2.1
2.14	Методы описания ПБ. Сравнительный анализ методов описания ПБ. Аналитический метод описания ПБ. Графовый метод описания ПБ. Объектный метод описания ПБ. Логический метод описания ПБ.	СРС	4	ПК-1	Л1.1 Л1.2 Л 2.1
2.15	Оценка эффективности систем защиты информа-	**ПЗ**	**4**	ПК-1	Л1.1

	ционных систем персональных данных 1.Определение эффективности систем защиты информационных систем персональных данных. 2.Оценка эффективности систем защиты информационных систем персональных данных.				Л1.2 Л 2.1 Л 3.1
	Экзамен 36 часов				
Итого – 144 часа					

4.2 Заочная форма обучения, 4 года 8 месяцев (всего 144 часа, контактной работы 18 часов)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
1	2	3	4	5	6
Курс 5 , Семестр 8					
Модуль 1. Защита персональных данных в инфокоммуникационных системах 10 часов (Лек 2+ПЗ 8) контактной работы 70 часов СР					
1.1	**Персональные данные в Федеральном законе и Трудовом кодексе Российской Федерации**. 1. Основные понятия и определения. Содержание категории «персональные данные». 2. Обработка персональных данных: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (передача), обезличивание, блокирование, уничтожение.	Лек.	2	ПК-1	Л1.1 Л1.2
1.2	Законность видеосъемки, фотосъемки и звукозаписи в общественных местах. Охрана изображения гражданина. Нарушение неприкосновенности частной жизни. Статья 137 УК РФ, статьи 151, 152, 152.1 Гражданского Кодекса РФ.	СРС	4	ПК-1	Л1.1 Л1.2 Л 2.1
1.3	**Принципы обработки персональных данных** 1. Принципы обработки персональных данных. Условия обработки персональных данных. Согласие субъекта. 2. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований по обращению с персональными данными. 3. Права субъектов персональных данных и их соблюдение при обработке.	СРС	12	ПК-1	Л1.1 Л1.2
1.4	**Защита персональных данных в нормативно-правовых актах РФ** 1.Конституция РФ о защите персональных данных. 2. Защита персональных данных в трудовом кодексе РФ.	ПЗ	4	ПК-1	Л1.1 Л1.2 Л 2.1 Л 3.1
1.5	Обработка биометрических данных.	СРС	4	ПК-1	Л1.1 Л1.2 Л 2.1
1.6	**Трансграничная передача персональных данных**. 1. Обработка персональных данных третьим лицом в интересах оператора. 2. Обязанности оператора персональных данных	СРС	8	ПК-1	Л1.1 Л1.2

	в ходе сбора и обработки персональных данных, ответы на запросы субъектов.				
1.7	**Административная ответственность за нарушение требований по обращению с персональными данными** 1. Безопасность обработки персональных данных. 2. Ответственность в Кодексе об Административных Правонарушениях Российской Федерации за нарушение требований ФЗ «О персональных данных».	СРС	8	ПК-1	Л1.1 Л1.2 Л 2.1 Л 3.1
1.8	Специальные категории персональных данных и особенности их обработки.	СРС	4	ПК-1	Л1.1 Л1.2 Л 2.1
1.9	**Ответственность за нарушение требований по обращению с персональными данными** 1. Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных. 2. Ответственность за нарушение требований по обращению с персональными данными.	СРС	8	ПК-1	Л1.1 Л1.2
1.10	**Уничтожение электронных данных.** 1. Уровни уничтожения электронных данных (очистка, очищение, разрушение). 2. Стандартизация уничтожения электронных данных.	СРС	8	ПК-1	Л1.1 Л1.2 Л 2.1
1.11	**Хранение персональных данных в «облаке»** 1. Необходимые свойства «облака» для построения «облачной» системы хранения персональных данных. 2. Требования регулирующих органов по защите персональных данных в «облаке».	СРС	4	ПК-1	Л1.1 Л1.2 Л 2.1
1.12	**Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных** 1. Мероприятия по защите сведений конфиденциального характера. 2. Основные внутренние нормативные документы, меры по охране конфиденциальности. 3. Формирование перечня персональных данных.	СРС	6	ПК-1	Л1.1 Л1.2
1.13	**Разграничение прав доступа в информационных системах персональных данных** 1. Структура механизмов разграничения доступа в информационной системе персональных данных. 2. Реализация механизмов разграничения доступа в информационной системе персональных данных.	ПЗ	4	ПК-1	Л1.1 Л1.2 Л 2.1 Л 3.1
1.14	**Нормативно-правовой подход к защите информационной системы персональных данных** 1. Аттестации информационной системы обработки персональных данных. 2. Подготовка пакета документов, необходимого для аттестации информационной системы персональных данных.	СРС	4	ПК-1	Л1.1 Л1.2 Л 2.1 Л 3.1
Модуль 2. Методы защиты персональных данных в инфокоммуникационных системах и оценка эффективности 8 часов (Лек 4+ПЗ 4) контактной работы 47 часов СР					

2.1	**Классификация информационных систем персональных данных** 1. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 г. Москва «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». 2. Порядок проведения классификации информационных систем персональных данных.	Лек.	2	ПК-1	Л1.1 Л1.2
2.2	Определение порядка обращения с персональными данными, контроля над его соблюдением, организация доступа к персональным данным.	СРС	2	ПК-1	Л1.1 Л1.2 Л 2.1
2.3	Внутренние нормативные документы организации по охране конфиденциальности сведений 1. Внутренние нормативные документы по охране конфиденциальности сведений, их содержание, порядок разработки и ввода в действие. 2. Контроль над соблюдением режима конфиденциальности.	СРС	4	ПК-1	Л1.1 Л1.2
2.4	Классификация информационных систем персональных данных 1.Определение уровня защищённости информационных систем персональных данных. 2. Исследование классов систем.	СРС	4	ПК-1	Л1.1 Л1.2 Л 2.1 Л 3.1
2.5	Определение уровня защищённости информационных систем персональных данных.	СРС	2	ПК-1	Л1.1 Л1.2 Л 2.1
2.6	Внутренние нарушители защиты персональных данных и негативные последствия их деятельности для предприятий и организаций.	СРС	2	ПК-1	Л1.1 Л1.2 Л 2.1
2.7	**Модель угроз для информационных систем персональных данных** 1.Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. 2.Модель злоумышленника информационных систем персональных данных. 3.Разработка частных моделей угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования.	Лек.	2	ПК-1	Л1.1 Л1.2
2.8	**Модель угроз для информационных систем персональных данных** 1. Разработка модели угроз для информационных систем персональных данных. 2. Разработка частной модели угроз информационной системы персональных данных.	ПЗ	4	ПК-1	Л1.1 Л1.2 Л 2.1 Л 3.1
2.9	Многофакторная аутентификация. Примеры многофакторной аутентификации. Протоколы аутентификации.	СРС	2	ПК-1	Л1.1 Л1.2 Л 2.1

2.10	**Мероприятия по обеспечению защиты персональных данных** 1. Организационные и технические мероприятия, направленные на минимизацию ущерба от возможной реализации угроз безопасности персональных данных. 2. Защита персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий.	СРС	4	ПК-1	Л1.1 Л1.2 Л 2.1
2.11	**Организация и обеспечение режимов защиты персональных данных** 1. Организация защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий. 2. Обеспечение защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий.	СРС	6	ПК-1	Л1.1 Л1.2 Л 2.1 Л 3.1
2.12	**Оценка эффективности системы защиты информационных систем персональных данных.** 1. Мероприятия по оценке соответствия принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных требованиям безопасности информации. 2. Мероприятия по контролю обеспечения безопасности персональных данных. Механизмы и средства контроля. 3. Периодичность и содержание работ. Ответственность оператора за нарушение правил обращения с персональными данными. Подготовка уведомлений об обработке персональных данных в уполномоченный орган.	СРС	8	ПК-1	Л1.1 Л1.2 Л 2.1
2.13	Определение политик безопасности (ПБ). Представление ПБ. Закрытые, открытые, гибридные политики информационной безопасности.	СРС	**4**	ПК-1	Л1.1 Л1.2 Л 2.1
2.14	Методы описания ПБ. Сравнительный анализ методов описания ПБ. Аналитический метод описания ПБ. Графовый метод описания ПБ. Объектный метод описания ПБ. Логический метод описания ПБ.	СРС	**6**	ПК-1	Л1.1 Л1.2 Л 2.1
2.15	Оценка эффективности систем защиты информационных систем персональных данных 1.Определение эффективности систем защиты информационных систем персональных данных. 2.Оценка эффективности систем защиты информационных систем персональных данных.	СРС	**3**	ПК-1	Л1.1 Л1.2 Л 2.1 Л 3.1
	Экзамен 9 часов				
Итого – 144 часа					

5 Учебно-методическое и информационное обеспечение дисциплины

5.1 Рекомендуемая литература

5.1.1 Основная литература

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л 1.1	Д.А. Скрипник	Обеспечение безопасности персональных данных : учебное пособие	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024.	Э1
Л 1.2	В.И. Петренко	Защита персональных данных в информационных системах : учебное пособие	Ставрополь : Северо-Кавказский федеральный университет, 2016.	Э2

5.1.2 Дополнительная литература

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л 2.1	К.Е. Шинаков, М.Ю. Рытов, О.М. Голембиовская.	Анализ рисков безопасности информационных систем персональных данных : монография	Москва : Ай Пи Ар Медиа, 2020.	Э3
Л2.2	А. В. Терехов, В. Н. Чернышов, А. В. Платенкин, А. В. Селезнев	Информационная безопасность и правовые основы защиты персональных данных: учебное пособие	Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2023.	Э4
Л2.3	"Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020)			Э5
Л2.4	Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" https://base.garant.ru/12148567/			Э6

5.1.3 Учебно-методическое обеспечение для самостоятельной работы обучающихся

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л 3.1	О.М. Голембиовская, М.Ю. Рытов, К.Е. Шинаков	Формализация подходов к обеспечению защиты персональных данных: монография	Саратов : Ай Пи Эр Медиа, 2019.	Э7
Л 3.2	В.И. Петренко, И.В. Мандрица.	Защита персональных данных в информационных системах : лабораторный практикум	Ставрополь : Северо-Кавказский федеральный университет, 2018.	Э8

5.2 Электронные образовательные ресурсы

Э1	https://www.iprbookshop.ru/133952.html
Э2	https://www.iprbookshop.ru/66023.html
Э3	https://www.iprbookshop.ru/95150.html
Э4	https://www.iprbookshop.ru/141049.html
Э5	https://www.consultant.ru/document/cons_doc_LAW_28399 /

Э 6	https://base.garant.ru/12148567/
Э7	https://www.iprbookshop.ru/81851.html
Э8	https://www.iprbookshop.ru/83198.html
5.3 Информационно-справочные системы и профессиональные базы данных	
5.3.1	Консультант Плюс – https://www.consultant.ru/
5.3.2	Гарант – https://www.garant.ru/
5.3.3	Консорциум Кодекс – https://docs.cntd.ru/
5.3.4	Научная электронная библиотека – https://www.elibrary.ru/
5.3.5	Электронный ресурс http://www.securitylab.ru/
5.3.6	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)
5.4.7	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим па: http://fcior.edu.ru/ (открытый доступ)
5.4 Программное обеспечение	
П.1	MS Excel – с лицензией
П.2	MS Word – с лицензией
П.3	Power Point – с лицензией

6 Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, ПК (ноутбуком), проектором
6.2 МТО лабораторных работ и практических занятий	
1	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
6.3 МТО рубежных контролей, зачета	
1	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
6.4 МТО самостоятельной работы студентов	
1	Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

7. Оценочные материалы

Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

8. Методические рекомендации для обучающихся по освоению дисциплины

Методические рекомендации по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

9. Особенности реализации дисциплины (модуля) при обучении инвалидов и лиц с ограниченными возможностями здоровья

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков.

Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь.

Текущий контроль успеваемости осуществляется в устной форме.

При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины
«Б1.В.16 «Защита персональных данных»
для использования в 20___/20___ учебном году

Утверждаю
Зам. директора по УР _____
«___» _____ 20__ г.

Направление 11.03.02 Инфокоммуникационные технологии и системы связи
Профиль Защищенные инфокоммуникационные системы
Формы обучения: очная, заочная

(Возможны следующие варианты):
а) Рабочая программа действует без изменений.
б) В рабочую программу вносятся следующие изменения:
1) ……..;
2) ……..;
3) ……

Разработчик (и): _____
(ФИО, ученая степень, ученое звание)
«__» _____20___г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИТСС
Протокол № _____ от «__» _____20____г.

Заведующий кафедрой _____

Приложение 1

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	**Уровень освоения компетенции**	**Критерии оценивания**
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного учебного материала, умеет свободно выполнять задания, предусмотренные программой; усвоил основную и знаком с дополнительной рекомендованной литературой; может объяснить взаимосвязь основных понятий дисциплины в их значении для последующей профессиональной деятельности; проявляет творческие способности в понимании, изложении и использовании учебного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знаний в пределах основного учебного материала, без существенных ошибок выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий дисциплины при дополнительных вопросах преподавателя. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся показывает знания основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с основной литературой, рекомендованной программой. Допускает существенные погрешности в ответах, но обладает необходимыми знаниями для их устранения под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не достигнут	Обучающийся обнаруживает пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не знаком с рекомендованной литературой, не может исправить допущенные ошибки. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение или приступить к профес-

		сиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Критерии оценивания	Шкала оценивания
ПК-1: Способен обеспечить защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи		
Знать:		
Основные понятия и определения. Содержание категории «персональные данные»; Порядок обработки персональных данных. Контроль и надзор за обработкой персональных данных; Ответственность за нарушение требований по обращению с персональными данными. Права субъектов персональных данных и их соблюдение при обработке; Трансграничная передача персональных данных. Ответственность за нарушение требований по обращению с персональными данными. Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.	Контрольная работа	*Модуль 1* 0÷18 «Неудовлетворительно» -0-8 «Удовлетворительно» -9 «Хорошо» - 11 «Отлично» - 17
Классификацию информационных систем персональных данных; Внутренние нормативные документы организации по охране конфиденциальности сведений; Модель угроз для информационных систем персональных данных; Организацию и обеспечение режимов защиты персональных данных; Оценку эффективности системы защиты информационных систем персональных данных. Порядок лицензирования операторов информационных систем персональных данных.	Контрольная работа	*Модуль 2* 0÷18 «Неудовлетворительно» -0-8 «Удовлетворительно» -9 «Хорошо» - 11 «Отлично» - 17
Уметь:		
Пользоваться нормативно-правовыми актами РФ по защите персональных данных;	Практическое занятие 1	Модуль 1 0÷8 «Неудовлетворительно» -0 2 «Удовлетворительно» - 3 «Хорошо» - 5 «Отлично» - 6
Проводить классификацию информационных систем персональных данных;	Практическое занятие 5	Модуль 2 0÷8 «Неудовлетворительно» -0 2 «Удовлетворительно» - 3 «Хорошо» - 5 «Отлично» - 6
Определять административную ответствен-	Практическое	Модуль 1

ность за нарушение требований по обращению с персональными данными;	занятие 2	0÷8 «Неудовлетворительно» -0 2 «Удовлетворительно» - 3 «Хорошо» - 5 «Отлично» - 6
Пользоваться моделью угроз для информационных систем персональных данных;	Практическое занятие 6	Модуль 2 0÷8 «Неудовлетворительно» -0 2 «Удовлетворительно» - 3 «Хорошо» - 5 «Отлично» - 6
Проводить разграничение прав доступа в информационных системах персональных данных;	Практическое занятие 3	Модуль 1 0÷8 «Неудовлетворительно» -0 2 «Удовлетворительно» - 3 «Хорошо» - 5 «Отлично» - 6
Организовывать и обеспечивать режимы защиты персональных данных; ;	Практическое занятие 7	Модуль 2 0÷8 «Неудовлетворительно» -0 2 «Удовлетворительно» - 3 «Хорошо» - 5 «Отлично» - 6
Реализовывать Нормативно-правовой подход к защите информационной системы персональных данных;	Практическое занятие 4	Модуль 1 0÷8 «Неудовлетворительно» -0 2 «Удовлетворительно» - 3 «Хорошо» - 5 «Отлично» - 6
Проводить оценку эффективности систем защиты информационных систем персональных данных. .	Практическое занятие 8	Модуль 2 0÷8 «Неудовлетворительно» -0 2 «Удовлетворительно» - 3 «Хорошо» - 5 «Отлично» - 6
Владеть:		
Навыками применения нормативно-правовых актов РФ по защите персональных данных;;	Практическое занятие 1	Модуль 1 0÷8 «Неудовлетворительно» -0 2 «Удовлетворительно» - 3 «Хорошо» - 5 «Отлично» - 6
Методикой классификации информационных систем персональных данных;	Практическое занятие 5	Модуль 2 0÷8 «Неудовлетворительно» -0 2 «Удовлетворительно» - 3 «Хорошо» - 5 «Отлично» - 6
Методикой определения административной ответственности за нарушение требований по обращению с персональными данными;	Практическое занятие 2	Модуль 1 0÷8 «Неудовлетворительно» -0 2 «Удовлетворительно» - 3 «Хорошо» - 5 «Отлично» - 6
Навыками работы с моделью угроз для	Практическое	Модуль 2

информационных систем персональных данных;	занятие 6	0÷8 «Неудовлетворительно» -0 2 «Удовлетворительно» - 3 «Хорошо» - 5 «Отлично» - 6
Методикой разграничения прав доступа в информационных системах персональных данных;	Практическое занятие 3	Модуль 1 0÷8 «Неудовлетворительно» -0 2 «Удовлетворительно» - 3 «Хорошо» - 5 «Отлично» - 6
Организацией и обеспечением режимов защиты персональных данных;	Практическое занятие 7	Модуль 2 0÷8 «Неудовлетворительно» -0 2 «Удовлетворительно» - 3 «Хорошо» - 5 «Отлично» - 6
Нормативно-правовым подходом к защите информационной системы персональных данных. .	Практическое занятие 4	Модуль 1 0÷8 «Неудовлетворительно» -0 2 «Удовлетворительно» - 3 «Хорошо» - 5 «Отлично» - 6
Методикой оценки эффективности систем защиты информационных систем персональных данных.	Практическое занятие 8	Модуль 2 0÷8 «Неудовлетворительно» -0 2 «Удовлетворительно» - 3 «Хорошо» - 5 «Отлично» - 6
	Экзамен:	0-100 «Неудовлетворительно» -0-40 «Удовлетворительно» - 41-60 «Хорошо» - 61-80 «Отлично» - 81-100

1.3 Оценочные материалы для текущего контроля и промежуточной аттестации: типовые контрольные задания, иные материалы

1.3.1 Оценочные материалы для очной формы обучения

Модуль 1 (50 баллов)

Модуль содержит **5** лекционных занятия и **4** практических занятия. Знание лекционного материала оценивается по выполненной контрольной работе, максимальное количество баллов за контрольную работу составляет **18.** За выполненные и защищенные практические занятия студент получает максимум **32** балла. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы **(ПК-1):**

1. Определение персональных данных (ПДн) и информационной системы персональных данных.
2. Нормативно-правовая база в сфере защиты и обработки ПДн (№ 149-ФЗ, № 152-ФЗ).
3. Защита персональных данных в трудовом кодексе РФ.
4. Категории персональных данных.

5. Принципы обработки персональных данных. Условия обработки персональных данных. Согласие субъекта.
6. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований по обращению с персональными данными.
7. Права субъектов персональных данных и их соблюдение при обработке.
8. Обработка персональных данных третьим лицом в интересах оператора.
9. Обязанности оператора персональных данных в ходе сбора и обработки персональных данных, ответы на запросы субъектов.
10. . Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных.
11. Ответственность за нарушение требований по обращению с персональными данными.
12. Мероприятия по защите сведений конфиденциального характера.
13. Основные внутренние нормативные документы, меры по охране конфиденциальности.
14. Формирование перечня персональных данных
15. Уничтожение электронных данных.
16. Хранение персональных данных в «облаке».
17. Права оператора персональных данных и проблемные вопросы их реализации.
18. Обезличивание ПДн. Абсолютное обезличивание и относительное обезличивание.

Практическое занятие №1. Защита персональных данных в нормативно-правовых актах РФ

Контрольные вопросы ПЗ1 (**ПК-1**):
1. Правовое и нормативное обеспечение защиты ПДн.
2. Назначение и средства антивирусной защиты.
3. Категории ПДн.
4. Назначение и средства идентификации и аутентификации субъектов.
5. Контролирующие органы в области ПДн, их функции.
6. Назначение и способы ограничения программной среды.
7. Мероприятия по обеспечению защиты ПДн при их обработке в информационных системах ПДн.
8. Согласие субъекта на обработку ПДн.
9. Назначение и способы физической защиты технических средств компьютерной системы.

Практическое занятие №2. Административная ответственность за нарушение требований по обращению с персональными данными

Контрольные вопросы (**ПК-1**):
1. Документы определяющие административную ответственность за нарушение требований по обращению с персональными данными.
2. Назначение и способы обеспечения доступности персональных данных.
3. Назначение выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них.
4. Условия обработки персональных данных.
5. Назначение средств обнаружения (предотвращения) вторжений.

Практическое занятие №3. Разграничение прав доступа в информационных системах персональных данных

Контрольные вопросы (**ПК-1**):
1. Информация как объект правовой защиты.
2. Раскройте понятие "информационное общество" и дайте его основные признаки?
3. Какими документами на международном уровне регулируется вопрос о защите персональных данных?
4. Какими основными законодательными актами регулируется вопрос защиты персональных данных на территории Российской Федерации?
5. Перечислите основные положения Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных".

6. Понятие и состав персональных данных. Что относится к специальным категориям персональных данных?
7. Понятие оператора персональных данных. Его основные права и обязанности.
8. Субъект персональных данных: понятие, права и обязанности.
9. При каком условии оператор персональных данных может начать осуществлять обработку персональных данных?

Практическое занятие №4. **Нормативно-правовый подход к защите информационной системы персональных данных**

Контрольные вопросы (**ПК-1**):

1. Какие документы по защите и обработке персональных данных должны быть, опубликованы на официальном сайте государственного или муниципального органа в соответствии с положениями постановления Правительства РФ от 21.03.2012 N 211?
2. 2Какие виды ответственности предусмотрены действующим законодательством Российской Федерации за нарушения существующих требований по защите персональных данных?
3. Какие виды ответственности предусмотрены действующим законодательством Российской Федерации за нарушения существующих требований по обработке персональных данных?
4. Какая ответственность предусмотрена за нарушение трудового законодательства Российской Федерации в части персональных данных?
5. Какая ответственность предусмотрена за нарушение гражданского кодекса Российской Федерации в части персональных данных?
6. Какие документы являются обязательными при организации системы защиты персональных данных?

Модуль 2 (50 баллов):

Модуль содержит **5** лекционных занятия и **4 практических занятия**. Знание лекционного материала и материала выносимого на самостоятельную работу оценивается по выполненной контрольной работе, максимальное количество баллов за контрольную работу составляет **18**, За выполненные и защищенные практические занятия студент получает максимум **32** балла. Общее максимальное количество баллов за модуль 2 составляет 50.

Вопросы для контрольной работы 2 **(ПК-1):**

1. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 г. Москва «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
2. Классификация информационных систем персональных данных.
3. Внутренние нормативные документы организации по охране конфиденциальности сведений.
4. Контроль над соблюдением режима конфиденциальности.
5. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
6. Модель злоумышленника информационных систем персональных данных.
7. Разработка частных моделей угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования.
8. Организационные и технические мероприятия, направленные на минимизацию ущерба от возможной реализации угроз безопасности персональных данных.
9. Защита персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных
10. Мероприятия по оценке соответствия принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных требованиям безопасности информации.

11. Мероприятия по контролю обеспечения безопасности персональных данных. Механизмы и средства контроля.
12. Периодичность и содержание работ. Ответственность оператора за нарушение правил обращения с персональными данными. Подготовка уведомлений об обработке персональных данных в уполномоченный орган.

Практическое занятие №5. **Классификация информационных систем персональных данных**

Контрольные вопросы (**ПК-1**):

1. Какие информационные системы называют типовыми?
2. Какие информационные системы называют специальными?
3. Какие категории ИСПД выделяют в зависимости от объема обрабатываемых в ИСПД данных?
4. Что определяется на основе частной модели угроз организации в соответствии с методическими документами ФСТЭК?
5. Когда может быть пересмотрен класс ИСПД ?
6. Как оформляется результат классификации ИСПД?
7. От чего должна быть защищена информационная система при обработке персональных данных в ней?
8. В чем заключается построение частной модели угроз организации?
9. Какие мероприятия применяют для исключения утечки через ПЭМИН в ИСПД 1 класса?

Практическое занятие №6. **Модель угроз для информационных систем персональных данных**

Контрольные вопросы (**ПК-1**):

1. Существуют ли временные ограничения на обработку персональных данных?
2. В каких случаях оператор персональных данных не может осуществлять обработку персональных данных?
3. 3.Дайте определение понятию «Нарушитель информационной безопасности».
4. Какие типы нарушителей информационной безопасности существуют согласно действующим правилам разграничения доступа к информации?
5. На сколько категорий делится внутренний нарушитель информационной безопасности и по каким критериям?
6. Какими возможностями обладают лица, отнесенные к первой категории внутренних нарушителей?
7. Что такое информационная система персональных данных?
8. Что такое модель угроз безопасности персональных данных?
9. 9.Какими возможностями обладает Федеральная Служба Безопасности Российской Федерации в части решения вопросов по защите и обработке персональных данных?
10. Какими возможностями обладает Федеральная Служба Технического и Экспертного Контроля Российской Федерации в части решения вопросов по защите и обработке персональных данных?

Практическое занятие №7. **Организация и обеспечение режимов защиты персональных данных**

Контрольные вопросы (**ПК-1**):

1. Особенности гарантированного уничтожения информации на полупроводниковых носителях с использованием термических воздействий.
2. Перечислить и описать угрозы безопасной передачи данных в телекоммуникационных системах.
3. Перечислить и описать задачи защиты информации в телекоммуникационных системах.
4. Перечислить и описать механизмы защиты информации в телекоммуникационных системах.
5. Физический уровень модели OSI. Назначение, вид обрабатываемой информации,

механизмы защиты, протоколы.
6. Канальный уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.
7. Сетевой уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.
8. Транспортный уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.
9. Сеансовый уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.
10. Уровень представления модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.
11. Прикладной уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.
12. Структура семиуровневой модели OSI с примерами протоколов на каждом уровне.

Практическое занятие №8. **Оценка эффективности систем защиты информационных систем персональных данных**

Контрольные вопросы (**ПК-1**):

1. Что разрабатывается в случае выявления несоответствия ИСПД установленным требованиям?
2. Метод с установлением логического соединения. Схема и описание. Пример протокола, использующего метод.
3. Адресация в сетях. IP-адрес, IP-порт и MAC-адрес. Назначение, структура адресов. Специальные и фиктивные IP-адреса.
4. IP-сети класса A. Характеристика класса: диапазон IP-адресов, идентификатор сети, граница «сеть-узел», количество сетей и узлов.
5. IP-сети класса B. Характеристика класса: диапазон IP-адресов, идентификатор сети, граница «сеть-узел», количество сетей и узлов.
6. IP-сети класса C. Характеристика класса: диапазон IP-адресов, идентификатор сети, граница «сеть-узел», количество сетей и узлов.
7. Межсетевое экранирование. Принципы межсетевого экранирования.
8. Виды и варианты подключения межсетевых экранов.
9. Назовите последовательность испытания ИСПД на соответствие требованиям по защищенности ПД от угроз безопасности ПД?
10. Назовите порядок оценки соответствия ИСПД организационно-техническим требованиям по защите ПД?

Вопросы, выносимые на экзамен для студентов очной формы обучения по дисциплине «Защита персональных данных»:

1. Определение персональных данных (ПДн) и информационной системы персональных данных.
2. Нормативно-правовая база в сфере защиты и обработки ПДн (№ 149-ФЗ, № 152-ФЗ).
3. Категории персональных данных.
4. Постановление Правительства РФ от 01.04. 2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
5. Уровни защищённости информационных систем персональных данных.
6. Процесс подготовки пакета документов к аккредитации ИСПДн: обязательство о неразглашении информации, содержащей ПДн; согласие на обработку ПДн; перечень ИСПДн.
7. Процесс подготовки пакета документов к аккредитации ИСПДн: перечень ПДн, обрабатываемых и хранящихся в ИСПДн; положение об обработки ПДн работников; акт определения уровня защищённости ИСПДн.
8. Принципы обеспечения безопасности ПДн.
9. Обезличивание ПДн. Абсолютное обезличивание и относительное обезличивание.
10. Нормативно-правовая база в области обезличивания ПДн (Приказ Роскомнадзора от 5

