

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Экономический факультет

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Кафедра «**Экономическая безопасность, анализ и аудит**»
экономического факультета

Образовательная программа
38.05.01 Экономическая безопасность

Направленность (профиль) программы
Судебная экономическая экспертиза

Уровень высшего образования
специалитет

Форма обучения
очная, заочная

Статус дисциплины: Часть ОПОП, формируемая участниками
образовательных отношений,
Дисциплины по выбору Б1.В.ДВ.3,
Б1.В.ДВ.03.02

Махачкала, 2022

Рабочая программа дисциплины Защита персональных данных составлена в 2022 году в соответствии с требованиями ФГОС ВО - специалитет по специальности 38.05.01 Экономическая безопасность от 14 апреля 2021 г. №293

Разработчик: кафедра Экономической безопасности, анализа и аудита
Алиева М.Ю., к.э.н., доцент

Рабочая программа дисциплины одобрена:
на заседании кафедры «Экономическая безопасность, анализ и аудит»
от «25» февраля 2022г., протокол № 6
Зав. кафедрой _____ Гаджиев Н.Г.
(подпись)

на заседании Методической комиссии экономического факультета
от «3» марта 2022г., протокол № 7
Председатель _____ Сулейманова Д.А.
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим
управлением « 10 » марта 2022г. _____
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина Защита персональных данных входит в часть, формируемую участниками образовательных отношений, дисциплины по выбору Б1.В.ДВ.3 образовательной программы специалитета 38.05.01 по специальности Экономическая безопасность, направленность (профиль) «Судебная экономическая экспертиза».

Дисциплина реализуется на экономическом факультете кафедрой «Экономическая безопасность, анализ и аудит».

Содержание дисциплины охватывает круг вопросов, связанных с формированием у обучающихся знаний о персональных данных, умений и навыков выявления угроз для их раскрытия, усвоение методов обеспечения безопасности персональных данных, обрабатываемых в информационных системах государственных, муниципальных органов, органов местного самоуправления и организаций различных форм собственности, физических лиц, организующих и (или) осуществляющих обработку персональных данных с целью определения мер и механизмов обеспечения защиты персональных данных при решении профессиональных задач в сфере экономической безопасности.

Дисциплина нацелена на формирование следующих компетенций выпускника:

обще профессиональных: ОПК-5, профессиональных: ПК-1, ПК-9

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: *лекционные занятия, практические занятия, самостоятельная работа.*

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме:

контроль текущей успеваемости – *контрольная работа*,
промежуточный контроль - *зачет*.

Объем дисциплины 3 зачетных единицы, в том числе в академических часах по видам учебных занятий:

Очная форма обучения

Семестр	Учебные занятия							Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	в том числе:							
	всего	Контактная работа обучающихся с преподавателем				СРС, в том числе контроль		
		всего	из них					
			Лекции	Практическое занятие	КСР	консультации		
9	108	50	34	20			54	зачет

Заочная форма обучения

Семестр	Учебные занятия							Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	в том числе:							
	всего	Контактная работа обучающихся с преподавателем				СРС, в том числе контроль		
		всего	из них					
			Лекции	Практическое занятия	КСР	консультации		
6 курс	108	14	8	6			94	зачет

1. Цели освоения дисциплины

Цели освоения дисциплины Защита персональных данных:

- формирование у обучающихся знаний о персональных данных, умений и навыков выявления угроз для их раскрытия, усвоение методов обеспечения безопасности персональных данных, обрабатываемых в различных информационных системах с целью определения мер и механизмов обеспечения защиты персональных данных при решении профессиональных задач в сфере экономической безопасности;

- воспитание у студентов чувства ответственности, закладка нравственных, эстетических норм поведения в обществе и коллективе, формирование патриотических взглядов, мотивов социального поведения и действий, финансово-экономического мировоззрения, способностей придерживаться законов и норм поведения, принятых в обществе и в своей профессиональной среде.

Цели освоения дисциплины Защита персональных данных соотносятся с общими целями ОПОП ВО по специальности: 38.05.01 Экономическая безопасность, специализация «Судебная экономическая экспертиза».

2. Место дисциплины в структуре ОПОП специалитета

Дисциплина Защита персональных данных входит часть, формируемую участниками образовательных отношений, дисциплины по выбору Б1.В.ДВ.3 образовательной программы специалитета 38.05.01 по специальности Экономическая безопасность, направленность (профиль) «Судебная экономическая экспертиза».

Для усвоения дисциплины Защита персональных данных необходимо знание дисциплин: История, Теория государства и права, Административное право, Основы правоохранительной деятельности, Основы информационной безопасности, Экономическая теория, Деньги, кредит, банки, Оценка экономических рисков, Экономические преступления, Экономика организаций, Финансы, Экономическая безопасность, Бухгалтерский учет, Экономический анализ, Национальная экономическая безопасность, Налоги и налогообложение, Экономическая безопасность региона, Финансовая безопасность, Судебная экономическая экспертиза.

Освоение данной дисциплины необходимо как параллельное для изучения дисциплин: Государственный аудит, а также производственной практики (преддипломной) и подготовке к процедуре защиты и защите выпускной квалификационной работы

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения и процедура освоения).

Код и наименование компетенции из ОПОП	Код и наименование индикатора достижения компетенций (в соответствии с ОПОП)	Планируемые результаты обучения	Процедура освоения

ОПК-5. Способен осуществлять профессиональную деятельность в соответствии с нормами профессиональной этики, нормами права, нормативными правовыми актами в сфере экономики, исключая противоправное поведение	ОПК-5. И-1. Демонстрирует знание норм профессиональной этики, норм права, нормативных правовых актов в сфере экономики, исключая противоправное поведение	Знает: нормы профессиональной этики, обеспечивающие защиту персональных данных; Знает: содержание, источники норм права, нормативные правовые акты в сфере защиты персональных данных, квалифицирующие признаки преступлений и административных правонарушений в сфере защиты персональных данных	Опрос, дискуссия, тесты, рефераты
	ОПК-5. И-2. Следует в своей профессиональной деятельности нормам профессиональной этики, нормам права, нормативным правовым актам в сфере экономики, исключая противоправное поведение	Умеет: квалифицированно применять нормативные правовые документы в защите персональных данных	
ПК-1 Способен собирать, анализировать и оценивать информацию о финансовых операциях (сделках) организации, в том числе с использованием информационных технологий и программных средств в целях ПОД/ФТ	ПК-1.И-1 Собирает и анализирует информацию о финансовых операциях (сделках) организации в целях ПОД/ФТ	Знает: источники информации о финансовых операциях (сделках), способы ее сбора, обработки и учета в системе защиты персональных данных Умеет: анализировать информацию о финансовых операциях (сделках) в системе защиты персональных данных	Опрос, дискуссия, тесты, рефераты
	ПК-1.И-2 Оценивает и использует информацию о финансовых операциях организации в целях ПОД/ФТ	Умеет: оценивать информацию о финансовых операциях (сделках) организации в целях ПОД/ФТ и раскрытия преступлений в сфере защиты персональных данных; Владеет: навыками сбора и анализа информации о финансовых операциях (сделках) в целях ПОД/ФТ в сфере защиты персональных данных;	

	ПК-1.И-3 Применяет информационные технологии и программные средства для сбора, анализа и оценки информации о финансовых операциях (сделках) организации	Знает: информационные технологии и программные средства, используемые для сбора, анализа и оценки информации о финансовых операциях (сделках) организации; Владеет: навыками применения информационных технологий и программных средств в целях ПОД/ФТ и раскрытия преступлений в сфере защиты персональных данных;	
ПК-9 Способен проводить исследования финансово-экономических процессов и явлений, осуществлять анализ информационных данных, оформлять и представлять результаты научно-исследовательской работы	ПК-9.И-1.Проводит исследования финансово-экономических процессов и явлений, осуществляет анализ информационных данных	Знает: методы сбора, систематизации и анализа информационных данных в сфере защиты персональных данных; Владеет: навыками проведения исследования процессов и явлений в сфере защиты персональных данных;	Опрос, дискуссия, тесты, рефераты
	ПК-9.И-2. оформляет и представляет результаты научно-исследовательской работы	Знает: методы и способы обобщения результатов научного исследования в сфере защиты персональных данных; Умеет: делать аналитические выводы и рекомендации по результатам научного исследования в сфере защиты персональных данных; Владеет: навыками представления результатов научно-исследовательской работы в сфере защиты персональных данных	

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 3 зачетных единицы, 108 академических часов.

4.2. Структура дисциплины.

4.2.1. Структура дисциплины в очной форме

Разделы и темы дисциплины по модулям	Семестр	Виды учебной работы, включая самостоятельную работу студентов (в часах)			Формы текущего контроля успеваемости и промежуточной аттестации
		Лекции	Практические занятия	Самостоятельная работа в т.ч. контроль	
Модуль 1. Основы защиты персональных данных					
Тема 1. Понятия информационной безопасности и защиты персональных данных. Классификация информационных систем персональных данных.	9	4	2	10	Опрос, рефераты, дискуссия, тесты
Тема 2. Правовая защита персональных данных	9	6	4	10	Опрос, рефераты, дискуссия, тесты
Итого по модулю 1	36	10	6	20	Контрольная работа
Модуль 2. Информация и система защиты персональных данных					
Тема 3. Виды угроз персональным данным	9	6	4	8	Опрос, рефераты, дискуссия, тесты
Тема 4. Виды тайн. Служебная и конфиденциальная информация. Коммерческая тайна.	9	6	2	10	Опрос, рефераты, дискуссия, тесты
Итого по модулю 2	36	12	6	18	Контрольная работа
Модуль 3. Организация и методы защиты персональных данных					
Тема 5. Методы защиты персональных данных. Организация работы по защите персональных данных	9	6	4	8	Опрос, рефераты, дискуссия, тесты
Тема 6. Оценка эффективности защиты персональных данных	9	6	4	8	Опрос, рефераты, дискуссия, тесты
Итого по модулю 3	36	12	8	16	Контрольная работа
Итого:	108	34	20	54	зачет

4.2.2. Структура дисциплины в заочной форме

Разделы и темы дисциплины по модулям	Семестр	Виды учебной работы, включая самостоятельную работу студентов (в часах)	Формы текущего контроля успеваемости и промежуточной аттестации
--------------------------------------	---------	---	---

		Лекции	Практические занятия	Самостоятельная работа в т.ч. контроль	
Тема 1. Понятия информационной безопасности и защиты персональных данных. Классификация информационных систем персональных данных.	9	2	2	14	Опрос, рефераты, дискуссия, тесты
Тема 2. Правовая защита персональных данных	9	2	1	16	Опрос, рефераты, дискуссия, тесты
Тема 3. Виды угроз персональным данным	9		2	14	Опрос, рефераты, дискуссия, тесты
Тема 4. Виды тайн. Служебная и конфиденциальная информация. Коммерческая тайна.	9	2	-	16	рефераты
Тема 5. Методы защиты персональных данных. Организация работы по защите персональных данных	9		1	16	Опрос, рефераты, дискуссия, тесты
Тема 6. Оценка эффективности защиты персональных данных	9	2	-	18	рефераты
Итого:	108	8	6	94	зачет

4.3. Содержание дисциплины, структурированное по темам (разделам).

4.3.1. Содержание лекционных занятий по дисциплине

Модуль 1. Основы защиты персональных данных

Тема 1. Понятия информационной безопасности и защиты персональных данных. Классификация информационных систем персональных данных.

Основные понятия и определения. Содержание категории "персональные данные". Обработка персональных данных: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (передача), обезличивание, блокирование, уничтожение. Понятие оператора обработки персональных данных. Согласие субъекта персональных данных на обработку его персональных данных. Конфиденциальность персональных данных. Специальные категории персональных данных. Общедоступные источники персональных данных, автоматизация обработки данных в информационных системах различного назначения, развитие рынка "интернета вещей", создание центров обработки данных (ЦОД), формирующих так называемые "большие данные" в региональном и глобальном масштабе. Историческое развитие персональных данных. Классификация информационных систем персональных

данных (ИСПДн).

Тема 2. Правовая защита персональных данных

Законодательство Российской Федерации в области персональных данных: Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"; Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"; Постановление Правительства РФ от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"; Постановление Правительства РФ от 06.07.2008 N 512 (ред. от 27.12.2012) "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных"; Постановление Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"; Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", "Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. ФСТЭК РФ, Приказ ФСТЭК России от 11.02. 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" и др.

Принципы обработки персональных данных. Условия обработки персональных данных. Права субъекта персональных данных. Обязанности оператора при сборе персональных данных. Персональные данные в Федеральном законе и Трудовом кодексе РФ. Нормативно-методическое обеспечение безопасности информационных систем персональных данных. Руководящие документы ФСТЭК и ФСБ России по защите персональных данных. Нормативно-методическое обеспечение безопасности информационных систем персональных данных в органах власти, учреждениях (предприятиях). Порядок лицензирования операторов информационных систем персональных данных.

Требование к документации предприятия по защите персональных данных. Требование к документации юридических лиц по защите персональных данных. Требования к документации по обработке персональных данных работников. Типовые документы, регламентирующие получение, обработку, хранение и передачу персональных данных.

Модуль 2. Информация и система защиты персональных данных

Тема 3. Виды угроз персональным данным

Классификация угроз безопасности персональных данных. Анализ и характеристики угроз возможной утечки информации по техническим каналам. Анализ и характеристики угроз несанкционированного доступа к информации в информационной системе персональных данных. Типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах (автоматизированных рабочих местах, локальных и распределенных информационных системах), не имеющих и имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена. Формирование перечня актуальных угроз безопасности персональным данным

Тема 4. Виды тайн. Служебная и конфиденциальная информация.

Коммерческая тайна.

Понятие тайны, служебная тайна, коммерческая тайна, конфиденциальная информация. Виды конфиденциальной информации: государственная тайна; профессиональная тайна; коммерческая тайна; служебная тайна; личная тайна; семейная тайна; иная информация о частной жизни гражданина (физического лица); персональные данные граждан (физических лиц).

Элементы коммерческой тайны: секрет производства (ноу-хау); информация о содержании корпоративного договора, заключенного участниками непубличного общества (п. 4 ст. 67.2 ГК РФ); информация о новых решениях и технических знаниях, полученных сторонами по договору подряда (ст. 727 ГК РФ); сведения, касающиеся договоров на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ (ст. 771 ГК РФ); сведения, предоставляемые участниками торгов в соответствии с правилами организованных торгов (ст. 23 ФЗ от 21 ноября 2011 г. N 325-ФЗ "Об организованных торгах"); условия договора инвестиционного товарищества (ст. 12 ФЗ от 28 ноября 2011 г. N 335-ФЗ "Об инвестиционном товариществе"); сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них (п. 6 Перечня сведений конфиденциального характера, утвержденного Указом Президента РФ от 6 марта 1997 г. N 188).

Информация, доступ к которой ограничен законодательством

Модуль 3. Модуль 3. Организация и методы защиты персональных данных

Тема 5. Методы защиты персональных данных. Организация работы по защите персональных данных

Принципы обработки персональных данных. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом. Меры по обеспечению безопасности персональных данных при их обработке. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных. Уведомление об обработке персональных данных. Уполномоченный орган по защите прав субъектов персональных данных. Ответственность за нарушение требований Федерального закона

Организационно-административные меры защиты: формирование системы управления персональными данными; регламентация деятельности персонала по использованию персональных данных; регламентация порядка взаимодействия пользователей и администраторов информационных систем персональных данных; контроль над деятельностью персонала. Технические меры защиты от НСД в информационных системах персональных данных различного класса: защита от вредоносных программ и средства защиты от вторжений; идентификация и аутентификация пользователей; разграничение и контроль доступа к персональным данным; обеспечение целостности персональных данных; регистрация событий безопасности; защита каналов передачи персональных данных

Тема 6. Оценка эффективности защиты персональных данных

Анализ структурных особенностей системы, технологических особенностей обработки персональных данных субъектов, достаточности внутренней документации, её соответствия прописанным в нормативно-правовых актах требованиям, соответствия между структурой, составом программно-технической базы ИСПДн и подготовленной организационно-технической документацией, правильности определения уровней защищенности персональных данных и

способов защиты для каждого из них, подготовленности персонала и распределения ответственности, **наличия и результативности** физической охраны ИСПДн, состояния и выполнения работ по поддержанию безопасности информационной системы.

Подсистемы защиты персональных данных: учета и регистрации; контроля доступа; антивирусной защиты; поддержания целостности; межсетевого экранирования; выявления вторжений; каналов связи; оценки защищенности.

4.3.2. Содержание практических занятий по дисциплине

Модуль 1. Основы защиты персональных данных

Тема 1. Понятия информационной безопасности и защиты персональных данных. Классификация информационных систем персональных данных.

Вопросы к теме:

1. Основные понятия и определения. Содержание категории "персональные данные".
2. Понятие оператора обработки персональных данных. Согласие субъекта персональных данных на обработку его персональных данных.
3. Конфиденциальность персональных данных.
4. Специальные категории персональных данных.
5. Общедоступные источники персональных данных
6. Историческое развитие персональных данных.
7. Классификация информационных систем персональных данных (ИСПДн).

Ссылка на учебно-методическую литературу, указанную в п.8 (1,2,3,4)

Тема 2. Правовая защита персональных данных

Вопросы к теме:

1. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации";
2. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных";
3. Постановление Правительства РФ от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами";
4. Постановление Правительства РФ от 06.07.2008 N 512 (ред. от 27.12.2012) "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных";
5. Постановление Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
6. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
7. "Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. ФСТЭК РФ, Приказ ФСТЭК России от 11.02. 2013 г. N 17 "Об утверждении

Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" и др.

8. Принципы обработки персональных данных. Условия обработки персональных данных.

9. Права субъекта персональных данных. Обязанности оператора при сборе персональных данных.

10. Персональные данные в Федеральном законе и Трудовом кодексе РФ.

11. Нормативно-методическое обеспечение безопасности информационных систем персональных данных в органах власти, учреждениях (предприятиях). Порядок лицензирования операторов информационных систем персональных данных.

12. Требование к документации предприятия по защите персональных данных

13. Требование к документации юридических лиц по защите персональных данных.

14. Требования к документации по обработке персональных данных работников.

Ссылка на учебно-методическую литературу, указанную в п.8(1,2,3,6)

Модуль 2. Информация и система защиты персональных данных

Тема 3. Виды угроз персональным данным

Вопросы к теме:

1. Классификация угроз безопасности персональных данных.

2. Анализ и характеристики угроз возможной утечки информации по техническим каналам.

3. Анализ и характеристики угроз несанкционированного доступа к информации в информационной системе персональных данных.

4. Типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах (автоматизированных рабочих местах, локальных и распределенных информационных системах), не имеющих и имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

5. Формирование перечня актуальных угроз безопасности персональным данным

Ссылка на учебно-методическую литературу, указанную в п.8 (1,2,3,7,8)

Тема 4. Виды тайн. Служебная и конфиденциальная информация. Коммерческая тайна.

Вопросы к теме:

1. Понятие тайны, служебная тайна, коммерческая тайна, конфиденциальная информация.

2. Виды конфиденциальной информации: государственная тайна; профессиональная тайна; коммерческая тайна; служебная тайна; личная тайна; семейная тайна; иная информация о частной жизни гражданина (физического лица); персональные данные граждан (физических лиц).

3. Элементы коммерческой тайны

4. Информация, доступ к которой ограничен законодательством

Ссылка на учебно-методическую литературу, указанную в п.8(1,2,3,4, 5-9)

Модуль 3. Модуль 3. Организация и методы защиты персональных данных

Тема 5. Методы защиты персональных данных. Организация работы по защите персональных данных

Вопросы к теме:

1. Принципы обработки персональных данных.
2. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом.
3. Меры по обеспечению безопасности персональных данных при их обработке.
4. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных. Уведомление об обработке персональных данных.
5. Уполномоченный орган по защите прав субъектов персональных данных.
6. Ответственность за нарушение требований Федерального закона
7. Организационно-административные меры защиты: формирование системы управления персональными данными; регламентация деятельности персонала по использованию персональных данных; регламентация порядка взаимодействия пользователей и администраторов информационных систем персональных данных; контроль над деятельностью персонала.
8. Технические меры защиты от НСД в информационных системах персональных данных различного класса

Ссылка на учебно-методическую литературу, указанную в п.8(1,2,3,4, 6-8)

Тема 6. Оценка эффективности защиты персональных данных

Вопросы к теме:

1. Подсистемы защиты персональных данных.
2. Подсистема учета и регистрации персональных данных;
3. Подсистема контроля доступа к персональным данным;
4. Подсистема антивирусной защиты персональных данных;
5. Анализ структурных особенностей системы,
6. Анализ технологических особенностей обработки персональных данных субъектов,
7. Анализ достаточности внутренней документации, её соответствия прописанным в нормативно-правовых актах требованиям
8. Анализ соответствия между структурой, составом программно-технической базы ИСПДн и подготовленной организационно-технической документацией,
9. Анализ правильности определения уровней защищенности персональных данных и способов защиты для каждого из них,
10. Анализ подготовленности персонала и распределения ответственности
11. Анализ наличия и результативности физической охраны ИСПДн,

Ссылка на учебно-методическую литературу, указанную в п.8 (1,2,3,4, 6-8)

5. Образовательные технологии

С целью формирования профессиональных навыков, обучающихся в соответствии с требованиями ФГОС ВО по направлению подготовки по дисциплине предусматривается широкое использование в учебном процессе активных и интерактивных форм проведения занятий: презентаций, разбор конкретных практических ситуаций.

Лекции по дисциплине проводятся с использованием средств визуализации лекционного материала (мультимедийных презентаций) и применением таких методов и технологий, как тематическая дискуссия, проблемная лекция, обзорная лекция, лекция-информация с использованием фактических данных и т.п.

При ведении практических занятий используются стандартные методы обучения: тестирование, фронтальный опрос, индивидуальный опрос, и т.п. При проведении практических занятий в интерактивной форме используются анализ конкретных ситуаций, тематическая групповая дискуссия, блиц-опрос, проблемный семинар, научный кружок.

К участию в проведении занятий привлекаются представители российских компаний, государственных и общественных организаций.

Применяя различные методы и формы обучения, необходимо учитывать, что занятия должны выполнять не только информационную функцию, но также и мотивационную, воспитательную и обучающую.

Информационная функция лекции предполагает передачу необходимой информации по теме, которая должна стать основой для дальнейшей самостоятельной работы студента.

Мотивационная функция должна заключаться в стимулировании интереса студентов к науке. На лекции необходимо заинтересовывать студентов с целью выработки у них желания дальнейшего изучения той или иной экономической проблемы.

Воспитательная функция ориентирована на формирование у молодого поколения чувства ответственности, закладку нравственных, этических норм поведения в обществе и коллективе, формирование патриотических взглядов, мотивов социального поведения и действий, финансово-экономического мировоззрения.

Обучающая функция реализуется посредством формирования у студентов навыков работы с первоисточниками и научной и учебной литературой.

6. Учебно-методическое обеспечение самостоятельной работы студентов.

Для теоретического и практического усвоения дисциплины большое значение имеет самостоятельная работа студентов, она осуществляется студентами индивидуально и под руководством преподавателя. Самостоятельная работа по дисциплине, предусмотренная учебным планом в объеме 54 часов для очной формы и 94 часов для заочной формы, направлена на содержательное и глубокое усвоение изучаемого курса, формирование навыков исследовательской работы и ориентирование студентов на умение применять теоретические знания на практике.

Основными видами самостоятельной работы студентов в рамках освоения дисциплины выступают:

1. проработка учебного материала;
2. работа с электронными источниками;
3. работа с Законодательным материалом Российской Федерации о государственной тайне;

4. обработка данных;
5. подготовка докладов к участию в тематических дискуссиях;
6. работа с тестами и вопросами;
7. написание рефератов;
8. подготовка сообщений и презентаций

Результаты самостоятельной работы контролируются и учитываются при текущем и промежуточном контроле (зачет).

Виды и формы контроля самостоятельной работы студентов в рамках освоения дисциплины Защита персональных данных

Разделы дисциплины	Виды самостоятельной работы	Количество часов		Форма контроля
		очная форма	заочная форма	
<u>Раздел 1.</u> Основы защиты персональных данных	проработка учебного материала; работа с электронными источниками; работа с Законодательным материалом; обработка данных; подготовка докладов к участию в тематических дискуссиях; работа с тестами, вопросами, документами; написание рефератов; подготовка сообщений и презентаций.	20	30	Дискуссия, опрос, представление рефератов, сообщений, презентаций
<u>Раздел 2.</u> Информация и система защиты персональных данных	проработка учебного материала; работа с электронными источниками; работа с Законодательным материалом; обработка данных; подготовка докладов к участию в тематических дискуссиях; работа с тестами, вопросами, документами; написание рефератов; подготовка сообщений и презентаций.	18	30	Дискуссия, опрос, представление рефератов, сообщений, презентаций
<u>Раздел 3.</u> Организация и методы защиты персональных данных	проработка учебного материала; работа с электронными источниками; работа с Законодательным материалом; обработка данных; подготовка докладов к участию в тематических дискуссиях; работа с тестами, вопросами, документами; написание рефератов; подготовка сообщений и презентаций.	16	34	Дискуссия, опрос, представление рефератов, сообщений, презентаций
Итого		54	94	

Методические рекомендации по написанию рефератов

Написание реферата используется в учебном процессе с целью развития у студентов умения и навыков самостоятельного научного поиска: изучения литературы по выбранной теме, анализа различных источников и точек зрения, обобщения материала, выделения главного, формулирования выводов. С помощью рефератов студент глубже изучает разделы и темы дисциплины, учится логически мыслить, оформлять, докладывать, презентовать и защищать результаты самостоятельно проведенного научного исследования.

Процесс подготовки, написания и защиты реферата включает:

- выбор темы;
- подбор специальной литературы и иных источников, их изучение;
- составление плана;
- написание и оформление текста (5-15 машинописных страниц);
- подготовка тезисов доклада (на 7-10 минут);
- устное изложение в виде доклада, в том числе виде презентации.

Выбор темы реферата осуществляется в соответствии с предложенной тематикой. В отдельных случаях студент может выбрать для своего реферата тему в соответствии с направлением его НИР.

Материал в реферате располагается в последовательности:

- титульный лист;
- план работы;
- введение;
- текст работы (разбитый на разделы);
- заключение
- список литературы.

Содержание реферата студент докладывает на практическом занятии, заседании научного кружка, научно-практической конференции. По результатам написания, защиты и обсуждения реферата студенту выставляется соответствующий балл за СРС (0-40 баллов).

Примерная тематика рефератов по дисциплине Защита персональных данных

1. Понятие персональных данных работника
2. Нормативно-правовое регулирование обработки персональных данных
3. Получение, хранение и использование персональных данных работника
4. Принципы и условия обработки персональных данных работника
5. Базовые вопросы управления безопасностью персональных данных.
6. Место ИБДПД в рамках общей системы управления предприятием.
7. Стандартизация в области построения систем управления ИБДПД.
8. История развития Защиты персональных данных
9. Основные процессы ИБДПД и требования, предъявляемые
10. Область деятельности безопасности персональных данных.
11. Ролевая структура безопасности персональных данных.
12. Политика безопасности персональных данных
13. Понятие области деятельности ИБДПД.
14. Механизм выбора области деятельности. Состав области деятельности (процессы, структурные конфиденциальной информации как научная дисциплина.
15. Ролевая структура ИБДПД (основные и дополнительные роли).
16. Роль высшего руководства организации в ИБДПД.

17. Рискология безопасности персональных данных
18. Цель процесса анализа рисков ИБДПД.
19. Этапы и участники процесса анализа рисков ИБДПД.
20. Разработка Методики анализа рисков ИБДПД.
21. Планирование мер по обработке выявленных рисков ИБДПД.
22. Основные процессы безопасности персональных данных
23. Аудит безопасности персональных данных
24. Внешние аудиты ИБДПД на соответствие требованиям нормативных документов.
25. Внедрение разработанных процессов безопасности персональных данных
26. Этапы внедрения процессов и их последовательность.
27. Обеспечение соответствия требованиям законодательства РФ системы безопасности персональных данных
28. Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках ИБДПД (авторское право, защита персональных данных и т.д.).
29. Разработка процессов или дополнение существующих процессов управления ИБДПД с целью удовлетворения требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).
30. Правовая защита служебной тайны
31. Налоговая тайна как вид служебной тайны, содержащей персональные данные.
32. Юридические санкции в области защиты персональных данных на предприятии.

Примерные документы для выполнения самостоятельной работы по дисциплине Защита персональных данных

1. Акт внутреннего аудита соответствия обработки персональных данных требованиям к защите персональных данных.
2. Акт об уничтожении персональных данных по достижении цели обработки.
3. Дополнительное соглашение с работником, допущенным к обработке персональных данных.
4. Журнал регистрации выявленных нарушений в сфере защиты персональных данных и иной конфиденциальной информации.
5. Журнал регистрации уничтожения персональных данных работников.
6. Журнал учета выданных персональных данных работников.
7. Журнал учета мероприятий по контролю защиты персональных данных.
8. Журнал учета носителей информации с персональными данными.
9. Журнал учета обращений субъектов персональных данных и их законных представителей.
10. Журнал учета передачи персональных данных работников внутри организации.
11. Журнал учета передачи персональных данных работников организациям и государственным органам.
12. Журнал учета согласий субъектов персональных данных на обработку персональных данных.
13. Заявление об изменении персональных данных в учетных документах.

14. Инструкция сотрудника, ответственного за обработку персональных данных.

15. Инструкция сотрудника, ответственного за организацию обработки персональных данных.

16. Лист ознакомления работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, требованиями к защите персональных данных, политикой оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

17. Лист ознакомления работников (представителей работников) с локальными актами, регламентирующими порядок и условия обработки их персональных данных, а также об их правах и обязанностях в этой области.

18. Обязательство о неразглашении информации, содержащей персональные данные.

19. Ответ на запрос о предоставлении персональных данных сотрудника.

20. Отзыв работника своего согласия на обработку персональных данных.

21. Отказ на запрос о предоставлении персональных данных работника.

22. Перечень должностей, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным.

23. Перечень мест хранения материальных носителей персональных данных.

24. Перечень помещений для обработки персональных данных.

25. Перечень сведений конфиденциального характера.

26. Политика оператора в отношении обработки персональных данных.

27. Положение о внутреннем аудите соответствия обработки персональных данных установленным требованиям.

28. Положение о разграничении прав доступа к обрабатываемым персональным данным.

29. Положение об обработке и защите персональных данных работников.

30. Положение об обработке и защите персональных данных обучающихся (воспитанников) и их родителей (законных представителей).

31. Правила, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных.

32. Приказ о внесении изменений в документы, содержащие персональные данные работника.

33. Приказ о внесении изменений в Политику оператора в отношении обработки персональных данных и локальные нормативные акты, регламентирующие вопросы обработки и защиты персональных данных.

34. Приказ о назначении должностного лица, представляющего интересы организации при проведении проверки соблюдения установленных требований по обработке персональных данных.

35. Приказ о назначении ответственного за обеспечение безопасности персональных данных.

36. Приказ о назначении ответственного за организацию обработки персональных данных.

37. Приказ о назначении ответственного за техническую защиту персональных данных.

38. Приказ о создании комиссии по уничтожению документов по обработке персональных данных.

39. Приказ об утверждении перечня должностей работников, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным.

40. Приказ об утверждении перечня мест хранения материальных носителей персональных данных.

41. План внутреннего контроля соответствия обработки персональных данных требованиям защиты персональных данных.

42. Регламент ведения журналов, содержащих ПДн, необходимые для однократного пропуска субъекта ПДн на территорию организации.

43. Регламент допуска работников к обработке персональных данных.

44. Регламент по проведению контрольных мероприятий и реагированию на инциденты, связанные с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных.

45. Регламент реагирования на запросы/обращения субъектов персональных данных.

46. Сведения о реализуемых требованиях к защите персональных данных.

47. Согласие законного представителя обучающегося (воспитанника) на обработку персональных данных обучающегося (воспитанника).

48. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

49. Согласие на получение персональных данных от третьих лиц.

50. Согласие обучающегося на обработку своих персональных данных.

51. Согласие работника на обработку персональных данных.

52. Согласие соискателя на обработку персональных данных.

53. Согласие сотрудника на хранение копии личных документов в личном деле.

54. Требование о прекращении передачи (распространения, предоставления, доступа) персональных данных, разрешенных субъектом персональных данных для распространения.

55. Уведомление Роскомнадзора об инциденте, связанном с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных, повлекшей нарушение прав субъектов персональных данных.

56. Уведомление Роскомнадзора о результатах внутреннего расследования выявленного инцидента, связанного с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных.

57. Уведомление Роскомнадзора о прекращении обработки персональных данных.

58. Уведомление Роскомнадзора об обработке (о намерении осуществлять обработку) персональных данных.

59. Уведомление работнику о необходимости получить его персональные данные у третьей стороны.

60. Учетный лист доведения требований нормативных (руководящих) документов и проведения занятий по вопросам обработки и защиты персональных данных.

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

7.1. Типовые контрольные задания

Примерные тестовые задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины

1. Коммерческую тайну организации или предпринимателя составляют:

- a. Документы об уплате налогов и других обязательных платежей
- b. Учредительные документы и Устав
- c. Документы о платежеспособности
- d. Данные о клиентской базе предприятия

2. Информация о деятельности органов государственной власти и органов местного самоуправления является:

- a. Особо секретной
- b. Секретной
- c. Конфиденциальной
- d. Открытой

3. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам – это:

- a. Оператор информационной системы
- b. Информатор
- c. Носитель информации
- d. Владелец информации

4. Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц – это:

- a. Документирование информации
- b. Распространение информации
- c. Предоставление информации
- d. Доступ к информации

5. Судебная защита прав субъектов в сфере информационных процессов и информатизации не осуществляется:

- a. Конституционным судом РФ
- b. Судами субъектов Федерации
- c. Судом общей юрисдикции
- d. Верховным судом РФ

6. В соответствии с Уголовным кодексом Российской Федерации, предмет шпионажа

- a. персональные данные работника
- b. сведения, переданные священнику на исповеди
- c. сведения, составляющие государственную тайну

7. Автоматизированная обработка персональных данных – это

- a) Обработка персональных данных с использованием средств автоматизации;
- b) Обработка персональных данных с помощью средств вычислительной техники;
- c) Обработка персональных данных пользователя с применением компьютера;

8. Информация – это

- a) Любые данные, представленные на материальном носителе;
- b) Сведения, принадлежащие кому либо и защищаемые законом;
- c) Сведения (сообщения, данные), независимо от формы их представления;

9. Информационная система персональных данных – это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

- d) Пользователь, средства автоматизации, базы данных;
- e) Контролируемое пространство, в котором происходит обработка персональных данных;
- f) Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

10. Безопасность персональных данных – это

- a) Состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных;
- b) Состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность персональных данных;
- c) Состояние защищенности персональных данных, характеризующееся способностью технических средств обеспечить конфиденциальность персональных данных.

11. Блокирование персональных данных – это

- a) Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- b) Временное прекращение обработки персональных данных;
- c) Временное прекращение обработки персональных данных для уточнения персональных данных.

12. Доступ к информации – это

- a) Возможность получения информации и ее использования;
- b) Возможность использования информации;
- c) Возможность доступа к информации;
- d) Возможность доступа к информации, но не ее использования;

13. Закладочное устройство – это

- a) Элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации);
- b) Элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в технические средства и системы обработки информации);
- c) Элемент средства съема информации, скрытно внедряемый в оборудование, предметы интерьера, транспортные средства.

14. Защищаемая информация – это

- a) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;
- b) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, устанавливаемыми собственником информации;
- c) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов;
- d) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями Федерального закона «О защищаемой информации в Российской Федерации»

15. Идентификация – это

- a) Присвоение субъектам и объектам доступа идентификатора и сравнение предъявляемого идентификатора с вводимым идентификатором;
- b) Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;
- c) Присвоение субъектам и объектам доступа идентификатора;
- d) Присвоение субъектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с вводимым идентификатором.

16. Информационные технологии – это

- a) Средства поиска, сбора, хранения, обработки, предоставления, распространения информации
- b) Методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких методов;
- c) Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- d) Процессы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов.

17. Что понимается под понятием «Конфиденциальность персональных данных»?

- а) Обязательное для соблюдения оператором или иным лицом требование не допускать их распространения без согласия субъекта персональных данных;
- б) Обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;
- с) Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

18. Материальный носитель (носитель информации) - это

- а) Любой материальный объект, используемый для хранения или передачи информации;
- б) Любой материальный объект, используемый для хранения информации;
- с) Любой материальный субъект, используемый для хранения или передачи информации.

19. Межсетевой экран – это

- а) Функционально-распределенное программно-аппаратное средство, реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы;
- б) Локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы;
- с) Локальное программное средство, реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

20. Нарушитель безопасности персональных данных – это

- а) Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных;
- б) Физическое лицо, преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных;
- с) Физическое или юридическое лицо, преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

21. Недекларированные возможности – это

- а) Функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании

которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации;

б) Функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых появляются новые возможности для работы;

с) Функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

22. Общедоступные персональные данные – это

а) Персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных;

б) Персональные данные, доступ неограниченного круга лиц к которым предоставлен в соответствии с федеральными законами;

с) Персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

23. Правила разграничения доступа – это

а) Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;

б) Совокупность правил для обеспечения информационной безопасности в организации;

с) Совокупность правил, для объектов доступа.

24. Специальные категории персональных данных – это

а) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

б) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных убеждений, интимной и личной жизни жизни;

с) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, состояния здоровья, интимной жизни;

д) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни и судимости.

25. Трансграничная передача персональных данных это

а) Передача персональных данных на территорию иностранного государства;

б) Передача персональных данных на территорию другого субъекта РФ органу власти данного субъекта, физическому лицу или юридическому лицу данного субъекта РФ;

с) Передача персональных данных на территорию иностранного государства или органу власти иностранного государства;

d) Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

26. Целостность информации – это способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

- a) Состояние информации, при котором отсутствует любое ее изменение;
- b) Состояние информации, при котором изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- c) Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

27. Что такое персональные данные

- a) любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- b) информация о частной жизни физического лица, доступ к которой он решил ограничить;
- c) Сведения о религиозных убеждениях, политических взглядов, расовой и национальной принадлежности субъекта персональных данных;
- d) Любые сведения независимо от формы их представления.

28. Оператор персональных данных это:

- a) Государственный орган, осуществляющий автоматизированную обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке;
- b) государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- c) Юридическое лицо, осуществляющее автоматизированную обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке;
- d) государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, но не определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

29. Обработка персональных данных это

- a) любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение(обновление, изменение), извлечение,

использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных);

б) сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, осуществляемые с помощью средств вычислительной техники;

с) чтение, запись, сортировка, модификация, передача персональных данных в информационной системе.

30. Распространение персональных данных это

а) действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

б) действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

с) передача персональных данных оператору персональных данных;

31. Предоставление персональных данных это

а) действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

б) действия, направленные на раскрытие персональных данных по мотивированному запросу;

32. Уничтожение персональных данных это

а) Действия, в результате которых становится невозможно определить субъекта персональных данных в информационной системе персональных данных;

б) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

с) удаление персональных данных из информационной системы персональных данных;

д) действия, направленные на уничтожение носителей персональных данных.

33. Обезличивание персональных данных – действия, в результате которых

а) Невозможно распространять персональные данные

б) Невозможно выполнять сбор персональных данных

с) Выполняется уничтожение персональных данных в информационной системе

д) Становится невозможно без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

34. Что понимается под понятием «Контролируемая зона»

а) Пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств;

б) Пространство, в котором не исключается неконтролируемое пребывание сотрудников и посетителей оператора, но исключается неконтролируемое пребывание посторонних транспортных, технических и иных материальных средств;

с) Пространство, в котором не исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

35. Что такое биометрические персональные данные

а) Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются оператором для установления личности субъекта персональных данных;

б) Сведения, которые характеризуют физиологические особенности человека, на основании которых можно установить его личность;

с) Сведения, которые характеризуют биологические особенности человека, на основании которых можно установить его личность.

36. Как расшифровывается аббревиатура «НСД»

а) Национальные скоростные дороги;

б) Несанкционированный доступ;

с) Национальный союз дзюдо;

д) Национально-социалистическое движение.

37. Как расшифровывается аббревиатура «НДВ»

а) норматив допустимого воздействия;

б) недеklarированная возможность;

с) Небо для всех;

д) Национальный директор по вооружению.

38. Какое из свойств защищаемой информации не является основным

а) Целостность;

б) Регистрируемость;

с) Доступность;

д) Конфиденциальность.

39. Законодательство Российской Федерации в области персональных данных:

а) ФЗ «О Государственной тайне»;

б) ФЗ «Об электронной цифровой подписи»;

с) ФЗ «О персональных данных»;

д) ФЗ, ПП и НПА уполномоченных органов государственной власти РФ в сфере информации и персональных данных.

40. Дата официального опубликования ФЗ «О персональных данных»:

а) 26 июня 2006 года;

- b) 26 июля 2007 года;
- c) 27 июля 2006 года;
- d) 27 июня 2007 года

41. Целью Федерального закона «О персональных данных» является:

- a) Обеспечение защиты информации в Российской Федерации;
- b) Осуществление права на поиск, получение, передачу, производство и распространение информации;
- c) Обеспечение защиты персональных данных;
- d) Обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных.

42. На какие отношения не распространяется действие Федерального закона "О персональных данных"

- a) на отношения, возникающие при обработке персональных данных физическими лицами, исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
- b) на отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;
- c) не распространяется на оба перечисленных варианта.

43. Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся:

- a) Расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, наличия судимости, интимной жизни субъектов персональных данных;
- b) Расовой, национальной принадлежности, политических взглядов, философских или религиозных убеждений, состояния здоровья, интимной жизни субъектов персональных данных;
- c) Расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, наличия судимости, физиологических особенностей субъектов персональных данных;
- d) Расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, физиологических особенностей субъектов персональных данных.

44. Оператор персональных данных:

- a) Физическое лицо;
- b) Юридическое лицо;
- c) Муниципальный орган;
- d) Государственный орган;
- e) Гражданин;
- f) Государственный служащий.

45. Неправомерные действия или бездействие работодателя при обработке и защите персональных данных работник может обжаловать:

- a) в инспекции труда;
- b) у мирового судьи;
- c) в районном суде;
- d) в Роскомнадзоре.

46. Перед кем оператор персональных данных несет ответственность

- a) Перед субъектом персональных данных;
- b) Перед Роскомнадзором;
- c) Не перед кем не несет ответственности.

47. На какие отношения распространяется действие Федерального закона «О персональных данных»

a) На отношения, возникающие при обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

b) на отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

c) на отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами;

d) Распространяется на все перечисленные варианты.

48. В какой орган нужно отправить Уведомление об обработке персональных данных

- a) Администрация района;
- b) Департамент информационных технологий;
- c) Управление Роскомнадзора;
- d) Управление Роскомнадзора по УрФО.

49. Что нужно разместить на официальном сайте муниципального органа

- a) Форму согласия на обработку персональных данных;
- b) Положение о защите персональных данных;
- c) Документы, определяющие политику в отношении обработки персональных данных.

50. Какой срок в соответствии с ФЗ-152 предусмотрен для сообщения субъекту (его представителю) Оператором информации о наличии ПДн и предоставить возможность ознакомления с ними

- a) в течение 7 дней;
- b) в течение 30 дней;
- c) в течение 7 рабочих дней;
- d) в течение 180 дней.

51. Управление Роскомнадзора уведомляет оператора персональных данных о проведении внеплановой проверки:

- а) Не менее чем за 24 часа до начала ее проведения любым доступным способом;
- б) Не менее чем за 3 дня до начала ее проведения любым доступным способом;
- с) Не менее чем за 24 часа до начала ее проведения только в письменном виде.

52. Срок проведения плановой проверки не может превышать:

- а) 35 рабочих дней;
- б) 4 недели либо 20 рабочих дней;
- с) 20 рабочих дней;
- д) Срок проведения проверок не ограничен.

53. В течение какого времени со дня получения запроса Оператор обязан предоставить в Управление Роскомнадзора необходимую информацию

- а) В течение 30 дней;
- б) В течение двух рабочих дней;
- с) В течение 5 рабочих дней;
- д) Срок предоставления документов не ограничен.

54. В случае отзыва субъектом ПДн согласия на обработку своих ПДн, оператор обязан прекратить обработку ПДн, и, если сохранение ПДн более не требуется для целей обработки, уничтожить ПДн в срок, не превышающий с даты поступления указанного отзыва:

- а) 30 рабочих дней;
- б) 30 дней;
- с) 20 дней;
- д) 10 рабочих дней;

55. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором, оператор обязан прекратить неправомерную обработку ПДн с даты этого выявления в срок, не превышающий:

- а) 5 рабочих дней;
- б) 7 рабочих дней;
- с) 10 рабочих дней;
- д) 30 дней;

56. В случае достижения цели обработки ПДн оператор обязан прекратить обработку ПДн и уничтожить соответствующие ПДн в срок, не превышающий с даты достижения цели обработки ПДн:

- а) 10 дней;
- б) 30 дней;
- с) 7 рабочих дней;

57. Если ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные в срок не превышающий:

- а) 7 рабочих дней;
- б) 10 рабочих дней;
- с) 15 дней;
- д) 30 рабочих дней.

58. Управление Роскомнадзора уведомляет о проведении плановой проверки:

а) не позднее, чем в течение 3-х рабочих дней до начала ее проведения посредством направления копии приказа руководителя, заместителя руководителя Управления Роскомнадзора с уведомлением о вручении или иным доступным способом;

б) не позднее, чем в течение 7-ми рабочих дней до начала ее проведения посредством направления копии приказа руководителя, заместителя руководителя Управления Роскомнадзора с уведомлением о вручении или иным доступным способом;

с) не менее чем за 24 часа до начала ее проведения любым доступным способом;

д) предварительное уведомление Оператора о начале проведения плановой проверки не требуется.

59. Контроль за выполнением требований ПП РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» проводится не реже 1 раза в:

- а) 5 лет;
- б) 3 года;
- с) 1 год

60. Кто должен осуществлять внутренний контроль за соблюдением оператором законодательства Российской Федерации о персональных данных

- а) Администратор безопасности ИСПДн;
- б) Ответственный за организацию обработки ПДн;
- с) Ответственный за обеспечение безопасности ПДн;
- д) Руководитель.

61. Какие меры по обеспечению безопасности персональных данных при неавтоматизированной обработке являются обязательными в соответствии с постановлением Правительства РФ от 15.09.2008г. № 687

а) Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

б) Использование средств контроля и управления доступом;

с) Использование запираемых шкафов, сейфов и решеток на окнах;

д) Должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный доступ к ним. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, устанавливаются оператором.

62. Какая ответственность предусмотрена за нарушение законодательства РФ о персональных данных

- a) Дисциплинарная;
- b) Административная;
- c) Уголовная;
- d) Все перечисленные.

63. Укажите ошибочное требование технологий хранения биометрических персональных данных вне информационных систем персональных данных:

- a) ограничение доступа к информации, содержащейся на материальном носителе, для уполномоченных лиц;
- b) применение средств электронной цифровой подписи или иных информационных технологий, позволяющих сохранить целостность и неизменность биометрических персональных данных, записанных на материальный носитель;
- c) проверка наличия письменного согласия субъекта персональных данных на обработку его биометрических персональных данных или наличия иных оснований обработки персональных данных, установленных законодательством Российской Федерации в сфере отношений, связанных с обработкой персональных данных.

64. Какой срок установлен законодательством для согласования проекта технического задания для каждой организации

- a) не должен превышать 14 рабочих дней со дня получения технического задания;
- b) не должен превышать 15 дней со дня получения технического задания;
- c) не должен превышать 30 календарных дней со дня получения технического задания;
- d) не должен превышать 20 рабочих дней со дня получения технического задания.

65. Как называется документ, который составляется по результатам проверки и в нем указываются нарушения, которые необходимо устранить

- a) предписание;
- b) заключение;
- c) акт о выявленных нарушениях;
- d) акт проверки.

66. Какие виды проверок бывают

- a) документарные и выездные;
- b) только документарные;
- c) только выездные.

67. Какое из свойств защищаемой информации не является основным

- a) целостность;
- b) регистрируемость;

- c) доступность;
- d) конфиденциальность.

68. Для выполнения работ по обеспечению безопасности персональных данных при их обработке в информационной системе в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридическое

лицо или индивидуальный предприниматель, имеющие лицензию:

- a) на осуществление деятельности по техническому обслуживанию шифровальных (криптографических) средств;
- b) лицензия на осуществление деятельности по технической защите конфиденциальной информации;
- c) лицензия на право проектирования систем с использованием шифровальных (криптографических) средств.

69. Согласно требованиям и методам, установленным уполномоченным органом по защите прав субъектов персональных данных, обезличивание персональных данных обязаны осуществлять:

- a) все операторы персональных данных;
- b) операторы, являющиеся государственными или муниципальными органами;
- c) операторы, осуществляющие обработку персональных данных в государственных информационных системах;
- d) операторы, осуществляющие обработку персональных данных в информационных системах, обеспечивающих обезличивание данных.

70. При использовании Оператором процедуры обезличивания из исходной ИСПДн (ФИО, Дата рождения, Адрес, Телефон, Диагноз) была получена обезличенная ИСПДн (ФИО, Дата рождения, Телефон). Какой метод обезличивания был использован Оператором

- a) метод изменения состава или семантики;
- b) метод декомпозиции;
- c) метод декомпиляции;
- d) метод состава и семантики.

71. При хранении обезличенных данных Оператору следует:

- a) организовать раздельное хранение обезличенных данных и дополнительной (служебной) информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания;
- b) обеспечивать конфиденциальность дополнительной (служебной) информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания;
- c) обеспечить конфиденциальность канала (способа) передачи данных при передаче вместе с обезличенными данными информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания;
- d) правильны все варианты.

72. Является ли биометрическими персональными данными фотографическое изображение, содержащиеся в личном деле работника

а) Является, т.к. составляет сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность;

б) Является, поскольку действия с использованием фотографического изображения направлены на подтверждение их принадлежности конкретному физическому лицу, чья личность уже определена и чьи персональные данные уже имеются в распоряжении оператора;

с) Не является, т.к. не используется оператором для установления личности субъекта персональных данных;

д) Не является, т.к. изображение получено без применения специальных технологий и технических средств, позволяющих выполнять требования предъявляемые к форматам записи изображения (ГОСТ Р ИСО\ МЭК 19794-5-2006).

73. В каких случаях возможно использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) без согласия этого гражданина:

а) при использовании изображения в государственных, общественных или иных публичных интересах;

б) если изображение гражданина получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях, за исключением случаев, когда такое изображение является основным объектом использования;

с) гражданин позировал за плату;

д) во всех выше указанных случаях.

74. Когда сканирование паспорта субъекта Оператором не считается обработкой биометрических персональных данных:

а) когда сканирование паспорта осуществляется Оператором для подтверждения осуществления определенных действий конкретным лицом (например, заключение договора на оказание услуг, в том числе банковских, медицинских и т.п.) без проведения процедур идентификации (установления личности);

б) когда Оператором получено согласие субъекта на обработку персональных данных;

с) сканирование паспорта субъекта Оператором всегда считается обработкой биометрических персональных данных.

Примерные вопросы для подготовки к промежуточной аттестации по итогам освоения дисциплины

1. Основные понятия и определения. Содержание категории "персональные данные".

2. Понятие оператора обработки персональных данных. Согласие субъекта персональных данных на обработку его персональных данных.

3. Конфиденциальность персональных данных.

4. Специальные категории персональных данных.
5. Общедоступные источники персональных данных
6. Историческое развитие персональных данных.
7. Классификация информационных систем персональных данных (ИСПДн).
8. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации";
9. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных";
10. Постановление Правительства РФ от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами";
11. Постановление Правительства РФ от 06.07.2008 N 512 (ред. от 27.12.2012) "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных";
12. Постановление Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
13. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных",
14. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. ФСТЭК РФ, Приказ ФСТЭК России от 11.02. 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" и др.
15. Принципы обработки персональных данных. Условия обработки персональных данных.
16. Права субъекта персональных данных. Обязанности оператора при сборе персональных данных.
17. Персональные данные в Федеральном законе и Трудовом кодексе РФ.
18. Нормативно-методическое обеспечение безопасности информационных систем персональных данных в органах власти, учреждениях (предприятиях). Порядок лицензирования операторов информационных систем персональных данных.
19. Требование к документации предприятия по защите персональных данных
20. Требование к документации юридических лиц по защите персональных данных.
21. Требования к документации по обработке персональных данных работников.
22. Классификация угроз безопасности персональных данных.
23. Анализ и характеристики угроз возможной утечки информации по техническим каналам.
24. Анализ и характеристики угроз несанкционированного доступа к информации в информационной системе персональных данных.

25. Типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах (автоматизированных рабочих местах, локальных и распределенных информационных системах), не имеющих и имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

26. Формирование перечня актуальных угроз безопасности персональным данным

27. Понятие тайны, служебная тайна, коммерческая тайна, конфиденциальная информация.

28. Виды конфиденциальной информации: государственная тайна; профессиональная тайна; коммерческая тайна; служебная тайна; личная тайна; семейная тайна; иная информация о частной жизни гражданина (физического лица); персональные данные граждан (физических лиц).

29. Элементы коммерческой тайны

30. Информация, доступ к которой ограничен законодательством

31. Принципы обработки персональных данных.

32. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом.

33. Меры по обеспечению безопасности персональных данных при их обработке.

34. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных. Уведомление об обработке персональных данных.

35. Уполномоченный орган по защите прав субъектов персональных данных.

36. Ответственность за нарушение требований Федерального закона

37. Организационно-административные меры защиты: формирование системы управления персональными данными; регламентация деятельности персонала по использованию персональных данных; регламентация порядка взаимодействия пользователей и администраторов информационных систем персональных данных; контроль над деятельностью персонала.

38. Технические меры защиты от НСД в информационных системах персональных данных различного класса

39. Подсистемы защиты персональных данных.

40. Подсистема учета и регистрации персональных данных;

41. Подсистема контроля доступа к персональным данным;

42. Подсистема антивирусной защиты персональных данных;

43. Анализ структурных особенностей системы защиты персональных данных

44. Анализ технологических особенностей обработки персональных данных субъектов

45. Анализ достаточности внутренней документации, её соответствия прописанным в нормативно-правовых актах требованиям

46. Анализ соответствия между структурой, составом программно-технической базы ИСПДн и подготовленной организационно-технической документацией

47. Анализ правильности определения уровней защищенности

персональных данных и способов защиты для каждого из них

48. Анализ подготовленности персонала и распределения ответственности

49. Типовые документы, регламентирующие получение, обработку, хранение и передачу персональных данных.

50. Защита от вредоносных программ и средства защиты от вторжений; идентификация и аутентификация пользователей; разграничение и контроль доступа к персональным данным; обеспечение целостности персональных данных; регистрация событий безопасности; защита каналов передачи персональных данных

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

Общий результат выводится как интегральная оценка, складывающаяся из текущего контроля - 50% и промежуточного контроля – 50 %.

Текущий контроль по дисциплине включает:

- посещение занятий – 10 баллов,
- участие в практических занятиях – до 60 баллов,
- самостоятельная работа- до 40 баллов.

Промежуточный контроль по дисциплине включает:

письменная контрольная работа - до 100 баллов.

Устный опрос – до 60 баллов

Тестирование – до 40 баллов

8. Учебно-методическое обеспечение дисциплины.

а) основная литература:

1. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"; Справочно-правовая система «Консультант Плюс» [Электронный ресурс] – URL: <http://www.consultant.ru> (дата обращения 21.02.2022)

2. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" Справочно-правовая система «Консультант Плюс» [Электронный ресурс] – URL: <http://www.consultant.ru> (дата обращения 21.02.2022)

3. Аверченков В. И. Защита персональных данных в организации / В.И. Аверченков. - М.: Флинта, 2016. - 260 С.

б) дополнительная литература:

4. Трудовой кодекс Российской Федерации от 30 ноября 2001 N 197-ФЗ: по сост. на 1 июня 2019 г.// Собрание законодательства Российской Федерации. — 2002. — № 1.

5. Гражданский кодекс Российской Федерации (часть вторая) от 26 января 1996 г. № 14-ФЗ: по сост. на 1 июня 2019 г. // Собрание законодательства Российской Федерации. — 1996. — № 5. — Ст. 410.

6. Приказ Минкомсвязи России от 31.03.2020 N 148 (ред. от 01.07.2021) "О проведении эксперимента об оказании гражданам на безвозмездной основе услуг связи по передаче данных и по предоставлению доступа к информационно-телекоммуникационной сети "ИНТЕРНЕТ" на территории Российской Федерации для использования социально значимых информационных ресурсов в информационно-телекоммуникационной сети "ИНТЕРНЕТ"

7. Корнилова А.А. Защита персональных данных: учебное пособие / Башкирский государственный университет. — Уфа: РИЦ БашГУ, 2020. — Электронная версия печатной публикации. — Доступ возможен через Электронную библиотеку БашГУ. —

<URL:https://elib.bashedu.ru/dl/local/Kornilova_Yunusova_Ismagilova_Zachita_personalnyh_dannyh_up_2020.pdf>.

8. Бачило И.Л. Персональные данные в структуре информационных ресурсов. Основы правового регулирования /И.Л. Бачило, Л.А. Сергиенко, Б.А. Кристальный., А.Г. Арешев // Информационное право. — 2016. — N 3

9. Бондаренко, Э.Н. Конфиденциальная информация в трудовых отношениях. / Э.Н. Бондаренко, Иванов ДВ. — СПб.; Издательство «Юридический центр-Пресс». — 2014

10. Дупан А. С. Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет, 2016 г. - 440 стр.

11. Журавлев М.С. Персональные данные в трудовых отношениях: допустимые пределы вмешательства в частную жизнь работника // Информационное право. 2017.- №4.- С. 35

12. Жукова В. В. Обеспечение защиты персональных данных в информационной системе [Текст] / В. В. Жукова // Вестник научного общества студентов, аспирантов и молодых ученых. — 2015. — № 3. — С. 68–71.

13. Журавлев М.С. Персональные данные в трудовых отношениях: допустимые пределы вмешательства в частную жизнь работника // Информационное право. 2017.- №4.- С. 35 — 38.

14. Терещенко Л.К. Правовой режим персональных данных и безопасность личности /Л. К. Терещенко //Закон. -2018.- №6.- С. 37 -43. Трофимова И.А. Обработка и хранение персональных данных/ И.А. Трофимова // Делопроизводство.- 2015. — № 3. — С. 107 — 110.

15. Чернова О. А. Делопроизводство и режим секретности. М.:КноРус, 2020

16. Яковец Е.Н. Своеобразие состава защищаемой конфиденциальной информации / Е.Н. Яковец // Право и кибербезопасность. — 2014. — № 2. — С. 51 — 58.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

1. Официальный сайт Министерства экономического развития РФ [Электронный ресурс] – URL: <http://www.economy.gov.ru> (дата обращения 21.02.2022)

2. Официальный сайт Министерства финансов РФ [Электронный ресурс]– URL:<http://www.economy.gov.ru/https://www.minfin.ru/ru/> (дата обращения 16.02.2022).

3. Официальный интернет-портал правовой информации [Электронный ресурс] – URL: <http://pravo.gov.ru/> (дата обращения 16.02.2022).

4. Официальный сайт органов государственной власти Российской Федерации и субъектов, адрес доступа: <http://www.gov.ru/>. доступ неограниченный

5. Справочно-правовая система «Право.ру» [Электронный ресурс] – URL: <http://docs.pravo.ru/> (дата обращения 11.02.2022).

6. Справочно-правовая система «КонсультантПлюс» [Электронный ресурс] – URL: <http://www.consultant.ru> (дата обращения 08.02.2022).
7. Информационно-правовой портал «Гарант.ру» [Электронный ресурс] – URL: <http://www.garant.ru> (дата обращения 16.02.2022).
8. Официальный интернет-портал правовой информации [Электронный ресурс] – URL: <http://pravo.gov.ru/> (дата обращения 16.03.2022).
9. Электронный каталог НБ ДГУ [Электронный ресурс]: база данных содержит сведения о всех видах литературы, поступающих в фонд НБ ДГУ/Дагестанский гос. ун-т. – Махачкала, 2021. – URL: <http://elib.dgu.ru> (дата обращения 16.02.2022).
10. eLIBRARY.RU [Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва. – URL: <http://elibrary.ru/defaultx.asp> (дата обращения 05.02.2022).

10. Методические указания для обучающихся по освоению дисциплины.

Оптимальным путем освоения дисциплины является посещение лекций, практических занятий, выполнение предлагаемых заданий в виде рефератов, докладов, сообщений, тестов, решения задач и устных вопросов.

На лекциях рекомендуется деятельность студента в форме активного слушания, т.е. предполагается возможность задавать вопросы на уточнение понимания вопросов темы и рекомендуется конспектирование основных положений лекции. На практических занятиях деятельность студента заключается в активном обсуждении вопросов темы, тематических докладов, рефератов, решении ситуационных задач, выполнении контрольных заданий и т.п.

При подготовке к практическому занятию студенты должны изучить конспект лекций по заданной теме, ознакомиться с соответствующим разделом в учебнике, рекомендованном в качестве основной литературы. Студент должен ознакомиться с дополнительной литературой, периодическими изданиями, интернет-источниками. Форма работы с литературой может быть разнообразной: начиная от комментированного чтения и завершая выполнением различных заданий на основе изученной литературы. Например: составление плана, подбор выписок из литературы по заданным вопросам; конспектирование текста и т.п.

Подготовка к зачету предполагает изучение конспектов лекций, рекомендуемой литературы, повторение материала практических занятий, разбор типовых задач и заданий.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

В процессе преподавания дисциплины используются современные технологии визуализации учебной информации (создание и демонстрация презентаций), ресурсы электронной информационно-образовательной среды университета.

Проведение дисциплины не предполагает использование специального программного обеспечения. Используется следующее лицензионное программное обеспечение общего назначения и информационные справочные системы: прикладные программы пакета OfficeStd 2016 RUSOLPNLAcadmс (Microsoft OfficeWord для создания текстовых файлов; Microsoft Office Excel для составления

аналитических таблиц и расчета показателей; Microsoft Office Power Point для создания презентаций, визуального сопровождения докладов), Справочно Правовая Система Консультант Плюс, Электронный периодический справочник «Система ГАРАНТ»

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий по дисциплине используются специальные помещения: учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации с достаточным количеством посадочных мест, укомплектованные специализированной мебелью.

Учебные аудитории для проведения занятий оснащены современным демонстрационным (мультимедийным) оборудованием для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета