

**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
«28» 09 2026 г.

Рабочая программа дисциплины

**Б1.О.39 Обеспечение безопасности персональных данных
в информационных системах**

Кафедра **Инфокоммуникационных технологий и систем связи**
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль **Безопасность компьютерных систем (по отрасли или в
сфере профессиональной деятельности)**
Формы обучения **очная**

Распределение часов дисциплины по семестрам (очная форма обучения (ОФО))

Вид учебной работы	ОФО	
	ЗЕ	часов/семестр
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3	108/7
Контактная работа, в том числе (по семестрам, курсам):		48/7
Лекции		24/7
Лабораторных работ		12/7
Практических занятий		12/7
Семинаров		
Самостоятельная работа		60/7
Контроль		
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам		1/7
Число экзаменов с разбивкой по семестрам (курсам)		

Программу составил:

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

Рабочая программа дисциплины

«Обеспечение безопасности персональных данных в информационных системах»

Разработана в соответствии с ФГОС ВО:

направления подготовки **10.03.01 «Информационная безопасность»**,
утвержденным приказом Министерства науки и высшего образования Российской
Федерации от 17 ноября 2020 г. N 1427

Составлена на основании учебного плана

направления подготовки **10.03.01 Информационная безопасность**,
профиль «Безопасность компьютерных систем (по отрасли или в сфере
профессиональной деятельности)», одобренного Учёным советом СКФ МТУСИ,
протокол № 8 от 31.03 2026г., и утвержденного директором СКФ
МТУСИ 31.03 2026г.

Рассмотрена и одобрена на заседании кафедры

Инфокоммуникационные технологии и системы связи

Протокол от «28» 04 2026 г. № 9

Зав. кафедрой *В.И. Юхнов* Юхнов В.И.

1. Цели изучения дисциплины

Целями освоения дисциплины «Обеспечение безопасности персональных данных в информационных системах» являются: изучение нормативно-правовых актов РФ по обеспечению безопасности информации, формирование правовой грамотности, овладение понятийным аппаратом дисциплины, приемами и методами защиты по обеспечению персональных данных в современных информационных системах в рамках действующих и перспективных информационных систем и технологий.

2 Планируемые результаты обучения

Изучение дисциплины направлено на формирование у обучающегося способности, решать профессиональные задачи в соответствии с *эксплуатационным* видом деятельности.

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

Компетенции, формируемые у обучающегося в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)	
ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	
Знать:	
Структуру и содержание нормативной и правовой документации, применимой для защиты информации, касающейся персональных данных; Принципы применения нормативной и правовой документации, характерной для области инфокоммуникационных технологий и систем связи, для защиты персональных данных пользователей и сотрудников этих систем; Особенности применения нормативной и правовой документации, характерной для защиты персональных данных в области инфокоммуникационных технологий и систем связи.	
Уметь:	
Соблюдать основные требования информационной безопасности по защите персональных данных; Применять решения по организации защиты персональных данных; Анализировать и оценивать эффективность результатов применения решений по организации защиты персональных данных; Применять регламенты, стандарты и иные нормативные документы в области защиты персональных данных при использовании инфокоммуникационных технологий; Производить обоснованный выбор решений по защите персональных данных.	
Владеть:	
Навыками применения нормативной и правовой документации, необходимой для защиты персональных данных; Навыками принятия решений по защите персональных данных; Навыками выбора оборудования и программных средств необходимых для защиты персональных данных.	
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	
Знать:	
Структуру и комплекс задач по защите информации в современных и перспективных информационных системах, решаемых в рамках будущей профессиональной деятельности; Требования нормативных и правовых руководящих документов по обеспечению успешного решения профессиональных задач при планировании и организации комплекса мероприятий	

по защите информации ограниченного доступа;

Порядок применения нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Уметь:

Анализировать текущее состояние комплекса вопросов по безопасности информации в информационных системах и аргументировано оценивать его в соответствии с требованиями нормативных и методических документов;

Планировать мероприятия по обеспечению безопасности и защите персональных данных и информации ограниченного доступа согласно требованиям нормативных правовых актов, нормативных и методических документов соответствующих федеральных служб;

Применять процедуры поиска и обнаружения угроз для обеспечения безопасности информации ограниченного доступа.

Владеть:

Практическими навыками планирования и организации проведения мероприятий по обеспечению безопасности компьютерных систем и сетей;

Навыками применения нормативной и правовой документации, нормативными и методическими документами соответствующих федеральных служб по защите персональных данных;

Навыками обоснованного выбора решений по защите персональных данных.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):		
1	Б1.О.27	Основы информационной безопасности
2	Б1.О.28	Организационное и правовое обеспечение информационной безопасности»
3	Б1.О.33	Программно-аппаратные средства защиты информации
4	Б1.О.32	Основы управления информационной безопасностью
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:		
1	Б1.В.02	Комплексное обеспечение защиты информации объекта информатизации
2	Б2.В.02(П)	Производственная (эксплуатационная) практика

4 Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часов, 48 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМНО
1	2	3	4	5	6
Курс 4 , Семестр 7					
Модуль 1. Нормативно-правовые акты по обеспечению безопасности информации компьютерных систем и систем – (24+30) =54 часа					
1.1	Персональные данные в Федеральном законе и Трудовом кодексе Российской Федерации. 1. Основные понятия и определения. Содержание категории «персональные данные».	Лек.1	2	ОПК-5, ОПК-6	Л1.1 Л1.2 Л2.3 Л2.4

	2. Обработка персональных данных: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (передача), обезличивание, блокирование, уничтожение.				
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	5	ОПК-5, ОПК-6	Л1.1 Л1.2 Л2.1 Л2.2
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	2	ОПК-5, ОПК-6	Л1.1 Л1.2
1.4	Вопросы защиты персональных данных в нормативно-правовых актах РФ 1. Конституция РФ о защите персональных данных. 2. Защита персональных данных в трудовом кодексе РФ.	Лек.3	2	ОПК-5, ОПК-6	Л1.1 Л1.2 Л2.3 Л2.4
1.5	Обработка биометрических данных.	СРС	4	ОПК-5, ОПК-6	Л1.1 Л1.2 Л2.1 Л2.2
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.4	2	ОПК-5, ОПК-6	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 1	4	ОПК-5, ОПК-6	Л1.1 Л1.2 Л3.1 Л2.4
1.8	Специальные категории персональных данных и особенности их обработки.	СРС	4	ОПК-5	Л1.1 Л1.2 Л2.1 Л2.2
1.9	Ответственность за нарушение требований по обращению с персональными данными	Лек.5	2	ОПК-5, ОПК-6	Л1.1 Л1.2

	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.				
1.10	Уничтожение электронных данных. 1. Уровни уничтожения электронных данных (очистка, очищение, разрушение). 2. Стандартизация уничтожения электронных данных.	СРС	8	ОПК-5, ОПК-6	Л1.1 Л1.2 Л2.1 Л2.2
1.11	Определение перечня угроз безопасности персональных данных при их обработке в информационных системах персональных данных	ЛР1	4	ОПК-5	Л1.1 Л1.2 Л2.1 Л3.2
1.12	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	9	ОПК-5, ОПК-6	Л1.1 Л1.2 Л2.1 Л2.2
1.13	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.6	2	ОПК-5, ОПК-6	Л1.1 Л1.2
1.14	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 2	4	ОПК-5, ОПК-6	Л1.1 Л1.2 Л2.2
Модуль 2. Классификация информационных систем персональных данных и обеспечение режимов защиты персональных данных. (24+30) =54 часа					
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.7	2	ОПК-5, ОПК-6	Л1.1 Л1.2
2.2	Определение порядка обращения с персональными данными, контроля над его соблюдением, организация доступа к персональным данным.	СРС	5	ОПК-5, ОПК-6	Л1.1 Л1.2 Л2.1 Л2.2

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.8	2	ОПК-5, ОПК-6	Л1.1 Л1.2
2.4	Уровни и классы информационных систем персональных данных 1.Определение уровня защищённости информационных систем персональных данных. 2. Исследование классов систем.	Лек.9	2	ОПК-5, ОПК-6	Л1.1 Л1.2
2.5	Внутренние нарушители защиты персональных данных и негативные последствия их деятельности для предприятий и организаций.	СРС	5	ОПК-5, ОПК-6	Л1.1 Л1.2 Л2.1 Л2.2
2.6	Определение частоты (вероятности) реализации рассматриваемой угрозы (Y2	ЛР2	4	ОПК-5	Л1.1 Л1.2 Л2.1
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.10	2	ОПК-5, ОПК-6	Л1.1 Л1.2
2.8	Многофакторная аутентификация. Примеры многофакторной аутентификации. Протоколы аутентификации.	СРС	5	ОПК-5, ОПК-6	Л1.1 Л1.2 Л2.1
2.9	Организация и обеспечение режимов 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. 11	2	ОПК-5, ОПК-6	Л1.1 Л1.2
2.10	Определение типа актуальной угрозы	ЛР3	4	ОПК-5, ОПК-6	Л1.1 Л1.2 Л2.1
2.11	Принципы и этапы защиты персональной информации в ИСПДн	ПЗЗ	4	ОПК-5, ОПК-6	Л1.1 Л1.2

	1. Принципы и этапы защиты персональных данных в ИСПДн. 2. Процедура оформления доступа к персональным данным				Л2.2
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.12	2	ОПК-5, ОПК-6	Л1.1 Л1.2
2.13	Определение политик безопасности (ПБ). Представление ПБ. Закрытые, открытые, гибридные политики информационной безопасности.	СРС	5	ОПК-5, ОПК-6	Л1.1 Л1.2 Л2.1 Л2.2
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	5	ОПК-5, ОПК-6	Л1.1 Л1.2 Л2.1 Л2.2
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	5	ОПК-5, ОПК-6	Л1.1 Л1.2 Л2.1 Л2.2
	Зачет			ОПК-5, ОПК-6	Л1.1 Л1.2 Л2.1 Л2.2 Л2.3 Л2.4 Л3.1 Л3.2
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. — 121 с.	Э1
Л 1.2	В.И. Петренко	Защита персональных данных в информационных системах : учебное пособие	Ставрополь : Северо-Кавказский федеральный университет, 2016. — 201 с.	Э2
5.1.2 Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л 2.1	О.М. Голембиовская, М.Ю. Рытов, К.Е. Шинаков	Формализация подходов к обеспечению защиты персональных данных: монография	Саратов : Ай Пи Эр Медиа, 2019. — 198 с	Э7
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. — 80 с.	Э4
Л2.3	"Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) Принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года			Э5
Л2.4	Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных"			Э6
5.1.3 Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
ЛЗ.1	А. М. Макаров, И. В. Калиберда, К. О. Бондаренко..	Организация защиты персональных данных: лабораторный практикум	Ставрополь: Северо-Кавказский федеральный университет, 2015. — 92 с.	Э3
ЛЗ.2	В.И. Петренко, И.В. Мандрица.	Защита персональных данных в информационных системах: лабораторный практикум	Ставрополь: Северо-Кавказский федеральный университет, 2018. — 118 с.	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/81851.html			
Э4	https://www.iprbookshop.ru/141049.html			

Э5	https://www.consultant.ru/document/cons_doc_LAW_28399/
Э6	https://base.garant.ru/12148567/
Э7	www.iprbookshop.ru/62971.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/
5.3.2	Консорциум Кодекс – https://docs.cntd.ru/
5.3.3	Научная электронная библиотека – https://www.elibrary.ru/
5.3.4	Электронный ресурс http://www.securitylab.ru/
5.3.5	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)
5.3.6	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)
5.4 Программное обеспечение СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:	
П.1	Kaspersky Endpoint Security
П.2	Операционная система Linux – свободное ПО
П.3	MS Office – лицензионное ПО

6 Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная интерактивной доской, проектором, ПК (ноутбуком), экраном.
6.2 МТО практических занятий	
1	Лаборатория «Технической защиты информации», укомплектованная специализированной мебелью, оснащенная техническими средствами защиты информации
6.3 МТО рубежных контролей, зачетов	
1	Учебные аудитории, оборудованные компьютерной техникой с возможностью выхода в локальную сеть Филиала и Интернет.
6.4 МТО самостоятельной работы обучающихся	
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, прочесть задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Б1.О.39 Обеспечение безопасности персональных данных в информационных системах» для использования в 20__/20__ учебном году

Утверждаю

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

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения: очная

(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 _____

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

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Критерии оценивания	Шкала оценивания
ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности		
Знать:		
Структуру и содержание нормативной и правовой документации, применимой для защиты информации, касающейся персональных данных.	Контрольная работа	Модуль 1 0÷7 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Принципы применения нормативной и правовой документации, характерной для области инфокоммуникационных технологий и систем связи, для защиты персональных данных пользователей и сотрудников этих систем; Особенности применения нормативной и правовой документации, характерной для защиты персональных данных в области инфокоммуникационных технологий и систем связи.	Контрольная работа	Модуль 2 0÷7 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Уметь:		
Соблюдать основные требования информационной безопасности по защите персональных данных.	Практическое занятие 1	Модуль 1 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
	Лабораторное занятие 2	Модуль 2 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
Применять решения по организации защиты персональных данных; Анализировать и оценивать эффективность результатов применения решений по организации защиты персональных данных	Лабораторное занятие 1	Модуль 1 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3

	Лабораторное занятие 3	Модуль 2 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
Применять регламенты, стандарты и иные нормативные документы в области защиты персональных данных при использовании инфокоммуникационных технологий; Производить обоснованный выбор решений по защите персональных данных	Практическое занятие 2	Модуль 1 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
	Практическое занятие 3	Модуль 2 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
Владеть		
Навыками применения нормативной и правовой документации, необходимой для защиты персональных данных;	Практическое занятие 1	Модуль 1 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
	Лабораторное занятие 2	Модуль 2 0 -3 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
Навыками принятия решений по защите персональных данных	Лабораторное занятие 1	Модуль 1 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
	Лабораторное занятие 3	Модуль 2 0 -3 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
Навыками выбора оборудования и программных средств необходимых для защиты персональных данных	Практическое занятие 2	Модуль 1 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
	Практическое занятие 3	Модуль 2 0 -3 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3

ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю		
Знать:		
Порядок применения нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	Контрольная работа	Модуль 1 0÷7 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Структуру и комплекс задач по защите информации в современных и перспективных информационных системах, решаемых в рамках будущей профессиональной деятельности; Требования нормативных и правовых руководящих документов по обеспечению успешного решения профессиональных задач при планировании и организации комплекса мероприятий по защите информации ограниченного доступа.	Контрольная работа	Модуль 2 0÷7 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Уметь:		
Анализировать текущее состояние комплекса вопросов по безопасности информации в информационных системах и аргументировано оценивать его в соответствии с требованиями нормативных и методических документов	Практическое Занятие 1	Модуль 1 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
	Лабораторное занятие 2	Модуль 2 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
Применять процедуры поиска и обнаружения угроз для обеспечения безопасности информации ограниченного доступа	Лабораторное занятие 1	Модуль 1 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
	Лабораторное занятие 3	Модуль 2 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
Планировать мероприятия по обеспечению безопасности и защите персональных данных и информации ограниченного доступа согласно требованиям нормативных правовых актов,	Практическое Занятие 2	Модуль 1 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1

нормативных и методических документов соответствующих федеральных служб.		«Хорошо» - 2 «Отлично» - 3
	Практическое занятие 3	Модуль 2 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
Владеть		
Практическими навыками планирования и организации проведения мероприятий по обеспечению безопасности компьютерных систем и сетей	Практическое Занятие 1	Модуль 1 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
	Лабораторное занятие 2	Модуль 2 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
Навыками обоснованного выбора решений по защите персональных данных	Лабораторное занятие 1	Модуль 1 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
	Лабораторное занятие 3	Модуль 2 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
Навыками применения нормативной и правовой документации, нормативными и методическими документами соответствующих федеральных служб по защите персональных данных.	Практическое занятие 2	Модуль 1 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
	Практическое занятие 3	Модуль 2 0 -3 «Неудовлетворительно» - 0 «Удовлетворительно» - 1 «Хорошо» - 2 «Отлично» - 3
	Зачет	0-100 «Не зачтено» - 0-40 «Зачтено» - 41-100

1.3 Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные материалы текущего контроля для очной формы обучения

Данная дисциплина формирует у обучающегося 2 компетенции, которые связаны, взаимодействуют между собой и объективно оценить каждую в отдельности при ответе обучающегося на контрольный вопрос или при выполнении практического или лабораторного задания достаточно сложно. Предлагается считать, что вклад 2-х компетенций в общую оценку при ответе на вопрос примерно одинаков.

Модуль 1 (50 баллов):

Модуль содержит 6 лекционных занятий, 2 практических и 1 лабораторное занятия. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 14. За каждое выполненное и защищенное практическое занятие обучающийся получает максимум 12 баллов, за 2 практических занятия обучающийся получает 24 балла; за лабораторную работу - максимум 12 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы 1. (ОПК-5, ПК-6):

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.
3. Принципы обработки персональных данных. Условия обработки персональных данных. Согласие субъекта.
4. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований по обращению с персональными данными.
5. Права субъектов персональных данных и их соблюдение при обработке.
6. Конституция РФ о защите персональных данных.
7. Защита персональных данных в трудовом кодексе РФ.
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.

Практическое занятие № 1. Административная ответственность за нарушение требований по обращению с персональными данными

Контрольные вопросы (ОПК-5, ОПК-6):

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.

Лабораторная работа № 1. Определение перечня угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Контрольные вопросы (ОПК-5, ОПК-6):

1. Определение понятия информационная система персональных данных.
2. Определение понятия угрозы безопасности персональных данных.
3. Типы структур ИСПДн информационных системах персональных данных.
4. Структура автономной информационной системы персональных данных.
5. Структура локальной информационной системы персональных данных.
6. Структура распределенной информационной системы персональных данных.
7. Категории обрабатываемых в информационной системе персональных данных.
8. Объем обрабатываемых в ИСПДн персональных данных.
9. Режимы обработки персональных данных.
10. режимы разграничения прав доступа пользователей ИСПДн.

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

Контрольные вопросы (ОПК-5, ОПК-6):

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?

Модуль 2: (50 баллов):

Модуль содержит 6 лекционных занятий, 1 практическое и 2 лабораторных занятия. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет **14**. За выполненное и защищенное практическое занятие обучающийся получает максимум **12** баллов. За каждую выполненную и защищенную лабораторную работу обучающийся получает максимум по **12** баллов. За две лабораторные работы обучающийся получает **24** балла. Общее максимальное количество баллов за модуль 2 составляет 50.

Вопросы для контрольной работы 2 (ОПК-5, ОПК-6):

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.
3. Внутренние нормативные документы по охране конфиденциальности сведений, их содержание, порядок разработки и ввода в действие.
4. Контроль над соблюдением режима конфиденциальности.