сентября 2013 г. №996 «Об утверждении требований и методов по обезличиванию ПДн».
11. Свойства обезличенных данных.
12. Свойства методов обезличивания.
13. Методы обезличивания персональных данных. Сравнительный анализ методов обезличивания.
14. Алгоритм перемешивания данных в общем виде.
15. Формальное описание алгоритма обезличивания ПДн методом перемешивания с помощью циклических перестановок.
16. Анализ эффективности алгоритма перемешивания ПДн с помощью циклических перестановок.
17. Определение политик безопасности (ПБ). Представление ПБ.
18. Закрытые, открытые, гибридные политики информационной безопасности.
19. Методы описания ПБ. Сравнительный анализ методов описания ПБ.
20. Аналитический метод описания ПБ.
21. Графовый метод описания ПБ.
22. Объектный метод описания ПБ.
23. Логический метод описания ПБ.
24. Пример графового метода описания ПБ: визуальный язык объектных ограничений «Language on Objects for Security Constraints» (LaSCO) (ПК – 1).
25. Определение графа атак. Формальное описание построения модели графа атак.
26. Анализ графа атак. Модель злоумышленника.
27. Определение гарантированной (верифицируемой) защиты.
28. Методы обеспечения гарантированности защиты.
29. Каналы несанкционированного доступа, утечки информации и деструктивных воздействий на информационную среду (НСДУВ).
30. Вероятностная оценка реализации канала НСДУВ.

1.3.2 Оценочные материалы для заочной формы обучения

Практическое занятие №1. Защита персональных данных в нормативно-правовых актах РФ

Контрольные вопросы (**ПК-1**):

1. Правовое и нормативное обеспечение защиты ПДн.
2. Назначение и средства антивирусной защиты.
3. Категории ПДн.
4. Назначение и средства идентификации и аутентификации субъектов.
5. Контролирующие органы в области ПДн, их функции.
6. Назначение и способы ограничения программной среды.
7. Мероприятия по обеспечению защиты ПДн при их обработке в информационных системах ПДн.
8. Согласие субъекта на обработку ПДн.
9. Назначение и способы физической защиты технических средств компьютерной системы.

Практическое занятие №2. Разграничение прав доступа в информационных системах персональных данных

Контрольные вопросы (**ПК-1**):

1. Информация как объект правовой защиты.
2. Раскройте понятие "информационное общество" и дайте его основные признаки?
3. Какими документами на международном уровне регулируется вопрос о защите персональных данных?
4. Какими основными законодательными актами регулируется вопрос защиты персональных данных на территории Российской Федерации?
5. Перечислите основные положения Федерального закона от 27.07.2006 N 152–ФЗ "О персональных данных".

6. Понятие и состав персональных данных. Что относится к специальным категориям персональных данных?
7. Понятие оператора персональных данных. Его основные права и обязанности.
8. Субъект персональных данных: понятие, права и обязанности.
9. При каком условии оператор персональных данных может начать осуществлять обработку персональных данных?

Практическое занятие №3. **Классификация информационных систем персональных данных**

Контрольные вопросы (**ПК-1**):
1. Какие информационные системы называют типовыми?
2. Какие информационные системы называют специальными?
3. Какие категории ИСПД выделяют в зависимости от объема обрабатываемых в ИСПД данных?
4. Что определяется на основе частной модели угроз организации в соответствии с методическими документами ФСТЭК?
5. Когда может быть пересмотрен класс ИСПД ?
6. Как оформляется результат классификации ИСПД?
7. От чего должна быть защищена информационная система при обработке персональных данных в ней?
8. В чем заключается построение частной модели угроз организации?
9. Какие мероприятия применяют для исключения утечки через ПЭМИН в ИСПД 1 класса?

Практическое занятие №4. **Модель угроз для информационных систем персональных данных**

Контрольные вопросы (**ПК-1**):
1. Существуют ли временные ограничения на обработку персональных данных?
2. В каких случая оператор персональных данных не может осуществлять обработку персональных данных?
3.Дайте определение понятию «Нарушитель информационной безопасности».
4. Какие типы нарушителей информационной безопасности существуют согласно действующим правилам разграничения доступа к информации?
5. На сколько категорий делится внутренний нарушитель информационной безопасности и по каким критериям?
6. Какими возможностями обладают лица, отнесенные к первой категории внутренних нарушителей?
7. Что такое информационная система персональных данных?
8. Что такое модель угроз безопасности персональных данных?
9.Какими возможностями обладает Федеральная Служба Безопасности Российской Федерации в части решения вопросов по защите и обработке персональных данных?
10. Какими возможностями обладает Федеральная Служба Технического и Экспертного Контроля Российской Федерации в части решения вопросов по защите и обработке персональных данных?

Практическое занятие №5. **Организация и обеспечение режимов защиты персональных данных**

Контрольные вопросы (**ПК-1**):
1. Особенности гарантированного уничтожения информации на полупроводниковых носителях с использованием термических воздействий.
2. Перечислить и описать угрозы безопасной передачи данных в телекоммуникационных системах.
3. Перечислить и описать задачи защиты информации в телекоммуникационных системах.
4. Перечислить и описать механизмы защиты информации в телекоммуникационных системах.
5. Физический уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.

6. Канальный уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.
7. Сетевой уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.
8. Транспортный уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.
9. Сеансовый уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.
10. Уровень представления модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.
11. Прикладной уровень модели OSI. Назначение, вид обрабатываемой информации, механизмы защиты, протоколы.
12. Структура семиуровневой модели OSI с примерами протоколов на каждом уровне.

Вопросы, выносимые на экзамен по дисциплине «Защита персональных данных»**: такие же, как и для обучающихся очной формы обучения**

2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

2.1 Порядок и методика проведения текущего контроля и промежуточной аттестации

Предусмотрены следующие виды контроля:

- текущий контроль по каждому модулю – в форме написания контрольной работы для оценки теоретических знаний;
- текущий контроль по каждому модулю – в форме отчетов по лабораторным работам и практическим занятиям для оценки практических навыков;
- промежуточная аттестация по дисциплине – в форме экзамена.

Текущий контроль успеваемости в форме защиты практических занятий проводится в два этапа:

- 1-й этап: допуск к выполнению занятий – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний студентов теоретической части занятия и готовности к выполнению практических исследований;
- 2-й этап выполняется по окончании каждого практического занятия в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки студентом практических навыков исследования на аппаратуре.

Контрольные работы выполняются в виде короткого письменного ответа на один вопрос, изученный на предыдущей лекции в начале каждой последующей лекции. Ответ на вопрос дается в течение 5-10 минут. Таким образом, после лекционного курса каждого модуля формируется общая оценка за теоретические знания.

С целью повышения качества обучения за счет побуждения студентов к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности студентов в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранным обучающимся баллам соответствуют оценки:

- «неудовлетворительно» - от 0% до 40% от максимального количества баллов;
- «удовлетворительно» - от 41% до 60% максимального количества баллов;
- «хорошо» - от 61% до 80% максимального количества баллов;
- «отлично» - от 81% до 100% максимального количества баллов.

Соотношения максимального количества баллов, полученных студентом по блокам модулей, показаны в Таблице .

Таблица - Распределение баллов по блокам модулей дисциплины «Защита персональных данных»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Компьютерное тестирование)	Практический блок (Распределение баллов по занятиям)
Модуль 1	50	18	32=8+8+8+8
Модуль 2	50	18	32=8+8+8+8
Модуль – Экзамен	100	100	

Как правило, теоретический блок оценивается по результатам контрольной работы. Практический блок оценивается по результатам выполнения заданий на практических занятиях.

На экзамене производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуется формировать вопросы в экзаменационных билетах таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

2.2 Методика проведения экзамена в группах заочной формы обучения

Экзамен по дисциплине «Защита персональных данных» у обучающихся заочной формы обучения проводится письменно по классической методике. Вопросы сгруппированы в билетах. В каждом билете содержится по 2-3 вопроса, скомпонованные таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины. Количество билетов должно быть не менее числа обучающихся в группе. Обучающиеся готовят письменные ответы на вопросы.

3 Промежуточная аттестация

Промежуточная аттестация проводится в форме экзамена.

Экзамен проводится по расписанию экзаменационной сессии в письменном виде. Количество вопросов в экзаменационном билете – 3. Проверка ответов и объявление результатов производится в день экзамена. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку обучающегося.

Обучающиеся, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Образец **экзаменационного билета**

	МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»	Утверждаю Зав. кафедрой «ИТСС» _____ Юхнов В.И. «____» _____ 20____ г.

Направление подготовки: 10.03.01 ***Информационная безопасность***
Курсы: 4, 5
Дисциплина: ***Обеспечение безопасности персональных данных в информационных системах***

Билет №1

1. Основные понятия и определения. Содержание категории «персональные данные».
2. Порядок проведения классификации информационных систем персональных данных.
3. Организационные и технические мероприятия, направленные на минимизацию ущерба от возможной реализации угроз безопасности персональных данных.

Доцент каф., к.т.н., доцент «ИТСС» _____Ершов В.В.

«_____» _____20__ г

Один комплект отпечатанных экзаменационных билетов, подписанных преподавателем кафедры и утвержденных заведующим кафедрой хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину

4 Тестовые задания для проведения оценки сформированности компетенций ПК-1

На компетенцию **ПК-1** сформировано 20 тестовых заданий. Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень содержит 50% тестовых заданий. Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.);

Повышенный уровень составляет 35 % заданий. В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень составляют – 15 % заданий. В заданиях используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Один комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

ПК-1: Способен обеспечить защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Тексты заданий
1	Обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну закреплено: 1. в Федеральном законе №152, 2. в Трудовом кодексе, 3. в Конституции РФ.
2	Обработка персональных данных – это совокупность действий включающих: 1. сбор персональных данных, 2. запись персональных данных, 3. дублирование персональных данных. Укажите правильные ответы.
3	Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных: 1. обрабатываемых в соответствии с трудовым законодательством, 2. полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, 3. полученных по закрытым каналам. Укажите правильные ответы.
4	Примерный перечень конфиденциальной информации включает в себя: 1. Информация, составляющая коммерческую тайну, 2. Банковская тайна — сведения об операциях, о счетах и вкладах организаций, 3. Информация служебного пользования (ДСП), Укажите правильные ответы.
5	Различают уровни системы защиты конфиденциальной информации:

№ задания	Тексты заданий
	1. Правовой, 2. Вербальный, 3. Согласованный.
6	Отнесение конкретной информации о деятельности Компании к конкретной категории конфиденциальной производится на основании: 1. Перечня сведений, составляющих коммерческую тайну, 2. Перечня сведений, составляющих административную тайну, 3. Сведений для служебного пользования.
7	К конфиденциальной технической, технологической, коммерческой, организационной или иной используемой в предпринимательской деятельности следует относить информацию: 1. которая обладает действительной или потенциальной коммерческой ценностью в силу неизвестности ее третьим лицам, 2. о численности, составе, об условиях труда работников и о наличии свободных рабочих мест, 3. содержащаяся в свидетельствах о регистрации гражданина в качестве индивидуального предпринимателя, лицензиях и иных документах на право занятия отдельными видами деятельности.
8	В случае определения оператором необходимости обеспечения безопасности персональных данных с использованием криптосредств при формировании модели угроз используются методические документы: 1. ФСТЭК России, 2. Федеральный закон от 27.07.2006 N 149-ФЗ, 3. Федеральный закон №152.
9	Требованиями какого документа подтверждается соответствие информационной системы персональных данных: 1. приказом ФСТЭК России от 2 декабря 2020 г. N 141, 2. приказом ФСТЭК России от 18.02.2013 №21, 3. приказом ФСТЭК России от 17 июля 2017 г. N 133.
10	В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных входят: 1. управление доступом субъектов доступа к объектам доступа, 2. ограничение программной среды, 3. испытания подсистемы регистрации и учета, Укажите правильные ответы.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия

Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Выделяют три этапа оценки угроз безопасности информации: 1 первый, 2.второй, 3.третий. Расставьте эти этапы в порядке их очередности А. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности. Б. Определение возможных объектов воздействия угроз безопасности информации. В. Определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации.
12	Этап оценки возможности реализации (возникновения) угроз безопасности информации и определение их актуальности состоит из трех подэтапов: 1.первый,

№ задания	Тексты заданий
	2.второй, 3.третий. Расставьте эти подэтаы в порядке их очередности А. Оценка способов реализации угроз безопасности информации. Б. Выявление источников угроз безопасности информации. В. Оценка актуальности угроз безопасности информации.
13	Как правило, выделяют три типа угроз безопасности за счет реализации технических каналов утечки: 1.первый, 2.второй, 3.третий. Расставьте их в порядке их очередности А. Угрозы утечки речевой информации. Б. угрозы утечки информации по каналам побочных электромагнитных излучений и наводок. В. Угрозы утечки видовой информации.
14	Уязвимости, можно классифицировать по четырем признакам: 1.первый, 2.второй, 3.третий. 4.четвертый Расставьте эти признаки в порядке их очередности А. По характеру последствий от реализации атак – изменение прав доступа, подбор пароля, вывод из строя системы в целом. Б. По причине возникновения уязвимости, например, недостатки механизмов аутентификации сетевых протоколов. В. По этапу жизненного цикла ПО, на котором возникла уязвимость. Г. По типу ПО – системное или прикладное. В. Определение круга сотрудников, которые должны иметь доступ к той или иной конфиденциальной информации, и оформление с ними соответствующих взаимоотношений.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Существует четыре метода разграничения доступа: 1.первый, 2.второй, 3.третий, 4четвертый. Расставьте эти методы в порядке их очередности А. Разграничение доступа по уровням секретности и категориям; Б. Использование матрицы установления полномочий; В. Парольное разграничение доступа. Г. Разграничение доступа по спискам.
16	Различают четыре категории обрабатываемых персональных данных: 1.первая, 2.вторая, 3.третья, 4.четвертая. Расставьте эти категории в порядке их очередности А. Персональные данные, позволяющие идентифицировать субъекта персональ-

№ задания	Тексты заданий
	ных данных; Б. Персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1; В. Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни; Г. Обезличенные и (или) общедоступные персональные данные.
17	Выделяют четыре уровня защищённости персональных данных 1. УЗ-4, 2.УЗ-3, 3.УЗ-2, 4.УЗ-1. Расставьте эти уровни в порядке возрастания защитных мер. А. Система обрабатывает общедоступные персональные данные, иные персональные данные работников или других лиц в количестве менее 100 000; **Б.** При угрозах 1-го типа система обрабатывает общедоступные персональные данные. При угрозах 2-го типа — специальные данные сотрудников организации либо лиц, не работающих у оператора, в количестве менее 100 000 человек **В.** Информационная система обрабатывает специальные, биометрические и иные персональные данные при угрозах 1-го типа, а также специальные данные более чем 100 000 человек; **Г.** При угрозе 2-го типа система обрабатывает общедоступные и иные персональные данные сотрудников, иных лиц числом менее 100 000 человек;

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом
Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются _____
19	Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий,_____
20	Обезличивание персональных данных Пользователя происходит по письменному заявлению Пользователя, при условии, что все договорные отношения завершены и от даты окончания последнего договора прошло_____

Критерии оценивания ответов на тестовые задания ПК-1

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.

Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует- 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 3 баллами; если допущена одна ошибка/неточность/ответ правильный, но не полный - 1 балл, если допущено более одной ошибки/ответ неправильный/ ответ отсутствует- 0 баллов.

Приложение 2

Методические рекомендации по освоению дисциплины

1. Методические рекомендации преподавателю

Дисциплина «Защита персональных данных» включает в себя:

- лекционные занятия – 20 часов;
- практические занятия – 30 часов;
- промежуточную аттестацию – экзамен.

Перед началом изучения дисциплины преподаватель должен ознакомить обучающихся с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

1) формулирует тему и цель занятия, объявляет учебные вопросы;

2) излагает основные теоретические положения;

3) с помощью технических средств обучения и/или под запись дает определения основных понятий, расчетных формул;

4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;

5) в конце занятия выдает вопросы для самостоятельного изучения.

На практических занятиях следует обратить внимание на соответствие выбираемых обучающимся средств выполнения решаемых в работе задач.

Каждая лабораторная работа должна быть оформлена и защищена в соответствии с требованиями. Защита производится после оформления отчета по работе.

Во время выполнения заданий в учебной аудитории обучающийся может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается не выполненной, обучающийся может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего контроля и контроля знаний обучающихся при проведении промежуточной аттестации

2. Методические рекомендации обучающимся

Приступая к изучению новой учебной дисциплины, студенты должны ознакомиться с рабочей программой, оценочными материалами, учебной, научной и методической литературой, имеющейся в ЭИОС СКФ МТУСИ,

Глубина усвоения дисциплины зависит от активной и систематической работы студента на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по лекционным занятиям

Важно сосредоточить внимание на содержании лекции. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине.

Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности студентов.

2.2 Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации:

- изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д.;
- при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа студента под управлением преподавателя. На них пополняются теоретические знания студентов, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение студентов к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы.

После подведения итогов занятия студент обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

3. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа обучающихся является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
- подготовки к лабораторным работам (практическим занятиям);
- изучения учебной и научной литературы;
- решения задач, выданных на практических занятиях;
- подготовки к тестированию;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях;
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов по отдельным вопросам изучаемой дисциплины.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Обычно постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятий, предшествующему данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально.