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 УВР
_____А.Г. Жуковский
«30» 08 2021 г.

Защита персональных данных Б1.В.ДВ.06.01
рабочая программа дисциплины

Кафедра **«Инфокоммуникационные технологии и системы связи»**
Направление подготовки **11.03.02 Инфокоммуникационные технологии и системы связи**
Профиль **Защищенные системы и сети связи**

Формы обучения **очная, заочная**

Распределение часов дисциплины по семестрам (ОФ), курсам (ЗФ)

Вид учебной работы	ОФ		ЗФ	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	5	180/8	5	180/5
Контактная работа, в том числе (по семестрам, курсам):		50/8		18/5
Лекции		20/8		6/5
Лабораторных работ				
Практических занятий		30/8		12/5
Семинаров				
Самостоятельная работа		130/8		162/5
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с разбивкой по семестрам		1/8 (с оценкой)		1/5 (с оценкой)
Число экзаменов с разбивкой по семестрам				

Программу составил:

Доцент кафедры ИТСС, к. т. н., доцент Борисов Б.П.

Рецензент:
Ведущий сотрудник ФГУП «РНИИРС, д.т.н., доцент Елисеев А.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 системы и сети связи», одобренных Учёным советом СКФ МТУСИ, протокол №1 от 30.08.2021, и утвержденного директором СКФ МТУСИ 30.08.2021 г.

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

Протокол от «30» 08 2021 г. № 1

Зав. кафедрой _____ Юхнов В.И.

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

Визирование для использования в 20__/20__ уч. году
Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

Визирование для использования в 20__/20__ уч. году
Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

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 выпускника способности, решать профессиональные задачи в соответствии с ***технологическим видом деятельности.***

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции обучающегося, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ПК-10: Способен обеспечить защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи;
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 выбора решений по защите персональных данных; - навыками выбора оборудования и программных средств необходимых для защиты персональных данных.

3 Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.25 «Основы информационной безопасности сетей и систем»
2	Б1.В.10 «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 (преддипломная) практика»

4 Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 180 часа, 50 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компе-тенции	УМИО
1	2	3	4	5	6
Курс 4 , Семестр 8					
Модуль 1. Защита персональных данных в инфокоммуникационных системах. – 75(24+51) часов					
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.1	2	ПК-10	Л1.1 Л1.2 Л1.3
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.	Ср.	6	ПК-10	Л1.1 Л1.2 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	ПК-10	Л1.2 Л2.1 Л2.2
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 1	4	ПК-10	Л1.1 Л1.2 Л2.1 Л2.2 Л2.3 Л2.4

1.5	Обработка биометрических данных.	Ср.	6	ПК-10	Л1.2 Л2.5 Л2.7
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.3	2	ПК-10	Л1.2 Л2.2 Л2.6
1.7	Административная ответственность за нарушение требований по обращению с персональными данными 1. Безопасность обработки персональных данных. 2. Ответственность в Кодекс об Административных Правонарушениях Российской Федерации за нарушение требований ФЗ «О персональных данных».	ПЗ 2	2	ПК-10	Л1.2 Л1.3 Л2.2 Л2.5
1.8	Специальные категории персональных данных и особенности их обработки.	Ср.	6	ПК-10	Л1.2 Л3.1
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.4	2	ПК-10	Л1.2 Л2.2
1.10	Уничтожение электронных данных. 1. Уровни уничтожения электронных данных (очистка, очищение, разрушение). 2. Стандартизация уничтожения электронных данных.	Ср.	6	ПК-10	Л2.2 Л2.6 Л3.1 Л3.3
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».	Ср.	8	ПК-10	Л1.2 Л2.5 Л3.4
1.12	Внешние нарушители защиты персональных данных и негативные последствия их деятельности для предприятий и организаций.	Ср.	6	ПК-10	Л1.2 Л3.1 Л2.4
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.5	2	ПК-10	Л1.2 Л2.2 Л2.5
1.14	Разграничение прав доступа в информационных системах персональных данных 1. Структура механизмов разграничения доступа в информационной системе персональных данных.	ПЗ 3.	4	ПК-10	Л1.2 Л2.5 Л2.6