5. Определение уровня защищённости информационных систем персональных данных.
6. Исследование классов систем.
7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
8. Модель злоумышленника информационных систем персональных данных.
9. Разработка частных моделей угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования.
10. Организационные и технические мероприятия, направленные на минимизацию ущерба от возможной реализации угроз безопасности персональных данных.
11. Защита персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий.
12. Мероприятия по оценке соответствия принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных требованиям безопасности информации.
13. Мероприятия по контролю обеспечения безопасности персональных данных. Механизмы и средства контроля.
14. Периодичность и содержание работ. Ответственность оператора за нарушение правил обращения с персональными данными. Подготовка уведомлений об обработке персональных данных в уполномоченный орган

Лабораторная работа №2. Определение частоты (вероятности) реализации рассматриваемой угрозы (Y2)

Контрольные вопросы (ОПК-5, ОПК-6):

1. Нормативный документ, определяющий методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
2. Какие показатели применяются для оценки возможности реализации угрозы?
3. Что понимается под уровнем исходной защищенности ИСПДн?
4. Что понимается под частотой (вероятностью) реализации угрозы?
5. Что понимается под частотой (вероятностью) реализации угрозы безопасности?
6. Перечислить градации частоты реализации угрозы.
7. Пояснить смысл понятия маловероятной угрозы.
8. Пояснить смысл понятия низкая вероятность угрозы.
9. Пояснить смысл понятия средняя вероятность угрозы.
10. Пояснить смысл понятия высокая вероятность угрозы.
11. Пример записи показателей Коэффициент вероятности реализации (Y2).

Лабораторная работа №3. Определение типа актуальной угрозы

Контрольные вопросы (ОПК-5, ОПК-6):

1. Нормативный документ, определяющий методику требований к защите персональных данных при их обработке в информационных системах персональных данных.
2. Определение понятия актуальные угрозы безопасности персональных при их обработке в информационных системах персональных данных.
3. Виды актуальных угроз для информационной системы.
4. Характеристика актуальных угроз 1-го типа.
5. Характеристика актуальных угроз 2-го типа.
6. Характеристика актуальных угроз 3-го типа.
7. Кем определяется тип угроз безопасности персональных данных, актуальных для информационной системы.

8. Нормативный документ, определяющий процедуру определения типа угроз безопасности персональные данные.
9. Какие меры включает в себя система защиты персональных данных?

Практическое занятие №3. Принципы и этапы защиты персональной информации в ИСПДн

Контрольные вопросы (ОПК-5, ОПК-6):

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.

1.3.2 Вопросы, выносимые на зачет по дисциплине «Обеспечение безопасности персональных данных в информационных системах» (ОПК-5, ОПК-6 (промежуточная аттестация)):

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.
3. Законность видеосъемки, фотосъемки и звукозаписи в общественных местах.
4. Принципы обработки персональных данных. Условия обработки персональных данных. Согласие субъекта.
5. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований по обращению с персональными данными.
6. Права субъектов персональных данных и их соблюдение при обработке.
7. Конституция РФ о защите персональных данных.
8. Защита персональных данных в трудовом кодексе РФ.
9. Обработка биометрических данных.
10. Обработка персональных данных третьим лицом в интересах оператора.
11. Обязанности оператора персональных данных в ходе сбора и обработки персональных данных, ответы на запросы субъектов.

12. Специальные категории персональных данных и особенности их обработки
13. Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных.
14. Ответственность за нарушение требований по обращению с персональными данными.
15. Уровни уничтожения электронных данных (очистка, очищение, разрушение).
16. Стандартизация уничтожения электронных данных.
17. Необходимые свойства «облака» для построения «облачной» системы хранения персональных данных.
18. Требования регулирующих органов по защите персональных данных в «облаке»
19. Мероприятия по защите сведений конфиденциального характера.
20. Основные внутренние нормативные документы, меры по охране конфиденциальности.
21. Формирование перечня персональных данных.
22. 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».
23. Порядок проведения классификации информационных систем персональных данных.
24. Определение порядка обращения с персональными данными, контроля над его соблюдением, организация доступа к персональным данным.
25. Внутренние нормативные документы по охране конфиденциальности сведений, их содержание, порядок разработки и ввода в действие.
26. Контроль над соблюдением режима конфиденциальности.
27. Определение уровня защищённости информационных систем персональных данных.
28. Исследование классов систем.
29. Внутренние нарушители защиты персональных данных и негативные последствия их деятельности для предприятий и организаций
30. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
31. Модель злоумышленника информационных систем персональных данных.
32. Разработка частных моделей угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования.
33. Многофакторная аутентификация.
34. Организационные и технические мероприятия, направленные на минимизацию ущерба от возможной реализации угроз безопасности персональных данных.
35. Защита персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий.
36. Мероприятия по оценке соответствия принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных требованиям безопасности информации.
37. Мероприятия по контролю обеспечения безопасности персональных данных. Механизмы и средства контроля.
38. Периодичность и содержание работ. Ответственность оператора за нарушение правил обращения с персональными данными. Подготовка уведомлений об обработке персональных данных в уполномоченный орган.
39. Определение политик безопасности (ПБ). Представление ПБ.
40. Методы описания ПБ. Сравнительный анализ методов описания ПБ.
41. Оценка эффективности систем защиты информационных систем персональных данных

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

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 лабораторных и практических проводится в два этапа:

- 1-й этап: допуск к выполнению лабораторной работы – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний обучающихся теоретической части лабораторной работы и готовности к выполнению практических исследований;
- 2-й этап выполняется по окончании каждой лабораторной работы (практического занятия) в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки обучающимся 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 обучающихся к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности обучающихся в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимся в рамках текущего контроля баллы переводятся в оценку в соответствии со следующей шкалой:

- «не зачтено» - от 0 до 40 от максимального количества баллов;
- «зачтено» - от 41 до 100 максимального количества баллов.

Соотношения максимального количества баллов, полученных обучающимся по блокам модулей, показаны в Таблице 1.

Таблица 1 - Распределение баллов по блокам модулей дисциплины «Обеспечение безопасности персональных данных в информационных системах»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок (Распределение баллов по занятиям)
Модуль 1	50	14	36=12+12+12
Модуль 2	50	14	36=12+12+12
Модуль – Зачет	100	100	

Теоретический блок оценивается по результатам контрольной работы. Практический блок оценивается по результатам выполнения лабораторных работ и заданий на практических занятиях.

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

3 Промежуточная аттестация

Промежуточная аттестация проводится в форме зачета. Зачет проводится по расписанию в устном виде по билетам к зачету. Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

Образец билета к зачету

	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 Курс: 4 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. Доцент кафедры ИТСС, к.т.н., доцент _____ Ершов В.В. «___» _____ 20__ г		

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

4. Тестовые задания по дисциплине «Обеспечение безопасности персональных данных в информационных системах»

Тестовые задания позволяют оценить уровень сформированности компетенции ОПК-5; ОПК-6.

Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень содержит примерно 50 % 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 в среднем составляет 35 % заданий.

В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень в среднем составляют – 15 % заданий.

В задании используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Количество заданий по каждой компетенции равно 20. Всего 40 заданий.

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

ОПК-5

Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

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	Актуальность процедуры защиты персональных данных обусловлена возможностью: <u>1.выследить человека,</u> <u>2.спланировать преступление против него</u> 3. нежелательного знакомства стороннего лица с субъектом персональных данных
2	В Федеральном законе ФЗ №152 "О персональных данных" определены основные понятия: <u>1. персональные данные</u> <u>2.оператор</u> 3.дублирование персональных данных
3	Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются: 1. <u>общедоступными</u> 2. общепринятыми 3. допустимыми
4	Оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, сведения, указанные в части 3 статьи 22: 1. <u>Федерального закона №152-ФЗ.</u> 2. Указа Президента РФ №188 3. Федерального закона от 27.07.2006 № 149-ФЗ
5	Перечень действий, совершаемых оператором с персональными данными: 1. <u>неавтоматизированная обработка персональных данных;</u> 2. систематизированная обработка персональных данных; 3. синхронизированная обработка персональных данных.
6	Лицензирование деятельности по технической защите конфиденциальной информации

№ задания	Тексты заданий
	осуществляет: 1. <u>ФСТЭК</u> 2. Роскомнадзор 3. ФСБ
7	Нормативной основой для понятия «конфиденциальности» информации являются: 1. <u>Статья 23, 24 Конституции РФ</u> ; 2. <u>Статья 727 Гражданского кодекса РФ</u> ; Укажите правильные ответы 3. <u>Статья 26 Конституции РФ</u>
8	В зависимости от порядка предоставления или распространения информации она подразделяется на: 1. <u>информацию, свободно распространяемую</u> ; 2. <u>информацию, распространяемую в рамках ведомства</u> ; 3. <u>общегосударственную информацию</u>
9	Актуальные угрозы безопасности персональных данных при их обработке в информационной системе определены в: 1. <u>Федеральном законе №152</u> 2. <u>Постановлении Правительства РФ от 01.11.2012 № 1119</u> 3. <u>Указе Президента РФ №188</u>
10	Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми: 1. <u>ФСБ РФ</u> 2. <u>ФСТЭК РФ</u> 3. <u>Роскомнадзором</u>

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

Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Вводятся четыре градации показателя - частота (вероятность) реализации угрозы: 1. Маловероятно 2. Низкая вероятность 3. Средняя вероятность 4. Высокая вероятность Расставьте описание этого показателя в соответствии с градацией А. Объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты. Б. Объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны; В. Объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации); Г. Отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);
12	Информация, используемая в предпринимательской деятельности разделяется на три группы: 1. первая группа, 2. вторая группа, 3. третья группа. Укажите соответствие групп номерам А. Информация ограниченного доступа. Б. Для служебного пользования. В. Несекретная (или открытая), которая предназначена для использования как внутри Организации.
13	В системе защиты конфиденциальной информации выделяют три уровня: 1 правовой, 2 организационный, 3 технический. Определите и расставьте уровни в плане их соответствия А. Защита информации содержит меры управленческого, ограничительного и технологического характера.

№ задания	Тексты заданий
	Б. Защита информации основывается на нормах информационного права. В. Программно-аппаратный элемент системы защиты информации.
14	Обеспечение защиты конфиденциальных документов достигается тремя основными методами: 1. первый, 2. второй, 3. третий. Расставьте описание методов в порядке их очередности А. Организация эффективной системы делопроизводства с конфиденциальными документами. Б. Определение состава информации, которую целесообразно отнести к категории конфиденциальной; 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	Применительно к организационным мерам защиты конфиденциальной информации выделяют три вида: 1. первый, 2. второй, 3. третий Расставьте эти методы в порядке их очередности А. Защита конфиденциальной информации от несанкционированного воздействия; Б. Защита информации от непреднамеренного воздействия; В. Защита конфиденциальной информации от утечки.
16	Применительно к техническим мерам защиты конфиденциальной информации выделяют три вида: 1. первый, 2. второй, 3. третий Расставьте эти методы в порядке их очередности А. Защита информации от разглашения; Б. Защита информации от преднамеренного воздействия; В. Защита информации от несанкционированного доступа.
17	Различают три типа актуальных угроз безопасности персональных данных: 1. угрозы 1-го типа, 2. угрозы 2-го типа, 3. угрозы 3-го типа Расставьте описание методов в порядке их очередности А. Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе, Б. Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе,

№ задания	Тексты заданий
	В. Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

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 _____ персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.
19	_____ объекта информатизации называется комплекс организационно-технических мероприятий, в результате которых специальным документом – «Аттестатом соответствия» подтверждается, что ИСПДн заказчика соответствуют требованиям стандартов и нормативно-технических документов по безопасности ПДн, утвержденных ФСТЭК России.
20	Опасность угроз может быть низкой, средней или высокой, в зависимости от того незначительные негативные, просто негативные или же значительные негативные последствия наступают при реализации _____ соответственно.

Система оценивания выполнения тестовых заданий по компетенции ОПК-5

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 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

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	Режим конфиденциальности определяется перечнями: 1. <u>Перечнем сведений, составляющих коммерческую тайну.</u> 2. <u>Перечнем конфиденциальной информации.</u> 3. Штатной структурой Организации
2	Конфиденциальная информация Компании состоит из: 1. <u>сведений, составляющих коммерческую тайну;</u> 2. сведений, составляющих уголовную тайну 3. сведений, составляющих административную тайну
3	Документам Компании, содержащим конфиденциальную информацию, присваиваются следующие грифы конфиденциальности: 1. <u>Коммерческая тайна.</u> 2. Административная тайна 3. Служебная тайна
4	Проверка наличия конфиденциальных документов производится комиссией, назначаемой приказом по Компании: 1. <u>не реже одного раза в год</u> 2. не реже одного раза в два года 3. не реже двух раз в года
5	Требование предъявляемое законодательством РФ по защите информационных систем: 1. <u>определение вероятных угроз;</u> 2. определение частоты появления угроз; 3. определение количества вероятных угроз..
6	Содержимое модели угроз полностью описано _____: 1. <u>Методикой оценки ФСТЭК от 05.02.2021;</u> 2. Трудовым кодексом 3. Федеральным законом №152
7	К информации, которая может быть объектом угроз и потребует защиты относится: 1. критически важная информация 2. <u>ключевая, аутентифицирующая и парольная информация криптосредства;</u> 3. <u>криптографически опасная информация (КОИ);</u>
8	Под оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных понимается комплекс _____ мероприятий: 1. <u>технико-экономических</u> 2. планово-технических 3. планово-предупредительных
9	Оценка эффективности мер по обеспечению безопасности ПДн предусмотрена: 1. <u>приказом ФСТЭК России от 18.02.2013 №21.</u> 2. <u>Федеральным законом № 152</u> 3. <u>приказом ФСТЭК России от 2 декабря 2020 г. N 141</u>
10	Проверка надежности защиты ИСПДн от несанкционированного проникновения осуществляется посредством испытания подсистем: 1. <u>учета и регистрации;</u> 2. <u>контроля доступа;</u> 3. видеоконтроля.

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, 2. второй, 3. третий Расставьте эти подэтапы 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, 4.четвертый 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 персональных 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	Персональные данные — это _____, а не техническое понятие
19	Под _____ реализации угрозы понимается определяемый экспертным путем показатель, характеризующий насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки.
20	Обезличивание персональных данных Пользователя происходит по письменному заявлению Пользователя, при условии, что все договорные отношения завершены и от даты окончания последнего договора прошло _____

Система оценивания выполнения тестовых заданий по компетенции ОПК-6

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 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

Методические рекомендации по освоению дисциплины

1. Методические рекомендации преподавателю

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 занятиях лабораторного цикла следует обратить внимание на соответствие выбираемых обучающимся средств выполнения решаемым в работе задачам.

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 промежуточной аттестации.

2. Методические рекомендации обучающимся

Приступая к изучению новой учебной дисциплины, обучающиеся 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 обучающегося 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 обучающихся.

2.2 Методические указания для обучающихся по подготовке к лабораторным работам

Лабораторные занятия по любой учебной дисциплине проводятся в соответствии с рабочей программой этой учебной дисциплины в установленные расписанием часы.

Инструктаж по технике безопасности, правилам пожарной безопасности и правилам внутреннего распорядка в лаборатории проводится преподавателем на первом лабораторном занятии. На этом же занятии обучающимся сообщаются:

- программа всего предстоящего лабораторного цикла;
- условия взаимодействия обучающихся с преподавателем в процессе выполнения лабораторных работ;
- условия контроля самостоятельной работы обучающихся, включая правила оформления отчетов по лабораторным работам и их последующей защиты;
- другая необходимая информация.

Организация лабораторных работ включает:

- самостоятельную внеаудиторную подготовку обучающегося к выполнению каждой отдельной лабораторной работы в соответствии с ее программой в рамках часов, выделенных на самостоятельную проработку материала в программе дисциплины;
- входной контроль преподавателем степени подготовленности каждого обучающегося к выполнению лабораторных работ;
- выполнение программы лабораторных работ в полном объеме;
- оформление отчета и его защиту каждым обучающимся в установленные сроки;
- формирование преподавателем рейтингов каждого из обучающихся по результатам выполнения и защиты им отдельных лабораторных работ и их циклов (используется Модульно-рейтинговая система).

Оценка качества выполнения лабораторных работ каждым обучающимся производится преподавателем отдельно за подготовку к работе, ее выполнение и защиту.

Для подготовки и выполнения лабораторной работы №1, №2, №3 используется методическая разработка: Организация защиты персональных данных : лабораторный практикум/ А. М. Макаров, И. В. Калиберда, К. О. Бондаренко. — Ставрополь : Северо-Кавказский федеральный университет, 2015. — 92 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/62971.html>

2.3 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 обучающегося под управлением преподавателя. На них пополняются теоретические знания обучающихся, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение обучающихся к будущей профессиональной деятельности.

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

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

Для подготовки и выполнения практических занятий по дисциплине используется методическая разработка: *Борисов Б.П. Методические указания к выполнению практических занятий по дисциплине «Защита персональных данных». (Для обучающихся по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи профиль «Защищенные системы и сети связи» квалификация «бакалавр»).*

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, предшествующем данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально.

Обучающимся очной формы обучения при освоении вопросов для самостоятельного изучения, представленных в подразделе 4.1 рабочей программы, рекомендуется соблюдать последовательность их изучения, представленную в таблице.

Таблица – Учебный материал, выносимый на самостоятельное изучение обучающимся очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ и др.	Часов всего: 60	Неделя
Модуль 1		30	1-8
1.	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.	5	1
2.	Обработка биометрических данных.	4	2
3.	Специальные категории персональных данных и особенности их обработки.	4	3
4.	Уровни уничтожения электронных данных (очистка, очищение, разрушение).	4	4
5.	Стандартизация уничтожения электронных данных.	4	5
6.	Необходимые свойства «облака» для построения «облачной» системы хранения персональных данных.	4	6
7.	Требования регулирующих органов по защите персональных данных в «облаке».	5	8
Модуль 2		30	9-17
1.	Определение порядка обращения с персональными данными, контроля над его соблюдением, организация доступа к персональным данным.	5	9
2.	Внутренние нарушители защиты персональных данных и негативные последствия их деятельности для предприятий и организаций.	5	12-13
3.	Многофакторная аутентификация. Примеры многофакторной аутентификации. Протоколы аутентификации.	5	14-15
4.	Определение политик безопасности (ПБ). Представление ПБ. Закрытые, открытые, гибридные политики информационной безопасности.	5	16
5.	Методы описания ПБ. Сравнительный анализ методов описания ПБ. Аналитический метод описания ПБ. Графовый метод описания ПБ. Объектный метод описания ПБ. Логический метод описания ПБ.	5	17
6.	Оценка эффективности систем защиты информационных систем персональных данных	5	17

Самостоятельная работа обучающихся над усвоением материала по дисциплине может выполняться в помещении для самостоятельной работы СКФ МТУСИ, посредством использования электронной библиотеки и ЭИОС.