	2. Реализация механизмов разграничения доступа в информационной системе персональных данных.				
1.15	Права оператора персональных данных и проблемные вопросы их реализации.	Ср.	6	ПК-10	Л1.2 Л2.2 Л3.2
1.16	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	4	ПК-10	Л1.2 Л1.3 Л1.4
1.17	Подготовка к практическим занятиям.	СР	7	ПК-10	Л3.1
Модуль 2. Методы защиты персональных данных в инфокоммуникационных системах и оценка эффективности 105 (26+79) часов					
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.6	2	ПК-10	Л1.2 Л3.1
2.2	Определение порядка обращения с персональными данными, контроля над его соблюдением, организация доступа к персональным данным.	Ср.	6	ПК-10	Л1.2 Л3.1 Л3.3
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.7	2	ПК-10	Л1.2 Л1.3 Л3.3
2.4	Классификация информационных систем персональных данных 1.Определение уровня защищённости информационных систем персональных данных. 2. Исследование классов систем.	ПЗ 5	4	ПК-10	Л1.2 Л3.6
2.5	Программные и программно-аппаратные средства механизмов разграничения доступа в информационной системе персональных данных.	Ср.	6	ПК-10	Л2.6 Л3.4
2.6	Документальное обеспечение проведения классификации информационных систем персональных данных.	Ср.	6	ПК-10	Л1.2 Л3.1 Л2.5
2.7	Определение уровня защищённости информационных систем персональных данных.	Ср.	6	ПК-10	Л1.2 Л2.4 Л2.6
2.8	Внутренние нарушители защиты персональных данных и негативные последствия их деятельности для предприятий и организаций.	Ср.	6	ПК-10	Л3.3

2.9	Способы реализации несанкционированного доступа к персональным данным и их предотвращение	Ср.	5	ПК-10	Л2.2 Л2.3 Л3.3
2.10	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.8	2	ПК-10	Л1.2, Л3.2 Л3.5
2.11	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 6	4	ПК-10	Л1.2, Л3.2 Л3.5 Л3.6
2.12	Многофакторная аутентификация. Примеры многофакторной аутентификации. Протоколы аутентификации.	Ср.	6	ПК-10	Л2.1 Л3.1
2.13	**О**рганизация 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.9	2	ПК-10	Л1.2 Л2.7
2.14	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 7	4	ПК-10	Л1.2 Л1.3 Л2.3 Л2.5
2.15	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	Лек.10	2	ПК-10	Л1.2 Л1.3 Л2.2 Л2.5

	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.				
2.16	Формальное описание алгоритма обезличивания ПДн методом перемешивания с помощью циклических перестановок. Анализ эффективности алгоритма перемешивания ПДн с помощью циклических перестановок.	Ср.	6	ПК-10	Л3.1 Л3.2 Л3.4
2.17	Определение политик безопасности (ПБ). Представление ПБ. Закрытые, открытые, гибридные политики информационной безопасности.	Ср	6	ПК-10	Л2.5 Л2.6 Л3.3
2.18	Методы описания ПБ. Сравнительный анализ методов описания ПБ. Аналитический метод описания ПБ. Графовый метод описания ПБ. Объектный метод описания ПБ. Логический метод описания ПБ.	Ср	6	ПК-10	Л2.5 Л2.6 Л3.3
2.19	Проверка предприятий на предмет защиты персональных данных: подготовка, процедура, оформление результатов и привлечение к ответственности.	Ср	6	ПК-10	Л1.2 Л2.2 Л2.5
2.20	Порядок лицензирования операторов информационных систем персональных данных.	Ср	6	ПК-10	Л1.2 Л2.1 Л2.5
2.21	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.	ПЗ 8	4	ПК-10	Л1.2 Л2.5 Л3.6
	Подготовка к практическому занятию.	СР	8	ПК-3	Л3.1
Итого – 180 часов					

4.2 Заочная форма обучения, 4года 8 месяцев (всего 180 часов, 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					
Модуль 1. Защита персональных данных в инфокоммуникационных системах. – 91 (8+83) часов					
1.1	Персональные данные в Федеральном законе и Трудовом кодексе Российской Федерации. 1. Основные понятия и определения. Содержание категории «персональные данные».	Лек.1	2	ПК-10	Л1.1 Л1.2 Л1.3

	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.	Ср.	6	ПК-10	Л1.1 Л1.2 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.	Ср	6	ПК-10	Л1.2 Л2.1 Л2.2
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 1	4	ПК-10	Л1.1 Л1.2 Л2.1 Л2.2 Л2.3 Л2.4
1.5	Обработка биометрических данных.	Ср.	6	ПК-10	Л1.2 Л2.5 Л2.7
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.	Ср	4	ПК-10	Л1.2 Л2.2 Л2.6
1.7	Административная ответственность за нарушение требований по обращению с персональными данными 1. Безопасность обработки персональных данных. 2. Ответственность в Кодекс об Административных Правонарушениях Российской Федерации за нарушение требований ФЗ «О персональных данных».	Ср	4	ПК-10	Л1.2 Л1.3 Л2.2 Л2.5
1.8	Специальные категории персональных данных и особенности их обработки.	Ср.	6	ПК-10	Л1.2 Л3.1
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.	Ср	8	ПК-10	Л1.2 Л2.2

1.10	Уничтожение электронных данных. 1. Уровни уничтожения электронных данных (очистка, очищение, разрушение). 2. Стандартизация уничтожения электронных данных.	Ср.	6	ПК-10	Л2.2 Л2.6 Л3.1 Л3.3
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».	Ср.	8	ПК-10	Л1.2 Л2.5 Л3.4
1.12	Внешние нарушители защиты персональных данных и негативные последствия их деятельности для предприятий и организаций.	Ср.	6	ПК-10	Л1.2 Л3.1 Л2.4
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.	Ср	6	ПК-10	Л1.2 Л2.2 Л2.5
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.	2	ПК-10	Л1.2 Л2.5 Л2.6
1.15	Права оператора персональных данных и проблемные вопросы их реализации.	Ср.	6	ПК-10	Л1.2 Л2.2 Л3.2
1.16	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.	Ср	8	ПК-10	Л1.2 Л1.3 Л1.4
1.17	Подготовка к практическим занятиям.	СР	3	ПК-10	Л3.6
Модуль 2. Методы защиты персональных данных в инфокоммуникационных системах и оценка эффективности 89 (10+79) часов					
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	2	ПК-10	Л1.2 Л3.1
2.2	Определение порядка обращения с персональными	Ср.	2	ПК-10	Л1.2

	данными, контроля над его соблюдением, организация доступа к персональным данным.				Л3.1 Л3.3
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.	Ср	4	ПК-10	Л1.2 Л1.3 Л3.3
2.4	Классификация информационных систем персональных данных 1.Определение уровня защищённости информационных систем персональных данных. 2. Исследование классов систем.	ПЗ 3	2	ПК-10	Л1.2 Л3.6
2.5	Программные и программно-аппаратные средства механизмов разграничения доступа в информационной системе персональных данных.	Ср.	4	ПК-10	Л2.6 Л3.4
2.6	Документальное обеспечение проведения классификации информационных систем персональных данных.	Ср.	4	ПК-10	Л1.2 Л3.1 Л2.5
2.7	Определение уровня защищённости информационных систем персональных данных.	Ср.	4	ПК-10	Л1.2 Л2.4 Л2.6
2.8	Внутренние нарушители защиты персональных данных и негативные последствия их деятельности для предприятий и организаций.	Ср.	4	ПК-10	Л3.3
2.9	Способы реализации несанкционированного доступа к персональным данным и их предотвращение	Ср.	3	ПК-10	Л2.2 Л2.3 Л3.3
2.10	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.3	2	ПК-10	Л1.2, Л3.2 Л3.5
2.11	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	2	ПК-10	Л1.2, Л3.2 Л3.5 Л3.6
2.12	Многофакторная аутентификация. Примеры многофакторной аутентификации. Протоколы аутентификации.	Ср.	4	ПК-10	Л2.1 Л3.1
2.13	**О**рганизация и обеспечение режимов защиты персональных данных.	Ср	8	ПК-10	Л1.2 Л2.7

	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.				
2.14	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 5	2	ПК-10	Л1.2 Л1.3 Л2.3 Л2.5
2.15	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.	Ср	6	ПК-10	Л1.2 Л1.3 Л2.2 Л2.5
2.16	Формальное описание алгоритма обезличивания ПДн методом перемешивания с помощью циклических перестановок. Анализ эффективности алгоритма перемешивания ПДн с помощью циклических перестановок.	Ср.	5	ПК-10	Л3.1 Л3.2 Л3.4
2.17	Определение политик безопасности (ПБ). Представление ПБ. Закрытые, открытые, гибридные политики информационной безопасности.	Ср	6	ПК-10	Л2.5 Л2.6 Л3.3
2.18	Методы описания ПБ. Сравнительный анализ методов описания ПБ. Аналитический метод описания ПБ. Графовый метод описания ПБ. Объектный метод описания ПБ. Логический метод описания ПБ.	Ср	6	ПК-10	Л2.5 Л2.6 Л3.3
2.19	Проверка предприятий на предмет защиты персональных данных: подготовка, процедура, оформление результатов и привлечение к ответственности.	Ср	6	ПК-10	Л1.2 Л2.2 Л2.5
2.20	Порядок лицензирования операторов информацион-	Ср	6	ПК-10	Л1.2

	ных систем персональных данных.				Л2.1 Л2.5
2.21	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.	Ср	4	ПК-10	Л1.2 Л2.5 Л3.6
2.22	Подготовка к практическому занятию.	СР	3	ПК-3	Л3.1
Итого – 180 часов					

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	"Конституция Российской Федерации" (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ)			Э1
Л 1.2	Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных" (с изм. и доп., вступ. в силу с 01.09.2015)			Э2
Л 1.3	А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин.	Защита информации: Учебное пособие / - 2-е изд.	М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.:	Э3
Л 1.4	Е.Б. Белов и др.	Основы информационной безопасности: Учебное пособие для вузов	Гор. линия-Телеком, 2011. - 558 с.: ил.;	Э4
5.1.2 Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л 2.1	Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 30.12.2015) "Об электронной подписи"			Э5
Л 2.2	Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 10.01.2016)			Э6
Л 2.3	Указ Президента РФ от 17 марта 2008 г. N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" (с изменениями и дополнениями от 21 октября 2008 г., 14 января 2011 г., 1, 25 июля 2014 г., 22 мая 2015 г.			Э7
Л 2.4	Закон РФ от 21 июля 1993 г. N 5485-I "О государственной тайне" (с изменениями и дополнениями от 6 октября 1997 г., 30 июня, 11 ноября 2003 г., 29 июня, 22 августа 2004 г., 1 декабря 2007 г., 18 июля 2009 г., 15 ноября 2010 г., 18, 19 июля, 8 ноября 2011 г., 21 декабря 2013 г., 8 марта 2015 г.)			Э8
Л 2.5	Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой	Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов	М.: Гор. линия-Телеком, 2013. - 214 с.	Э9
Л 2.6	В.А. Ворона, В.А. Тихонов	Комплексные интегрированные системы обеспечения безопасности: Учебное пособие	М.: Горячая линия - Телеком, 2013.- 160 с.-	Э10
Л 2.7	А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов	Технические средства и методы защиты информации: Учебное пособие	М.: Горячая линия - Телеком, 2012.- 616 с.-	Э11
5.1.3 Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	**Авторы,составители**	**Заглавие**	**Издательство,год**	**Кол.**
Л 3.1	А.В. Бабаш, Е.К. Баранова	Информационная безопасность и защита информации: Учебное пособие - 3-е изд.	М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.	Э12

Л 3.2	А.В. Бабаш, Е.К. Баранова	Моделирование системы защиты информации: Практикум: Учебное пособие.	М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с.	Э13
Л 3.3	В.Ф. Шаньгин	Комплексная защита информации в корпоративных системах: Учебное пособие.	М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2017. - 592 с.	Э14
Л 3.4	В.Ф. Шаньгин	Информационная безопасность компьютерных систем и сетей: Учебное пособие	М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2016. - 416 с.	Э15
Л 3.5	В.В. Бухтояров, В.Г. Жуков, В.В. Золотарев.	Поддержка принятия решений при проектировании систем защиты информации: Монография.	М.: НИЦ ИНФРА-М, 2018. - 131 с.:	Э16
Л 3.6	Борисов Б.П.	Методические указания к выполнению практических занятий по дисциплине «Защита персональных данных» для студентов по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи профиль «Защищенные системы и сети связи» квалификация «бакалавр».	Ростов-на-Дону: Северо-Кавказский филиал МТУСИ, 2019.	Э17

	5.2 Электронные образовательные ресурсы
Э1	http://www.consultant.ru/document/cons_doc_LAW_28399/
Э2	http://ivo.garant.ru/#/document/186117/paragraph/430816:2
Э3	http://znanium.com/catalog/product/474838
Э4	http://znanium.com/catalog/product/405159
Э5	http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=191956
Э 6	http://ivo.garant.ru/#/document/12148555/paragraph/3471:2
Э7	http://ivo.garant.ru/#/document/192944/paragraph/8911:2
Э8	http://ivo.garant.ru/#/document/10102673/paragraph/51952:4
Э9	http://znanium.com/catalog/product/560783
Э10	http://znanium.com/catalog/product/414537
Э11	http://znanium.com/catalog/product/390284
Э12	http://znanium.com/catalog/product/495249
Э13	http://znanium.com/catalog/product/549914
Э14	http://znanium.com/catalog/product/546679
Э15	http://znanium.com/catalog/product/549989
Э16	http://znanium.com/catalog/product/947806
Э17	http://www.skf-mtusi.ru/page_id=659
	5.3 Программное обеспечение
П.1	MS Excel.
П.2	MS Word.
П.3	Power Point.

6 Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория №№ 220, 308, оснащенные проектором, ПК (ноутбуком), экраном.
6.2 МТО практических занятий	
1	Лабораторная аудитория № 304 с возможностью выхода в локальную сеть Филиала и Интернет.
2	Компьютерная аудитория № 202 с возможностью выхода в локальную сеть Филиала и Интернет.
6.3 МТО рубежных контролей, зачетов	
1	Компьютерные аудитории №№ 202, 305 с возможностью выхода в локальную сеть Филиала и Интернет.

7. Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов 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.

Постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятии, предшествующему данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально.

Студентам очной формы обучения при освоении вопросов для самостоятельного изучения, представленных в подразделе 4.1, рекомендуется соблюдать последовательность их изучения, представленную в таблице 7.1.

Таблица 7.1 – Учебный материал, выносимый на самостоятельное изучение студентам очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 130	Неделя
Модуль 1		51	1-8
1	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.	6	1
	2. Обработка биометрических данных.	6	2
	3. Специальные категории персональных данных и особенности их обработки.	6	3
	4. Уничтожение электронных данных.	6	4

	5. Хранение персональных данных в «облаке».	8	5
	6. Внешние нарушители защиты персональных данных и негативные последствия их деятельности для предприятий и организаций.	6	6
	7. Права оператора персональных данных и проблемные вопросы их реализации.	6	7
	8. Подготовка к практическому занятию.	7	2-8
Модуль 2		79	9-17
2	1. Определение порядка обращения с персональными данными, контроля над его соблюдением, организация доступа к персональным данным.	6	9
	2. Программные и программно-аппаратные средства механизмов разграничения доступа в информационной системе персональных данных.	6	9
	3. Документальное обеспечение проведения классификации информационных систем персональных данных.	6	10
	4. Определение уровня защищённости информационных систем персональных данных.	6	10
	5. Внутренние нарушители защиты персональных данных и негативные последствия их деятельности для предприятий и организаций.	6	11
	6. Способы реализации несанкционированного доступа к персональным данным и их предотвращение	5	11
	7. Многофакторная аутентификация. Примеры многофакторной аутентификации. Протоколы аутентификации.	6	12
	8. Формальное описание алгоритма обезличивания ПДн методом перемешивания с помощью циклических перестановок.	6	12
	9. Определение политик безопасности (ПБ).	6	13
	10. Методы описания ПБ.	6	14
	11. Проверка предприятий на предмет защиты персональных данных: подготовка, процедура, оформление результатов и привлечение к ответственности.	6	15
	12. Порядок лицензирования операторов информационных систем персональных данных.	6	16
	13. Подготовка к практическим занятиям.	8	9-17

Студенты заочной формы обучения могут осваивать вопросы для самостоятельного изучения, представленные в подразделе 4.2 в произвольной последовательности, в удобное для них время. Однако к началу сессии они должны ориентироваться в материале, представленном в строках 1.2, 1.3, 1.5 - - 1.13, 1.15 – 1.17, 2.2, 2.3, 2.5 - 2.9, 2.12, 2.13, 2.15 – 2.22 подраздела 4.2.

Дополнения и изменения в Рабочей программе